

esentire[®]

What to Expect From a Penetration Test

CodeMash 2016



Introductions

esentire®

- » Chris Maddalena, OSCP
 - » @cmaddalena - [IRC](#), [GitHub](#), [Twitter](#)
 - » Information Security Consultant
 - » Penetration testing
 - » Phishing
 - » Security training
 - » Co-host of the PVCSec podcast
 - » #missec!

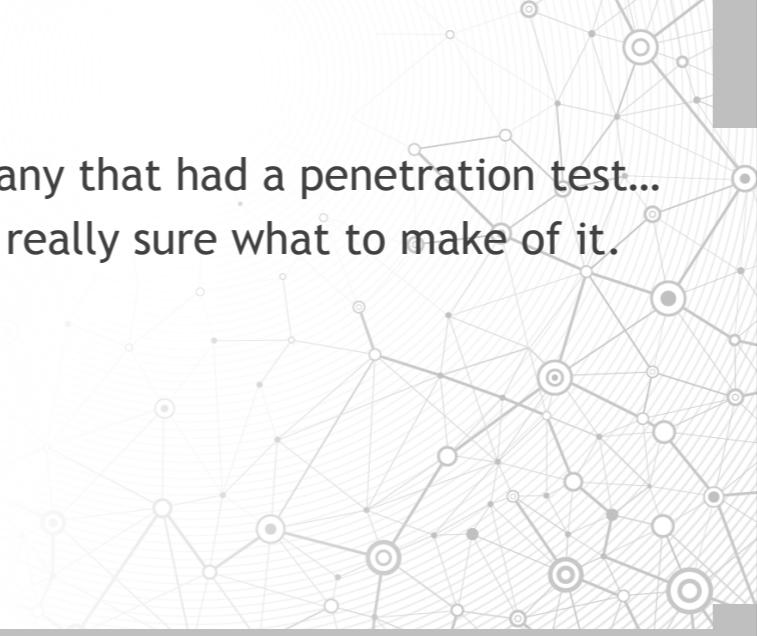


2

Brief Storytime

esentire®

There once was a company that had a penetration test...
...and no one was really sure what to make of it.

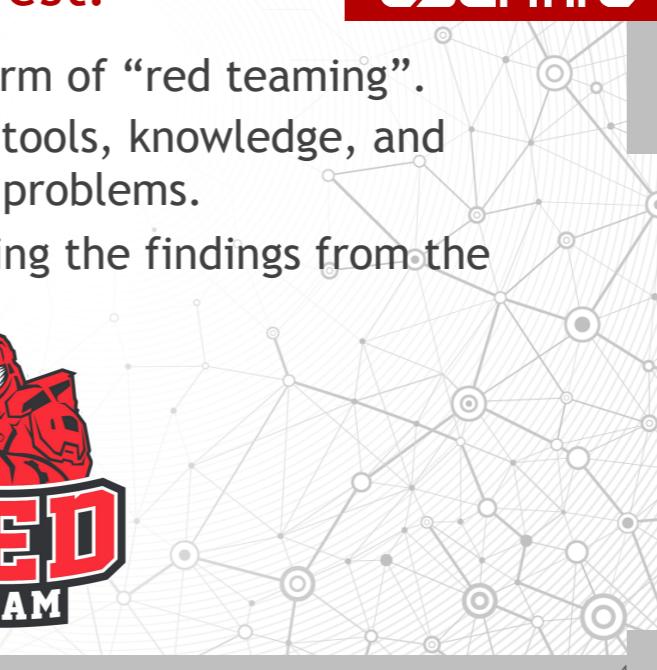


3

What is a Penetration Test?

esentire[®]

