Access Web Apps with Burp Suite

Today's Objectives

By the end of class, you will be able to:

- ☐ Configure Burp Suite and Foxy Proxy.
- ☐ Use Burp Repeater to modify and replay requests.
- ☐ Use Burp Intruder to script a series of requests.

OWASP
[The Open Web Application Security Project]

The OWASP Top 10 is an annual list of the year's most significant vulnerabilities.

The OWASP Top 10

Injection: Users "trick" an application into executing commands/code

Broken Authentication: A user's identity is compromised

Sensitive Data Exposure: A user's data is improperly secure (e.g., weak or no encryption is used; etc.)

XML External Entities: A user is able to upload a malicious XML file

Broken Access Control: A user is able to access unauthorized resources

The OWASP Top 10

Security Misconfigurations: Use of weak or default passwords; default scripts; error messages; etc.

Cross-Site Scripting (XSS): A user is able to insert malicious JavaScript into a web page.

Insecure Deserialization: Exploitation of the process by which an application converts a byte stream into an object within the application runtime.

Components with Known Vulnerabilities: Using insecure libraries, components, etc.

Insufficient Logging/Monitoring: Failure to keep adequate logs makes it difficult to detect a breach after it's occurred.

DVWA is an intentionally vulnerable web application, specifically designed to facilitate the study of OWASP Top 10.

Activity: Getting Familiar with OWASP

In this exercise you will research the categories of vulnerabilities featured in the OWASP Top 10.

Instructions sent via Slack.

Times Up! Let's Review.

OWASP

Launching DVWA // Configuring Burp Suite

Introduction to Burp Suite

Burp Suite is a collection of tools used to test web applications.

Detecting vulnerabilities while testing web applications involves:

- Determining how servers process user-submitted data
(to see if you can send a shell command to the server, or if it "cleans" user submissions first)

- Sending large numbers of requests over and over
(to brute-force a login form)

- Encoding/Decoding data in URLs
(to send a complicated exploit through a URL)

Burp Suite Tools

Of the nine tools featured in Burp Suite, we'll focus on the following four:

HTTP Proxy: Intercepts requests from the browsers

Spider: Generates maps of the files and folder of a given site.

Repeater: Edit and re-send a given request, with different parameters each time.

Intruder: Script resending of requests

Activity: Setting Up

In this exercise you will verify and launch your Burp Suite configuration and lab set-up.

Instructions sent via Slack.

Times Up! Let's Review.

Set-Up / Troubleshoot

Proxy
Target and Spider
Repeater
Intruder

Instructor Demonstration
A Tour of Burp Suite

Activity: Site Maps and Spider

In this exercise you will enumerate the files and folders in DVWA with Burp's Target and Spider tools.

Instructions sent via Slack.

Times Up! Let's Review.
Site Maps and Spider

Replaying Requests with Repeater

Cookies and Sessions

Cookies can be used to modify a wbe applications behavior by changing user preferences, etc.

HTTP is stateless: Servers can't "remember" old requests.

Cookies and sessions allow servers to circumvent this limitation.

Cookies store information about the user's web application instance in the browser.

Sessions store information about the user's web application instance on the server.

Fuzzing with Repeater

Pentesting requires testing how a server responds to different kinds of requests to different pages.

Often testers will send the **same request repeatedly**, but change just one or two pieces at a time.

Fuzzing is the process of changing the value of a parameter over a series of requests.

Fuzzing is used to identify potential vulnerabilities in targets.

Repeater and Intruder are common fuzzing tools.

Activity: Replaying Requests with Repeater

In this exercise you will use Burp Repeater to resend requests with different parameters and manipulate cookies to change an application's behavior.

Instructions sent via Slack.

Times Up! Let's Review.

