AppSec & OWASP Top 10 Primer

AppSec

& OWASP Top 10

March 21, 2019

Matt Scheurer

@c3rkah

Slides:

https://www.slideshare.net/cerkah

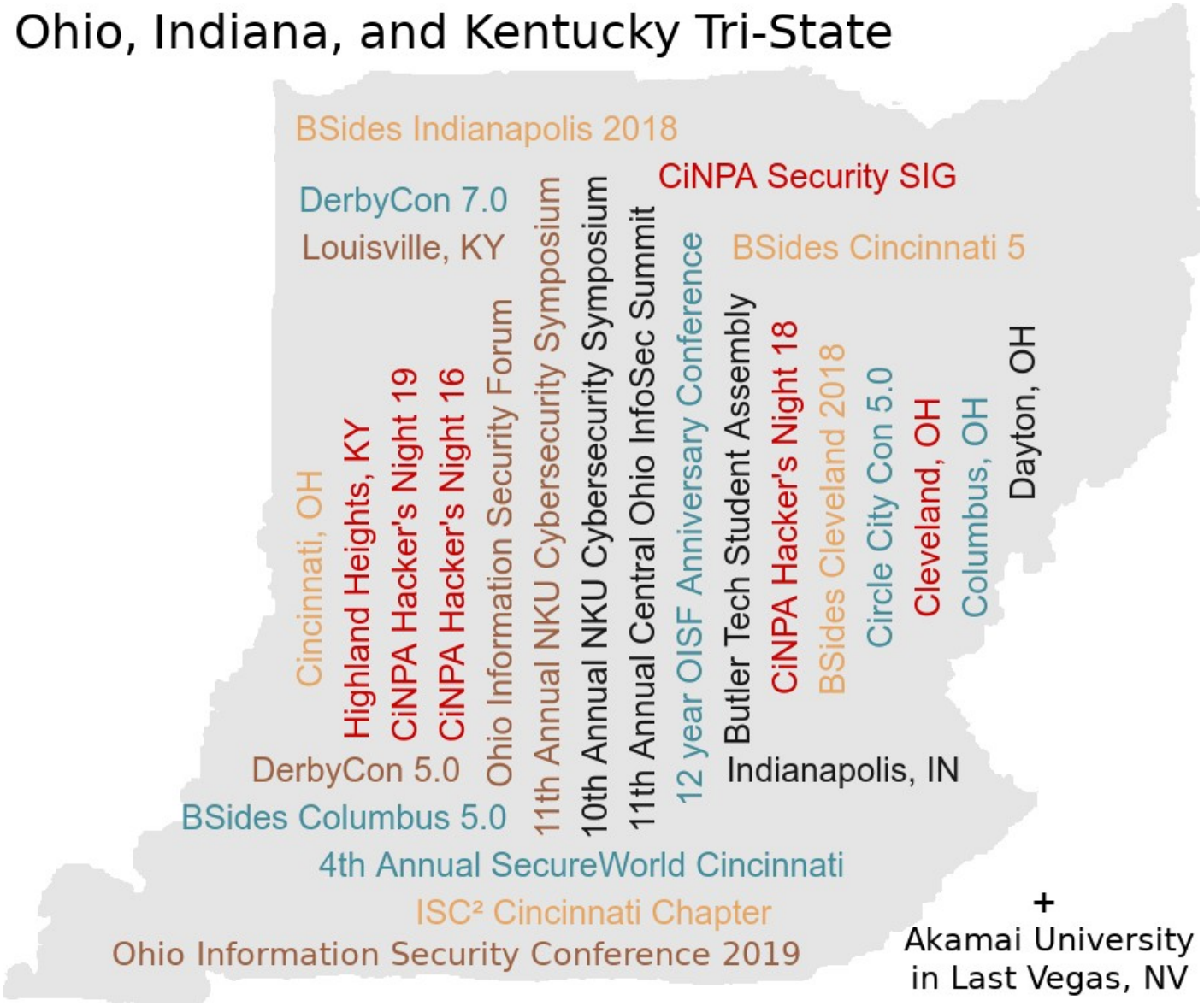
MOMENTUM

presented by The Circuit

About Me...

