Diving Into Security Testing

Prepared By:

Chintan Gurjar

Penetration Tester

18/09/2017

Who am I !

A little bit about my professional career

twitter

LinkedIn

HackCon

The Norwegian cyber security convention

C|EH

Certified Ethical Hacker

zendesk®

COUNTER STRIKE®

GLOBAL OFFENSIVE

Raw Experience 3

University of Bedfordshire

COMPUTER SECURITY AND FORENSICS

MSc

MASTER OF SCIENCE

MARVEL

Before you start!

curiosity and patience to learn hacking

- ✓ Basic knowledge of networking
- ✓ Web application life cycle
- ✓ Destructive mindset
- ✓ Do not rely on tools only
- ✓ Be ready to go to jail

Data Breach

If you are not hacked then it does not mean you are secured

Accounts Stolen

President Donald Trump's Website Hacked: P

ion Hacked — Hacker

Chinese Hackers won $215,000 f

Nexus at Mobile Pwn2Own

Million Baht Stolen

aqi

ATMs in

Prone to Hackers

Malv

Hackers Stole $32 Million in Ethereum; 3rd Heist in 20 Days

king iPhone and Google

Instead of spend

iPhone in

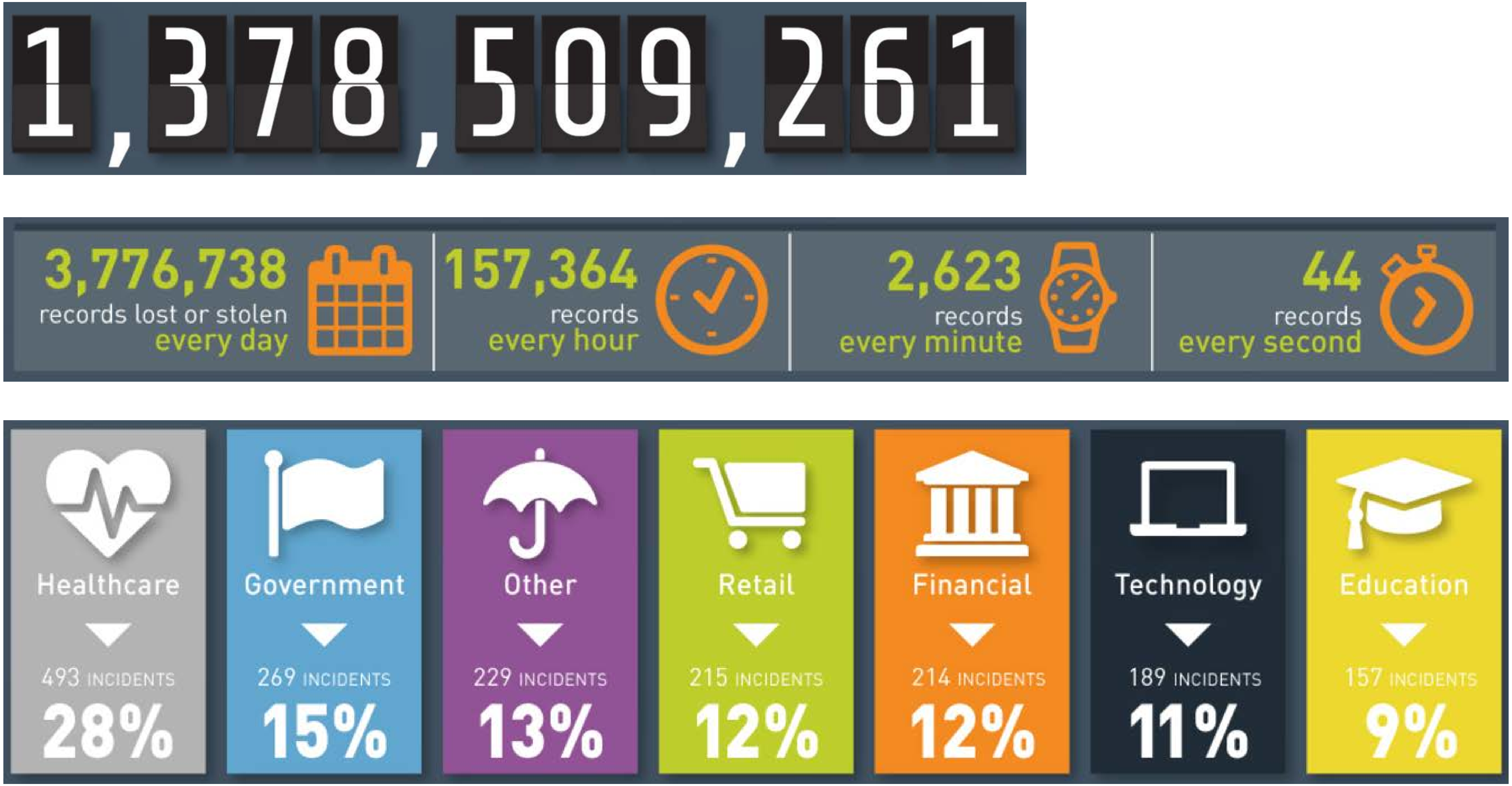
ion, FBI could have Hac

Massive ATM Hack Hits 3.2 Million Ind

Change Your PIN Now!

Data Breach cont..

Data breach landscape 2016



1,378,509,261

3,776,738 records lost or stolen every day

157,364 records every hour

2,623 records every minute

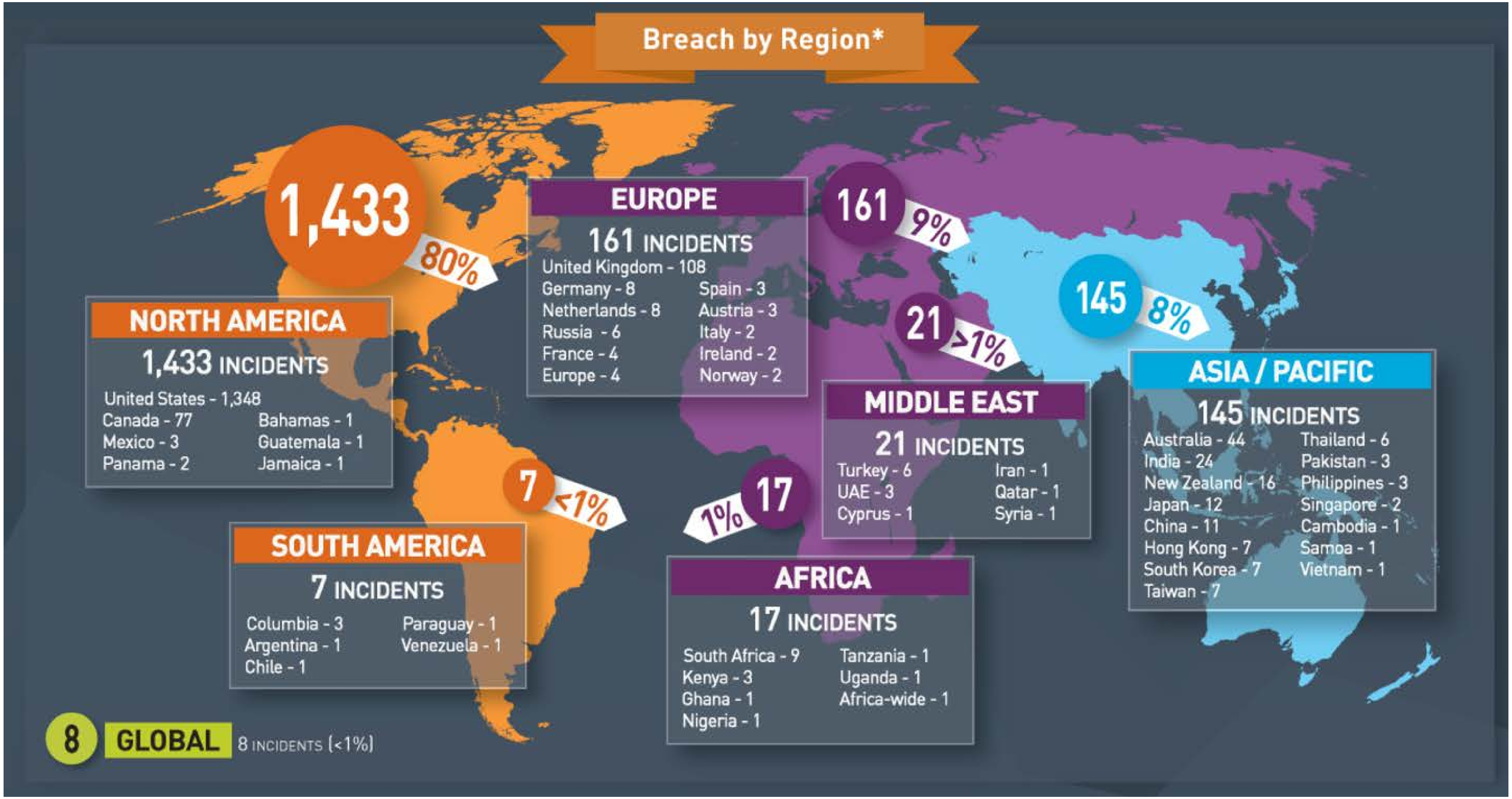
44 records every second

Healthcare	Government	Other	Retail	Financial	Technology	Education
493 INCIDENTS	269 INCIDENTS	229 INCIDENTS	215 INCIDENTS	214 INCIDENTS	189 INCIDENTS	157 INCIDENTS
28%	15%	13%	12%	12%	11%	9%

Data Breach cont..

Data breach landscape 2016

gemalto
security to be free



Breach by Region*

1,433 80%

NORTH AMERICA

1,433 INCIDENTS

United States - 1,348
Canada - 77
Mexico - 3
Panama - 2
Bahamas - 1
Guatemala - 1
Jamaica - 1

7 <1%

SOUTH AMERICA

7 INCIDENTS

Columbia - 3
Argentina - 1
Chile - 1
Paraguay - 1
Venezuela - 1

161 9%

EUROPE

161 INCIDENTS

United Kingdom - 108
Germany - 8
Netherlands - 8
Russia - 6
France - 4
Europe - 4
Spain - 3
Austria - 3
Italy - 2
Ireland - 2
Norway - 2

21 >1%

MIDDLE EAST

21 INCIDENTS

Turkey - 6
UAE - 3
Cyprus - 1
Iran - 1
Qatar - 1
Syria - 1

17 1%

AFRICA

17 INCIDENTS

South Africa - 9
Kenya - 3
Ghana - 1
Nigeria - 1
Tanzania - 1
Uganda - 1
Africa-wide - 1