Replaying Requests with Repeater

Burp Intruder

Burp Intruder is the tool used to send a large number of requests programmatically. In the following demo, we'll look at:
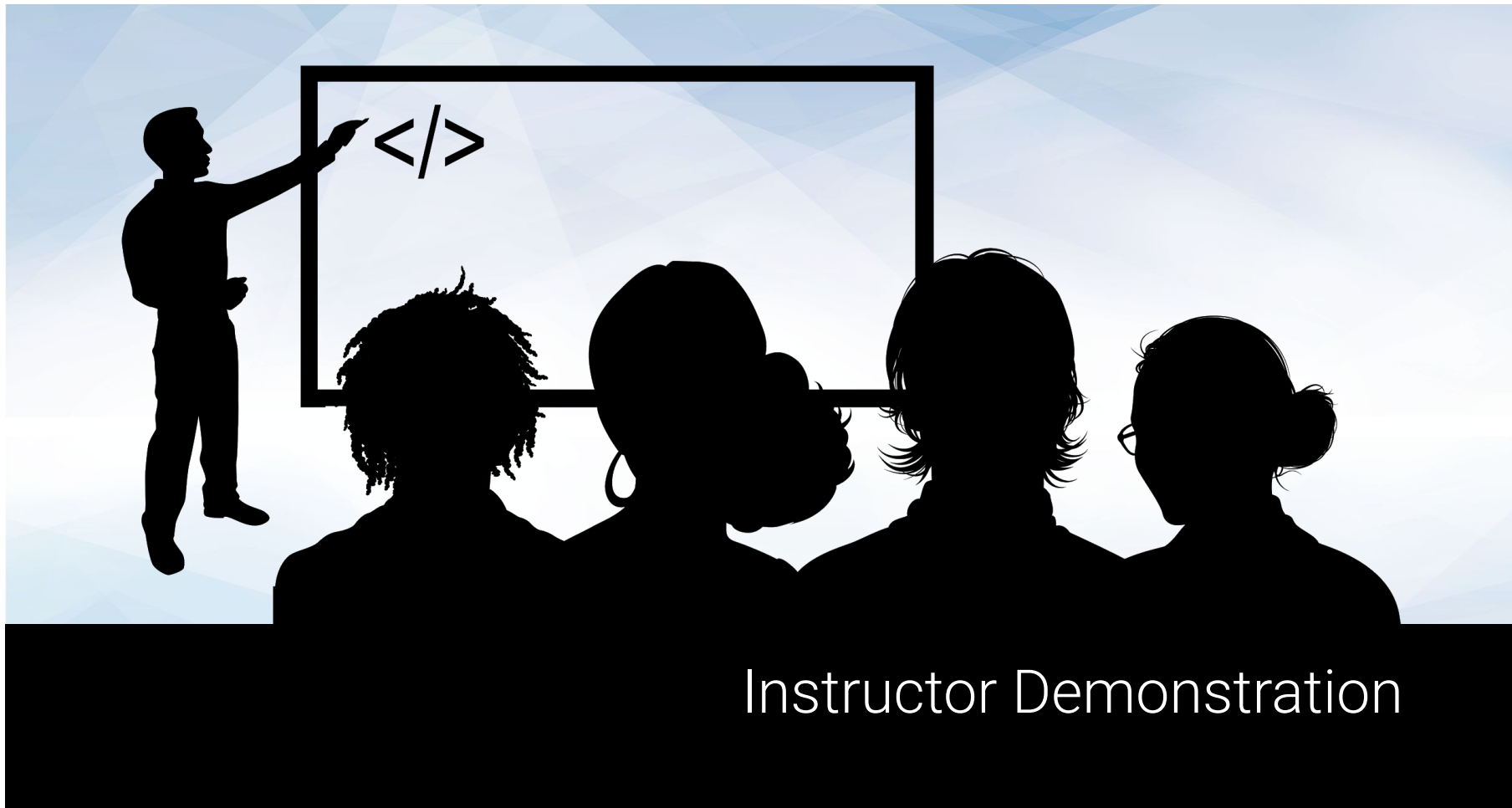
01 Intruder's Target Pane

02 The Positions Tab

03 Payloads

04 Analyzing Results

Instructor Demonstration

Activity: Brute Force Intrusion

In this exercise you will practice scripting request replays with Burp Intruder and launching brute-force attacks against weak login logic.

Instructions sent via Slack.

Times Up! Let's Review.

Brute Force Intrusion

Today's Objectives

By the end of class, you will be able to:

- ☑ Configure Burp Suite and Foxy Proxy.

- ☑ Use Burp Repeater to modify and replay requests.

- ☑ Use Burp Intruder to script a series of requests.