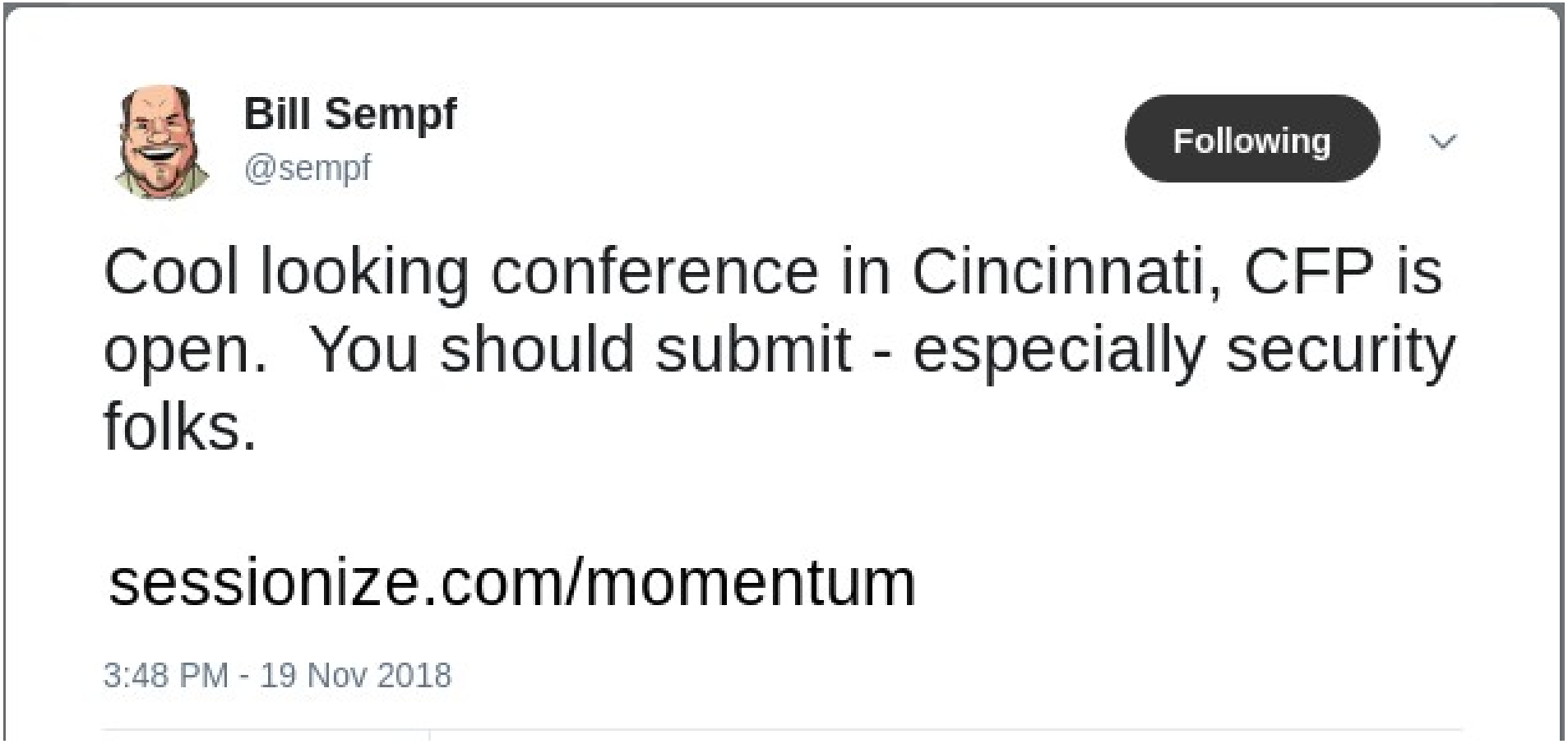
- Sr. Systems Security Engineer in the Financial Services Industry
- Frequent speaker at Information Security / Hacker conferences
- Teacher at heart!
- Chair of the

Places where I have presented...