145 8%

ASIA / PACIFIC

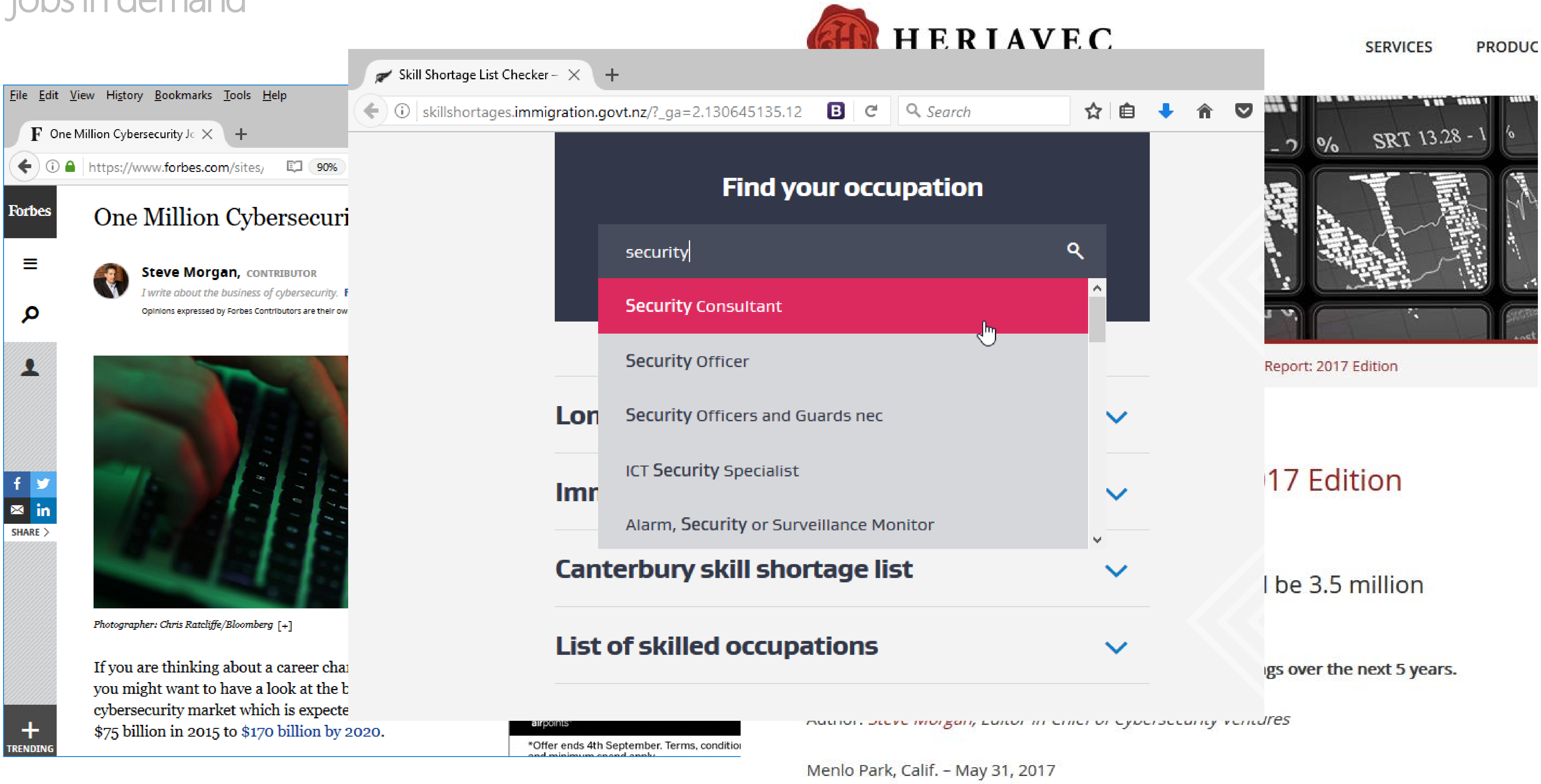
145 INCIDENTS

Australia - 44
India - 24
New Zealand - 16
Japan - 12
China - 11
Hong Kong - 7
South Korea - 7
Taiwan - 7
Thailand - 6
Pakistan - 3
Philippines - 3
Singapore - 2
Cambodia - 1
Samoa - 1
Vietnam - 1

8 GLOBAL 8 INCIDENTS (<1%)

Cyber Security Job Demand

jobs in demand



File Edit View History Bookmarks Tools Help
One Million Cybersecurity Jc
https://www.forbes.com/sites/
90%
Forbes
SHARE
TRENDING
Skill Shortage List Checker –
skillshortages.immigration.govt.nz/?_ga=2.130645135.12
Search
HERJAVEC
SERVICES
PRODUC
SRT 13.28 -

One Million Cybersecuri

Steve Morgan, CONTRIBUTOR

I write about the business of cybersecurity.

Opinions expressed by Forbes Contributors are their ow

Photographer: Chris Ratcliffe/Bloomberg [+]

If you are thinking about a career char
you might want to have a look at the b
cybersecurity market which is expecte
$75 billion in 2015 to $170 billion by 2020.

airpoints

*Offer ends 4th September. Terms, conditio
and minimum spend apply

Find your occupation

security

- Security Consultant
- Security Officer
- Security Officers and Guards nec
- ICT Security Specialist
- Alarm, Security or Surveillance Monitor

Lon

Imm

Canterbury skill shortage list

List of skilled occupations

Report: 2017 Edition

17 Edition

l be 3.5 million

gs over the next 5 years.

Author: Steve Morgan, Editor in Chief of Cybersecurity Ventures

Menlo Park, Calif. – May 31, 2017

Functional Testing vs Security Testing

odds and evens

Functional Tester vs Security Tester

- What we know should be true
  - Forget what is known, look for unknown
- Base assumptions of requirement
  - Base assumption is experience and skills
- Formalized testing structure and method
  - Anti-testing
- Established procedure for testing
  - Method varies from tester, tool, app and scope
- Defects are bad
  - Vulnerabilities are good ☺

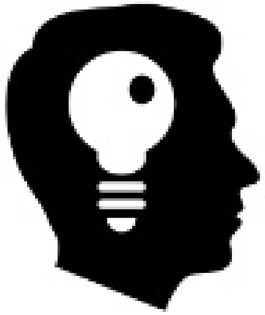
Becoming a hacker

what hacking requires?

- Terminology
  - Hacker, Cracker, Exploit, Vulnerability assessment, penetration testing
- Mindset
  - Deviate the application from its original programmed purpose
- Method
  - Comes from experience and critical thinking
- Tools
  - Use fusion of tools for better result
- Goal
  - Discover ways to make application act in most unintended way

Basic Security Principles

Authentication



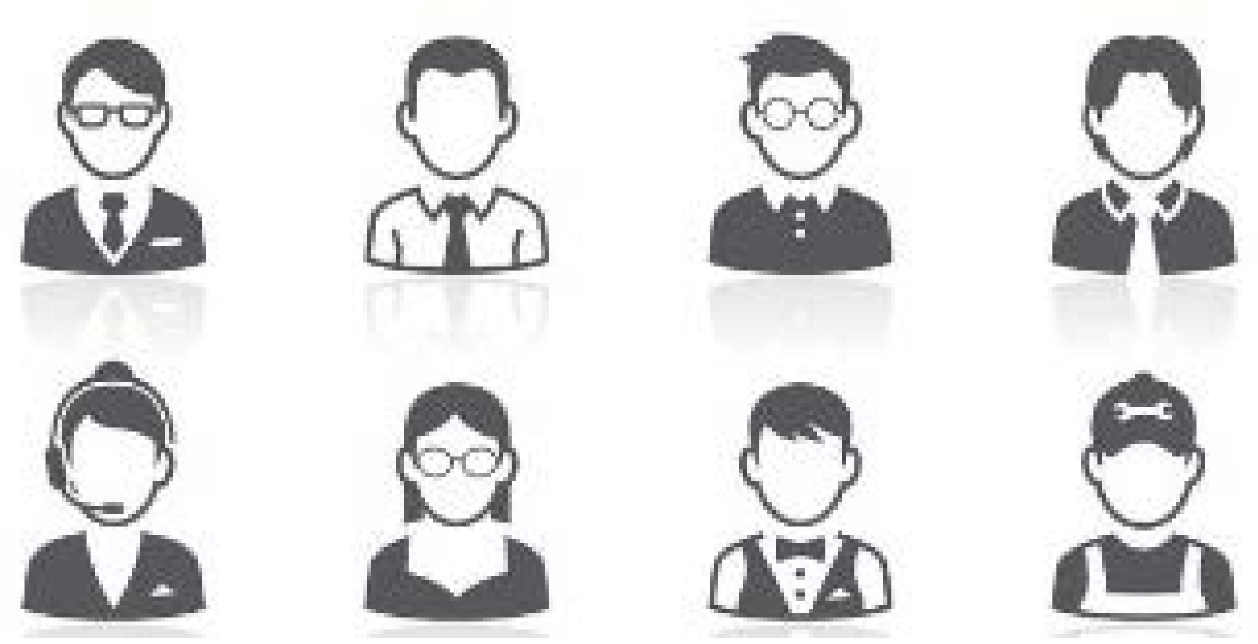
1. Something you **know**
(such as a password)

2. Something you **are**
(such as a fingerprint)

3. Something you **have**
(such as a smart card)

Basic Security Principles Cont…

Authorization

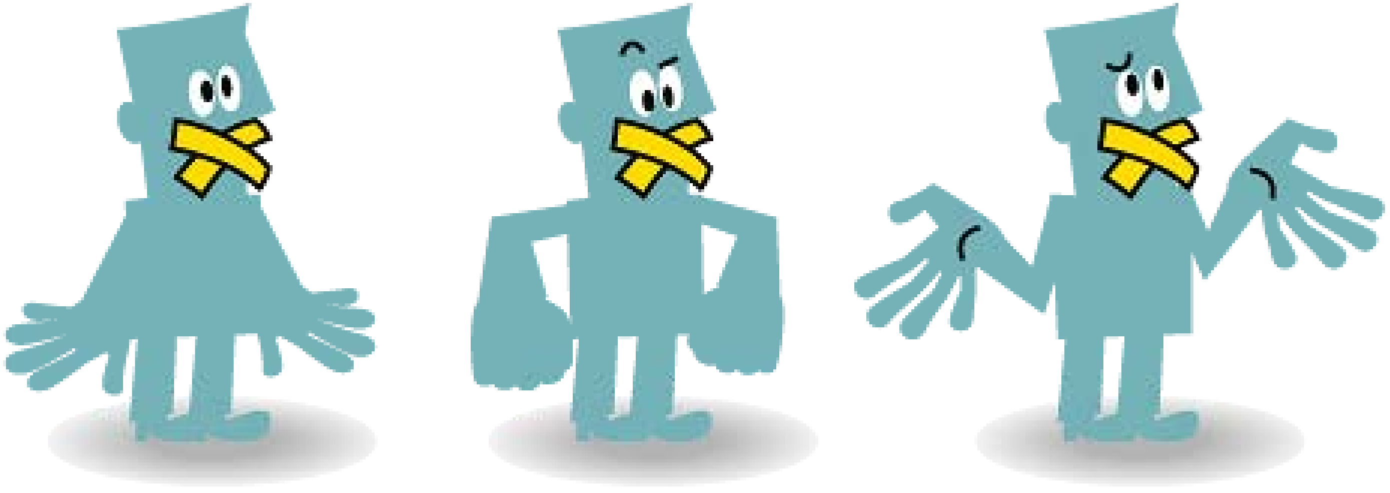


Basic Security Principles Cont...

Availability

Basic Security Principles Cont…

Confidentiality



Basic Security Principles Cont…

Integrity

Application Security Testing 101

lets dive in into magic world of hacking

Where to start?

OWASP

Open Web Application Security Project

open source

Application Security Testing 101

lets dive in magic world of hacking

- Famous Projects

OWASP
Open Web Application
Security Project

OWASP
Mobile Security Project

OWASP
Internet of Things Top 10

Application Security Testing 101

OWASP web application security project

- OWASP Top 10
  - A1 – Injection
  - A2 – Broken Authentication and Session Management
  - A3 – Cross Site Scripting (XSS)
  - A4 – Insecure Direct Object Reference
  - A5 – Security Misconfiguration
  - A6 – Sensitive Data Exposure
  - A7 – Missing Function Level Access Control
  - A8 – Cross-Site Request Forgery (CSRF)
  - A9 – Using Known Vulnerable Components
  - A10 – Unvalidated Redirects and Forwards
- Business logic testing ☛

Technical Vulnerabilities

Application Security Testing 101

Decoding business logic testing

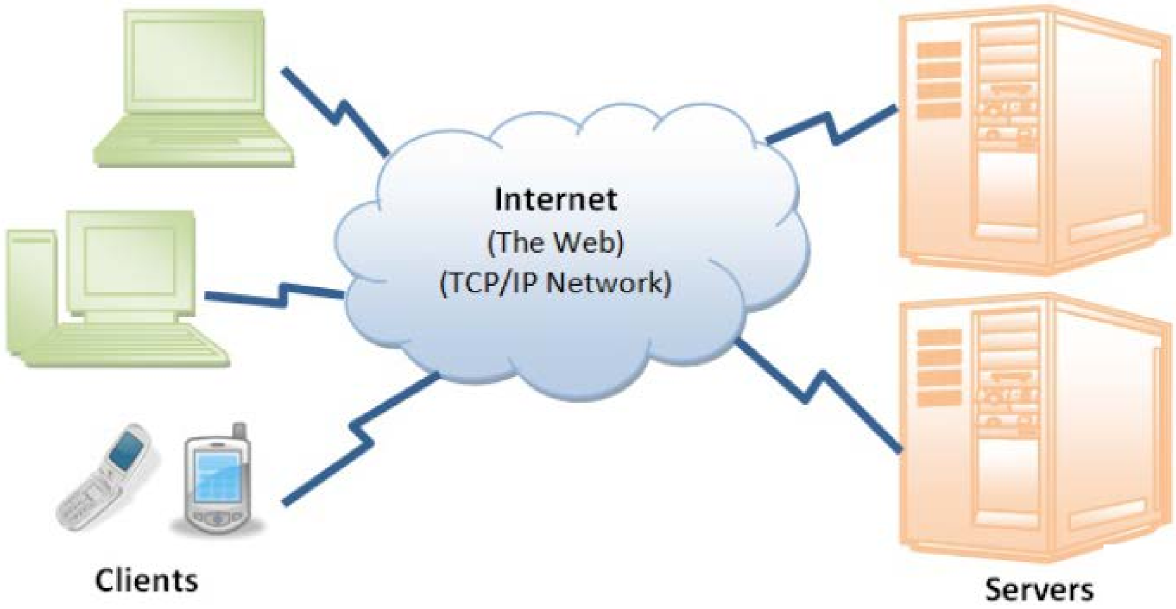
- Business logic vulnerability testing
  - Difficult to detect – why?
  - Highest impact
  - No scanner in the world will be able to detect it

