Practically Teaching the Next Generation

June 2019: International Workshop on Secure Software Engineering in DevOps and Agile Development

Chrissy Morgan

Practically Teaching the Next Generation

“In order to mitigate for the future we must find innovative ways in which to train the next generation of application developers and security professionals, on how to spot issues and rectify. This should come before entering their professional careers, ideally at university.

Students are actively taught on how to attack, however there is improvements to be made with the current state of practical mitigation teaching tools”

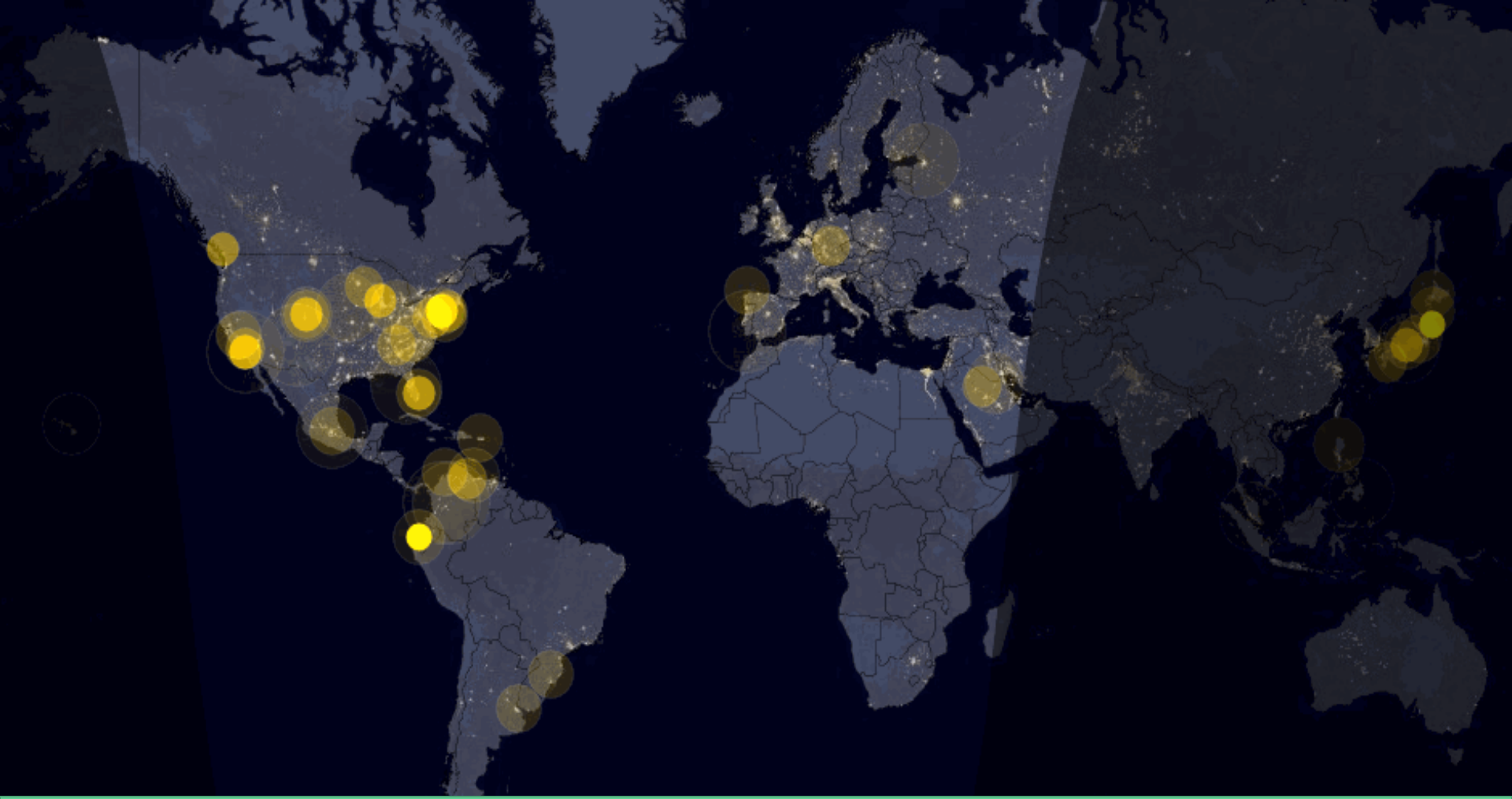
Some things you already know
Some things you don’t.
Inspire you to make a difference for the next generation

Let me tell you a story...

https://img.newatlas.com/ones-zeros-internet-art-25.png

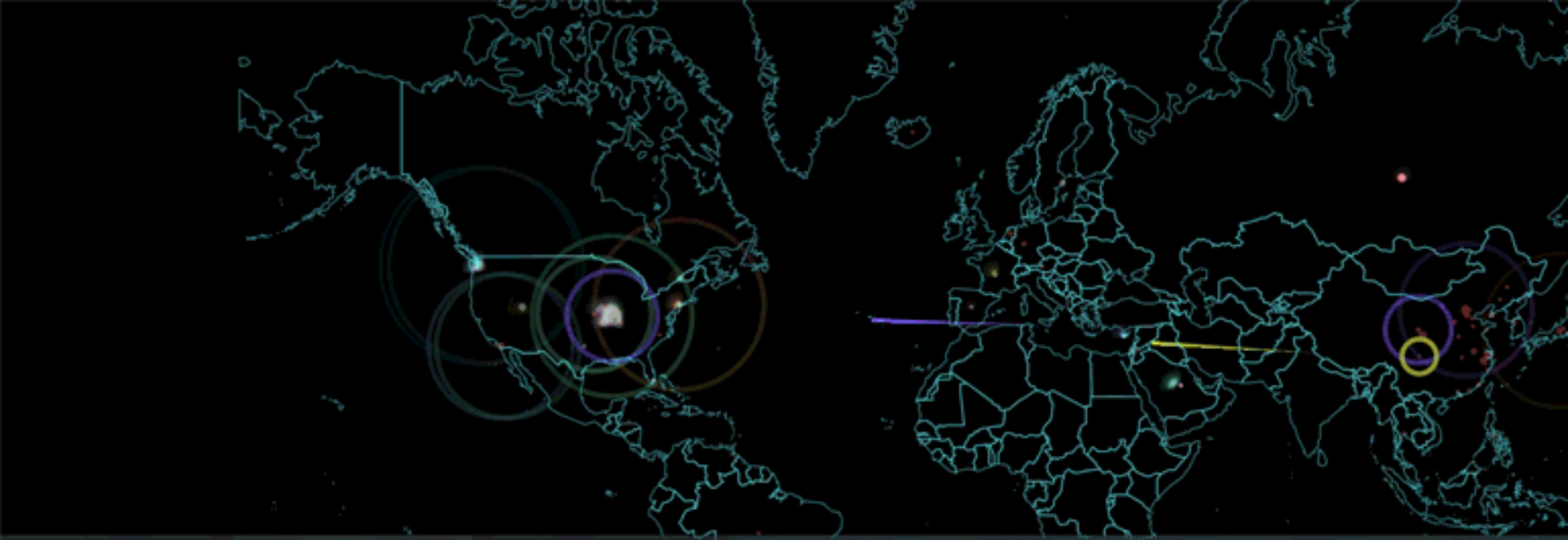
Map of the Internet : https://bostonraremaps.com/inventory/macuser-map-planet-internet/ Circa 1996

Map of the Internet opte.org Circa 2003



Tweet Use http://cartodb.s3.amazonaws.com/static_vizz/sunrise.html


2013 © Alexey Trofimov



ATTACK ORIGINS

#	COUNTRY
57	China
10	United States
8	Russia
6	Japan
4	Sweden
2	Saudi Arabia
2	Netherlands
2	South Korea
2	Jordan
2	Israel

ATTACK TYPES

#	PORT	SERVICE TYPE
6	53168	unknown
6	80	http
5	23	telnet
5	1	tcpmux
5	22	ssh
5	8080	http-proxy
4	20976	unknown
4	19962	unknown
3	4270	unknown
3	17500	unknown