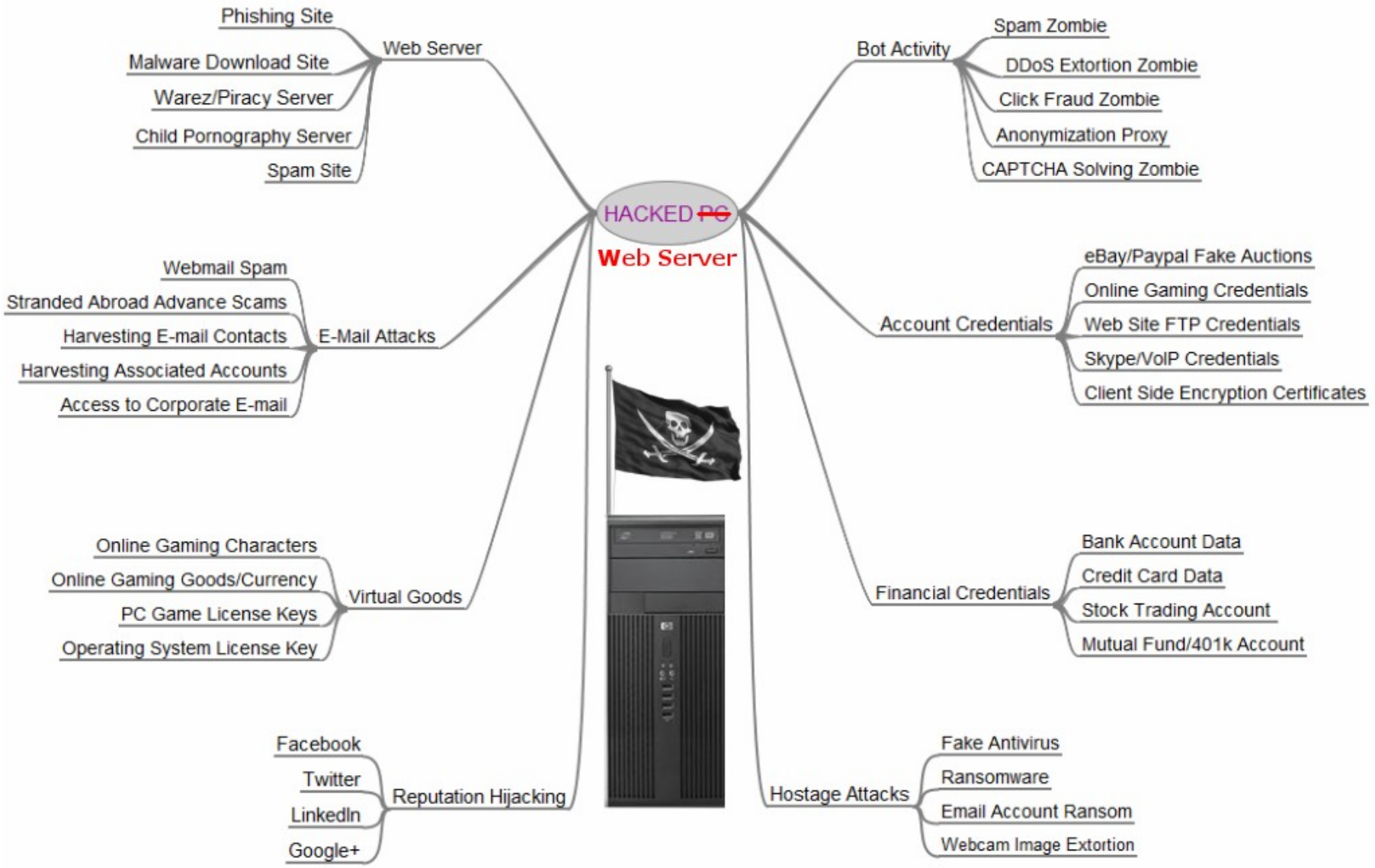


Why am I speaking at a Dev Con?

It all started with a tweet…



Why AppSec?



https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

What is OWASP?

The Open Web Application Security Project (OWASP), an online community, produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

- Web site - https://www.owasp.org/

OWASP

Open Web Application Security Project

OWASP History

- Started in December, 2001
- Obtained 501c3 (non-profit) Status in April 2004
- OWASP Top Ten List
  - The "Top Ten", first published in 2003, is regularly updated. It aims to raise awareness about application security by identifying some of the most critical risks facing organizations
- The OWASP foundation has produced many guides, projects, and publications, since their beginning

OWASP Top 10 List (2017)

- A1:2017-Injection
- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure
- A4:2017-XML External Entities (XXE)
- A5:2017-Broken Access Control
- A6:2017-Security Misconfiguration
- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization
- A9:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging&Monitoring

- **Current Version**
  - **https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project**
  - **https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf**

Recent OWASP Top 10 Changes

From 2013 to 2017...

- "**Cross-Site Scripting (XSS)**" Down from A3 to A7
- "**Insecure Direct Object References**" (A4) and "**Missing Function Level Access Control**" (A7)
  - Merged into "**Broken Access Control**" as A5
- "**Security Misconfiguration**" Down from A5 to A6
- "**Sensitive Data Exposure**" Up from A5 to A3
- "**Cross-Site Request Forgery (CSRF)**" Removed
- "**Unvalidated Redirects and Forwards**" Removed

Additions to the OWASP Top 10

From 2013 to 2017...

- A4:2017-XML External Entities (XXE)
- A8:2017-Insecure Deserialization
- A10:2017-Insufficient Logging & Monitoring