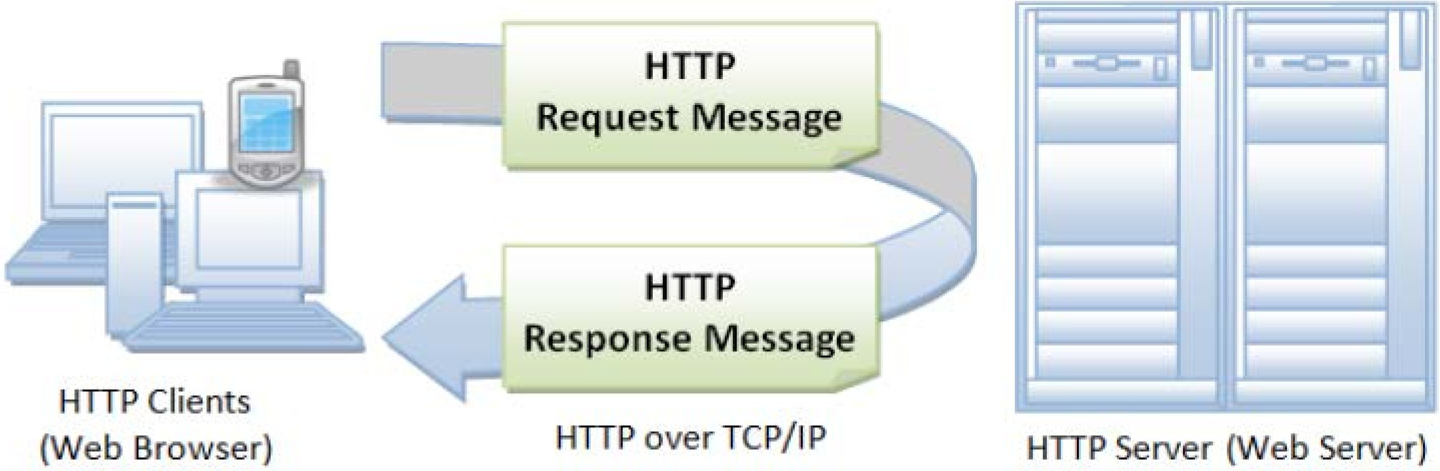
- Few examples of business logic vulnerabilities
  - Increasing bank account balance
  - Purchasing items free online
  - Purchasing multiple items at a price of one item
  - Posting Facebook status behalf of someone on his wall
  - Commenting on Facebook post behalf of your friend
  - Many more…

Application Security Testing 101

Web technology

Client – Server Technology

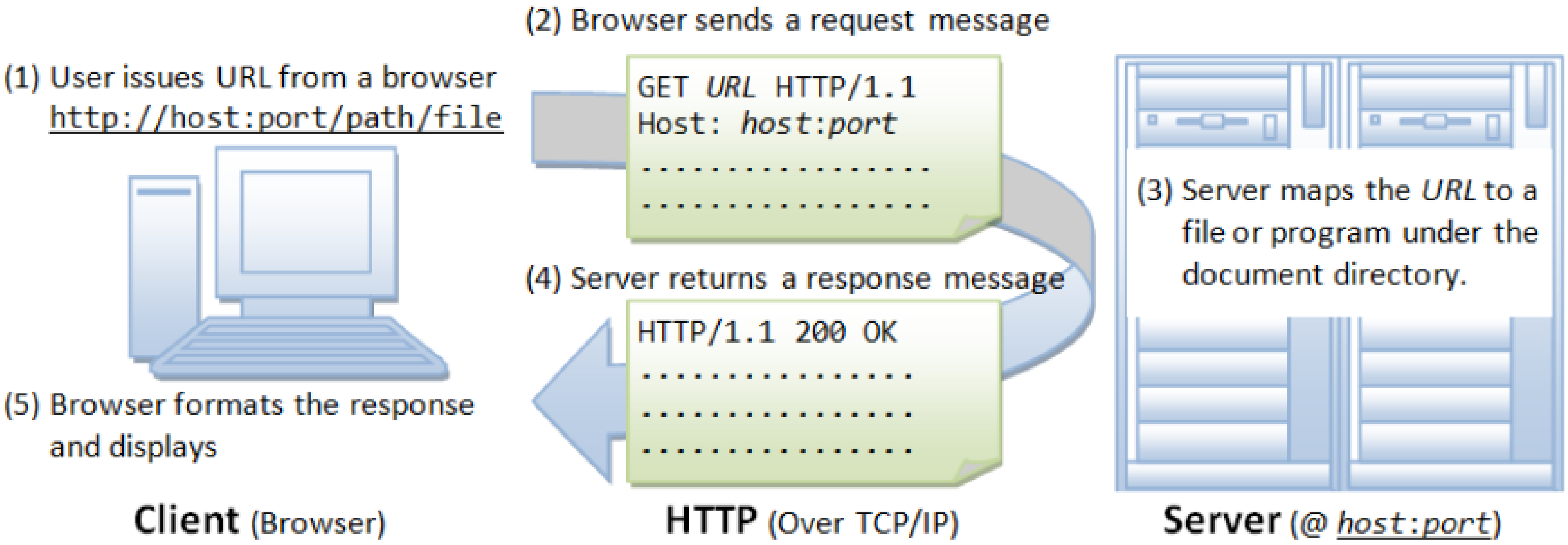




Application Security Testing 101

How web works

Client – Server Technology



(1) User issues URL from a browser
http://host:port/path/file

(2) Browser sends a request message

```
GET URL HTTP/1.1
Host: host:port
..................
..................
```

(3) Server maps the *URL* to a file or program under the document directory.

(4) Server returns a response message

```
HTTP/1.1 200 OK
.................
.................
.................
```

(5) Browser formats the response and displays

Client (Browser)

HTTP (Over TCP/IP)

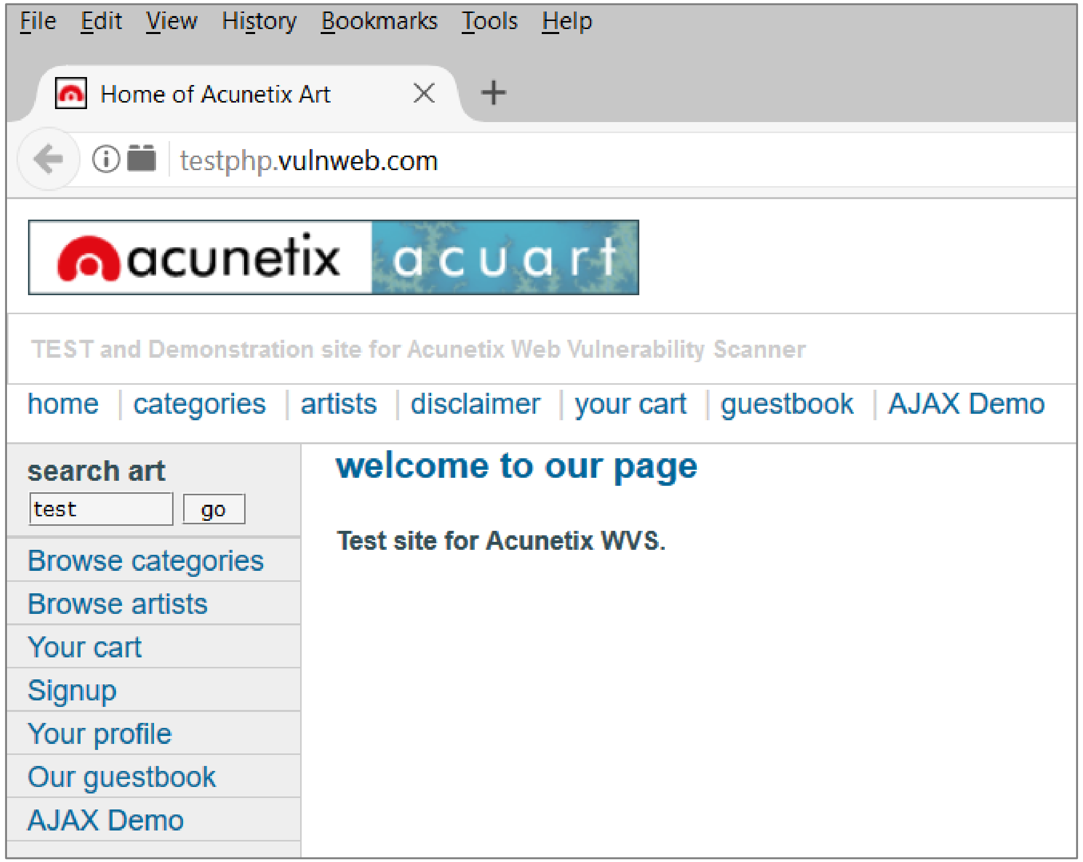
Server (@ *host:port*)

Application Security Testing 101

How web works

Real life Request and Response example

1

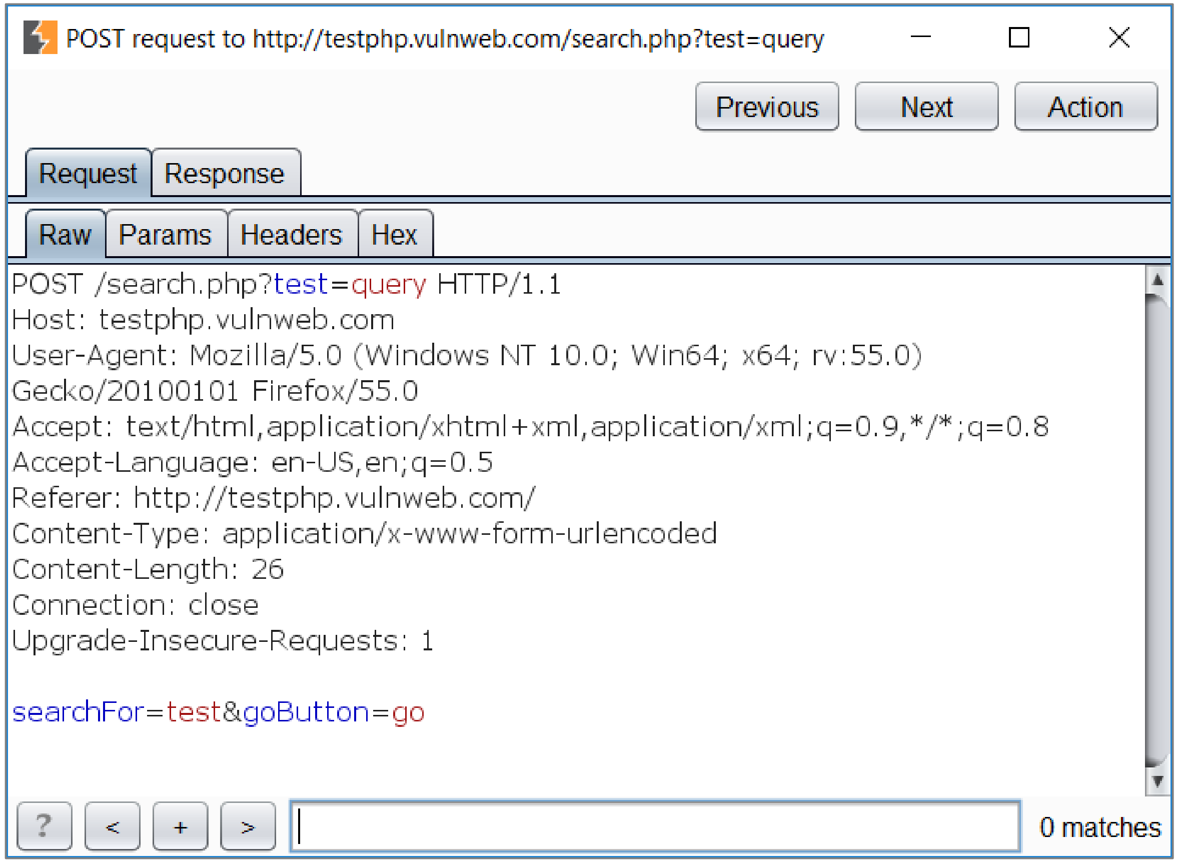


TEST and Demonstration site for Acunetix Web Vulnerability Scanner

welcome to our page

Test site for Acunetix WVS.

