IMMERSIVELABS

DATA SHEET

FOR DEVELOPMENT AND ENGINEERING TEAMS

As organizations digitize faster and at greater scale than ever before, achieving a secure software development lifecycle through skills development is increasingly important.

Achieving this on the ground is not easy. Recognized tensions between security and engineering aside, skills development involves a large outlay of time from expensive people, spreading already overburdened resources thinner to 'shift left'. The alternative is static click-through training questions dictating best practice. For a proudly creative and pragmatic talent-set, these are quickly forgotten and have minimal impact.

Our progressive platform is built to address this problem, embedding security in the human elements of the software lifecycle to deliver tangible business outcomes in three ways:

EQUIPPING

Arm people with a range of continually updated secure development capabilities relevant to a highly fluid sector, from underlying theory to specialist skills.

EXERCISING

Run engineering teams through real-world scenarios which engage hands-on individuals in a way proven to build cognition and reduce skills decay.

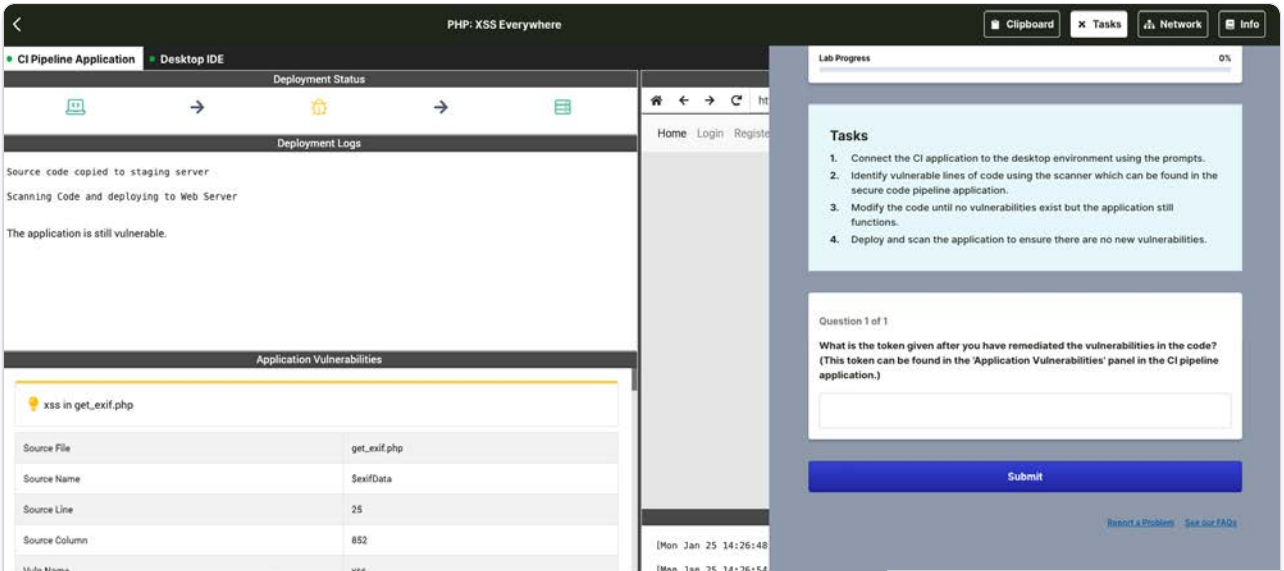
EVIDENCING

Understand and visualise the secure development capabilities of the entire team for better risk management and a more efficient CI/CD pipeline.

BUILDING HUMAN CYBER CAPABILITIES INTO DEVOPS TEAMS FROM THE GROUND UP

Immersive Labs for Development and Engineering Teams drops people into a range of continually updated SecDevOps challenges, scenarios, and simulations in the browser. Our platform teaches everything from basic underlying theory, such as authentication and authorization, to interactive challenges around the latest vulnerabilities, in a number of ways:

1. **Dynamic storylines:** Progress through real life gamified narratives based on everything from OWASP Top Ten and CWE Top 25, to breaking vulnerabilities. This encourages active learning in a way which appeals to the hands-on mindset of developers, embedding skills into the CI/CD pipeline. Ultimately, this prevents code being recalled once committed, reducing cost and friction in the innovation cycle.



```
Source code copied to staging server
Scanning Code and deploying to Web Server

The application is still vulnerable.
```

xss in get_exif.php

Source File	get_exif.php
Source Name	$exifData
Source Line	25
Source Column	852
Vuln Name	xss

```
[Mon Jan 25 14:26:48
[Mon Jan 25 14:26:54
```