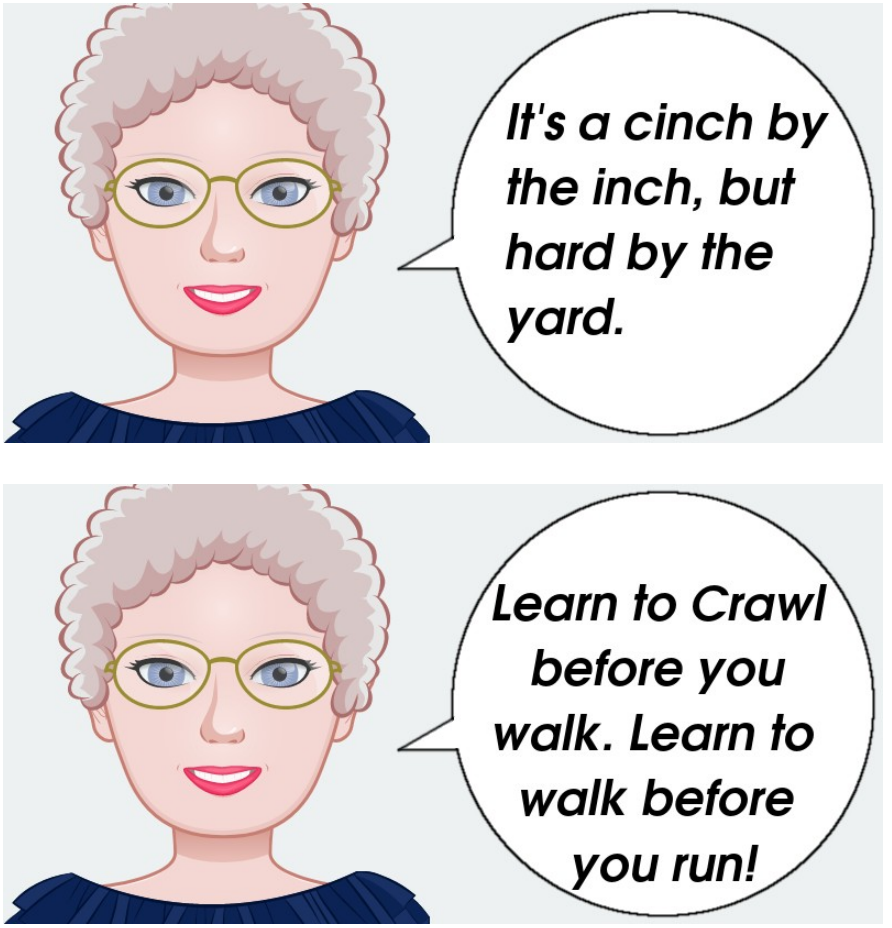
Where and How to Learn AppSec

- We will cover some basic resources to help get you started on a path towards self-learning...
  - Basic Vulnerability Scanners
  - AppSec Testing Platforms
  - Free places to learn AppDev
  - Free places to learn AppSec
  - Free Learning / Practice Platforms

NOTE: These are not exhaustive lists as there are many more resources available!

Starting Out...

- Advice my mother would offer about how to begin learning AppSec and testing web server, website and web application security...



Vulnerability Scanners

- Core Security: Core Impact
- Rapid7 products: Nexpose
- Tenable: Nessus
- Qualys: Web Application Scanning (WAS)
- Open Source: OpenVAS
- Open Source / Kali Linux: Sparta / Nikto

AppSec Testing Platforms

- Start with: OWASP ZAP (Zed Attack Proxy)
  - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- Move to: Fiddler - Free Web Debugging Proxy
  - https://www.telerik.com/fiddler
- Graduate to: Burp Suite Scanner
  - https://portswigger.net/burp
- Honorable Mention: Nmap w/ NSE Scripts
- Honorable Mention: Samurai Web Testing Framework

Free places to learn AppDev

- Codecademy
  - https://www.codecademy.com/
- Khan Academy
  - https://www.khanacademy.org/computing
- SQLCourse.com
  - http://www.sqlcourse.com/
- W3Schools
  - https://www.w3schools.com/

Free places to learn AppSec

- OWASP (Of course!)
  - https://www.owasp.org/
- Your nearest local OWASP Chapter
  - https://www.owasp.org/index.php/OWASP_Chapter
- YouTube
  - https://www.youtube.com/
- Cybrary
  - https://www.cybrary.it/course/web-application-pen-testing/
  - https://www.cybrary.it/course/ethical-hacking/
  - https://www.cybrary.it/course/advanced-penetration-testing/
  - https://www.cybrary.it/course/python/

Free Learning / Practice Platforms

- OWASP Mutillidae
  - https://www.owasp.org/index.php/OWASP_Mutillidae_2_Project
- OWASP WebGoat
  - https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
- OWASP Juice Shop
  - https://www.owasp.org/index.php/OWASP_Juice_Shop_Project
- Rapid7 Metasploitable
  - https://github.com/rapid7/metasploitable3
- PentesterLab
  - https://pentesterlab.com/exercises/