2



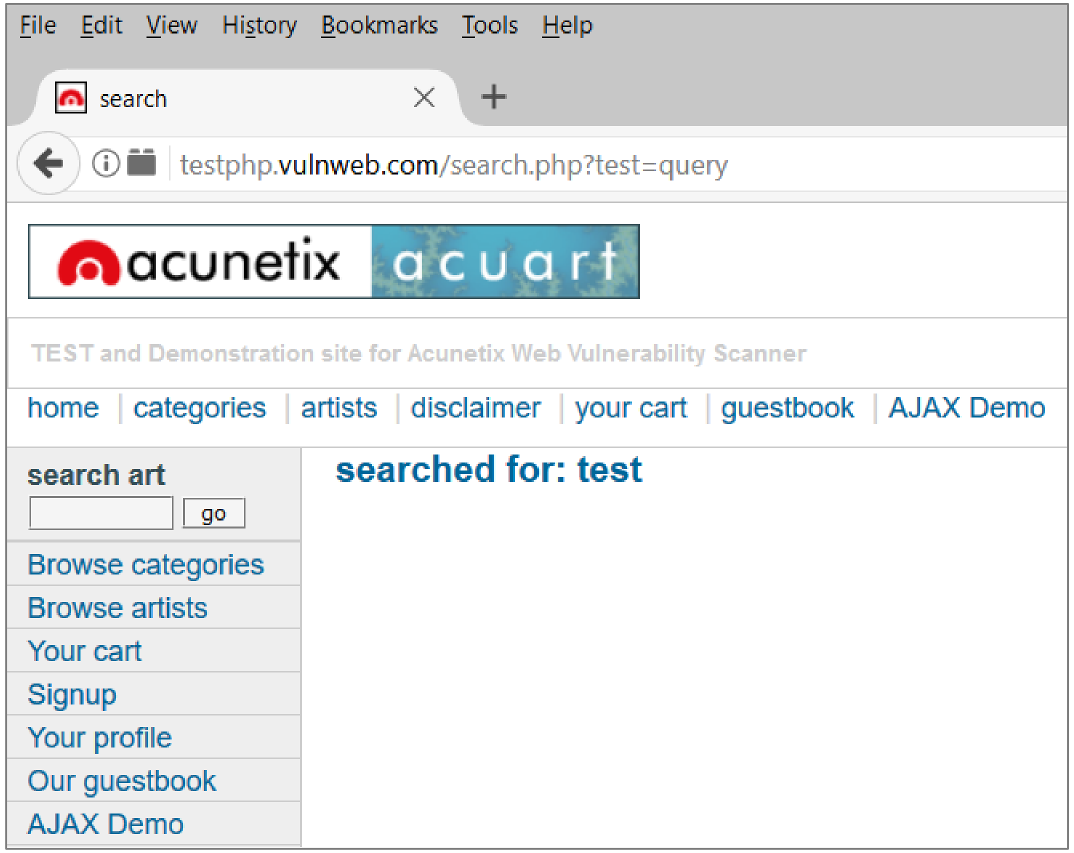
```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0)
Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://testphp.vulnweb.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Connection: close
Upgrade-Insecure-Requests: 1

searchFor=test&goButton=go
```

Application Security Testing 101

How web works

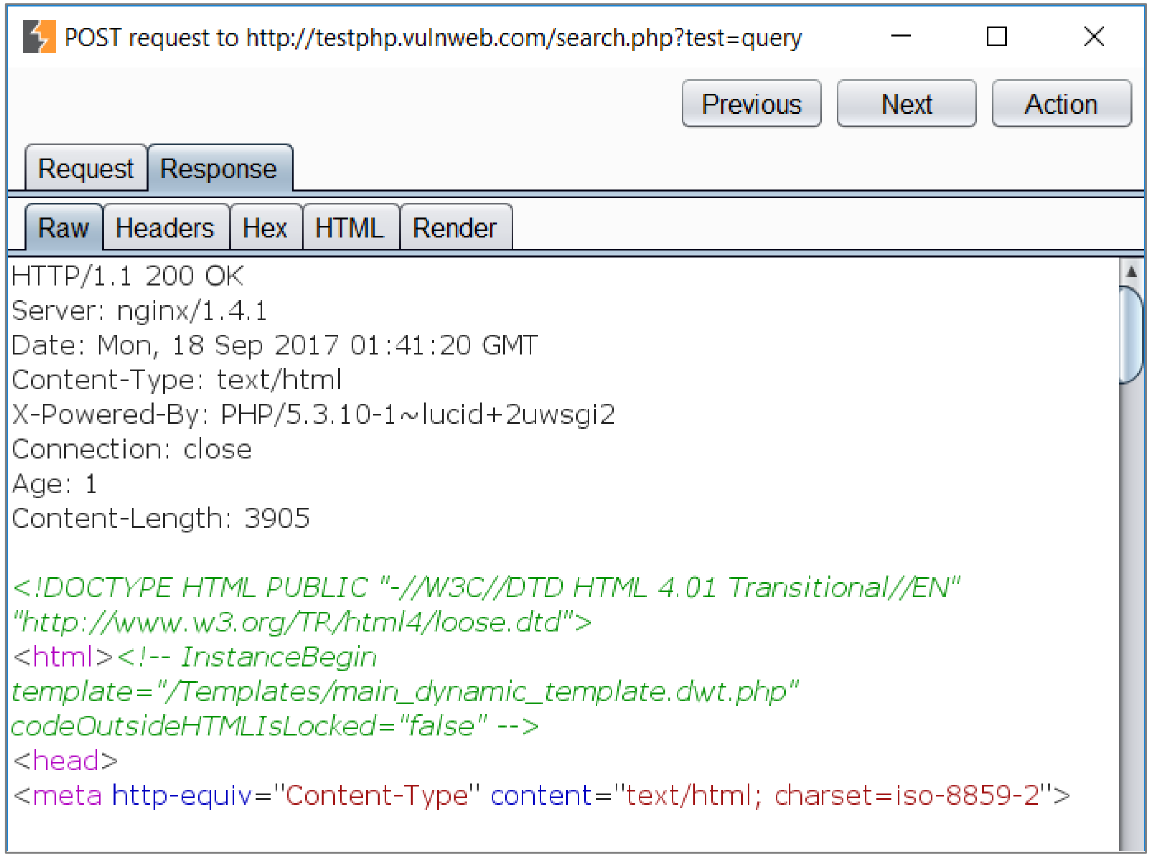
Real life Request and Response example

4


File Edit View History Bookmarks Tools Help
search
testphp.vulnweb.com/search.php?test=query
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

searched for: test

3

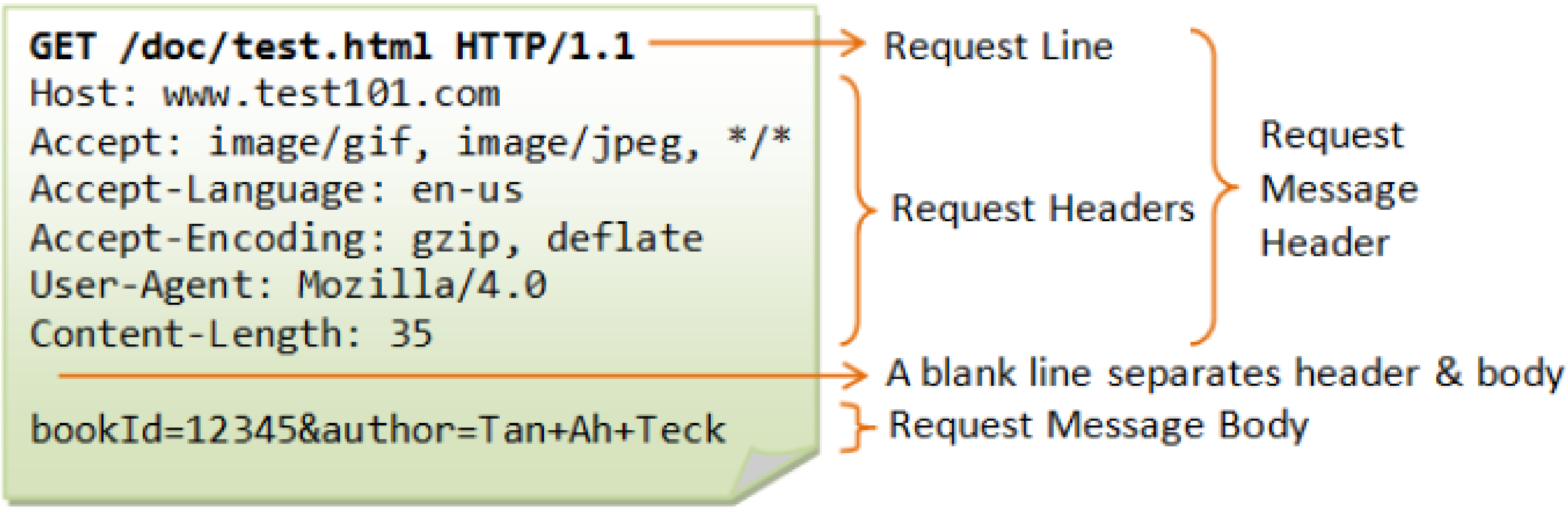

POST request to http://testphp.vulnweb.com/search.php?test=query
Previous
Next
Action
Request
Response
Raw
Headers
Hex
HTML
Render

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Mon, 18 Sep 2017 01:41:20 GMT
Content-Type: text/html
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Connection: close
Age: 1
Content-Length: 3905

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin
template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
```

Application Security Testing 101

HTTP basics

Decoding Request



```
GET /doc/test.html HTTP/1.1
Host: www.test101.com
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
Content-Length: 35

bookId=12345&author=Tan+Ah+Teck
```

Request Line

Request Headers

Request Message Header

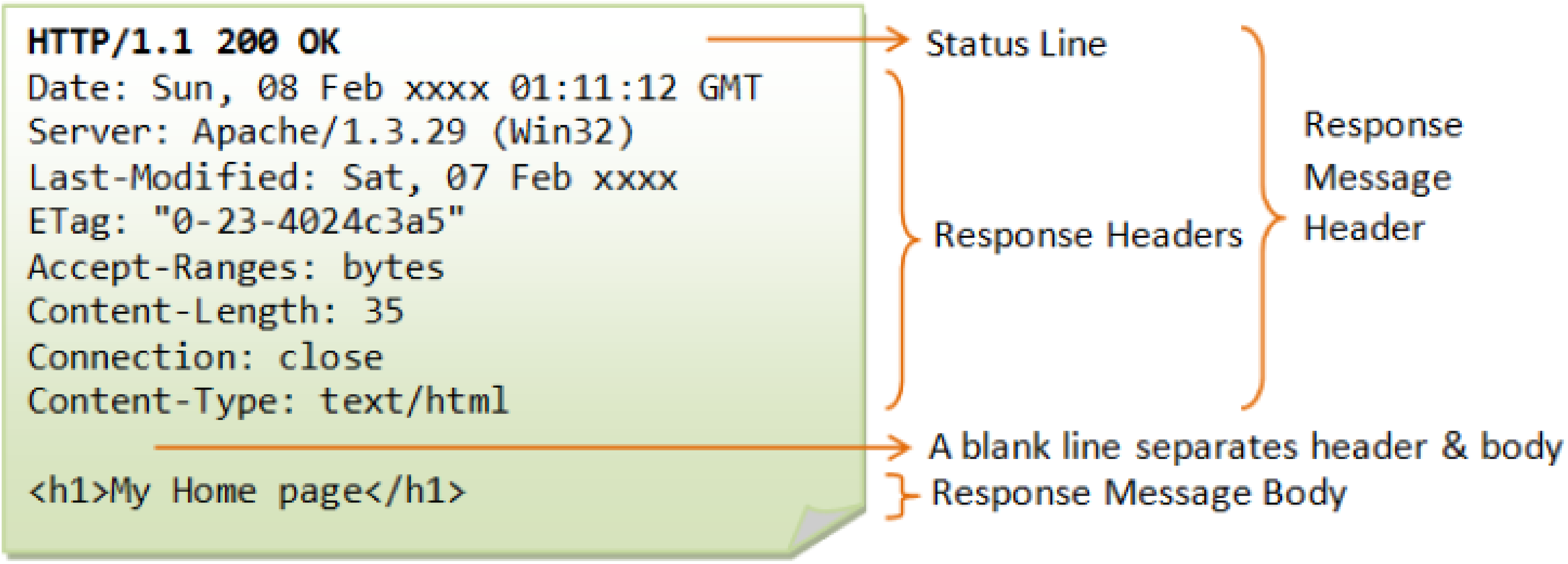
A blank line separates header & body

Request Message Body

Application Security Testing 101

HTTP basics

Decoding Response