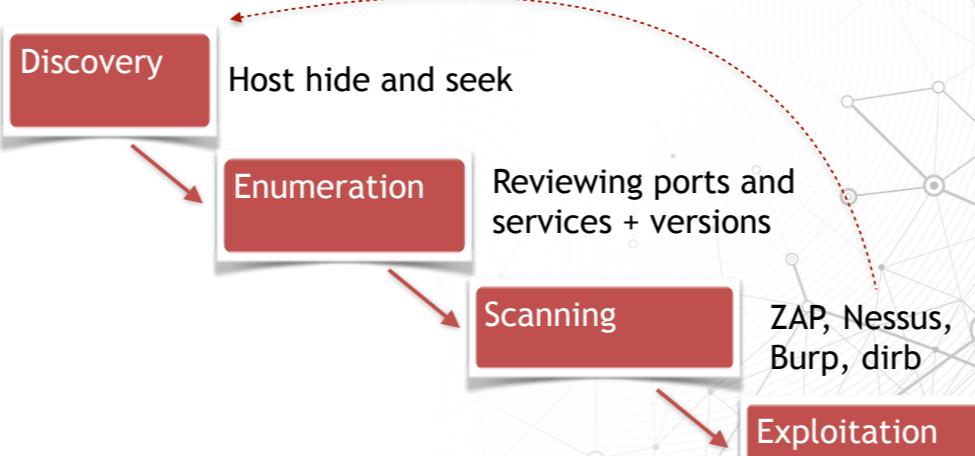
- » Penetration tests are one form of “red teaming”.
- » Security professionals using tools, knowledge, and creativity to try to discover problems.
- » The result is a report detailing the findings from the perspective of an attacker.



4

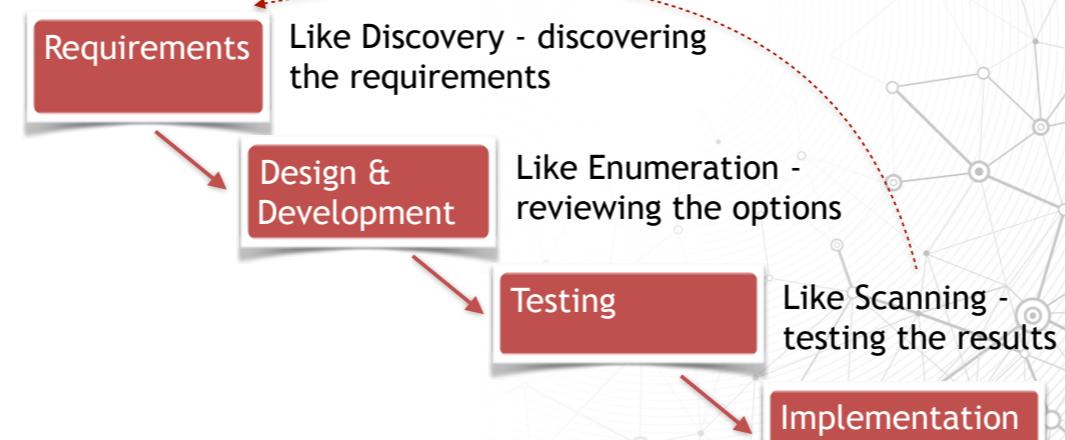
An Attacker's Methodology

esentire®



Similar to SDLC

esentire®



6

The SDLC is similar to the attacker's methodology

Both pen testers and QA testers are going to put the app through its paces

The end goal is just different

The Attacker's Toolbox

esentire®

- » Kali Linux's suite of tools
- » Vulnerability Scanners (OpenVAS, Nessus, NexPose)
- » Proxies (Burp, ZAP)
- » Scanners (nmap, sqlmap)
- » Recon tools (Google, Shodan)
- » And much more