Troy Hunt Resources

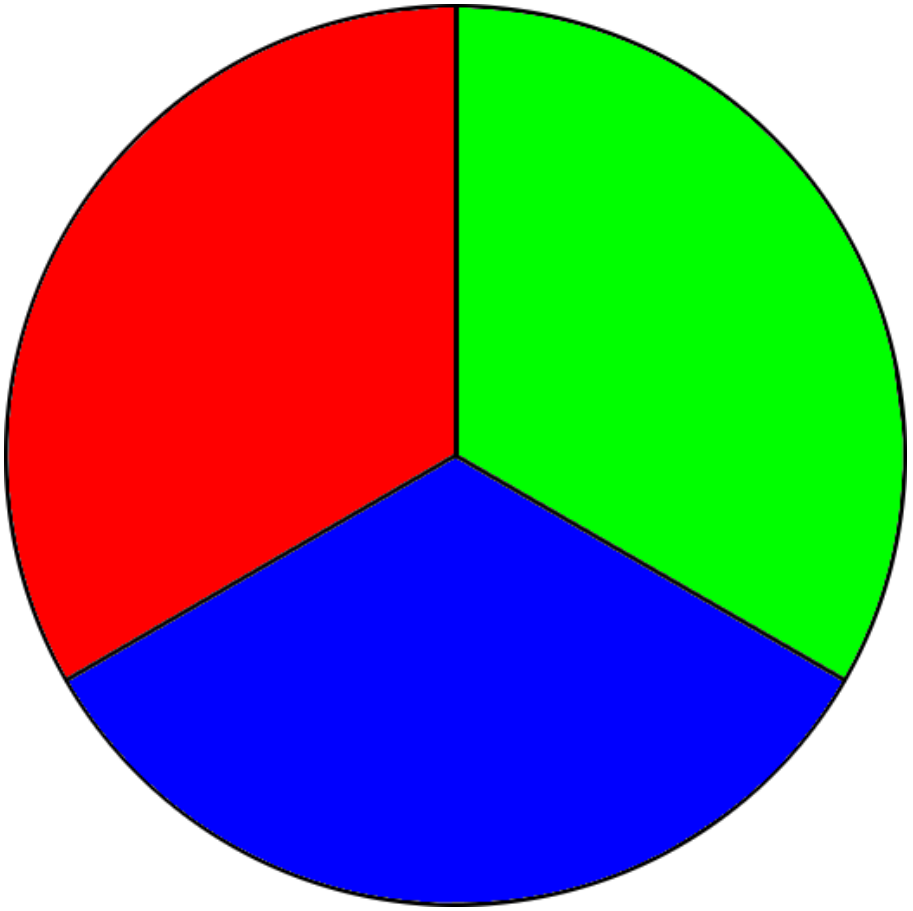
- Hack Yourself First
  - "Hack Yourself First" is all about developers building up cyber-offense skills and proactively seeking out security vulnerabilities in their own websites before an attacker does
  - There are 50 intentional very sloppy security practices to be found
  - http://hack-yourself-first.com/
- Free Accompanying Pluralsight Course
  - http://pluralsight.com/training/Courses/TableOfContents/hack-yourself-first

What about a WAF?

- A Web Application Firewall (WAF) filters, monitors, and blocks attack traffic to and from specific web applications.
  - Prevents attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations, etc.
- WAF's are good as a compensating control and a good defense-in-depth strategy, but...
  - Nobody should rely solely on a WAF for web app security
    - WAF bypasses are continuously being researched, published, and included in exploit kit updates
    - A WAF is not likely to stop all of the attacks

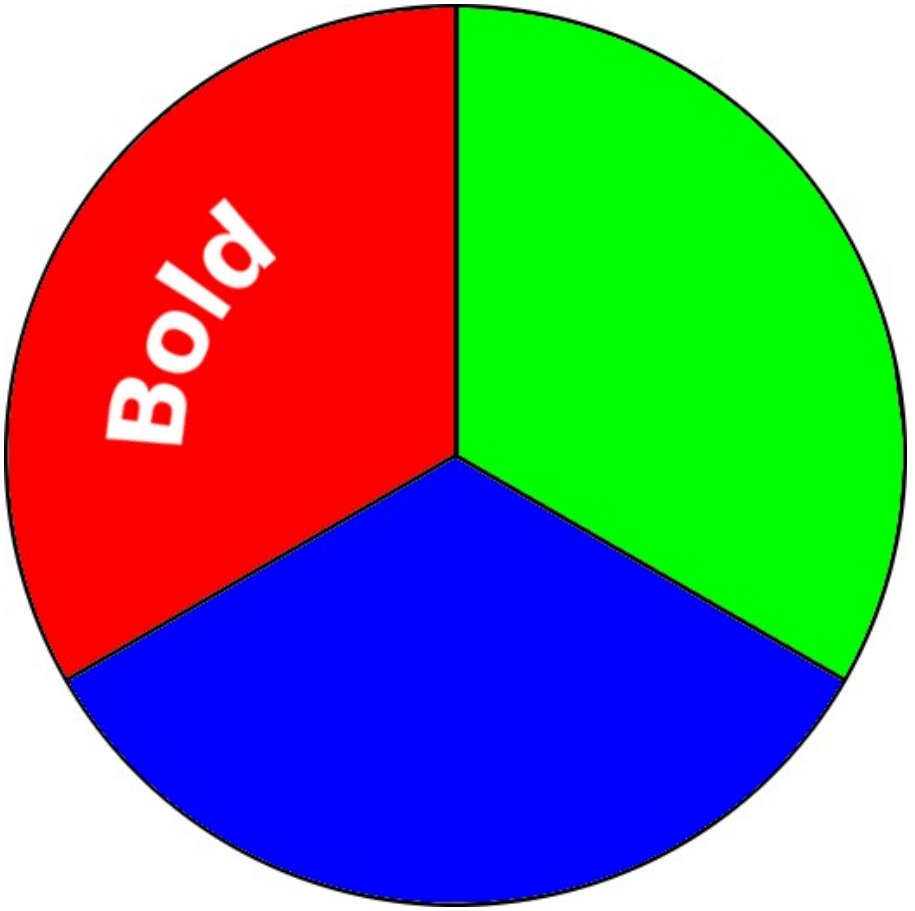
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