```
HTTP/1.1 200 OK
Date: Sun, 08 Feb xxxx 01:11:12 GMT
Server: Apache/1.3.29 (Win32)
Last-Modified: Sat, 07 Feb xxxx
ETag: "0-23-4024c3a5"
Accept-Ranges: bytes
Content-Length: 35
Connection: close
Content-Type: text/html

<h1>My Home page</h1>
```

Application Security Testing 101

HTTP basics

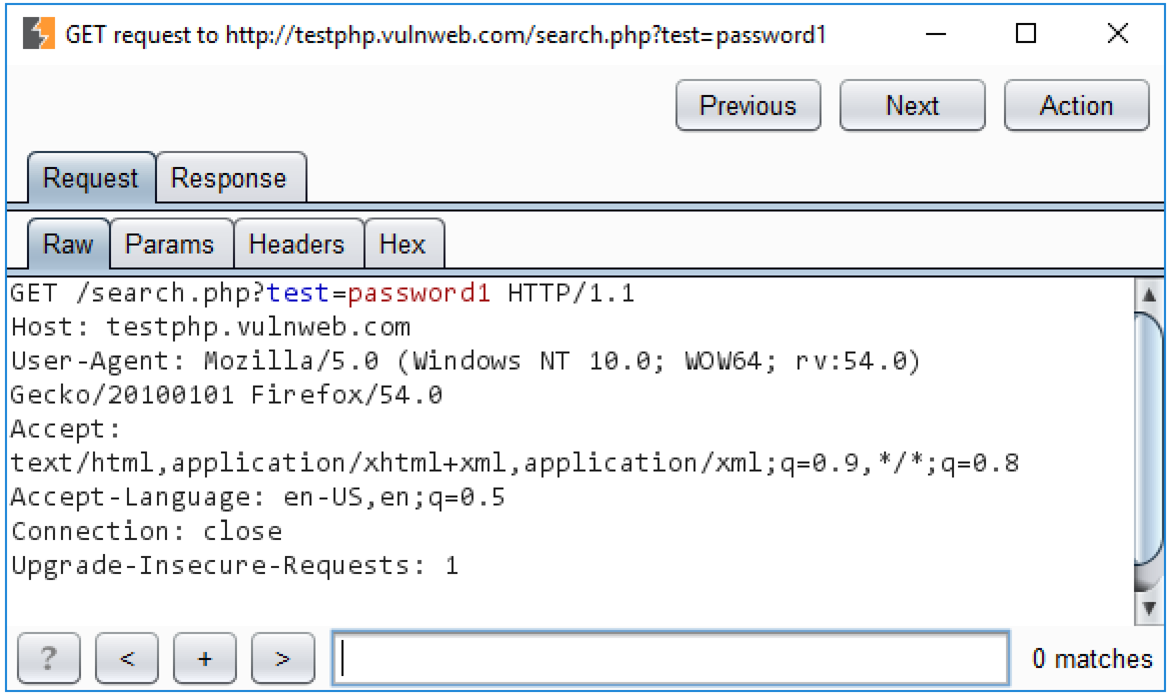
- Various HTTP Methods
  - GET – Client requests a web resource from the server
  - POST– Used to post data up to the server.
  - PUT – Upload file on the server to store
  - DELETE – Delete the resource from the web server.
  - Etc… (Other 15+ methods)

- We are going to focus on
  - GET
  - POST

Application Security Testing 101

GET vs POST Battle

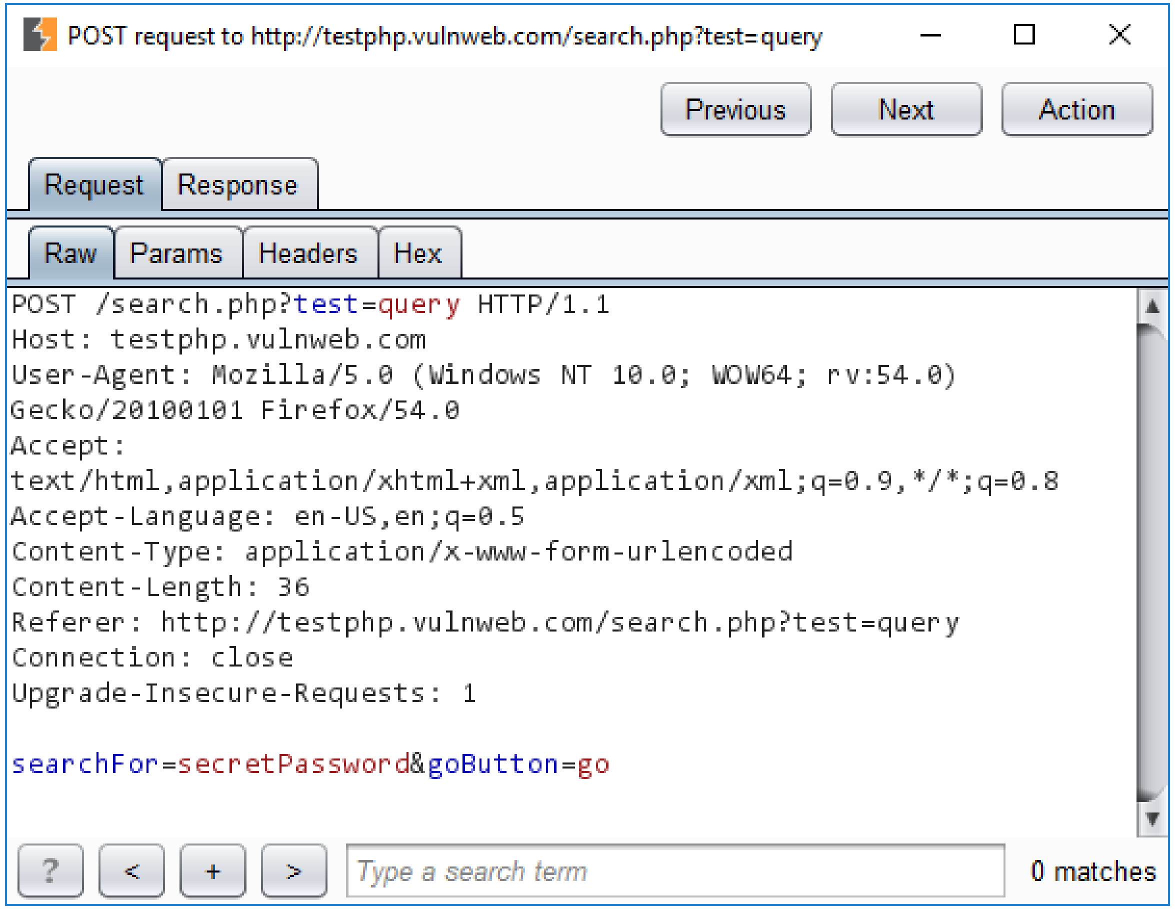
GET Request Method



GET request to http://testphp.vulnweb.com/search.php?test=password1
Previous
Next
Action
Request
Response
Raw
Params
Headers
Hex
?
<
+
>
0 matches

```
GET /search.php?test=password1 HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: close
Upgrade-Insecure-Requests: 1
```

POST Request Method

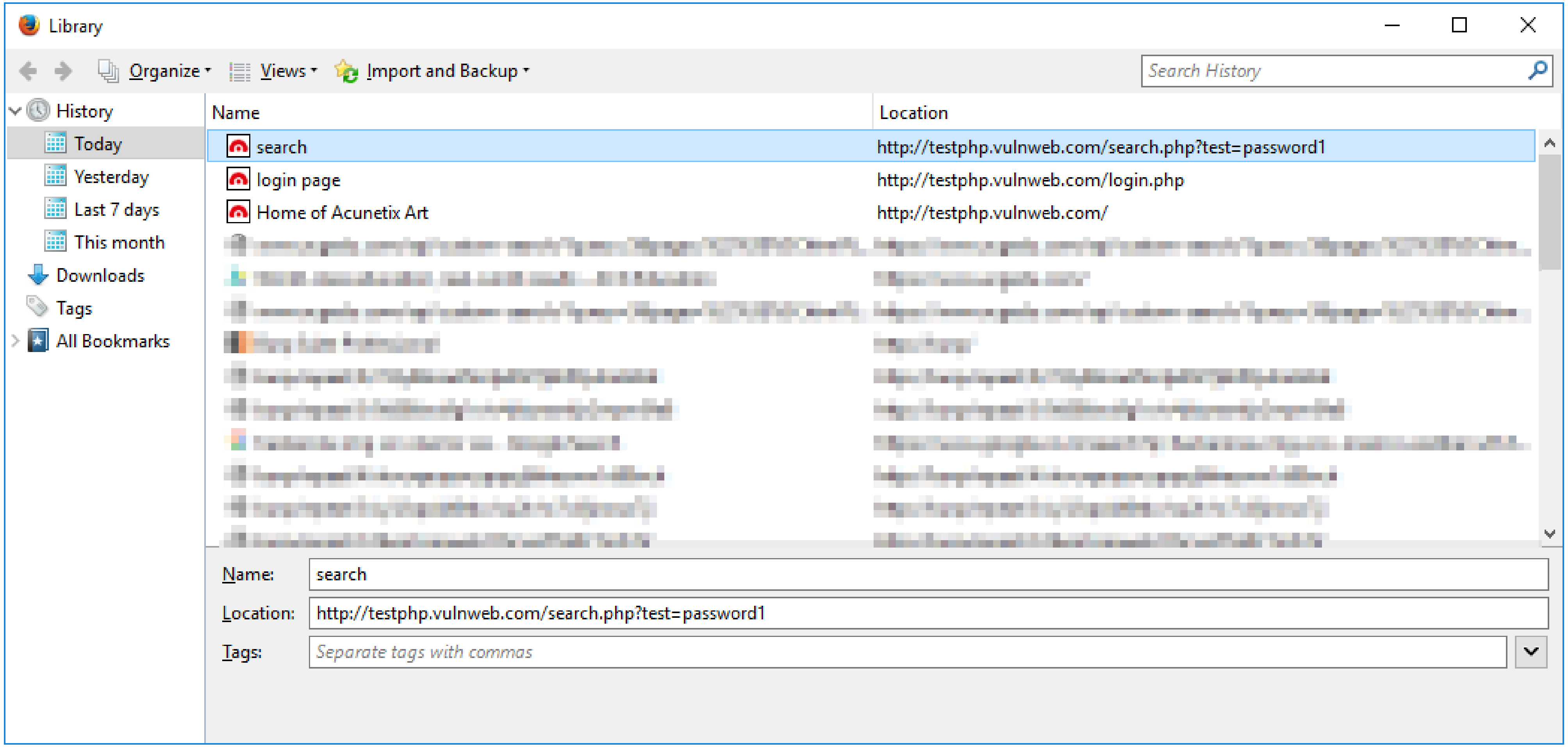