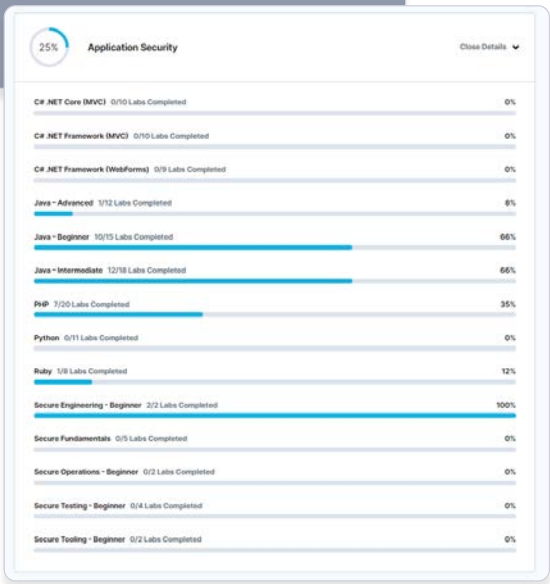
Tasks

1. Connect the CI application to the desktop environment using the prompts.
2. Identify vulnerable lines of code using the scanner which can be found in the secure code pipeline application.
3. Modify the code until no vulnerabilities exist but the application still functions.
4. Deploy and scan the application to ensure there are no new vulnerabilities.

Question 1 of 1

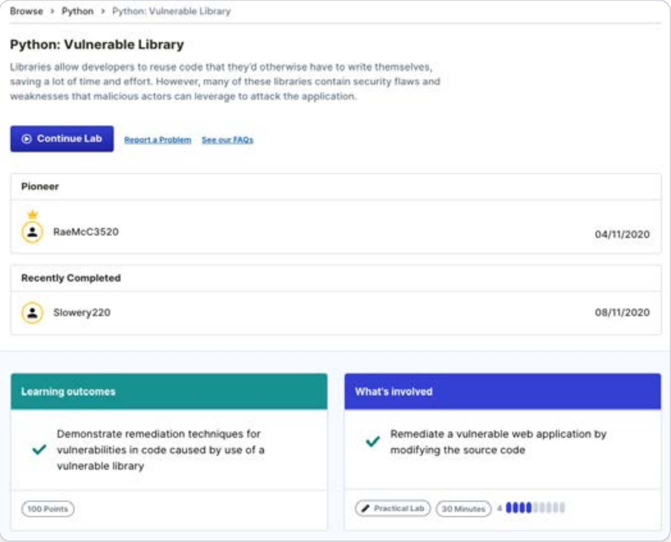
What is the token given after you have remediated the vulnerabilities in the code? (This token can be found in the 'Application Vulnerabilities' panel in the CI pipeline application.)

2. **Continuous development:** Upskill using regularly updated content which reflects the ever-changing nature of risk presented by a highly dynamic technology environment. As new vulnerabilities, tools and techniques emerge, so does the content your team learns from. This reduces friction and time-outlay from security teams and keeps the capabilities of developers and engineers relevant, encouraging more secure organizational transformation.



C# .NET Core (MVC)	0/10 Labs Completed	0%
C# .NET Framework (MVC)	0/10 Labs Completed	0%
C# .NET Framework (WebForms)	0/9 Labs Completed	0%
Java - Advanced	1/12 Labs Completed	8%
Java - Beginner	10/15 Labs Completed	66%
Java - Intermediate	12/18 Labs Completed	66%
PHP	7/20 Labs Completed	35%
Python	0/11 Labs Completed	0%
Ruby	1/8 Labs Completed	12%
Secure Engineering - Beginner	2/2 Labs Completed	100%
Secure Fundamentals	0/5 Labs Completed	0%
Secure Operations - Beginner	0/2 Labs Completed	0%
Secure Testing - Beginner	0/4 Labs Completed	0%
Secure Tooling - Beginner	0/2 Labs Completed	0%

3. **Across the entire SDLC:** Build skills and understanding of security across the whole software lifecycle with content designed to be understood and used by everyone from coders, to QA, testing, and security operations. Challenge your developers to experience a Python SQL Injection and help security teams understand the nuanced differences in delivery timescales between Kanban and scrum. With these understandings, once siloed teams integrate more effectively and unhelpful tensions are reduced.