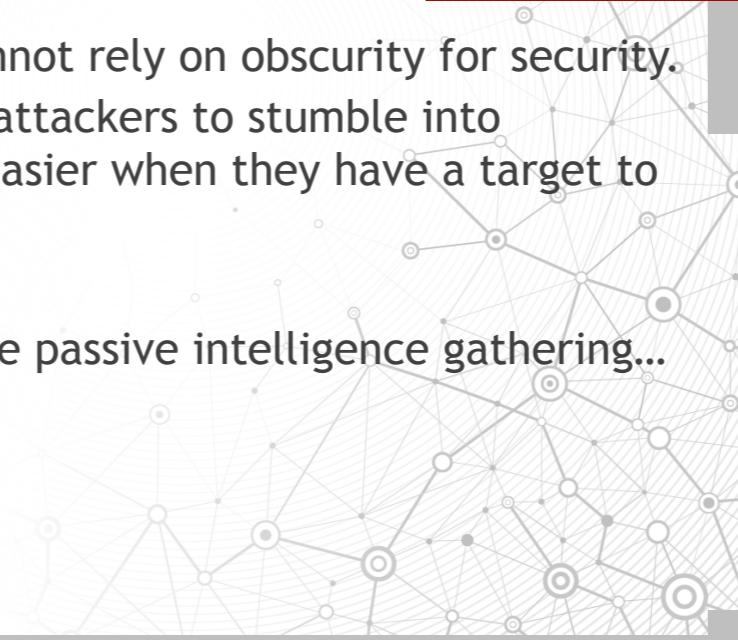
7

Kali comes with many of the popular tools pre-installed and ready to be used

Discovering Passive OSINT

esentire®

- » A big reason why we cannot rely on obscurity for security.
- » OSINT tools can enable attackers to stumble into opportunities, and it's easier when they have a target to narrow it down.
- » Let's take a look at some passive intelligence gathering...

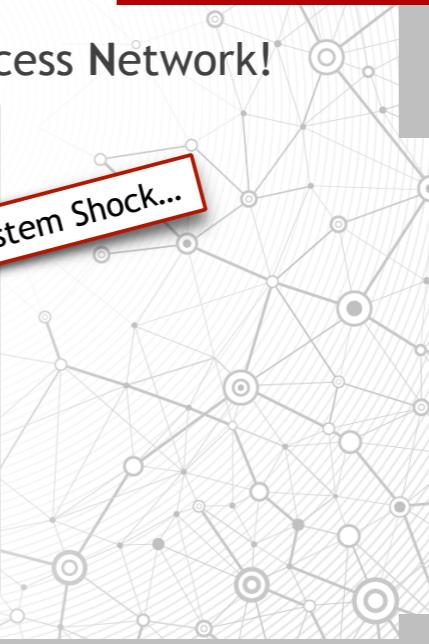


8

Introducing SHODAN

esentire®

- » The Sentient Hyper Optimized Data Access Network!



9

Introducing Shodan.io

esentire®

But this Shodan is pretty cool anyway.

The search engine for Refrigerators

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

Create a Free Account

Getting Started

- » A search engine for the *Internet of Things*.
 - » Reveals services rather than webpages.
 - » Free, with a subscription option...
 - » ...which was just \$5 on Black Friday.

10

Shodan is a search engine for the INTERNET OF THINGS

What that really means is it's designed to show you services, not webpages.

Shodan Delivers Domains

esentire®

Exploits Maps Download Results Create Report

TOP COUNTRIES

Country	Count
France	729
United States	652
Netherlands	216
Ireland	144
China	6

TOP SERVICES

Service	Count
HTTPS	700
HTTP	297
SMTP	179
POP3	104
SMTP + SSL	82

Showing results 1 - 10 of 1,764

205.251.242.55

Amazon.com
Added on 2015-12-06 23:58:11 GMT
United States, Seattle
[Details](#)

SSL Certificate
Issued By:
- Common Name: Symantec Class 3
Secure Server CA - G4
- Organization: Symantec Corporation
Issued To:
- Common Name: www.amazon.com
- Organization: Amazon.com, Inc.

HTTP/1.1 200 OK
Server: Server
Date: Sun, 06 Dec 2015 23:58:04 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: skin=moskin; path=/; domain=.amazon.com
pragma: no-cache
x-amz-id-1: H4K21EM08ZPBT56ABCH
p3p: policyref="https://www.am...

