PACIFIC NW SOFTWARE QUALITY CONFERENCE

Starting a Security Program on a Shoestring

BRIAN MYERS

OCTOBER 15, 2019

PNSQC™

Brian Myers, CISSP

Director, Information Security at WebMD Health Services

Five years in information security

Twenty-five years in software development

Borland, Netscape, Webridge, Softsource, Complí, WebMD

Goals

Gaining security knowledge

Managing application vulnerabilities

Empowering QA to learn and lead

Driving security into team processes

Creating a culture of security and quality

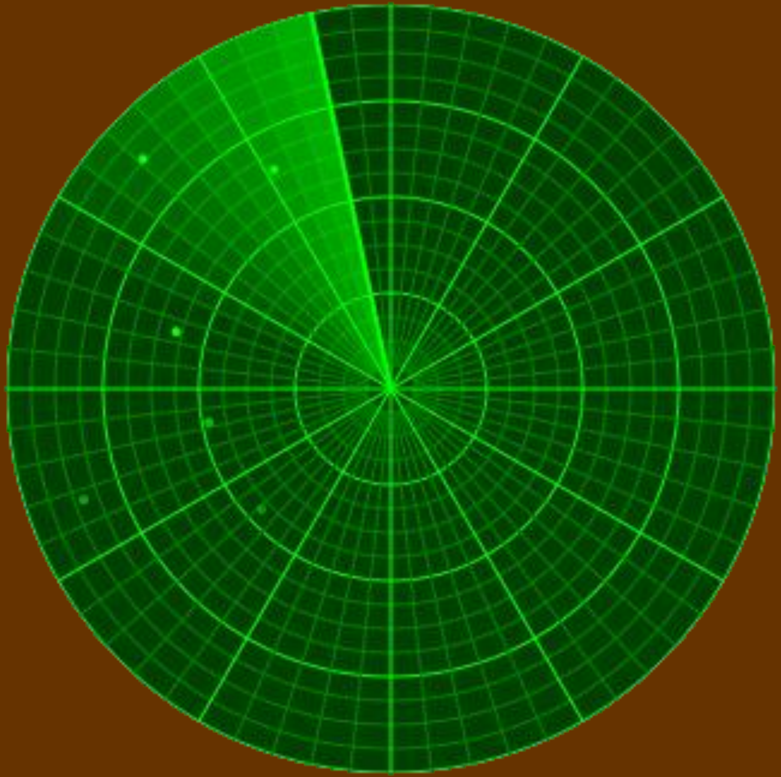
The Problem

- Small team
- Web application
- Desire to address security
- No resources
- Minimal security expertise

Two Approaches to the Problem

What is a Vulnerability Scanner?

Software that examines your product and identifies flaws or weaknesses that might let someone perform unwanted actions.



But what exactly does it look at?

Types of Vulnerability Scanners

Type	Target	Findings
Network	Infrastructure	Config and patching
Static (SAST)	Source code	Programming logic
Composition	Third-party libraries	Known vulnerabilities
Dynamic (DAST)	Running application	Flaws in web pages

Which Scanner Should I Choose?

Product	Free	Last Release	Active	General Purpose
Arachni	Yes	2017	No	Yes
Brakeman	Yes	2019	Yes	No
Grabber	Yes	2013	No	Yes
Grendel-Scan	Yes	2012	No	Yes
IronWasp	Yes	2015	No	Yes
OWASP ZAP	Yes	2019	Yes	Yes
RatProxy	Yes	2009	No	Yes
Scan My Server	Freemium	2019	Yes	Yes
Skipfish	Yes	2012	No	Yes
SQLMap	Yes	2019	Yes	No
Vega	Yes	2016	No	Yes
W3af	Yes	2019	Yes	Yes
Wapiti	Yes	2019	Yes	Yes
Watcher	Yes	2017	No	Yes
WATOBO	Yes	2017	No	Yes
WebScarab	Yes	2011	No	No
Wfuzz	Yes	2019	Yes	No

Basic Criteria for DAST Selection

- Is free
- Is actively maintained
- Detects a range of vulnerabilities
- Produces useful reports
- Integrates with build process

Finalists

Product	Last Release	Notes
Arachni	2017	Out of date library dependencies
OWASP ZAP	2019	Thriving community
Scan My Server	2019	Limited to scanning one domain once a week
W3af	2019	Out of date library dependencies
Wapiti	2019	Limited set of vulnerabilities

The Winner

ZAP

OWASP Zed Attack Proxy

What Does a Scanner Tell You?