```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Referer: http://testphp.vulnweb.com/search.php?test=query
Connection: close
Upgrade-Insecure-Requests: 1

searchFor=secretPassword&goButton=go
```

Application Security Testing 101

GET vs POST Battle

Why GET method is bad idea?



Name	Location
search	http://testphp.vulnweb.com/search.php?test=password1
login page	http://testphp.vulnweb.com/login.php
Home of Acunetix Art	http://testphp.vulnweb.com/

Name: search

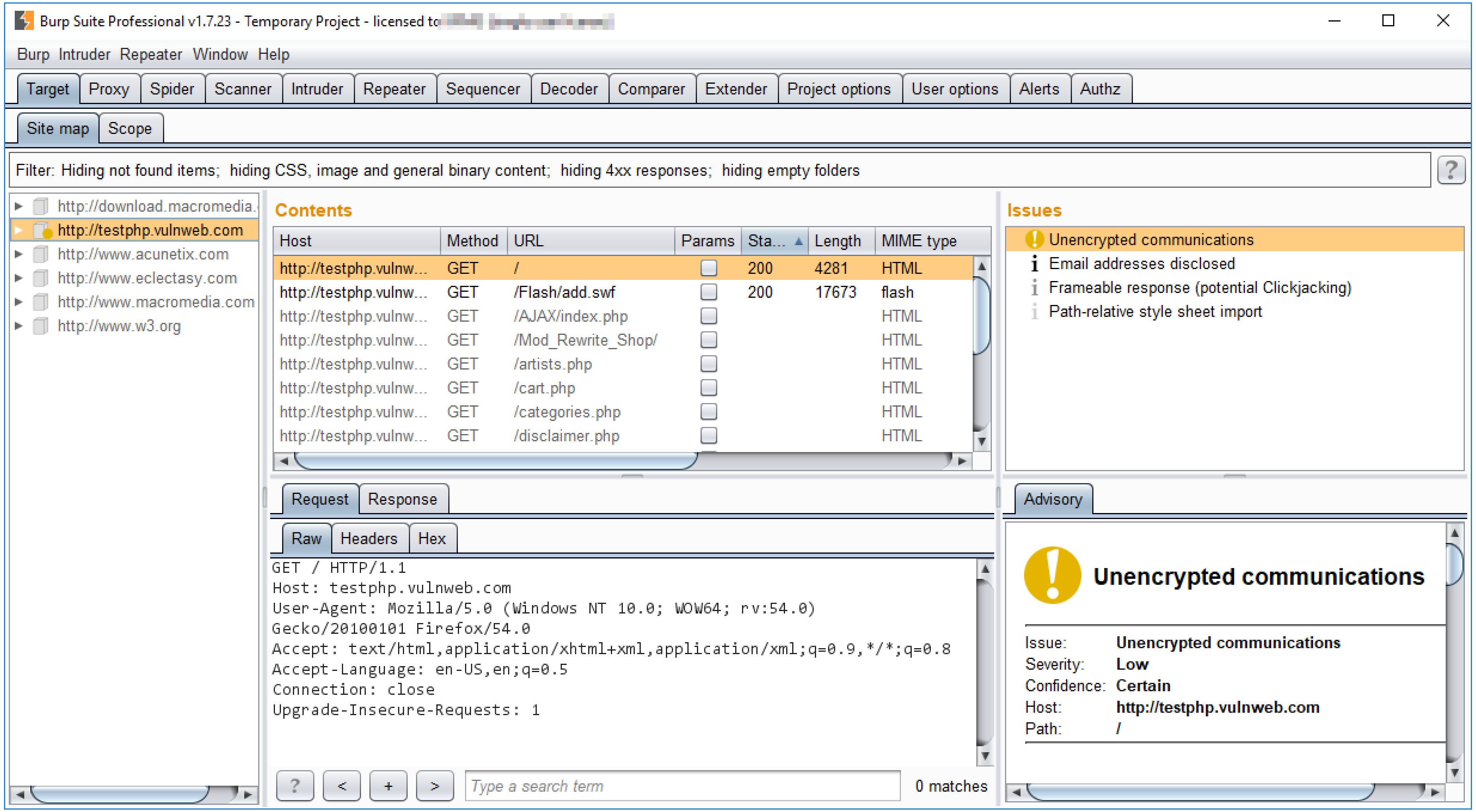
Location: http://testphp.vulnweb.com/search.php?test=password1

Tags: *Separate tags with commas*

Application Security Testing 101

The magic of Burp Suite

BURPSUITE
PROFESSIONAL



Burp Suite Professional v1.7.23 - Temporary Project - licensed to [redacted]

Burp Intruder Repeater Window Help
Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts | Authz
Site map | Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- http://download.macromedia.
- http://testphp.vulnweb.com
- http://www.acunetix.com
- http://www.eclectasy.com
- http://www.macromedia.com
- http://www.w3.org

Contents

Host	Method	URL	Params	Sta... ▲	Length	MIME type
http://testphp.vulnw...	GET	/	□	200	4281	HTML
http://testphp.vulnw...	GET	/Flash/add.swf	□	200	17673	flash
http://testphp.vulnw...	GET	/AJAX/index.php	□			HTML
http://testphp.vulnw...	GET	/Mod_Rewrite_Shop/	□			HTML
http://testphp.vulnw...	GET	/artists.php	□			HTML
http://testphp.vulnw...	GET	/cart.php	□			HTML
http://testphp.vulnw...	GET	/categories.php	□			HTML
http://testphp.vulnw...	GET	/disclaimer.php	□			HTML

Issues

- ! Unencrypted communications
- i Email addresses disclosed
- i Frameable response (potential Clickjacking)
- i Path-relative style sheet import