Error Processing Request
178.236.7.229
Amazon Data Services Ireland
Added on 2015-12-06 23:57:05 GMT
Ireland
[Details](#)

SSL Certificate
Issued By:
- Common Name: VeriSign Class 3
Secure Server CA - G3
- Organization: VeriSign, Inc.

HTTP/1.1 400 Bad Request
Date: Sun, 06 Dec 2015 23:56:52 GMT
Server: Server
x-amz-id-1: 11BRFQH93MRNQZREQHJ
x-amz-id-2: sp-audible-eu-1b-i-bea2fc5a.eu-west-1.amazon.com

11

You can search for domains, like amazon.com.

Shodan Delivers Webcams

The screenshot shows the Shodan search interface with the query "Server: SQ-WEBCAM". The results page displays various statistics and specific device details.

TOP COUNTRIES:

Country	Count
United States	50
Hungary	47
Italy	36
Germany	34
Poland	32

TOP SERVICES:

Service	Count
HTTP	262
HTTP (800)	57
HTTP (81)	33
HTTP (82)	19
Qoonn	5

TOP ORGANIZATIONS:

Organization	Count
Deutsche Telekom AG	17
UPC Hungary	16
TEO LT, AB	12
Telecom Italia	8
Magyar Telekom plc.	8

TOP PRODUCTS:

Product	Count
dvr1614n web-cam httpd	395

Device Details:

- 81.198.173.180**
Kopideja
Added on 2015-12-06 19:39:47 GMT
Latvia, Tukums
Details
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
Content-Length:434
- 77.255.214.114**
77.255.214.114.adsl.inetia.pl
Netis 8200
Added on 2015-12-06 18:55:19 GMT
Poland
Details
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
Content-Length:2935
- 151.74.102.100**
WIND Telecomunicazioni S.p.A
77.255.214.114.adsl.inetia.pl
Italy, Catania
Details
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
Content-Length:2936
- 151.26.84.206**
pop79-94.26-151.wind.it
Infostrada Uninet
Added on 2015-12-06 17:17:22 GMT
Italy, Modugno
Details
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
Content-Length:2936

A large network graph visualization on the right side of the page shows a complex web of connections between various IP addresses and nodes, representing the scale of the search results.

But where Shodan really signs is here, searching for products and services.

Yep, Those Are Webcams

esentire®



<https://www.shodan.io/host/213.168.188.38>

13

If you make something available externally, Shodan will find it.

Black Hat Shodan

esentire®

23

tcp

telnet

Connection refused: too many users

Black Hat Shodan

esentire®

The screenshot shows a Shodan search result for a MongoDB server. At the top, it displays '80.0 MB' in a green box and '3 Databases' in a blue box. Below this, there's a table with columns for 'Database Name'. The first row shows 'DELETED_BECAUSE_YOU_DIDNT_PASSWORD_PROTECT_YOUR_MONGODB' with a red arrow pointing from the text 'One of the ~35,000 MongoDB' below it. The second row shows 'admin' and the third row shows 'db'. To the right of the table, there's a 'MongoDB Server Information' section with some JSON-like code. At the bottom, the URL 'https://www.shodan.io/host/104.131.18.0' is shown.

One of the ~35,000 MongoDB

MongoDB Server Information

```
{  
    "metrics": {  
        "getLastError": {  
            "wtime": {  
                "num": 0,  
                "totalMillis": 0  
            },  
            "wtimeouts": 0  
        },  
        "storage": {  
            "freelist": {  
                "1": 1  
            },  
            "search": {  
                "1": 1  
            }  
        }  
    }  
}
```

https://www.shodan.io/host/104.131.18.0

This is where it gets nasty.