ATTACK TARGETS

#	COUNTRY
87	United States
8	Russia
6	Saudi Arabia
2	France
2	Cyprus
1	Spain
1	Canada

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE
13:41:31.265	China Unicom Heibei Province Network	120.13.138.62	Hebei, CN	Saint Louis, US	unknown
13:41:31.555	China Unicom Hebei province network	121.18.73.19	Baoding, CN	Saint Louis, US	unknown
13:41:31.931	S.E.A - Multimedia	199.203.59.121	Tel Aviv, IL	Saint Louis, US	ssh
13:41:32.594	N/A	43.255.188.131	JP	Clifton, US	ssh
13:41:32.941	Shodan	66.240.236.119	San Diego, US	Seattle, US	unknown
13:41:32.957	Shodan	66.240.236.119	San Diego, US	Seattle, US	unknown
13:41:33.255	China Unicom Hebei province network	101.28.166.2	Hebei, CN	Saint Louis, US	unknown
13:41:33.636	Computers & Tele-Comm	108.161.78.2	Independenc...	Saint Louis, US	shell
13:41:34.296	CHINANET Gansu province network	118.183.76.51	Lanzhou, CN	Saint Louis, US	unknown
13:41:34.625	CHINANET Sichuan province network	182.133.136.10	Chengdu, CN	Saint Louis, US	unknown


virus
backdoor
hackers
data dumps
spoofing
defacement
anonymous
financial institutions
cyber security
government
modern warfare
social engineering
stuxnet
servers
database
distributed denial of service
corporations
encryption
networks
surveillance

Developers Don't Have The Skills Or Resources To Code Securely

Today's reality is that developers don't code securely. When measured against major industry vulnerability standards, 70% of applications fail security testing on the first scan.[4] However, don't go blaming your developers. Developers face several challenges when it comes to writing secure code:

- **Developers aren't taught application security in school.** We looked at the top 40 computer science programs as ranked by US News and World Report and found that *none* of the top ranked computer science programs in the United States require a class about secure coding or secure application design.[5] In fact, none of the top 40 computer science programs even mention secure coding in the class descriptions of their required classes, and only five universities offer an elective computer science class that is explicitly about secure code or application security.[6] Looking at the top international schools for computer science, the situation is not drastically different. None of the top five international schools for computer science require a class on secure coding or secure application design, though the University of Cambridge does require students to take a software and security engineering course that includes elements of secure code design.[7]
- **General cybersecurity is an option but not a priority in schools.** Thirty-six of the 40 top computer science schools in the US offer at least one elective course on security, but only one, UC San Diego, requires a general cybersecurity course — not specifically secure coding or application design — to graduate with a degree in computer science. On average, the schools offer 1.8

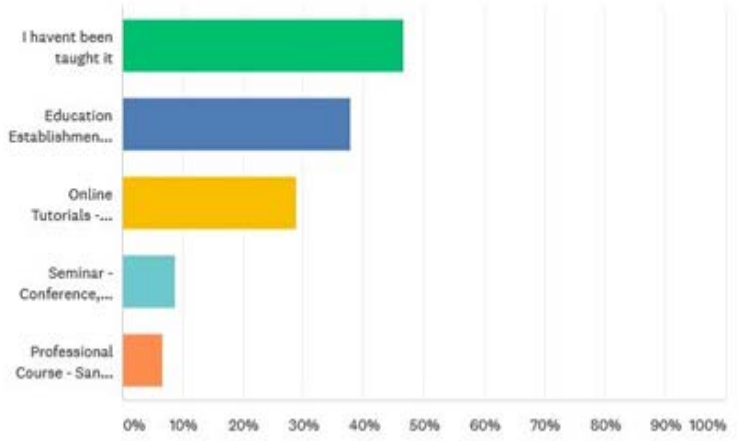
The Current state of Web Application Security Mitigation Training, What Can Be Done To Improve?

50 random participants (45 complete)

Asked to take part in the survey
Asked to use the platform and provide feedback

Have you been taught Web Application Security before, and if yes where did you learn?

Answered: 45 Skipped: 0



ANSWER CHOICES	RESPONSES	
I havent been taught it	46.67%	21
Education Establishment - University, College etc	37.78%	17
Online Tutorials - Youtube, Cybrary etc	28.89%	13
Seminar - Conference, Society lecture	8.89%	4
Professional Course - Sans etc	6.67%	3
Total Respondents: 45		

When being taught Web Application Security were you taught how to mitigate attacks?

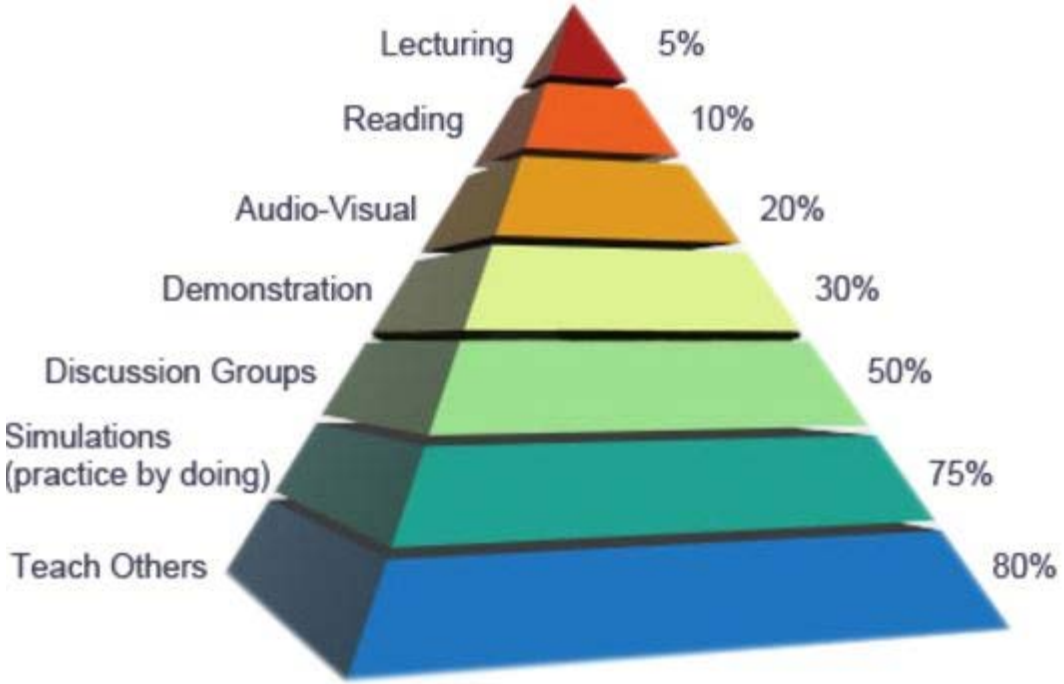
ANSWER CHOICES	RESPONSES	
Yes - Theory based, didactic teaching, show and tell but not practically implemented	23.26%	10
Yes - Practically based, taught how to remediate vulnerable web application code in order to defend	11.63%	5
No - Taught how to attack only	23.26%	10
No- No Previous learning undertaken	41.86%	18
TOTAL		43

A study by the National Training Laboratories found that the more active the teaching and learning methods, the higher the retention rates.

—Adapted from The Learning Triangle: National Training Laboratories

Practical learning stops at attacking stages.

Learning Pyramid
Methods of training and retention rates



Visual

- Visual learners prefer the use of images, maps, and graphic organizers to access and understand new information.

Auditory

- Auditory learners best understand new content through listening and speaking in situations such as lectures and group discussions. Aural learners use repetition as a study technique and benefit from the use of mnemonic devices.

Read & Write

- Students with a strong reading/writing preference learn best through words. These students may present themselves as copious note takers or avid readers, and are able to translate abstract concepts into words and essays.

Kinesthetic

- Students who are kinesthetic learners best understand information through tactile representations of information. These students are hands-on learners and learn best through figureing things out by hand (i.e. understanding how a clock works by putting one together.)

Whois
Identity for everyone

Microsoft

Forbes

(ISC)²

THE CO-LAB
ECURITY RESEARCH

44CON

WOMEN
IN SECURITY
AND PRIVACY

DA
UNIVERSE

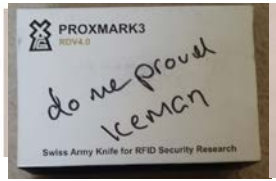
THE MANY HATS
CLUB

steelcon

CYBERCRIME
MAGAZINE

DEFCON

DEEPSEC



Cyber
Security
Challenge UK

tripwire

Akamai
Experience the Edge

Congratulations! Your first HackerOne cash bounty Inbox

HackerOne
to me
Yesterday View details

Hi Chrissy,

Today is a big day. You just earned your very first cash bounty on HackerOne. We hope you are as excited as we are about this - just think of the potential for how much you could earn! This is why we think of HackerOne as an awesome place to *hack, earn, and learn*.