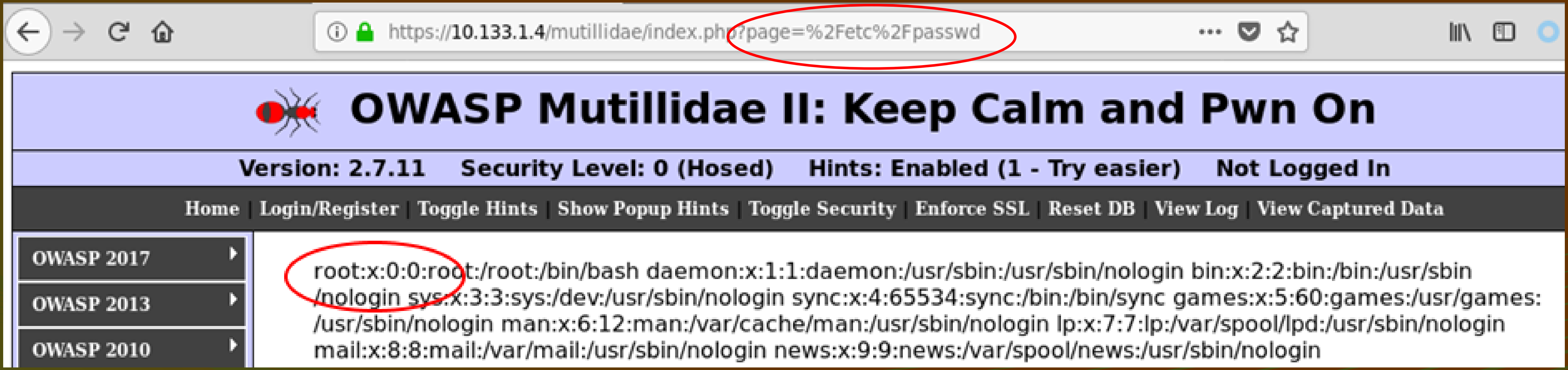
Generic Details	Page-Specific Details
Vulnerability Name	URL
Description	GET/POST
Risk Level	Parameter
Standard Defense	Attack String
CWE ID	Evidence String
Reference(s)	Full HTTP Request/Response

Example 1: Path Traversal

Item	Description
Alert Name	Path Traversal
Description	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory…
URL	http://10.133.1.4/mutillidae/index.php?page=%2Fetc%2Fpasswd
Risk	High
Parameter	Page
Attack	/etc/passwd
Evidence	root:x:0:0

Path Traversal Attack Explained

ZAP sees this	https://.../.../index.php?page= login.php	Parameter = page
ZAP tries this	https://.../.../index.php?page=/etc/passwd	Attack = /etc/passwd
ZAP receives this	<!DOCTYPE...><html>...<body>... <blockquote> root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/ usr/sbin:/...	Evidence = root:x:0:0



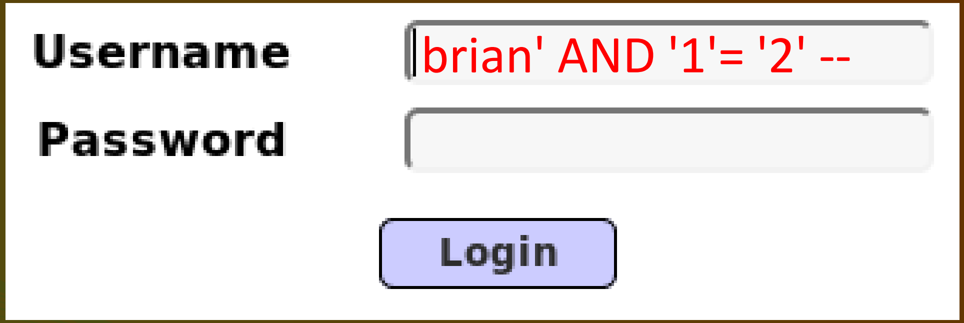
https://10.133.1.4/mutillidae/index.php?page=%2Fetc%2Fpasswd

OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.7.11 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin
/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:
/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

Example 2: SQL Injection

Item	Description
Alert Name	SQL Injection
URL	http://10.133.1.4/mutillidae/index.php?page=login.php
Risk	High
Parameter	username
Attack	brian' AND '1'='1' --
Other Info	The page results were successfully manipulated using the boolean conditions [brian' AND '1'='1' --] and [brian' AND '1'='2' --]

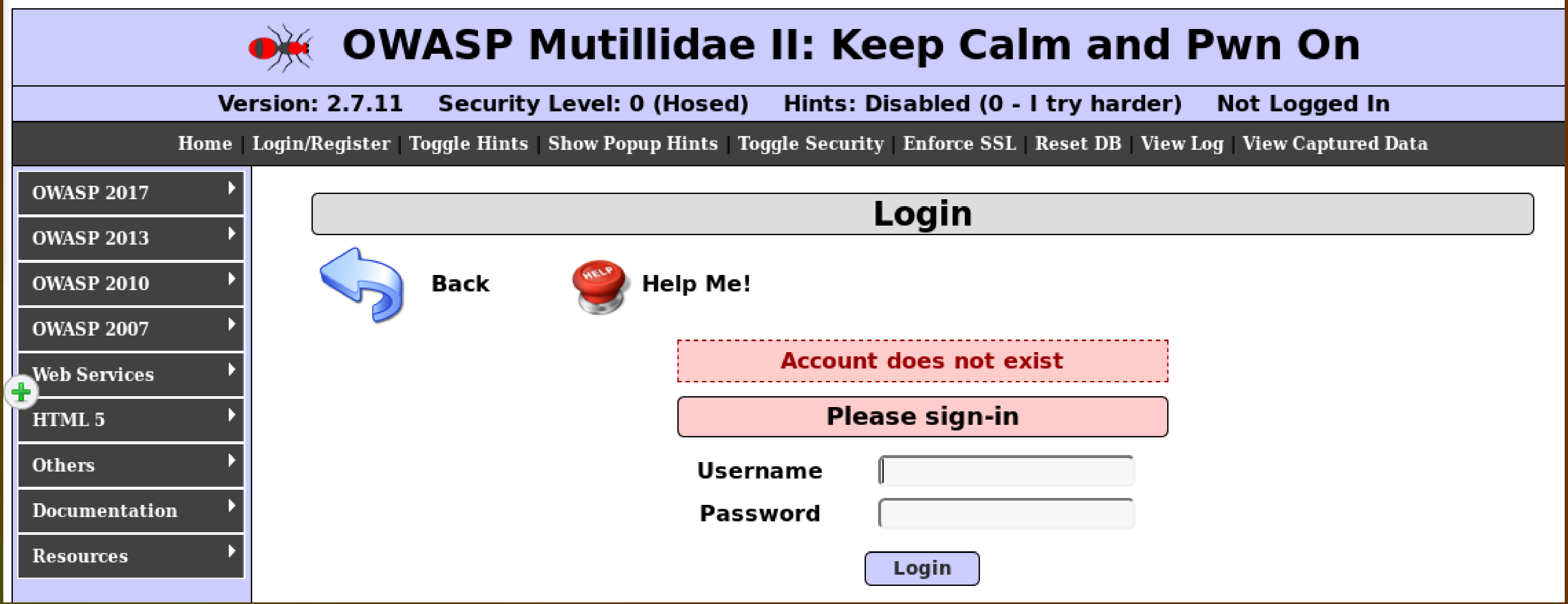


Username: brian' AND '1'= '2' --

Password:

```
<input type="text" name="username" />
```

brian' AND '1'='2' --



OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.7.11 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Back
Help Me!