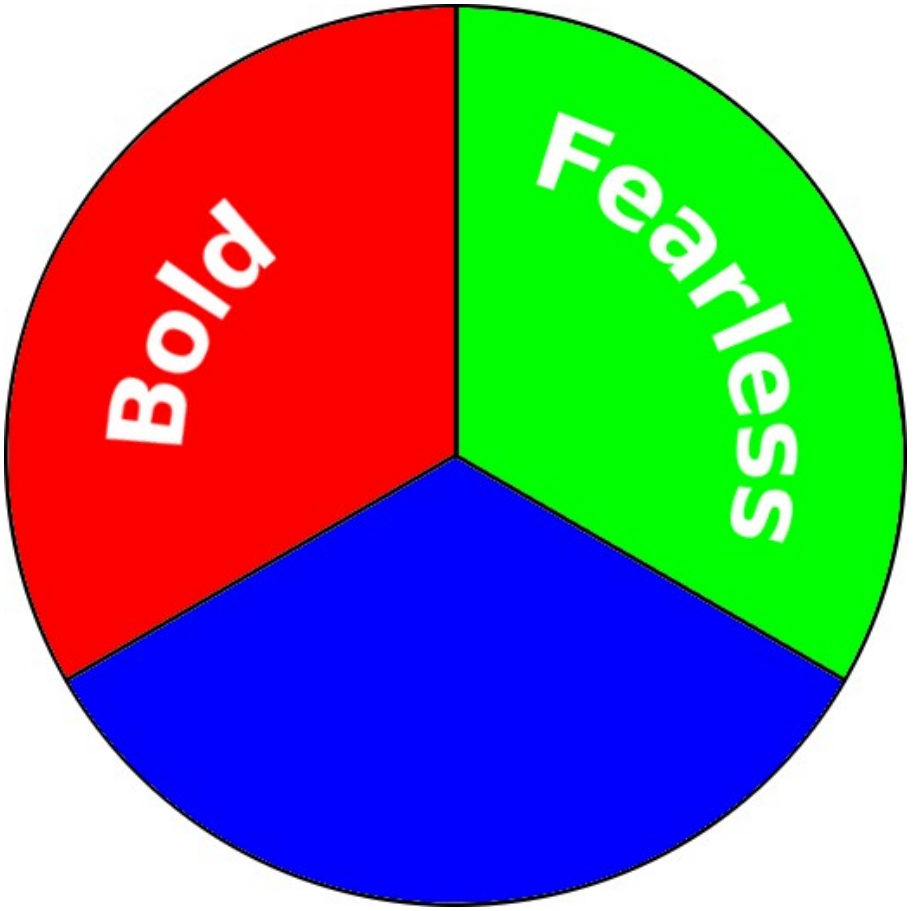
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