Do the Professionals even know?

Project managing Website for a SME

15 Years + designing

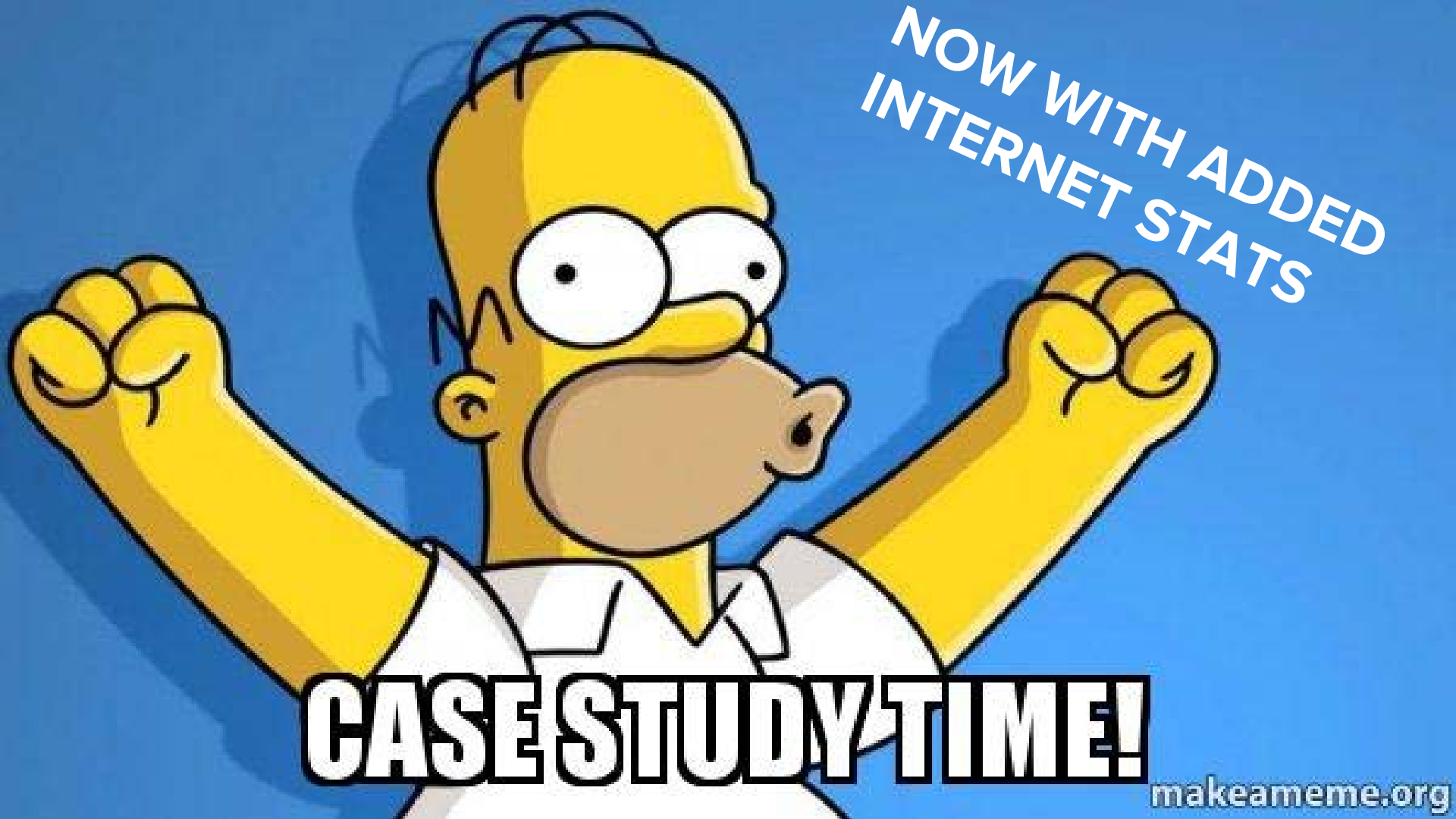
3 weeks!!!

OWASP Top Ten

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


NOW WITH ADDED INTERNET STATS
CASE STUDY TIME!
makeameme.org

Wordpress

1/3

“123,498,018 TOTAL THEME DOWNLOADS FROM WORDPRESS.ORG IN 2014.”

Wordfence 2018

11% of WordPress vulnerabilities are caused by WordPress themes.

Ithemes 2016

“ WORDPRESS.ORG PLUGINS RECEIVED 1 BILLION TOTAL DOWNLOADS, AND COUNTING.”

https://wordpress.org/plugins/

52% of the vulnerabilities reported by WPScan are due to WordPress plugins

61% of infected WordPress sites are out of date

https://blog.sucuri.net/2017/01/hacked-website-report-2016q3.html

“ Wordfence reports up to 90,000 attacks on WordPress sites every minute”

Wordfence 2018

Some Stats

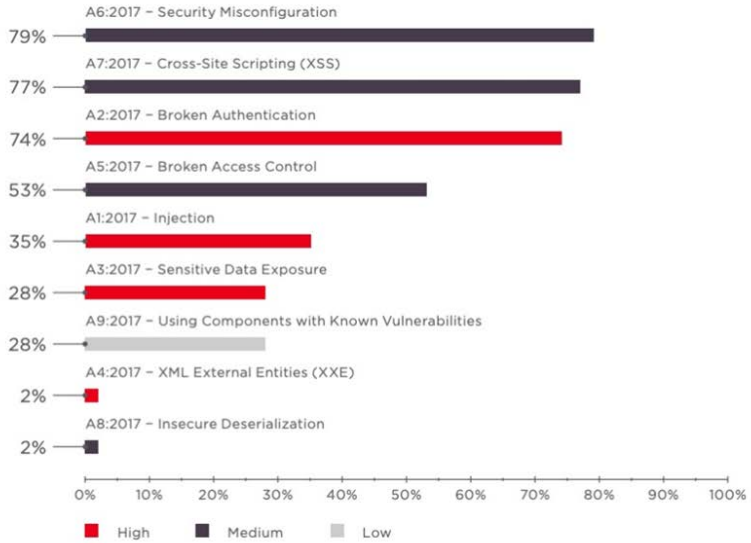
39% Cross-Site Scripting (XSS)

Other Known Attack Vectors…

- 5% — SQLI (Database Injections)
- 11% — Upload exploitation
- 7% — CSRF (Cross-Site Request Forgery forces logged in users to perform an action they didn't mean to do.)
- 6% — Multiple attack vectors at once
- 3% — LFI – (Local File Inclusion) (example)
- 2% — RFI – (Remote File Inclusion)
- 2% — Authentication Bypass
- 2% — FPD (Full Path Disclosure)
- <1% — Redirect
- <1% — XXE (XML External Entity Attack) (intercepting XML and
- reformatting before submission)
- <1% — DDOS (Denial of Service)
- <1% — SSRF (Server Side Request Forgery)
- 6% — Unknown

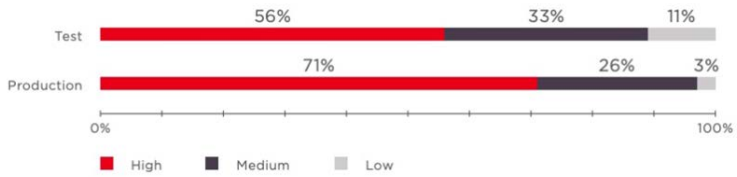
Figure 12. Vulnerabilities allowing attacks against users

Disable external entities and DTDs in XML parsers if not needed for web application functionality



Vulnerabilities in test and production applications

We observed a nearly three-fold increase in the percentage of production applications containing high-severity vulnerabilities (25% in 2017 compared to 71% in 2018). In addition, the average number of vulnerabilities per web application grew for both test and production applications.



https://www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019/ Positive Technologies 2019

Be wary of what you read online!

ABOUT ARCHIVES INFOQ OR EDITIONS SEARCH SUBSCRIBE TAGS PRIVACY

Secure coding practices in Java: challenges and vulnerabilities

JUNE 27, 2018

Secure coding practices in Java: challenges and vulnerabilities Meng et al., *ICSE'18*

TL;DR : don't trust everything you read on Stack Overflow.

Meng et al. conduct a study of Stack Overflow posts relating to secure coding practices in Java to find out the hot topics, what people struggle with, and whether or not the accepted answers are actually following security best practices.