Login

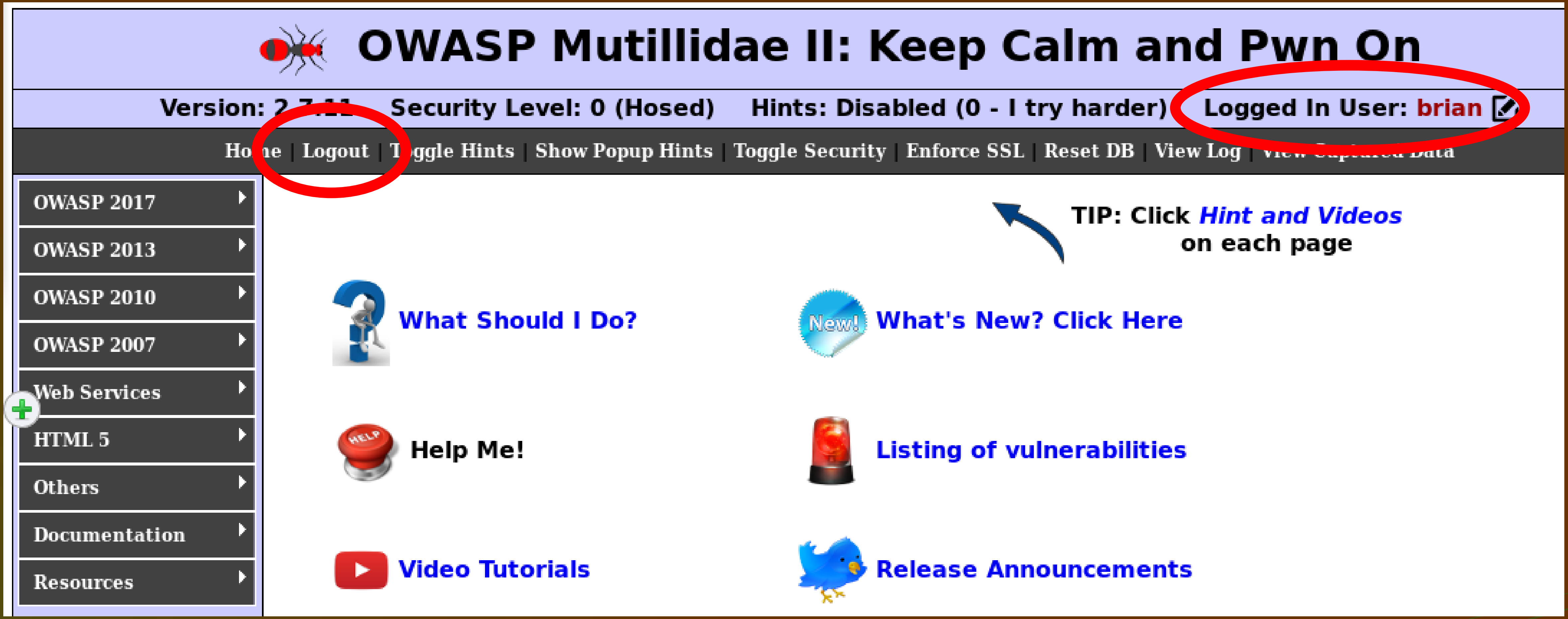
Account does not exist

Please sign-in

Username

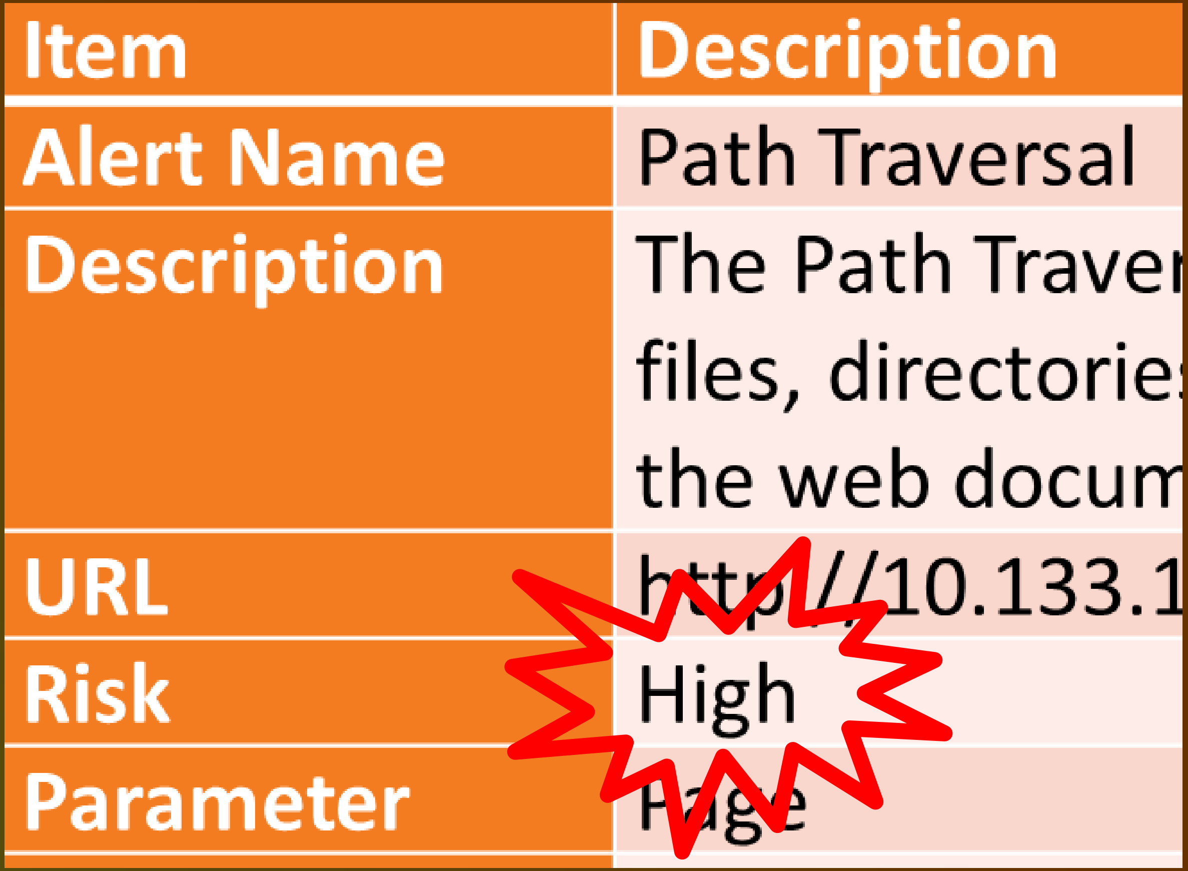
Password

brian' AND '1'='1' --



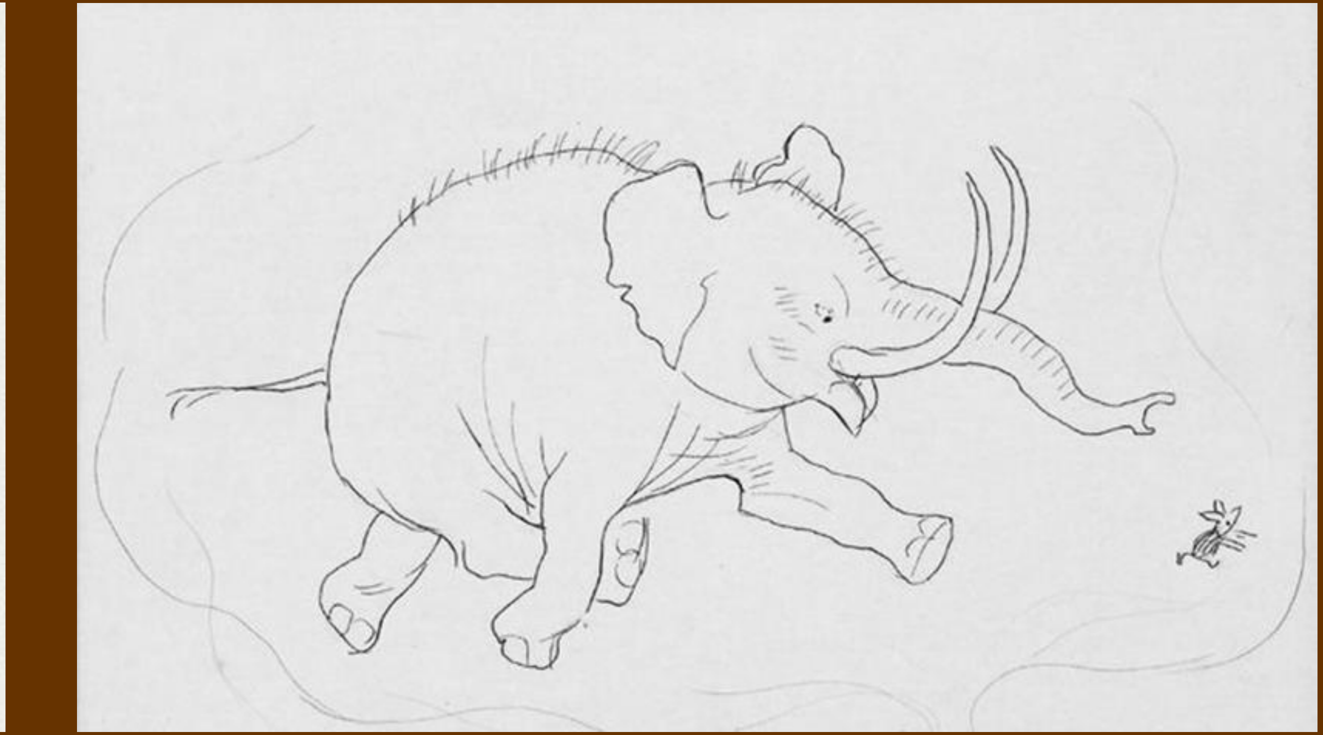
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.7.11 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Logged In User: brian
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
TIP: Click Hint and Videos on each page
What Should I Do?
What's New? Click Here
Help Me!
Listing of vulnerabilities
Video Tutorials
Release Announcements