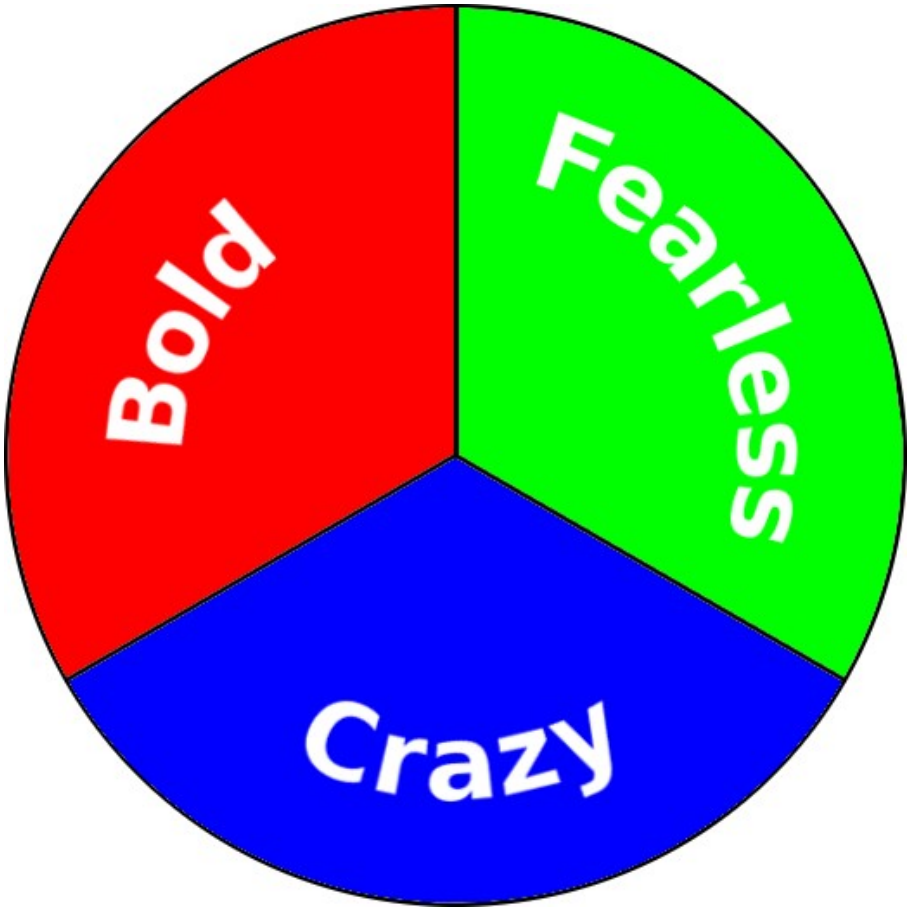
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



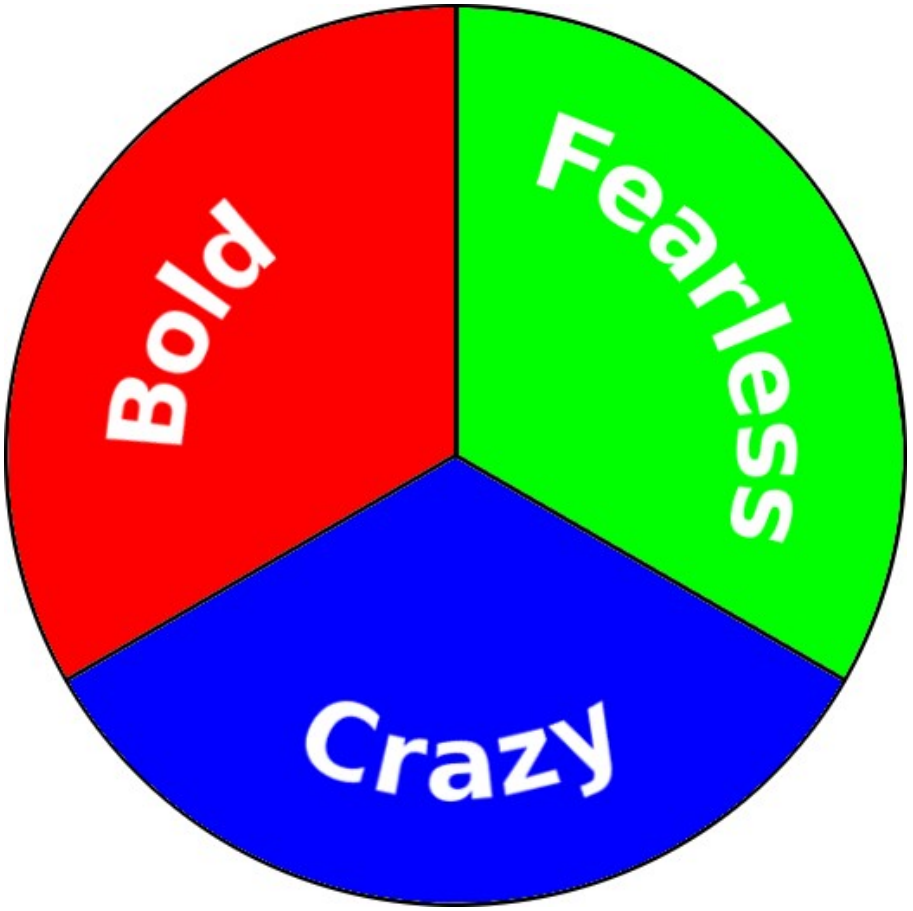
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