> We conducted an empirical study on Stack Overflow posts, aiming to understand developer's concerns on Java secure coding, their programming obstacles, and insecure coding practices. We observed a wide adoption of the authentication and authorization features provided by Spring Security — a third-party framework designed to secure enterprise applications...

Well, how could I resist reading that! (Some readers may know that I was for many years the CTO of SpringSource). Spring Security does come in for some flak in this paper for the high volume of questions that are asked relating to it. There's no calibration though for underlying popularity. One of the reasons there are a lot of questions, I posit, is that there are an awful lot of *users* of

- Lack of understanding where problems are introduced by third party plugins and themes
- No Software Design Lifecycle when code is just bolted on

- No code review, or checks against CVE's databases
- Supply chain attacks
- No education and awareness

?

Pushing left

“Empirical Study on the Relationship between Software Security Skills, Usage and Training Needs in Agile Settings” (Oyetoyan et al. 2016)

- Secure Design training was the highest requirement
- Only 50% of developers implemented secure coding and design
- 60% Defects were introduced within design phase
- Rectifying cost 100 times post deployment

START LEFT

Literature Review

20 Papers | last ten years | Web Application Security Training

Study Methodology
Pedagogy
Teaching Implementation

Study Methodology Comparision

Themes /Author	Year	Platform Name	Justification	Study Intention / Goals	Methodology	Study Size	Results
Chen, L.C. et al	2010	SWEET	Teaching Materials Limited Demand For Skills Retain Interest Teaching is more effective by hands on learning	Bridge the Gap of IA and Secure web Development Enrich Curriculum Portability and Flexible Learning To provide a new generation of professionals who will be able to identify iddues made in web development	Qualiative Feedback Study	45	Positive Feedback
Papanikolaou, A. et	a2011	Hackademic	Teaching is more effective with hands on teaching. Out of the box thinking required to match hackers.	Provide a hands on learning enviroment which is engaging and lets students learn through a hackers eyes Through scenario based learning	Qualiative Feedback Study	115	Positive Feedback
DU, W	2011	SEED	Teaching Materials Limited, Varied platforms, no generalist platform to standard avaliable. Found student prefered to use their own computers for learning (VM) Teaching is more effective by hands on learning	To develop hands on learning To provide a wide array of practical subject matter To provide an easy to use system	Qualiative Feedback Study	735 (as of 2010)	Positive Feedback
Idziorek, J	2012	Literacy Based Learning	Previous studies aimed at technical students, this course is directed on the demographic of students wishing to learn.	To provide practical computer security literacy to both technical and non teachnical students.	None Documented	250	None Documented

Justification	Percentage of papers mentioned
Demand for skills / Prepare students for careers	75%
Simple solutions need to be created	50%
Teaching is more effective by hands on learning	42%
Attack Landscape more complex and increasing	33%
Lack of current Research	25%
Teaching Materials Limited	17%
Lack of training platforms	17%
Software Security should be taught	8%
Out of the box thinking required	8%
Mitigation needs to be taught Effectively	8%
Mitigation is taught predominantly through attacking strategies	8%

Figure 4 Justification Findings

Pedagogy Comparison								
Themes /Author	Method of teaching	Subject Matter	Learning Type Didactic / Inquiry	Inquiry Level (1-4)	Discusses Pedagogy	Discusses Simulation	/Practical Assessment undertaken	Target Audience
Chen, L.C. et al 2010	Mixed - Taught Defensively	Secure Web Development	Mixed	2-Structured	Yes	No	No	Students
Papanikolaou, A. et al. 2011	Offensive	Web application Attacks	Inquiry	3-Guided	Yes	No	no - Theory based exam	Students
DU, W 2011	Mixed - Taught Defensively	Various Information Security	Inquiry for Attack Didactic for Mitigation	2-Structured	Yes - Learning by Doing	No	No	Students
Idziorek, J 2012	Defensive	High level Overview Computer Security Literacy	Didactic	1-Confirmation	Yes - Defines tier based learning	No	None Documented	Students
Sonntag, M 2013	Defensive	Web Application Security	Inquiry for investigation Didactic for resolution	3-Guided	Yes	No	No	Students

Inquiry based learning

(Idziorek et al. 2012) presented different types of learning styles and identified course based, inquiry based and literacy based.

Inquiry was selected to be used as a classifier

Figure 1.

The four levels of inquiry and the information given to the student in each one.

Inquiry Level	Question	Procedure	Solution
1—Confirmation Inquiry *Students confirm a principle through an activity when the results are known in advance.*	✔	✔	✔
2—Structured Inquiry *Students investigate a teacher-presented question through a prescribed procedure.*	✔	✔	
3—Guided Inquiry *Students investigate a teacher-presented question using student designed/ selected procedures.*	✔		
4—Open Inquiry *Students investigate questions that are student formulated through student designed/selected procedures.*			

Levels of Inquiry (banchi & Bell 2008)

Examples of how Inquiry based learning could be used in designing future platforms.

Level 1 - Confirmation: A simulation driven environment where the answers to mitigation are just shown within commented code, reinforced with lecture based materials.

Level 2 - Structured: Help is given to students through a procedure such as vulnerability analysis and shown how to use the tools in which to find out the insecure code.

Level 3 – Guided: Student investigate pieces of code using their own methods to find what is insecure. The problem is given initially; this could be in the style of a CTF.

Level 4 – Open: Students may perhaps formulate plans for review, look through code not knowing if there is an issue and identify insecure code using their own methodology and procedures (Similar to bug bounty)

		Implementation Comparison		
Themes /Author	Platform Type	Software Used	Future Work / Conclusion	Notes
Chen, L.C. et al 2010	Virtual Machine	Ubuntu VMs with pre loaded software. Web and application servers: IIS, Tomcat, Apache, GlassFish (Sun's Java EE 5 server reference mplementation),Web Security testing: Web Goat , .Net Security Toolkits,Web Proxy: Paros, Web Scarab	None given	Good teaching materials, could be further reinforced with video based demonstrations
Papanikolaou, A. et al. 2011	Online	Web browser based localhost implementation	Implementation of multiple choice questions to provide extra familisation of topics Improve Scoring,improve randomisation of challenges	Good Framework and extensible. Has been implemented in over 15 universities & colleges
DU, W 2011	Online and Virtual Machine	Ubuntu OS 12.04, Minix	Already at 80 establishments using SEED, they want to disseminate further. Improve on platform to have new attacks, further instructional videos	One of the oldest platforms Does not provide web application secure coding practical lessons Has been continually developed since 2002, The latest paper does not provide latest findings, however (DU 2010) had surveyed respondents over a 3 year period based on qualitative data.
Idziorek, J 2012	Classroom	None Documented	Future work is to have a lab for each subject.	Breaks down the types of learning into three tiers, provides a gap analysis
Sonntag, M 2013	Software	Java SQL server	Gather data on evaluation of use Qualiative	Very good and targeted paper dealing with the issues of web application Security training. However lacks practical implementation of the resolution of securing the code, the platform only shows examples.No implementation is expected of the student

WebDevSec

Simple and easy to use – just visit hack.me website

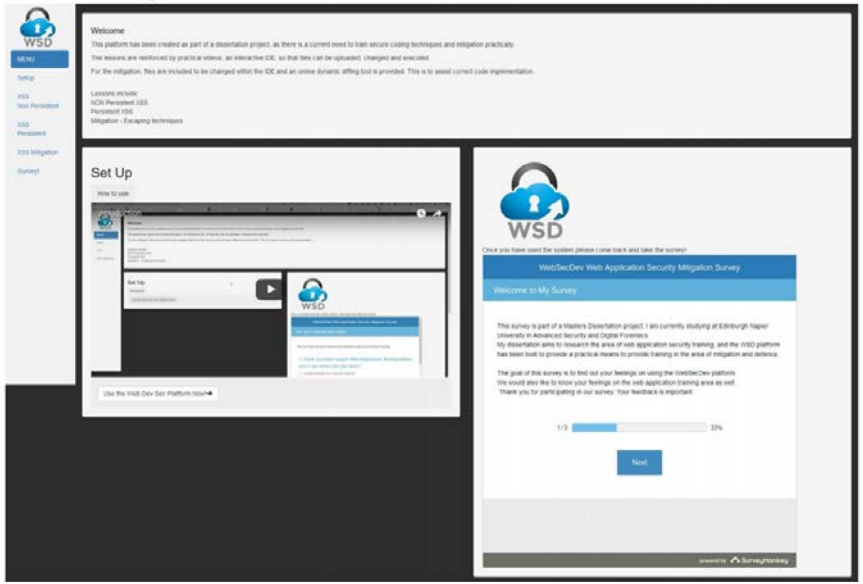
Would teach the attack and mitigation practically