A Note on the Scanner's Risk Level

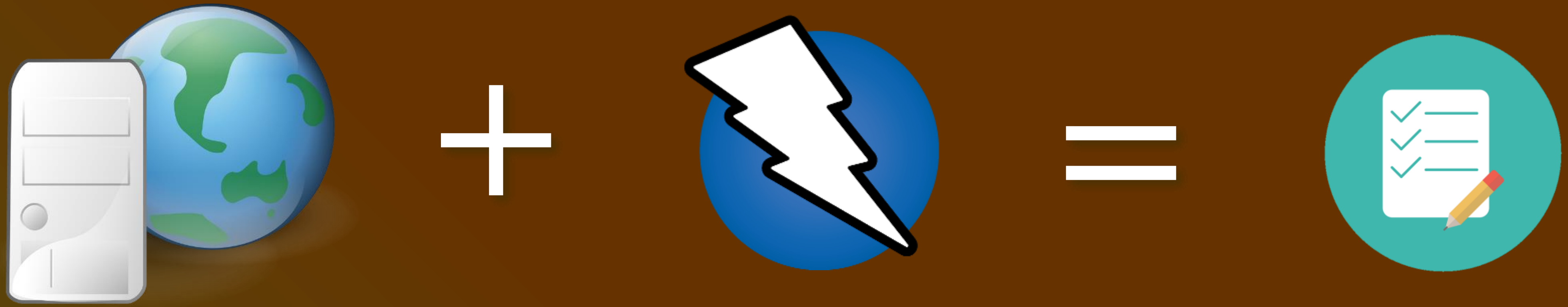


Item	Description
Alert Name	Path Traversal
Description	The Path Traver files, directorie the web docum
URL	http://10.133.1
Risk	High
Parameter	Page

False Positives



How to Learn About a Vulnerability



Am I Secure Now?

Benefits of Scanning

Application vulnerabilities get fixed.

You learn about security

The team:

- learns about vulnerabilities
- becomes more aware of security
- thinks about security sooner
- designs standard defenses

Commit to Scanning Regularly

- Who runs the scanner
- How often
- Who will process scanner reports
- How quickly

- Who will review progress over time
- How often

Other Artifacts and Practices That Might Follow

- Vulnerability management procedure
- Secure coding guidelines
- Training for new team members
- Metrics over time
- Artifacts of compliance

A Culture of Quality and Security

Requirements

- Privacy
- Regulations
- Compliance

Design

- Design Review
- Threat Modeling

Development

- Acceptance criteria
- SAST
- Code Review
- Code Guidelines

Test

- Security Test Cases
- DAST

Deployment

- Approvals
- Hardening

Maintenance

- Monitoring
- Patching
- Sunsetting

Resources

OWASP Top 10

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

Hacksplaining

https://www.hacksplaining.com/lessons

DevCentral

https://www.youtube.com/user/devcentral

OWASP Portland Chapter

https://www.meetup.com/OWASP-Portland-Chapter/

?

Brian Myers
brian@safetylight.dev