```
GET / HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: close
Upgrade-Insecure-Requests: 1
```

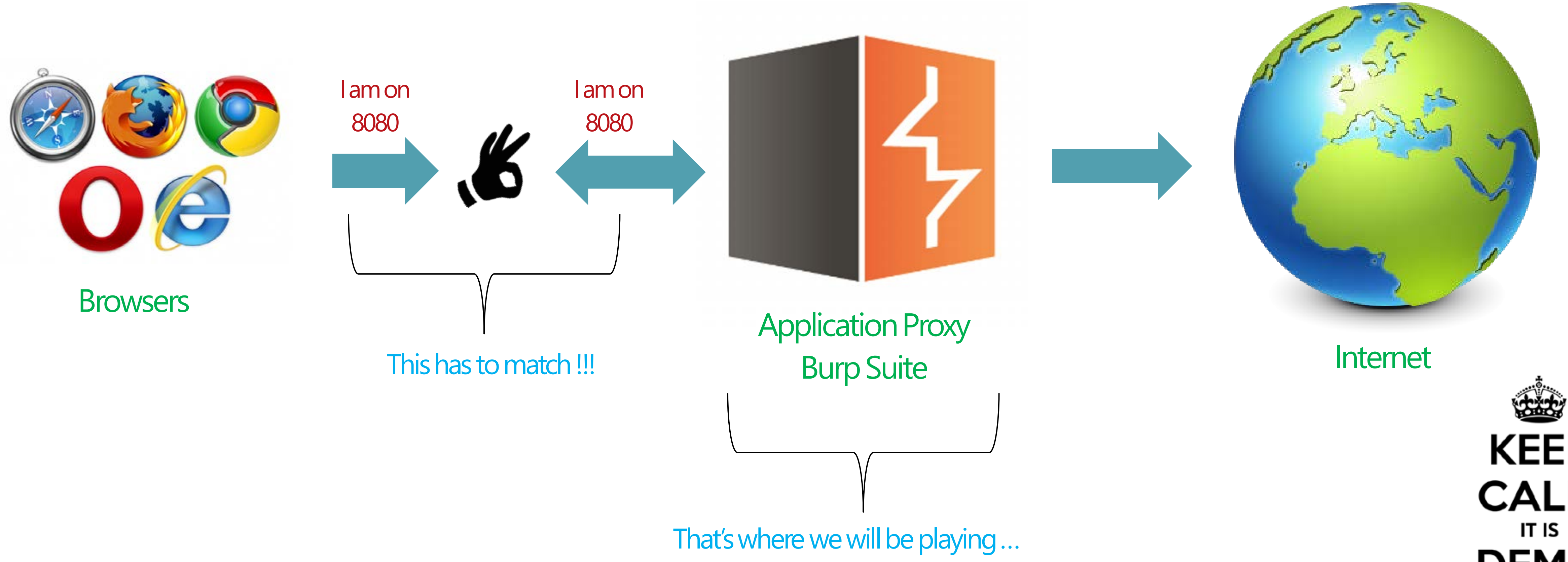
Unencrypted communications

Issue:	**Unencrypted communications**
Severity:	**Low**
Confidence:	**Certain**
Host:	**http://testphp.vulnweb.com**
Path:	**/**

Application Security Testing 101

Proxy where it starts

Connecting browser and proxy to kick start application security



I am on 8080

I am on 8080

Browsers

This has to match !!!

Application Proxy
Burp Suite

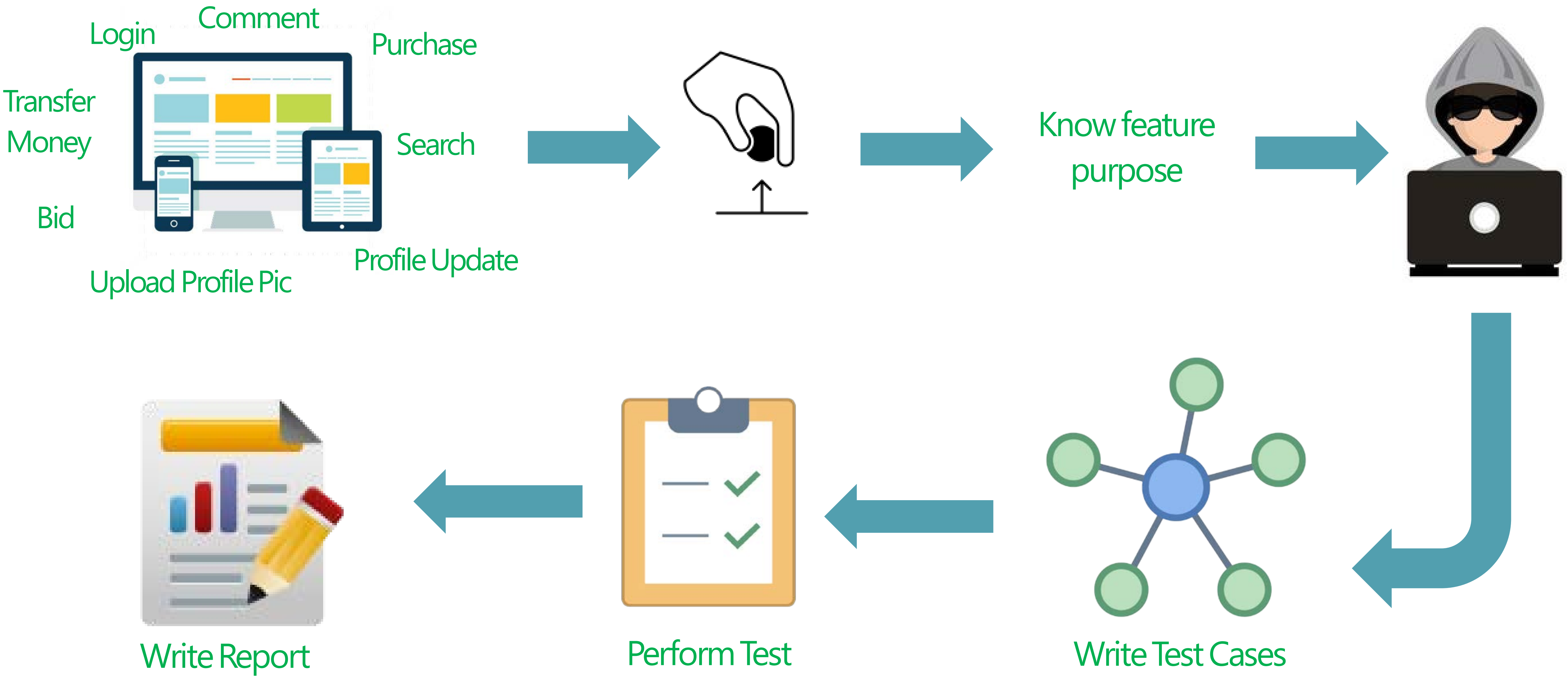
That's where we will be playing …

Internet

KEEP
CALM
IT IS
DEMO
TIME

Application Security Testing 101

Testing Methodology



Login

Comment

Purchase

Transfer Money

Search

Bid

Profile Update

Upload Profile Pic

Know feature purpose

Write Test Cases

Perform Test

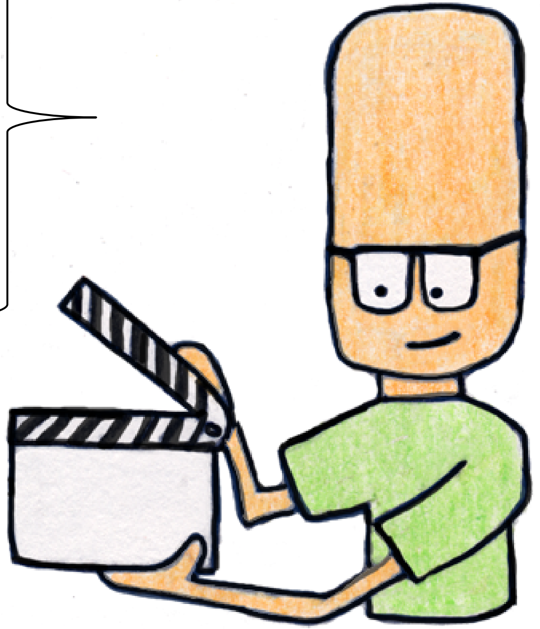
Write Report

Application Security Testing 101

Quick Recap

- Importance of Cyber Security
- Difference between Functional vs Security Testing

- OWASP top 10 vs Business Logic Testing
- Basic of Web Server Technology | Get vs POST | Request | Response
- Burp Suite Demo
- Testing Approach Methodology



Live Action

Application Security Testing 101

Common Test cases for known features

- Registration
  - Can a same email id be used for two account creation?
  - Can I perform registration on used email id again?
  - Can I register with email id without confirming activation through email?
  - Can I perform mass registration?
  - Is password complexity maintained?

- Forgot Password
  - Can I perform email bombing on victim's email id?
  - Can I perform password reset behalf of other users?
  - Does forgot password reset links has expiry dates?
  - Does old forgot password reset links gets invalidated upon requesting new?
  - Can usernames be enumerated from forgot password feature?

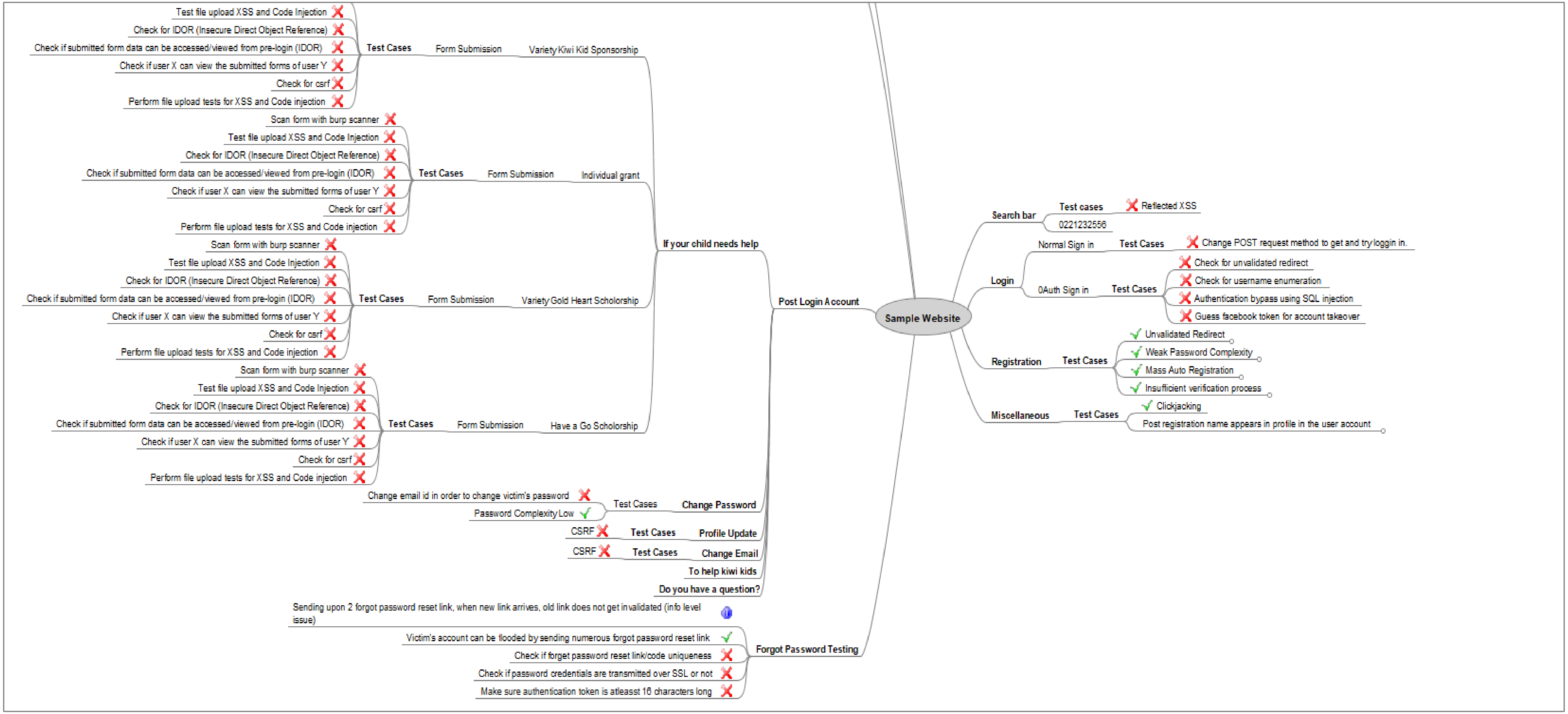
Application Security Testing 101

Common Testcases for known Features. Cont..

- Product Purchase
  - Can I purchase product behalf of other user?
  - Can I purchase product in less price than then actual?
  - Can I purchase more products at a price of single?
  - Can I add items into other user's cart?
  - Can I purchase product at $0 (free)?
  - Can I change someone's default shipping delivery address?
- Social Media
  - Can I post status on my wall without his/her permission?
  - Can I post status on someone's wall behalf of my friend?
  - Can I update profile pic of my friend's profile?
  - Can I turn off/on privacy/security settings of my friend's profile?

Application Security Testing 101

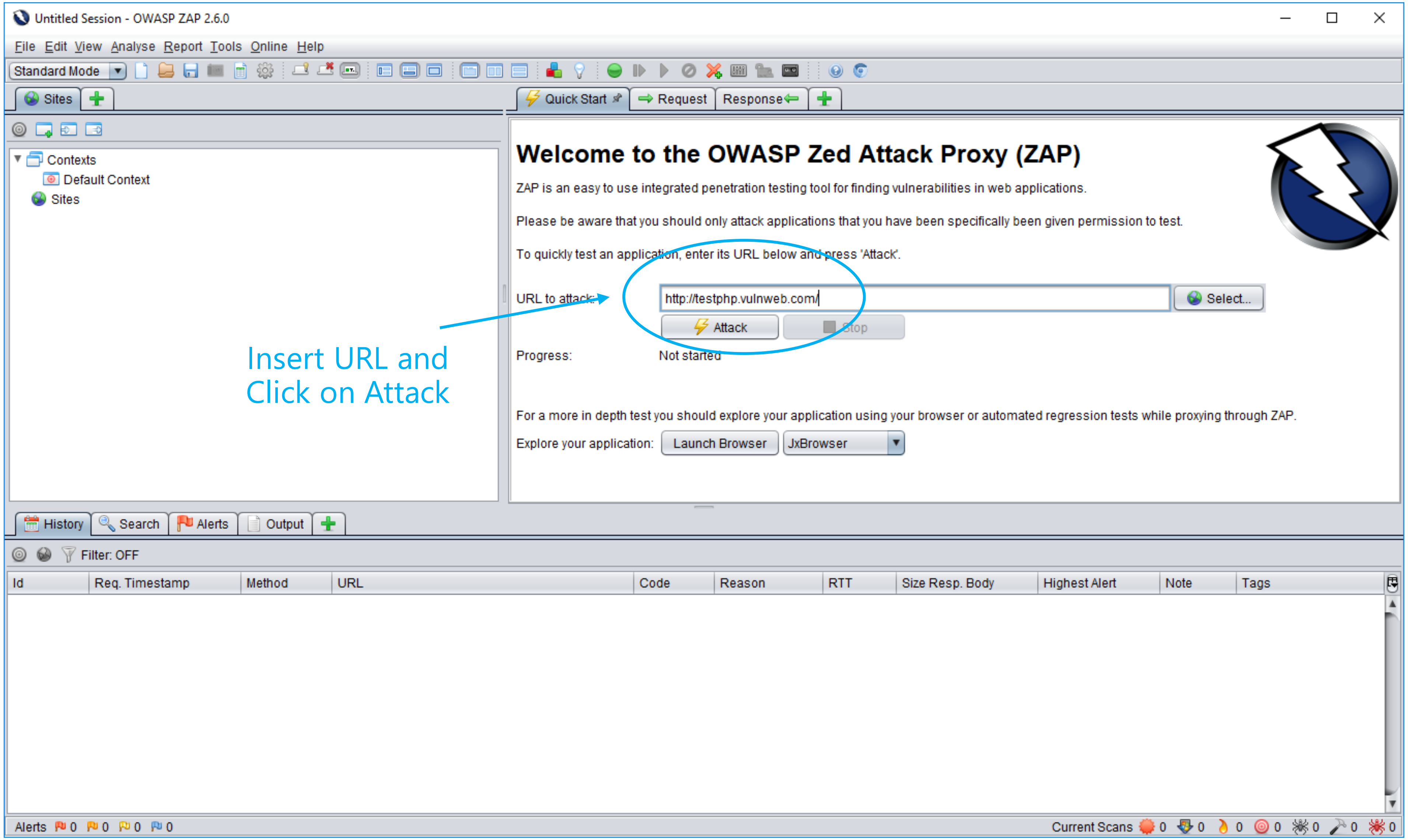
Final mind map of test cases



- Sample Website
  - Post Login Account
    - If your child needs help
      - Variety Kiwi Kid Sponsorship
        - Form Submission
          - Test Cases
            - Test file upload XSS and Code Injection ✗
            - Check for IDOR (Insecure Direct Object Reference) ✗
            - Check if submitted form data can be accessed/viewed from pre-login (IDOR) ✗
            - Check if user X can view the submitted forms of user Y ✗
            - Check for csrf ✗
            - Perform file upload tests for XSS and Code injection ✗
      - Individual grant
        - Form Submission
          - Test Cases
            - Scan form with burp scanner ✗
            - Test file upload XSS and Code Injection ✗
            - Check for IDOR (Insecure Direct Object Reference) ✗
            - Check if submitted form data can be accessed/viewed from pre-login (IDOR) ✗
            - Check if user X can view the submitted forms of user Y ✗
            - Check for csrf ✗
            - Perform file upload tests for XSS and Code injection ✗
      - Variety Gold Heart Scholorship
        - Form Submission
          - Test Cases
            - Scan form with burp scanner ✗
            - Test file upload XSS and Code Injection ✗
            - Check for IDOR (Insecure Direct Object Reference) ✗
            - Check if submitted form data can be accessed/viewed from pre-login (IDOR) ✗