Would provide learning materials in a mixture of styles :

Written form
Practical tasks
Video Demonstrations (for audio / visual)

4.4 Final Version Visual Overview

Introduction Page



WebDevSec

Non Persistent XSS tutorial page

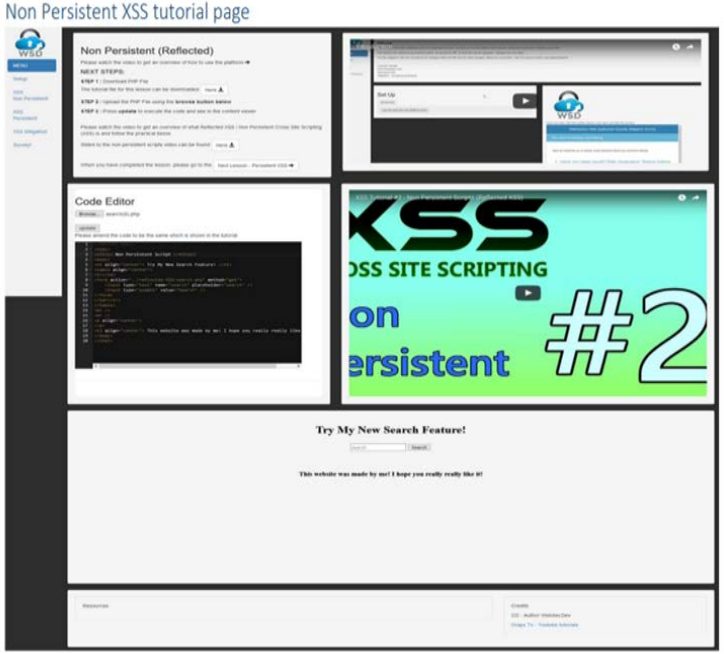


Figure 25 Non Persistent (Reflected Attack) Tutorial Page

Persistent XSS tutorial page

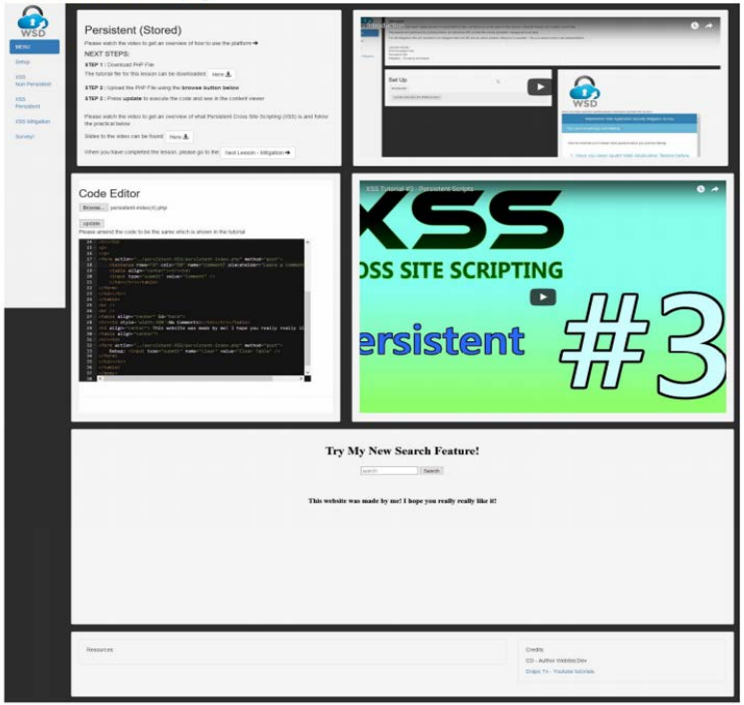


Figure 27 Persistent (stored) XSS tutorial page

WebDevSec

Mitigation Area tutorial page

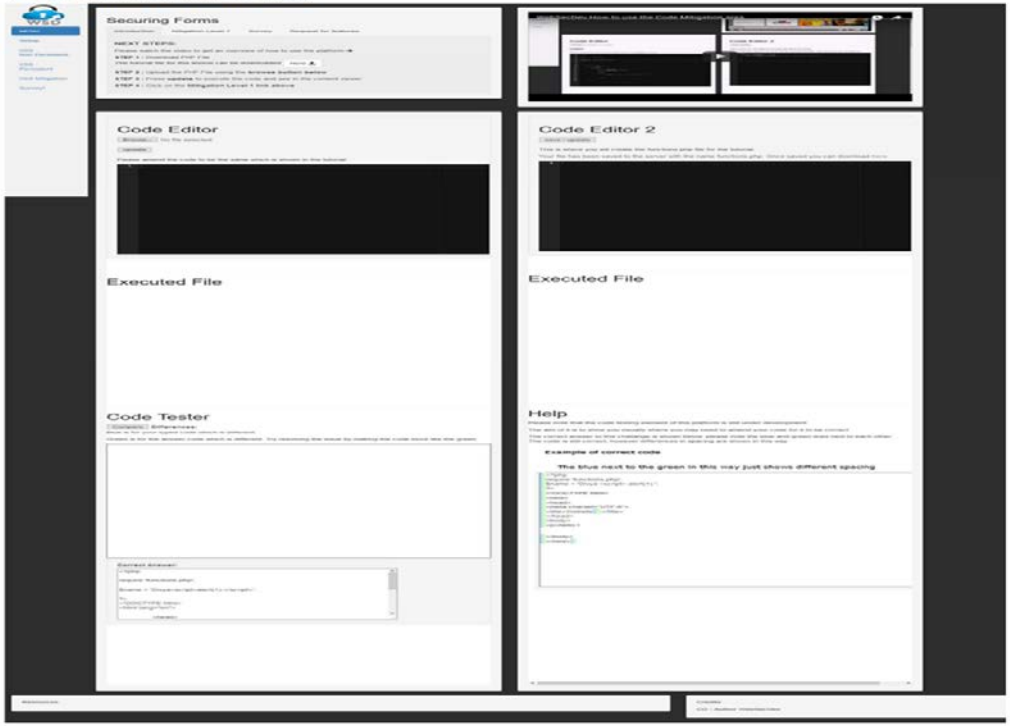


Figure 31 Close up of video pane

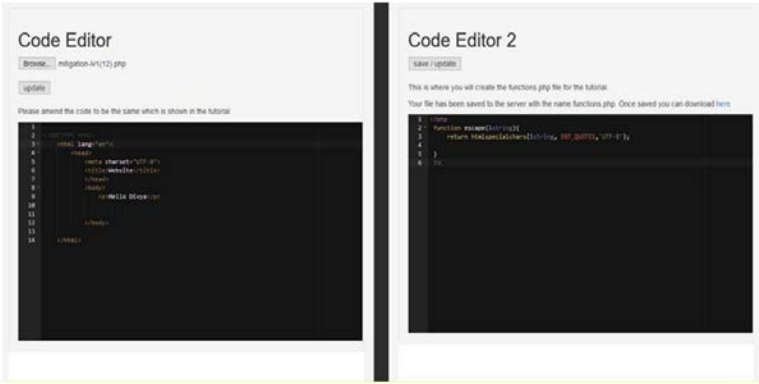


Figure 32 close up of Code Editor 1 and 2

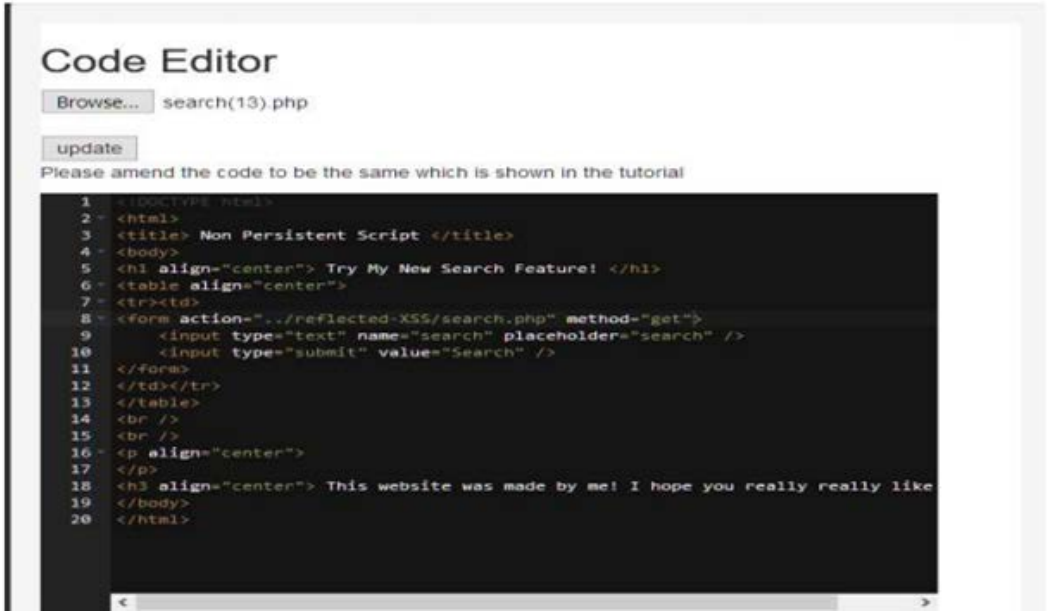
WebDevSec

Video demonstrations makes it different from anything else out there

Positive reviews but needs more lessons!

