Advanced Web Application Penetration Testing with Burp Suite

SETTING UP YOUR BURP SUITE ENVIRONMENT FOR THIS COURSE

Sunny Wear
SECURITY ARCHITECT AND PENETRATION TESTER

@SunnyWear www.sunnywear.org

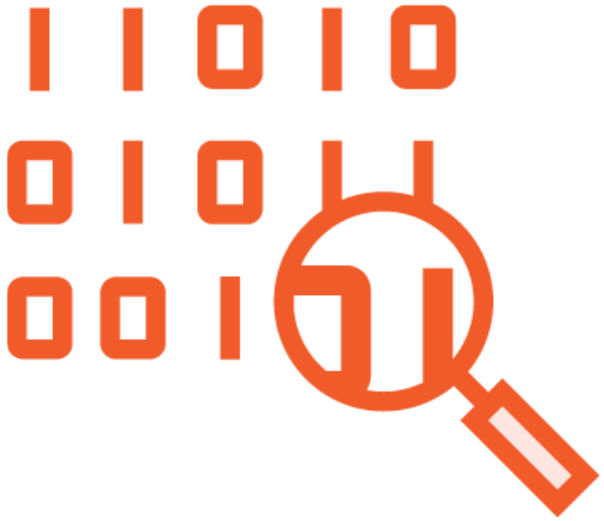
Audience

Who Benefits from This Course?

Pam the Pentester

Dan the Developer

Why That Audience?



Experience finding bugs

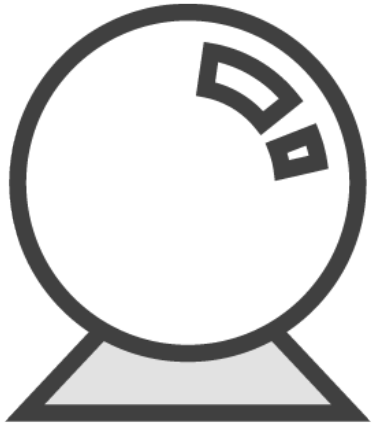
Experience fixing bugs

Rules of Engagement

Pentesting Scenarios

Black box

No knowledge of system



White box

Crystal clear access

Gray box

Authenticated accounts

Scope:

- Web application URLs
- IP Address ranges
- Admin & non-admin
- Database type

Scope: OWASP Juice Shop

Web application URL	http://localhost:3000
IP Address range	localhost
Admin & non-admin	Bob, Admin
Database type	sqlite

OWASP Juice Shop

Information:

https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

Download and Setup:

https://github.com/bkimminich/juice-shop#setup

Demo

Show the OWASP Juice Shop

Free vs. Professional

Burp Suite Product Options

Free	Professional
Most functionality tabs are enabled	All functionality tabs are enabled
Intruder functionality is throttled	No forced throttling
Payloads not available	Portswigger Payloads
Some plugins not available	*Supports Extenders Used in this course
*Burp Clickbandit	*Discover Content
	*CSRF PoC
	*Project File Support

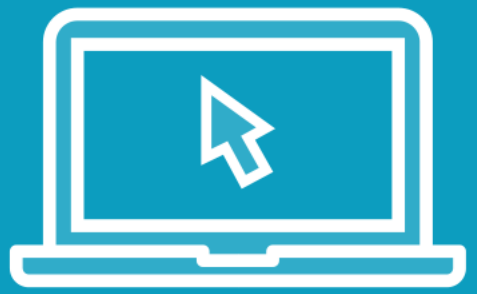
Setting up Your Project File

Let’s get started!

1. Create BurpProjectFiles directory on your home drive
2. Create Project File at Prompt:

   NonAdmin_Juice_Shop.burp

Demo



Starting Burp Suite

Create our project file

Non-admin account first

Option Configurations

Option Settings

Proxy

Spider

Scanner

Demo

Setting our options first

Summary

Environment setup

Project file

Proxy, Spider, and scanner options