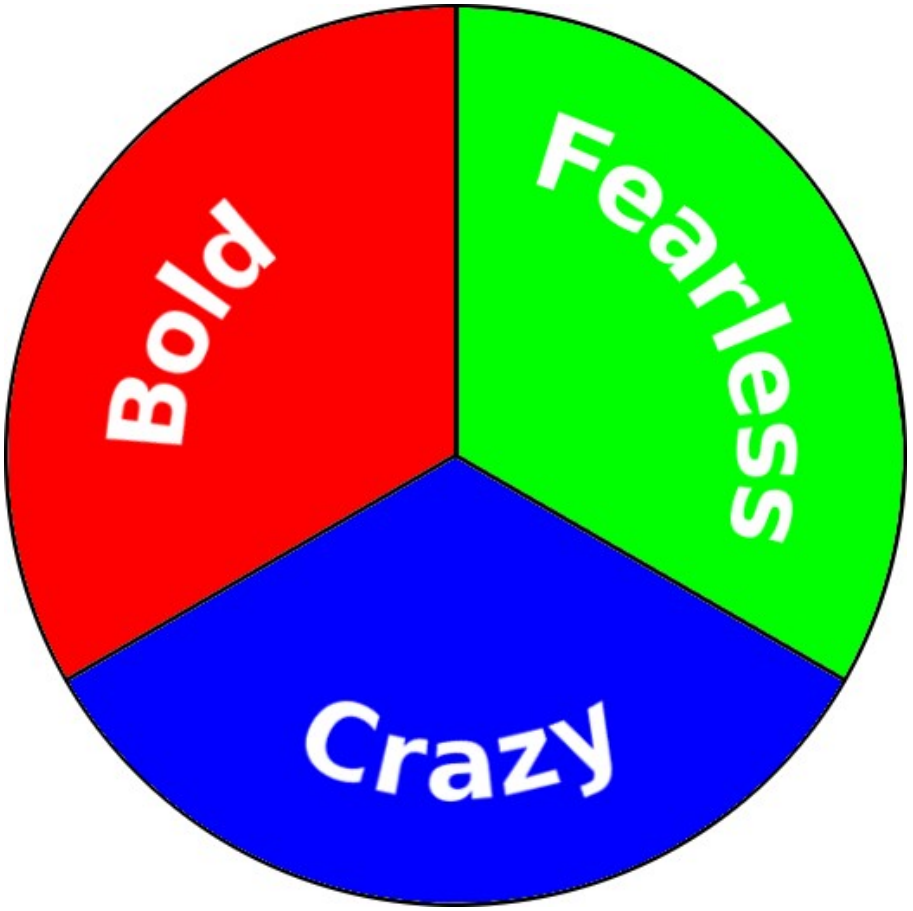
*** Live Demo Alert ***

Please pick 2…



*** Live Demo Alert ***

Please pick 2…
So I am not <u>just</u> **Crazy**!



Scanning Demo w/ Nikto!

- Nikto
  - Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.
  - https://cirt.net/Nikto2
- Nikto is available as a free download and is also included in Kali Linux

Accidental Exposure Demo w/ ZAP!

- OWASP ZAP
  - The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience including developers and functional testers who are new to penetration testing.
  - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- ZAP is available as a free download and is also included in Kali Linux

Conclusion

The need for AppSec practitioners is great…

- Because there's a whole lot of horrible out there!

Index of /public_html/idx_config

- Parent Directory
- [redacted]cpanel.txt
- [redacted]phpBB.txt

Apache Server at [redacted] *Port 80*

```
$acm_type = 'phpbb\\cache\\driver\\file';

@define('PHPBB_INSTALLED', true);
// @define('PHPBB_DISPLAY_LOAD_TIME', true);
// @define('DEBUG', true);
// @define('DEBUG_CONTAINER', true);
```

```
[client]
password="[redacted]"
user=[redacted]
```

```
<?php
// phpBB 3.1.x auto-generated configuration file
// Do not change anything in this file!
$dbms = 'phpbb\\db\\driver\\mysqli';
$dbhost = 'localhost';
$dbport = '';
$dbname = '[redacted]';
$dbuser = '[redacted]';
$dbpasswd = '[redacted]';
$table_prefix = '[redacted]_';
$phpbb_adm_relative_path = 'adm/';
$acm_type = 'phpbb\\cache\\driver\\file';

@define('PHPBB_INSTALLED', true);
// @define('PHPBB_DISPLAY_LOAD_TIME', true);
// @define('DEBUG', true);
// @define('DEBUG_CONTAINER', true);
```

Shout outs and thank you's...

- OWASP
  - https://www.owasp.org
- Cincinnati OWASP Chapter
  - https://www.owasp.org/index.php/Cincinnati
- Columbus OWASP Chapter
  - https://www.owasp.org/index.php/Columbus
- University of Cincinnati OWASP Chapter
  - https://www.cyberatuc.org/
  - https://www.youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Questions

Who ...

What ...

When ...

Where ...

Why ...

How ...

Thank you for attending!

AppSec

& OWASP Top 10

March 21, 2019

Matt Scheurer


@c3rkah

Slides:

https://www.slideshare.net/cerkah