Complete novices we able to use it

People felt the code comparer at the end really helped know when they were going wrong



How Can We Improve?

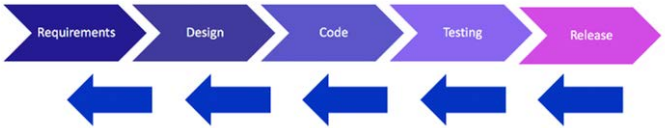
Out of the box thinking required!

Pushing Left, Like a Boss: Part 1

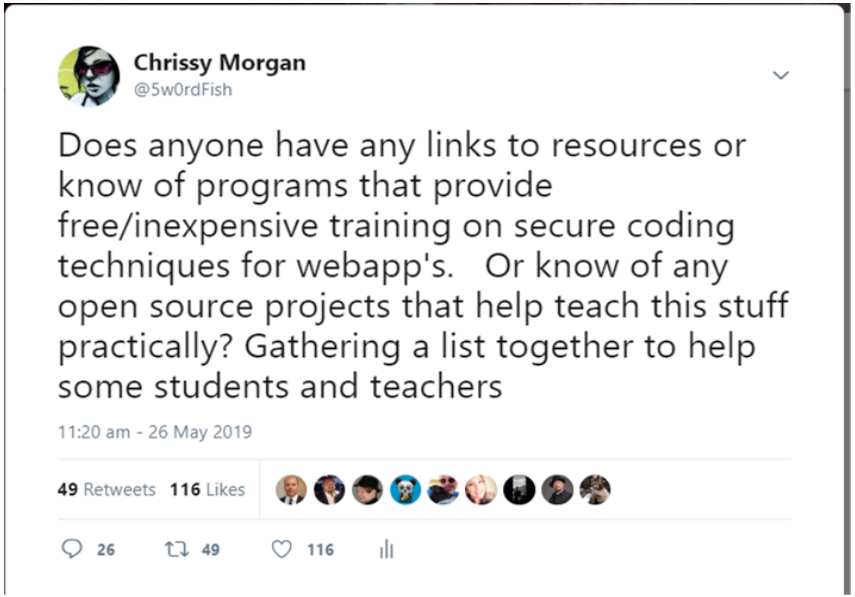
SheHacksPurple Follow
Jul 8, 2018 · 5 min read

In all of the talks and articles I have ever written and all the advice I have ever given, I am always telling people they should "push left". When security people say they want to "shift left", they are referring to the left side of the System Development Life Cycle (SDLC), which is the way software engineers describe the methodology or process for making software.

If you look at the image below, the further "left" you look, the earlier you are in the process. When we say we want to "push left", we mean we want to start security at the very beginning and perform security in every step of the SDLC.



You might be reading this and thinking "Of course! Doesn't everyone do that?



Chrissy Morgan
@5w0rdFish

Does anyone have any links to resources or know of programs that provide free/inexpensive training on secure coding techniques for webapp's. Or know of any open source projects that help teach this stuff practically? Gathering a list together to help some students and teachers

11:20 am - 26 May 2019

49 Retweets **116** Likes

26 49 116

Keep up to date and reach out to the community!

Education/Free Training

The following courses either have been offered or are being offered free of charge courtesy of the trainers and the OWASP Foundation to anyone interested in learning about application security. Additionally, the training slides/coursework is available under an open source license and we encourage you to use it to set up your own training event!

- NEW* 11-April 2016, OWASP is experimenting with GOTOTraining as a platform to enable project leaders to provide training on their project to the world. For more information CLICK HERE

If you are interested in setting up a training event through OWASP, submit your request here, we also have funding available to community members who may need help with travel, a venue or other logistics to get the event up and running. Click here for more information.

Here are some general guidelines we have set up for free training courses within the OWASP Community:

1. Use free and local when possible - donated venues or universities as well as trainers that are near by will help save on overhead costs
2. Use open source training materials - we ask that you make your training materials available after the course, preferably in an editable format
3. Use OWASP template for slides and keep any company branding to one bio slide
4. Do an open call for training when possible to avoid giving preference to any one vendor/trainer and give others in the community a chance to participate
5. If possible, do the training in a way and time that doesn't compete with paid training (especially at Global AppSec Conferences)

Credits: A sincere thank you to Eoin Keary, Jim Manico, Dan Cornell, Josh Sokol and others who generously donated training content referenced below.

Training Courses, Trainer Data, and Material					
Training Name/Topic	**Trainer Name(s)**	**Training Materials**	**Training Location**	**Training Date**	**Number of Attendees**
Analyzing (Java) Source Code for Cryptographic Weaknesses-Editable slides (ODP), with speaker's notes, and non-editable (PDF), without speaker's notes	Kevin W. Wall	File:Kwwall-owasp-prezo-CryptoCodeWeaknesses--2015-12-03.odp and File:Kwwall-owasp-prezo-CryptoCodeWeaknesses--2015-12-03.pdf	Columbus, OH OWASP Chapter	Dec 03, 2015	18
Introduction to Application Security - Editable slides (pptx)	Josh Sokol, Dan Cornell	Training Slides	LASCON 2015	October 21, 2015	100
Application Security – Where do I start?	Jim Manico, Eoin Keary, Michael Coates	Training Slides	Jillians San Francisco, CA	Feb 24, 2014	200
Approaching App Sec - Editable slides (pptx)	Jim Manico, Eoin Keary	How_Do_I_Approach_Application_Security-1	RSA 2013 EU, RSA 2013 USA, Lascon 2013		1000+

Category:OWASP Application Security Verification Standard Project

Help

Home
About OWASP
Acknowledgements
Advertising
Books
Brand Resources
Careers
Chapters
Donate to OWASP
Downloads
Events
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
Presentations
Press
Projects
Supporting Partners
Video

Reference
Activities
Attacks
Code Snippets
Controls
Glossary
How To...
Java Project
.NET Project
Principles
Technologies
Threat Agents
Vulnerabilities

Tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information

Home | Downloads | Acknowledgements | Glossary | ASVS Users | Precedents-Interpretations | Internationalization | Archive - Previous Version

FLAGSHIP mature projects

What is ASVS?

The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development.

The primary aim of the **OWASP Application Security Verification Standard (ASVS) Project** is to normalize the range in the coverage and level of rigor available in the market when it comes to performing Web application security verification using a commercially-workable open standard. The standard provides a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection. This standard can be used to establish a level of confidence in the security of Web applications. The requirements were developed with the following objectives in mind:

- **Use as a metric** - Provide application developers and application owners with a yardstick with which to assess the degree of trust that can be placed in their Web applications,
- **Use as guidance** - Provide guidance to security control developers as to what to build into security controls in order to satisfy application security requirements, and
- **Use during procurement** - Provide a basis for specifying application security verification requirements in contracts.

OWASP ASVS 4.0 Released!

Get the new version of the ASVS 4.0 from the Downloads page.