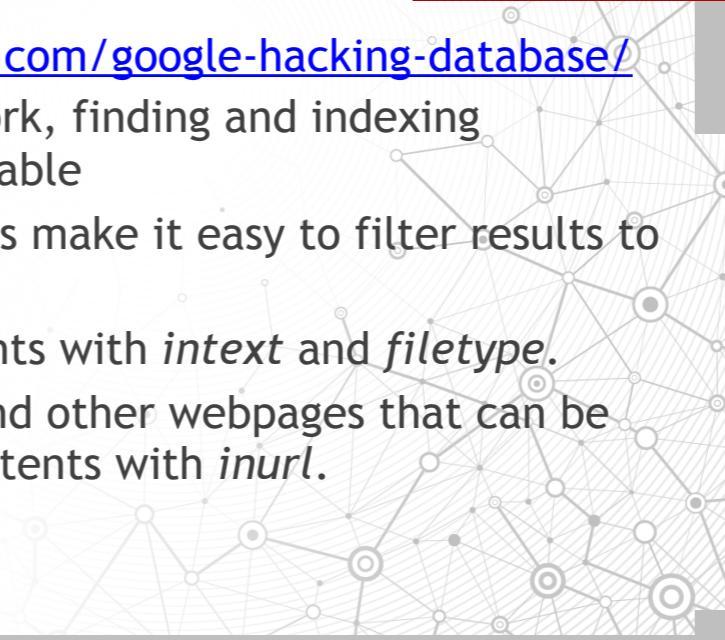
Latest news regarding the 35,000+ of open MongoDB DBs with 684.8TB

<http://www.csoonline.com/article/3016067/security/over-650-terabytes-of-data-up-for-grabs-due-to-publicly-exposed-mongodb-databases.html>

Introducing Google Hacking

esentire®

- » <https://www.exploit-db.com/google-hacking-database/>
- » Google does the hard work, finding and indexing everything publicly available
- » Google's search keywords make it easy to filter results to find:
 - » Files and their contents with *intext* and *filetype*.
 - » Webcams, routers, and other webpages that can be found by the URL contents with *inurl*.



16

Googling for Passwords, For Real

esentire®

A screenshot of a Google search results page. The search query is "intext:password filetype:xls". The results are filtered to show only web pages (Web). There are approximately 24,700 results found in 0.37 seconds. A specific result is highlighted, showing a portion of an Excel spreadsheet titled "Sheet1 - Network%20config.xls". The visible data includes:

	Network%20config.xls
18,	Router Password , @905012370W.
19,	DHCP Server Scope, 192.168.1.101-151.
20,	Remote Access IP & Port, [REDACTED]:1080.
	21. 22, Apple Wireless ...

You Don't Always Need an API



- » You can learn a lot from an organization without turning to anything like Shodan.
 - » *whois*
 - » *theharvester*
 - » Have I Been Pwned

Domain Name: CHRISMADDALENA.COM
Registry Domain ID: 1590194265_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2015-07-29T23:49:22Z
Creation Date: 2010-03-25T20:56:52Z
Registrar Registration Expiration Date: 2016-03-25T20:56:52Z
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Reseller: Hover

Moving on to Active Scanning



- » Once you find something of interest, the next step is to take action with active investigation techniques and tools.

```
kali# wpscan www.chrismaddalena.com
[WPSCAN] [!] WPSCAN v2.8 - WordPress Security Scanner
[WPSCAN] [!] Sponsored by Sucuri - https://Sucuri.net
[WPSCAN] [!] @_WPScan_, @_ethicalhack3r, @erwan_lr, pvdL, @_FireFart_
[WPSCAN] [!] It seems like you have not updated the database for some time.
[WPSCAN] [?] Do you want to update [2] [Y/N] [1] [N] [0] [INFO]
[WPSCAN] [!] Updating the Database
[WPSCAN] [!] Parameter: username (POST)
[WPSCAN] [!] Type: AND/OR time-based blind
[WPSCAN] [!] Title: MySQL > 5.0.11 AND time-based blind (SELECT)
[WPSCAN] [!] Payload: username='wrong' AND (SELECT * FROM (SELECT(SLEEP(5)))Cgms) AND 'sWoY='sWoY&password=wrong&submit=Log In'
[WPSCAN] [!] Started: Wed Dec 30 21:22:28 2015 [INFO]
[WPSCAN] [!] Back-end DBMS is MySQL
[WPSCAN] [!] web server operating system: Linux CentOS 5.10
[WPSCAN] [!] web application technology: Apache 2.2.3, PHP 5.1.6
[WPSCAN] [!] back-end DBMS: MySQL 5.6.11
```