Browse › Python › Python: Vulnerable Library

Python: Vulnerable Library

Libraries allow developers to reuse code that they'd otherwise have to write themselves, saving a lot of time and effort. However, many of these libraries contain security flaws and weaknesses that malicious actors can leverage to attack the application.

Pioneer

RaeMcC3520 04/11/2020

Recently Completed

Slowery220 08/11/2020

Learning outcomes

✓ Demonstrate remediation techniques for vulnerabilities in code caused by use of a vulnerable library

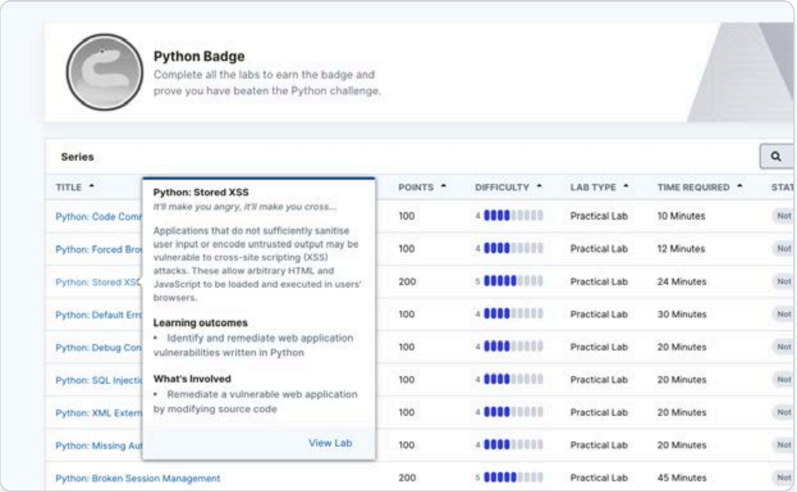
100 Points

What's involved

✓ Remediate a vulnerable web application by modifying the source code

Practical Lab · 30 Minutes · 4

4. **Actionable insights:** Analyse and visualize the security capabilities of the entire SDLC, either as an overview or in granular detail. This helps managers understand where skills lie and task teams appropriately, for example by only allowing skilled members to commit code on high-risk applications. Not only does this reduce organizational risk, it also makes for better budgeting and strategy decisions.



Python Badge

Complete all the labs to earn the badge and prove you have beaten the Python challenge.

Series

Python: Stored XSS

It'll make you angry, it'll make you cross...

Applications that do not sufficiently sanitise user input or encode untrusted output may be vulnerable to cross-site scripting (XSS) attacks. These allow arbitrary HTML and JavaScript to be loaded and executed in users' browsers.

Learning outcomes

- Identify and remediate web application vulnerabilities written in Python

What's Involved

- Remediate a vulnerable web application by modifying source code

TITLE	POINTS	DIFFICULTY	LAB TYPE	TIME REQUIRED	STAT
Python: Code Com	100	4	Practical Lab	10 Minutes	Not
Python: Forced Bro	100	4	Practical Lab	12 Minutes	Not
Python: Stored XSS	200	5	Practical Lab	24 Minutes	Not
Python: Default Err	100	4	Practical Lab	30 Minutes	Not
Python: Debug Con	100	4	Practical Lab	20 Minutes	Not
Python: SQL Injecti	100	4	Practical Lab	20 Minutes	Not
Python: XML Extern	100	4	Practical Lab	20 Minutes	Not
Python: Missing Au	100	4	Practical Lab	20 Minutes	Not
Python: Broken Session Management	200	5	Practical Lab	45 Minutes	Not

DON'T JUST TAKE OUR WORD FOR IT.

We have a network of customers, including some of the world's biggest names cross finance, defense, military, government, and more.

airbnb
citibank
P&G
METROPOLITAN POLICE

Immersive Labs is the world's first human cyber readiness platform.

Our technology delivers challenge-based cybersecurity content developed by experts and powered by the latest threat intelligence. Our unique approach enables businesses to battle-test and evidence their workforce's preparedness to face emerging cyber threats.