            - Check if user X can view the submitted forms of user Y ✗
            - Check for csrf ✗
            - Perform file upload tests for XSS and Code injection ✗
      - Have a Go Scholorship
        - Form Submission
          - Test Cases
            - Scan form with burp scanner ✗
            - Test file upload XSS and Code Injection ✗
            - Check for IDOR (Insecure Direct Object Reference) ✗
            - Check if submitted form data can be accessed/viewed from pre-login (IDOR) ✗
            - Check if user X can view the submitted forms of user Y ✗
            - Check for csrf ✗
            - Perform file upload tests for XSS and Code injection ✗
    - Change Password
      - Test Cases
        - Change email id in order to change victim's password ✗
        - Password Complexity Low ✓
    - Profile Update
      - Test Cases
        - CSRF ✗
    - Change Email
      - Test Cases
        - CSRF ✗
    - To help kiwi kids
    - Do you have a question?
  - Forgot Password Testing
    - Sending upon 2 forgot password reset link, when new link arrives, old link does not get invalidated (info level issue) ℹ
    - Victim's account can be flooded by sending numerous forgot password reset link ✓
    - Check if forget password reset link/code uniqueness ✗
    - Check if password credentials are transmitted over SSL or not ✗
    - Make sure authentication token is atleasst 16 characters long ✗
  - Search bar
    - Test cases
      - ✗ Reflected XSS
    - 0221232556
  - Login
    - Normal Sign in
      - Test Cases
        - ✗ Change POST request method to get and try loggin in.
    - 0Auth Sign in
      - Test Cases
        - ✗ Check for unvalidated redirect
        - ✗ Check for username enumeration
        - ✗ Authentication bypass using SQL injection
        - ✗ Guess facebook token for account takeover
  - Registration
    - Test Cases
      - ✓ Unvalidated Redirect
      - ✓ Weak Password Complexity
      - ✓ Mass Auto Registration
      - ✓ Insufficient verification process
  - Miscellaneous
    - Test Cases
      - ✓ Clickjacking
      - Post registration name appears in profile in the user account

Application Security Testing 101

OWASP ZAP



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://testphp.vulnweb.com/

Progress: Not started

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

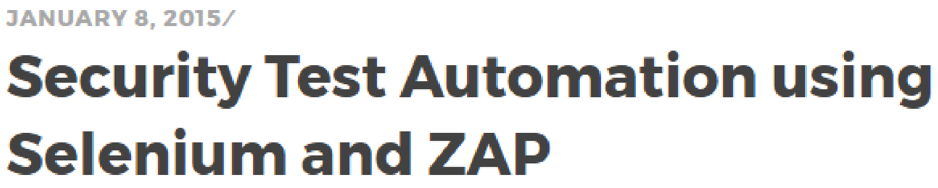
Explore your application: Launch Browser JxBrowser

Insert URL and Click on Attack

OWASP ZAP

Application Security Testing 101

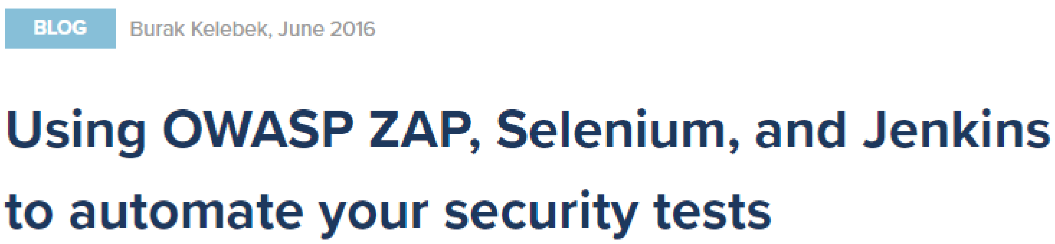
Integration of ZAP and Selenium



JANUARY 8, 2015/

Security Test Automation using Selenium and ZAP

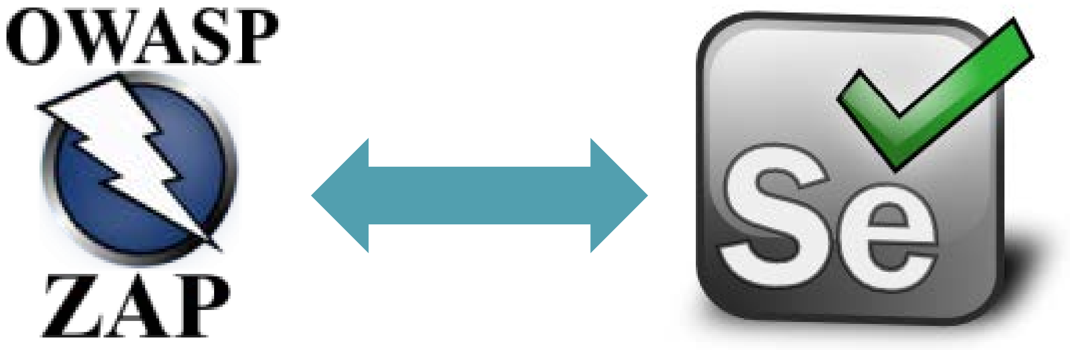
https://linkeshkannavelu.com/2015/01/08/security-test-automation-using-selenium-and-zap/



BLOG Burak Kelebek, June 2016

Using OWASP ZAP, Selenium, and Jenkins to automate your security tests

https://securify.nl/blog/SFY20160601/using_owasp_zap__selenium__and_jenkins_to_automate_your_security_tests_.html

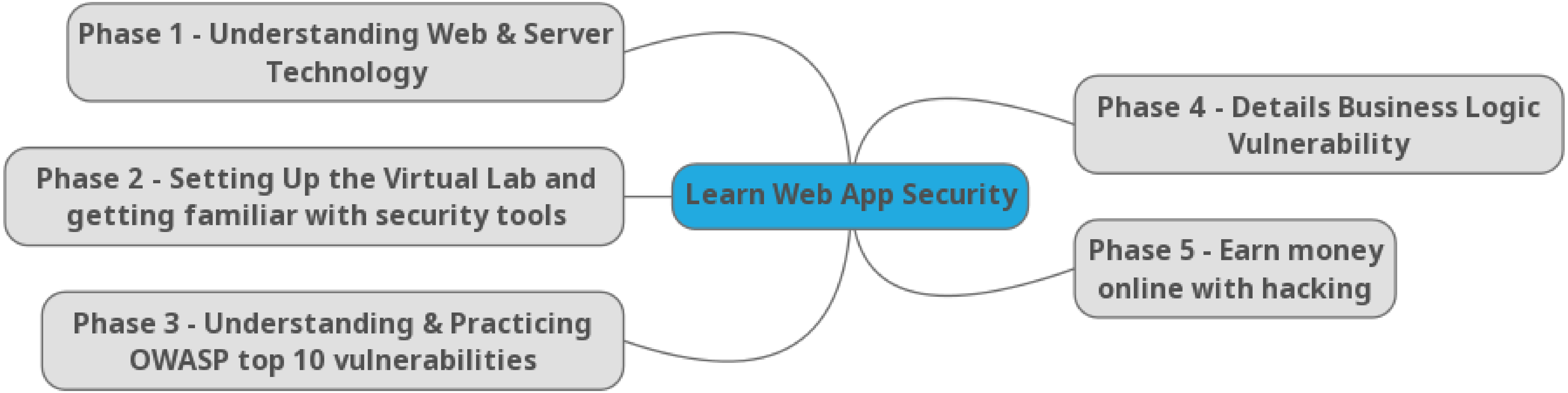


Automated Security Testing Using OWASP ZAP

http://www.swtestacademy.com/automated-security-testing-using-zap/

Application Security Testing 101

Complete guide to become web application security crackerjack



Learn Web App Security

Phase 1 - Understanding Web & Server Technology

Phase 2 - Setting Up the Virtual Lab and getting familiar with security tools

Phase 3 - Understanding & Practicing OWASP top 10 vulnerabilities

Phase 4 - Details Business Logic Vulnerability

Phase 5 - Earn money online with hacking

Follow me...

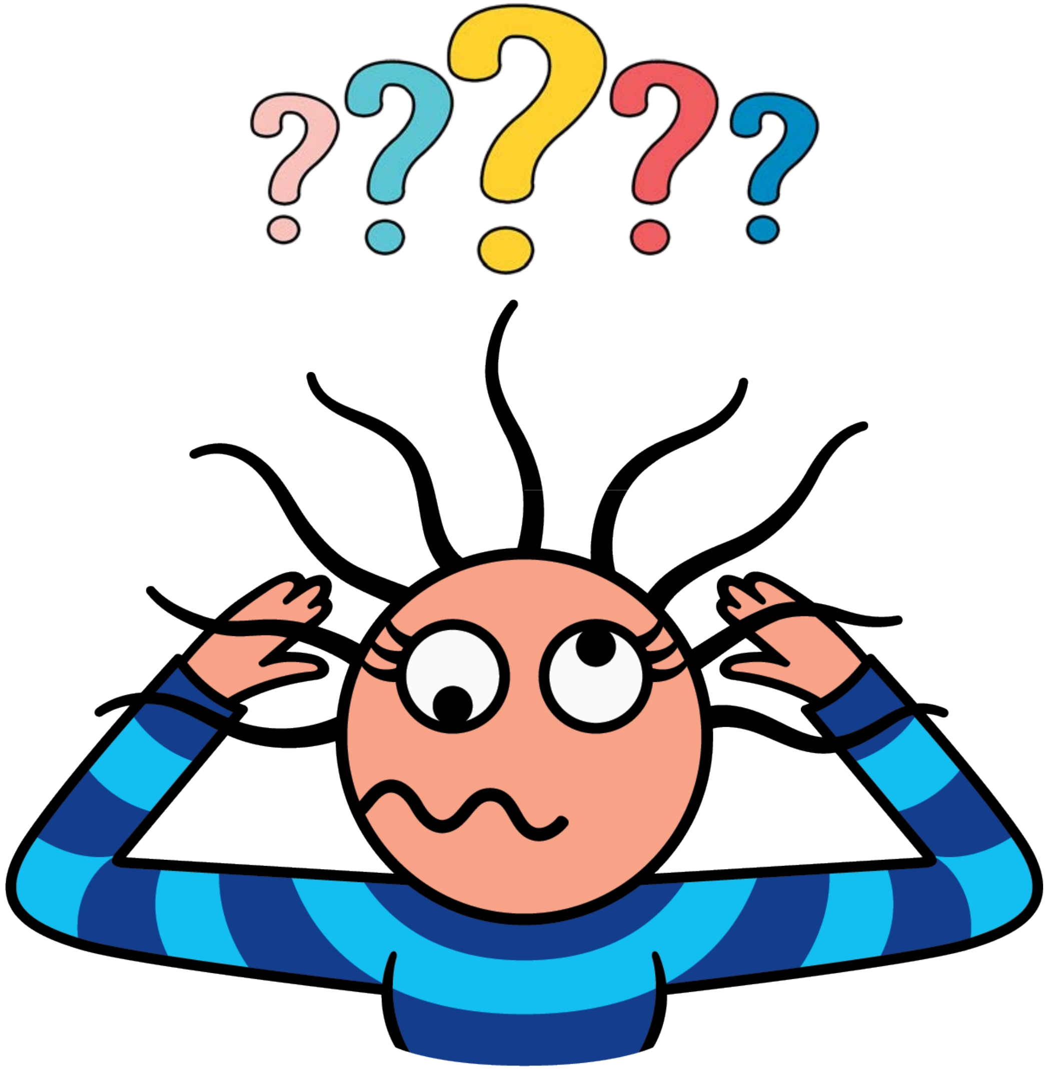
where I write and share

@iamthefrogy

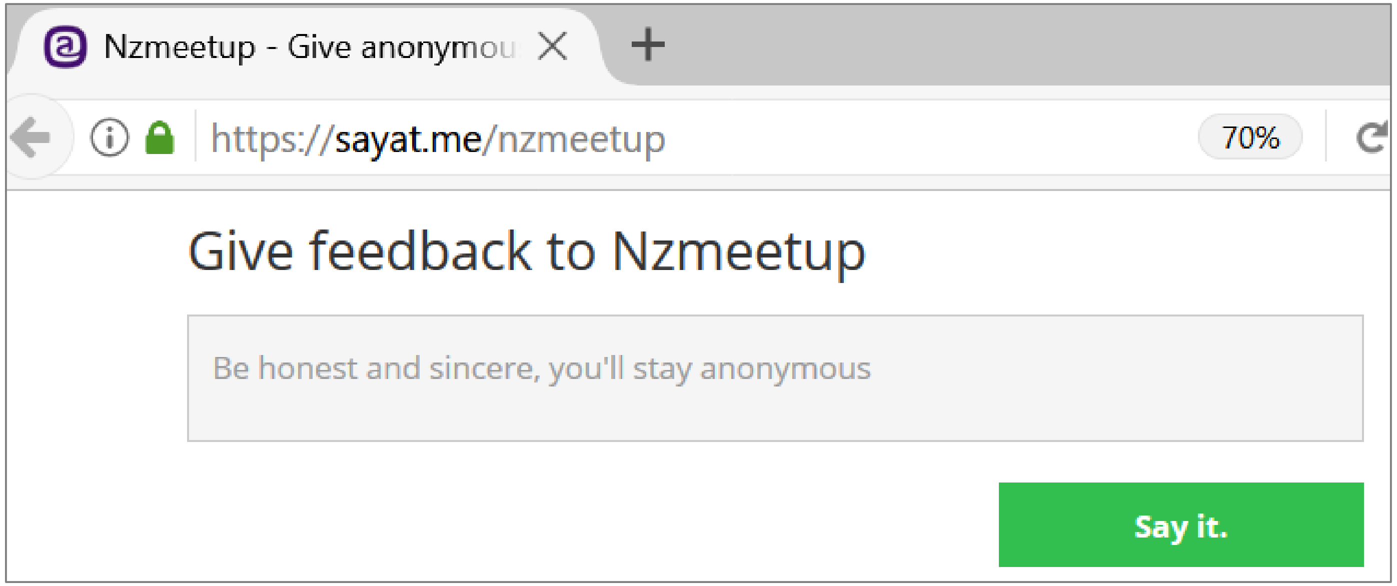
infosecninja.blogspot.com

chintan-gurjar-a6515648

github.com/iamthefrogy



Questions!!



https://sayat.me/nzmeetup

Give feedback to Nzmeetup

Be honest and sincere, you'll stay anonymous

Say it.

Anonymous Feedback Please…

Thanks & Cheers!

Special Thanks to **June Xu** for this picture ☺