Kali, theharvester, wpscan, and Nikto

DEMO TIME



20

Common Findings: OWASP Top 10



» Often discovered during penetration tests...



Common Findings



- » The OWASP Top 10 are penetration tester favorites.
- » They are also often targeted for sport and potential profit.
- » They can appear over time as new issues are discovered in aging versions of platforms and CMSs.
- » Bug bounty hunters enjoy the \$\$\$ rewards.
- » Others may simply enjoy finding the problems for mischief.



Why This Matters

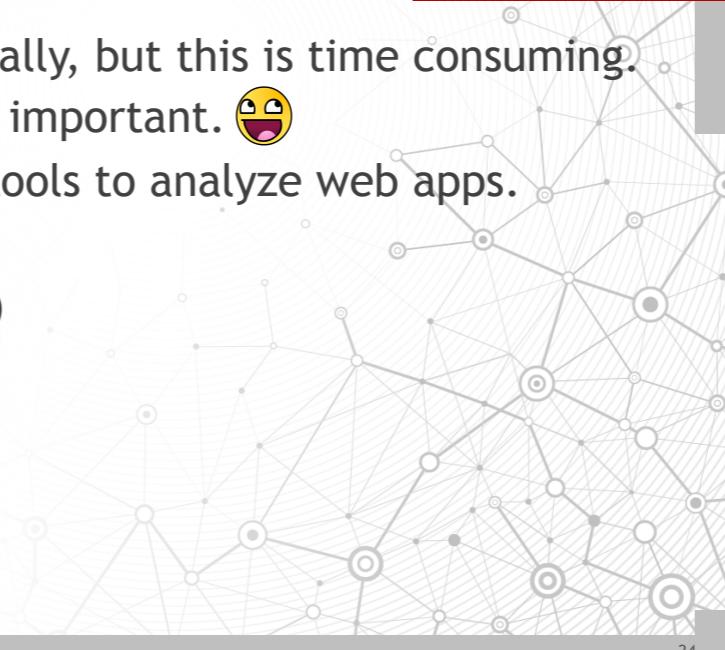


- » It can provide a foothold or access to data.
- » Possible outcomes to a web app's compromise during a test:
 - » Manipulation of the app. (ex: Auth Bypass, SQLi)
 - » Access to the server running the app, and the server's data and files. (ex: LFI)
 - » Control of the server running the app. (ex: RFI)
- » Malicious outcomes to a compromise:
 - » Compromise of the app's users. (ex: XSS)
 - » Destruction or manipulation of the app's data.

Finding These Vulnerabilities



- » They can be found manually, but this is time consuming.
 - » Manual testing is still important. 😊
- » Penetration testers use tools to analyze web apps.
 - » Acunetix (\$\$)
 - » Burp Suite (Free or \$)
 - » OWASP ZAP (Free)