Email List

Project Email List

Project Leaders

- Daniel Cuthbert @
- Andrew van der Stock @
- Jim Manico @
- Mark Burnett
- Josh C Grossman

GitHub Repo

ASVS GitHub Repo

Download

ASVS 4.0

- English PDF (1.1 MB)
- English Word (560 kB)
- English CSV (65 kB)

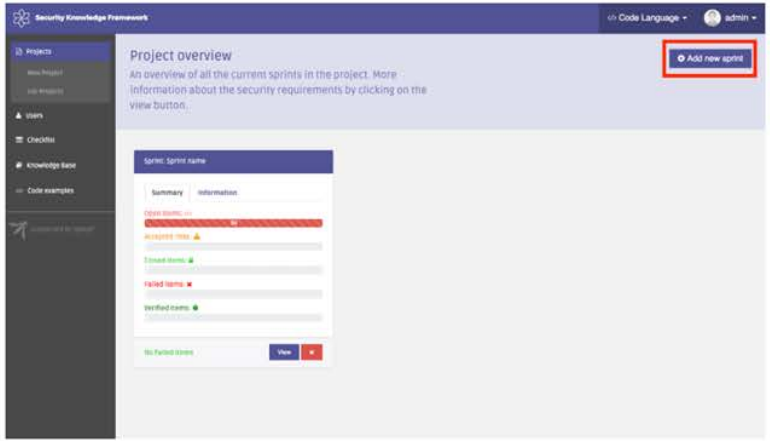
News and Events

- [1 March 2019] ASVS 4.0 released!
- [9 March 2018] OWASP Application Security Verification Standard 3.1 Spreadsheet created by August Detlefsen
- [29 June 2016] Version 3.0.1 released!
- [9 Oct 2015] Version 3.0 released
- [20 May 2015] "First Cut" Version 3.0 released
- [11 Aug 2014] Version 2.0 released

Project dashboard

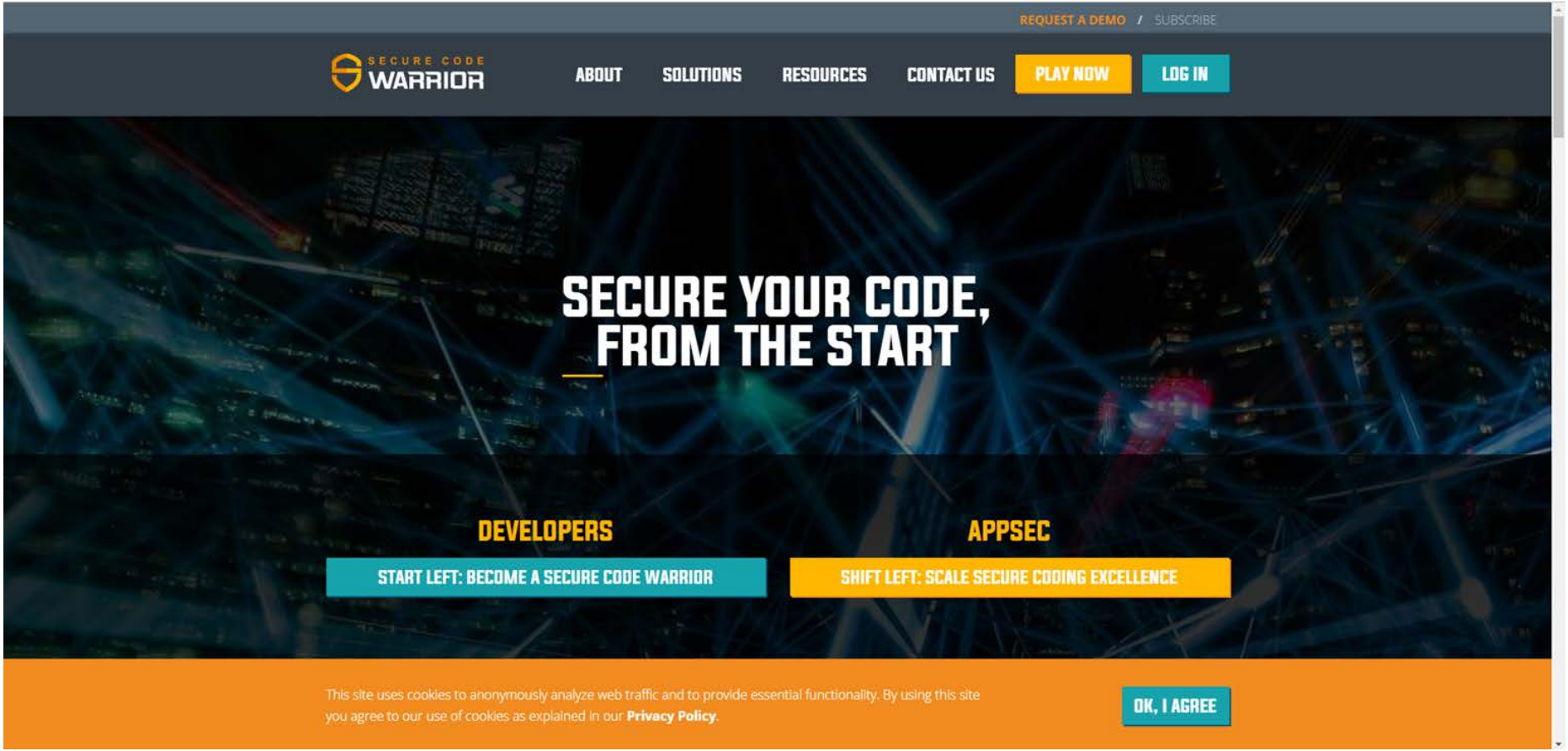
Suggest Edits

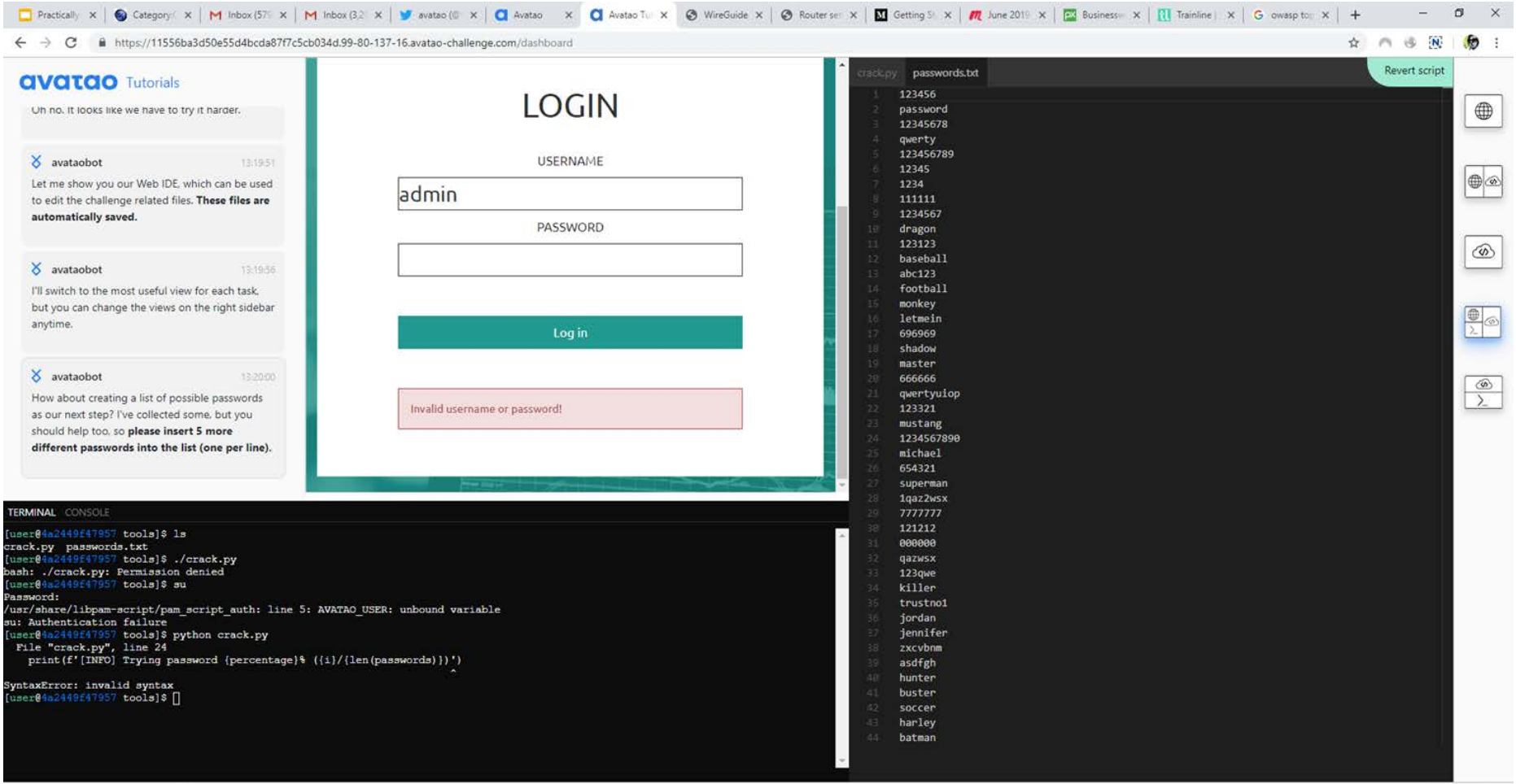
So, now we started a new project and added our very first sprint. As you may notice the very first sprint (depending on the pre-development settings) has a lot of security requirements selected for you. The volume of security requirements become les whenever you start adding more sprints. This has mainly to do with the first sprint also covering design and architecture and authentication/authorization. Highlighted in red is the button that shows a modal dat allows us to add new sprints to the project.



