CYBERTECH CLUB @ PSU | CTF WORKSHOP SERIES

MODULE 01

Recon & Web Proxies

Participant Handout • Spring 2026

HOW TO USE THIS HANDOUT

This packet mirrors the live workshop deck and gives you everything needed to study the material async. Each section maps to a slide in the deck.

1. Hook

> SET THE SCENE
>
> **Before any hacker attacks a system, they first gather information quietly.**
>
> Using tools like web proxies, they can see and manipulate every request your browser sends without you noticing.

2. Learning Objectives

By the end of this topic, a student can:

- ☐ Identify reconnaissance techniques used in web security.
- ☐ Use a web proxy to intercept and analyze HTTP requests.
- ☐ Modify requests to test web application behavior.

3. Core Concept

Reconnaissance (Recon)

The process of gathering information about a target before launching an attack. In web security, this includes identifying endpoints, parameters, technologies, and hidden functionalities.

Web Proxy

A middleman between the browser and the server. A web proxy lets attackers or testers intercept, inspect, and modify HTTP and HTTPS requests and responses. Burp Suite is the standard tool for this in the security industry.

Why it matters

Once you can see every request your browser sends, you can change parameters, replay calls, and probe for weak points. A proxy turns a black-box web app into a transparent one.

FIGURE 1: AN INTERCEPTED HTTP REQUEST

```
GET / HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
Accept: text/html,application/xhtml+xml
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Captured in Burp Suite under Proxy → Intercept. Every header and parameter the browser would have sent is visible here, and editable before the request reaches the server.

4. How It Works

The workflow below is the same pattern a pen tester follows on every new engagement.

STEP 01

Perform Reconnaissance

Map the target before you touch it.

- Identify the website structure (pages, admin areas, APIs).
- Discover endpoints (public routes, hidden ones, legacy URLs).
- Collect information about the stack, technologies, and versions.

STEP 02

Configure Web Proxy

Point your browser at Burp.

- Install Burp Suite (Community Edition is fine for the workshop).
- Set the browser proxy to 127.0.0.1:8080.
- Enable interception in the Proxy tab.

STEP 03

Intercept Requests

See exactly what the browser sends.

- Capture HTTP requests as the browser makes them.
- View headers, parameters, cookies, and body.

STEP 04

Modify Requests

Change the request before the server sees it.

- Change parameters (usernames, IDs, flags, pagination values).
- Replay the request to see how the server responds to variants.

STEP 05

Identify Weak Points

Look for where the app breaks.

- Look for vulnerabilities: IDOR, auth bypass, input validation gaps.

5. Demo Walkthrough

Run this end to end on your own machine after the workshop. The live demo follows the same script.

Prerequisites

TOOL	BROWSER	TARGET
Burp Suite	Chrome or Firefox	http://example.com

Step 1: Start Burp Suite

Action. Open Burp Suite and start a Temporary Project.

Expected. Proxy listener running on 127.0.0.1:8080.

Step 2: Configure browser proxy

Action. Set the browser proxy to 127.0.0.1:8080.

Expected. Traffic appears in Proxy → HTTP history.

Step 3: Intercept a request

Action. Turn “Intercept is ON” and open http://example.com.

Expected. Request appears in the Intercept tab.

Step 4: Modify the request

Action. Edit the request before forwarding (change the path or a parameter). Example: change the path to /admin.

Expected. The server responds differently (access denied, different page, or an error).

Example modified request

```
GET /admin HTTP/1.1
Host: example.com
```

Fallback if the live demo fails

- Screenshot of the intercepted HTTP request in Burp Suite (Proxy → Intercept tab), showing request headers and parameters.

- Screenshot of HTTP history (Proxy → HTTP history) demonstrating captured traffic between browser and server.

6. Common Pitfalls

When something does not work, check these first before asking for help.

SYMPTOM

No traffic in Burp Suite

Cause: Browser proxy is not configured correctly.

Fix: Set proxy to 127.0.0.1:8080 in browser settings.

SYMPTOM

HTTPS websites do not load

Cause: Burp certificate is not installed.

Fix: Install and trust the Burp CA certificate in the browser.

SYMPTOM

Requests are not being intercepted

Cause: Intercept option is turned off.

Fix: Turn “Intercept is ON” in Burp Suite.

SYMPTOM

Modified request has no effect

Cause: Incorrect parameter or format.

Fix: Double-check parameter names and values before sending.

7. Your Challenge

15 – 20 MIN **BEGINNER**

THE TASK

Use Burp Suite to intercept a login request from a website and modify the username or a parameter before sending it to the server.

SUCCESS CRITERION

Submit a screenshot showing the intercepted request and the modified response from the server.

Hints

1. Make sure interception is turned on.
2. Look for POST requests when logging in.
3. Modify a parameter before clicking Forward.

8. Cheatsheet

Keep this page next to you while you practice. Commands, payloads, and shortcuts only, no prose.

COMMAND / PAYLOAD	WHAT IT DOES	WHEN TO USE
`Intercept ON`	Stops the request before it is sent to the server.	When you want to modify a request.
`Forward`	Sends the request (modified or not) to the server.	To continue the normal flow.
`Repeater`	Resend and test a request with variations.	Testing changes without re-triggering the browser.
`HTTP History`	Shows all traffic that has passed through Burp.	Analysis and finding past requests.
`127.0.0.1:8080`	The default Burp proxy listener address.	Configure this in the browser proxy settings.

Sample HTTP request (memorize the shape)

```
GET / HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
Accept: text/html,application/xhtml+xml
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

9. Further Reading

Go deeper on your own time with these three resources.

01

OWASP Web Security Testing Guide

Official, detailed methodologies for testing web application security, including reconnaissance techniques.

https://owasp.org/www-project-web-security-testing-guide/

02

Burp Suite Documentation

Official guide explaining how to use Burp Suite features like proxy, intercept, repeater, and request analysis.

https://portswigger.net/burp/documentation

03

PortSwigger Web Security Academy

Interactive labs and real-world scenarios to practice web proxy usage and web security testing skills.

https://portswigger.net/web-security