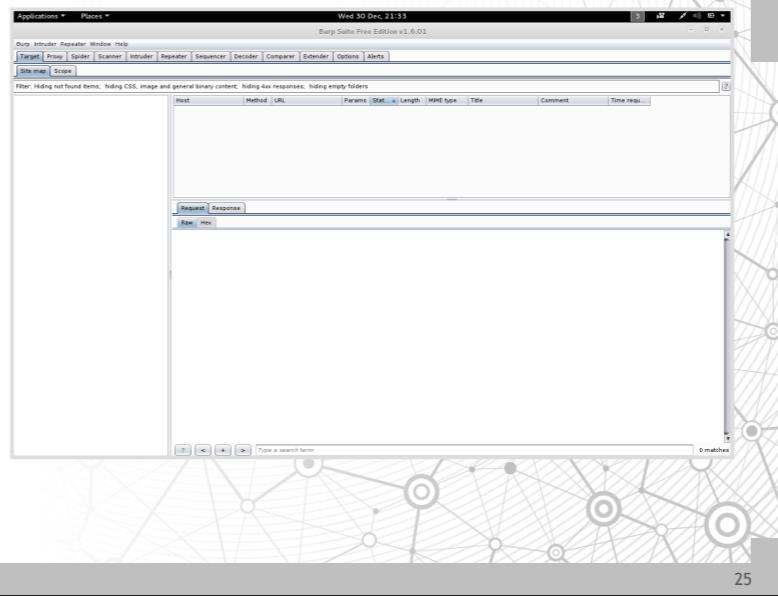


24

Burp (Excuse me) Proxy

esentire®

- » Free to use, only slightly limited.
- » Full license is \$300/year.
- » It can spider, capture GET/POST, brute force, repeat requests, and more.



25

Burp Proxy in Action

esentire®

- » Burp can do a LOT, but the proxy is fantastic.
- » You can capture and review requests!

The screenshot shows the Burp Proxy interface. On the left, the 'Request' pane displays a POST request to '/demo1' with various headers and a body containing the line 'year=res.write('SSJS Injection')'. On the right, the 'Response' pane shows the server's response with the status 'HTTP/1.1 200 OK' and the content 'SSJS Injection'.

```
POST /demo1 HTTP/1.1
Host: [REDACTED]:3000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 32

year=res.write('SSJS Injection')
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Date: Thu, 05 Feb 2015 17:41:53 GMT
Connection: keep-alive
Content-Length: 14

SSJS Injection
```

- » Here is a Server Side JavaScript exploit example.

Example from [s1gnalcha0s](#) on GitHub

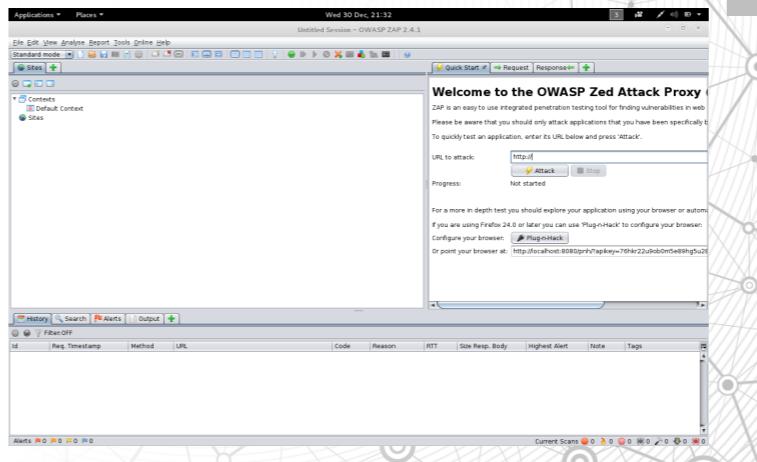
26

Server Side JavaScript Injection against Node.js example

ZAP (Zed Attack Proxy)

- » Totally free!
- » As easy as entering a URL to get started.
- » Runs through a whole battery of tests to find low hanging fruit.
- » Simple to run during the testing phase, while at lunch, whenever.