The screenshot below shows a close-up image of sprint statuses in the dashboard. It shows the status and the number of open tickets per sprint. When selecting the view button we find a summary of the tickets along with the correlated knowledgebase items. If we select the "X" we can delete the sprint from the project.

Capture the Flags & Bug Bounty Programs


REQUEST A DEMO / SUBSCRIBE
SECURE CODE WARRIOR
ABOUT
SOLUTIONS
RESOURCES
CONTACT US
PLAY NOW
LOG IN
SECURE YOUR CODE, FROM THE START
DEVELOPERS
START LEFT: BECOME A SECURE CODE WARRIOR
APPSEC
SHIFT LEFT: SCALE SECURE CODING EXCELLENCE
This site uses cookies to anonymously analyze web traffic and to provide essential functionality. By using this site you agree to our use of cookies as explained in our Privacy Policy.
OK, I AGREE


avatao Tutorials
Oh no. It looks like we have to try it harder.
avataobot 13:19:51
Let me show you our Web IDE, which can be used to edit the challenge related files. These files are automatically saved.
avataobot 13:19:56
I'll switch to the most useful view for each task, but you can change the views on the right sidebar anytime.
avataobot 13:20:00
How about creating a list of possible passwords as our next step? I've collected some, but you should help too, so please insert 5 more different passwords into the list (one per line).
https://11556ba3d50e55d4bcda87f7c5cb034d.99-80-137-16.avatao-challenge.com/dashboard
LOGIN
USERNAME
admin
PASSWORD
Log in
Invalid username or password!
crack.py
passwords.txt
Revert script
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
football
monkey
letmein
696969
shadow
master
666666
qwertyuiop
123321
mustang
1234567890
michael
654321
superman
1qaz2wsx
7777777
121212
000000
qazwsx
123qwe
killer
trustno1
jordan
jennifer
zxcvbnm
asdfgh
hunter
buster
soccer
harley
batman
TERMINAL
CONSOLE
[user@4a2449f47957 tools]$ ls
crack.py passwords.txt
[user@4a2449f47957 tools]$ ./crack.py
bash: ./crack.py: Permission denied
[user@4a2449f47957 tools]$ su
Password:
/usr/share/libpam-script/pam_script_auth: line 5: AVATAO_USER: unbound variable
su: Authentication failure
[user@4a2449f47957 tools]$ python crack.py
File "crack.py", line 24
print(f'[INFO] Trying password {percentage}% ({i}/{len(passwords)})')
SyntaxError: invalid syntax
[user@4a2449f47957 tools]$
Practically Teachi....pptx
Show all

CYBRARY CATALOG COMMUNITY CAREERS HIRE BUSINESS LIVE LOGIN REGISTER

Secure Coding

TIME	DIFFICULTY	CEU/CPE	
9 hours 31 minutes	Intermediate	10	Course

In the Secure Coding training course, Sunny Wear will show you how secure coding is important when it comes to lowering risk and vulnerabilities. Learn about XSS, Direct Object Reference, Data Exposure, Buffer Overflows, & ...

START COURSE

NEED TO TRAIN YOUR TEAM? LEARN MORE

Did you know Cybrary has FREE video training? Join more than **2,500,000** IT and cyber security professionals, students, career changers, and more, growing their careers on Cybrary.

Overview

In the Secure Coding training course, Sunny Wear will show you how secure coding is important when it comes to lowering risk and vulnerabilities. Learn about XSS, Direct Object Reference, Data Exposure, Buffer Overflows, & Resource Management.

Instructed By

Sunny Wear

Instructor

Course Content

Introduction

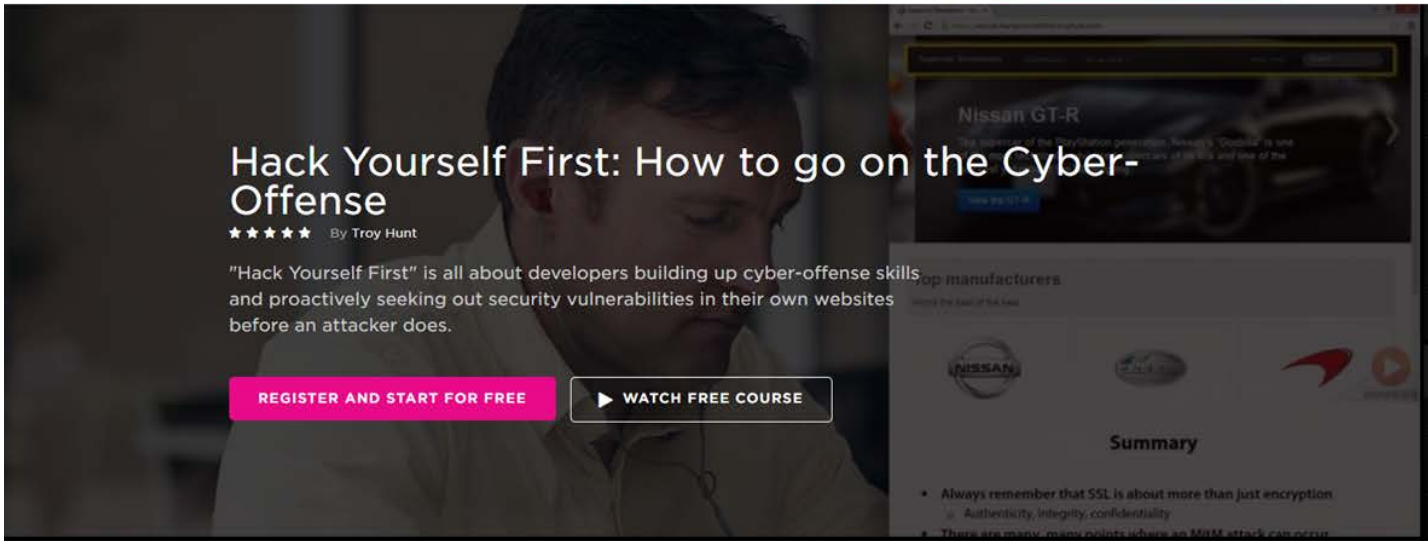
Part 1 Intro	06:48
Part 2 Lab Setup	05:28

Practically Teachi....pptx

Show all

PLURALSIGHT COURSES What do you want to learn? Business Personal LIVE 2019 Log in

roleIQ ROCK [AZURE] SEE ALL AZURE ROLES



Hack Yourself First: How to go on the Cyber-Offense

★★★★★ By Troy Hunt

"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.

REGISTER AND START FOR FREE ▶ WATCH FREE COURSE

Introduction
- About the course 2m
- Why hack yourself first 4m
- Introducing a vulnerable website – Supercar Showdown 5m
- Using Chrome's developer tools 5m
- Monitoring and composing requests with Fiddler 4m
- Modifying requests and responses in Fiddler 3m

Transport Layer Protection
- Introduction 1m
- The three objectives of transport layer protection 3m
- Understanding a man in the middle attack 3m

Course info

Rating ★★★★★ (852)

Level Intermediate

Description

The prevalence of online attacks against websites has accelerated quickly in recent years and the same risks continue to be readily exploited. However, these are very often easily identified directly within the browser; it's just a matter of understanding the vulnerable patterns to look for. This course comes at security from the view of the attacker in that their

Practically Teachi....pptx

Show all

What we should aim for

The perfect mix

More time on mitigation!!

Mixture of Learning styles and methods.

Theory and Reading

Show and tell

Audio and Visual

Practical implementation

Exploratory Learning

Free and Open Source!

Questions?

Dissertation on request.
LinkedIn: Chrissy Morgan Twitter : @5w0rdfish