esentire®



Burp, SQLMap, and OWASP ZAP

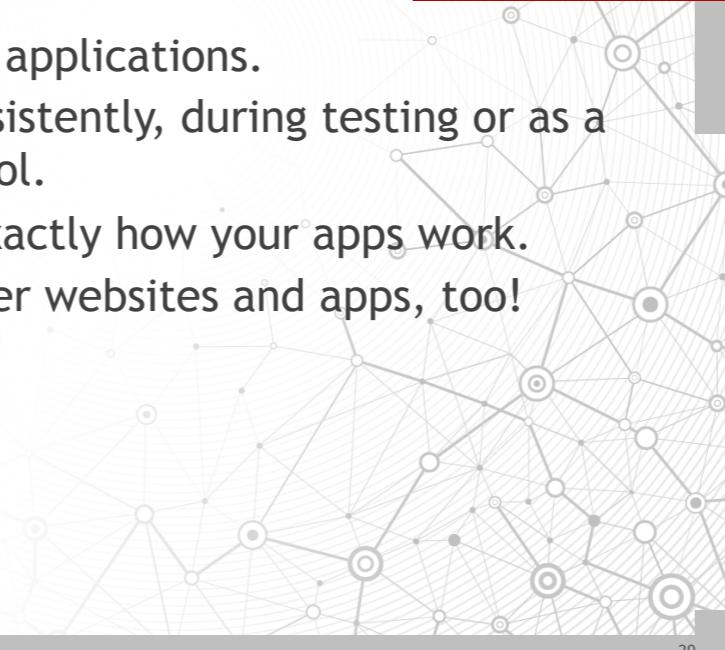
DEMO TIME



Applying This Information



- » Try out ZAP on your own applications.
 - » Consider using it consistently, during testing or as a semi-regular audit tool.
 - » Give Burp a try to see exactly how your apps work.
 - » You can use it on other websites and apps, too!
 - » Be curious and learn.

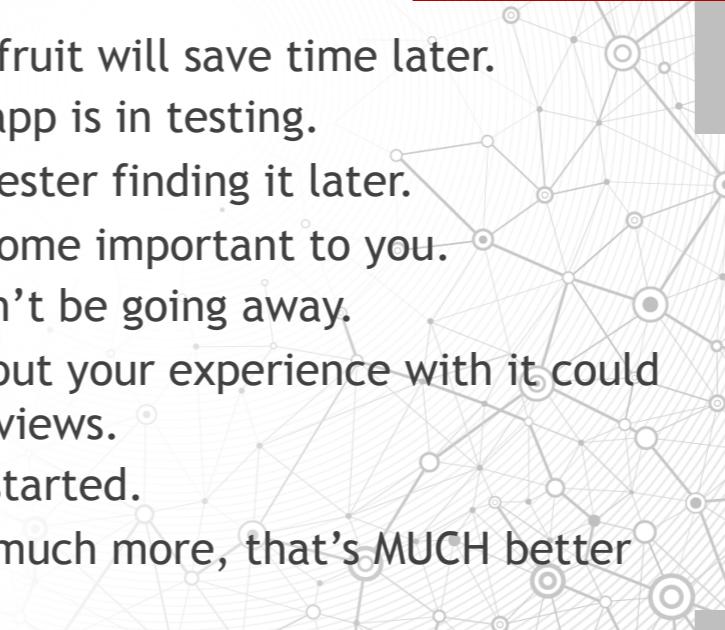


29

But Why?

esentire®

- » Finding the low hanging fruit will save time later.
 - » Fix it now while the app is in testing.
 - » Avoid a penetration tester finding it later.
- » ZAP experience may become important to you.
 - » Web app security won't be going away.
 - » Being able to talk about your experience with it could be beneficial in interviews.
- » It's really simple to get started.
 - » Even if you don't do much more, that's MUCH better than nothing.



30

Learning Resources

esentire®

- » Local security groups and conferences
 - » #misen
 - » #ohsec
 - » BSides - Great one day conferences.
 - » BSides Indy (March), BSides Cleveland (June),
BSides Detroit (July)
 - » CONverge (Detroit, July)
 - » CircleCityCon (Indy, June)
 - » Web Application Hacker's Handbook
 - » Bug Hunter's Methodology



31

Final Thoughts & Questions

» Questions?

esentire®



32

esentire®

Thank You!

Chris Maddalena
@cmaddalena

