CYBERTECH

MODULE 01 | CTF WORKSHOP SERIES

Recon & Web Proxies

THE HOOK

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.

CyberTech Club @ PSU

Spring 2026 | CTF Workshop Series

SECTION 02

Learning Objectives

By the end of this topic, a student can:

01

Identify

reconnaissance techniques used in web security.

02

Use a web proxy

to intercept and analyze HTTP requests.

03

Modify requests

to test web application behavior.

SECTION 03

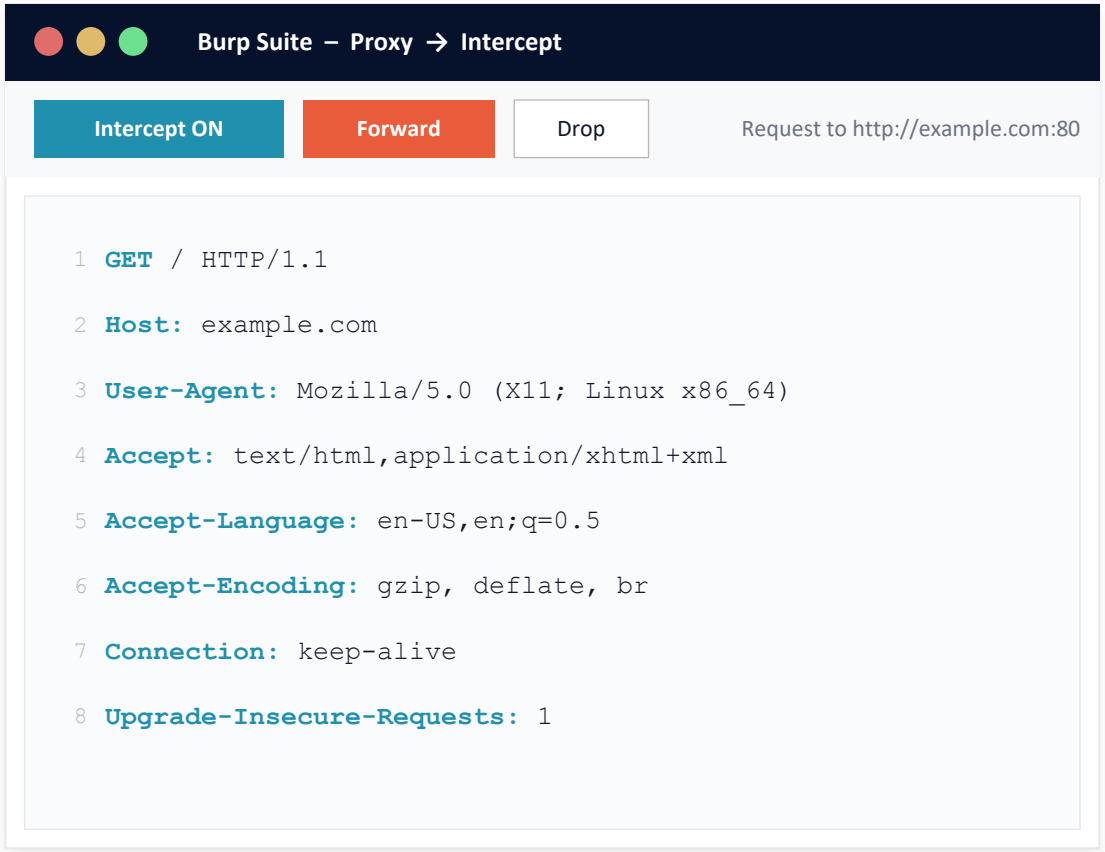
Core Concept

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 that lets attackers or testers intercept, inspect, and modify HTTP/HTTPS requests and responses. Burp Suite is the standard tool.



Intercepted HTTP request in Burp Suite showing how the browser communicates with the server.

SECTION 04 | STEP 01 OF 05

How It Works

STEP

01

Perform Reconnaissance

Map the target before you touch it.

- Identify website structure
- Discover endpoints
- Collect information

SECTION 04 | STEP 02 OF 05

How It Works

Configure Web Proxy

Point your browser at Burp.

- Install Burp Suite
- Set proxy to 127.0.0.1:8080
- Enable interception

SECTION 04 | STEP 03 OF 05

How It Works

STEP

03

Intercept Requests

See exactly what the browser sends.

- Capture HTTP requests
- View headers and parameters

SECTION 04 | STEP 04 OF 05

How It Works

STEP

04

Modify Requests

Change the request before the server sees it.

- Change parameters
- Replay the request

SECTION 04 | STEP 05 OF 05

How It Works

Identify Weak Points

Look for where the app breaks.

- Look for vulnerabilities

SECTION 05 | LIVE

DEMO.

Intercept and modify a request to example.com

Follow along on your laptop. We will run through this together.

PREREQUISITES

TOOL

Burp Suite

BROWSER

Chrome or Firefox

TARGET

http://example.com

SECTION 06

Common Pitfalls

When something does not work, check these first.

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

SECTION 07

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

01

Make sure interception is turned on.

02

Look for POST requests when logging in.

03

Modify a parameter before clicking Forward.

SECTION 08

Go Deeper

01

OWASP Web Security Testing Guide

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

02

Burp Suite Documentation

Official guide for Burp Suite features: proxy, intercept, repeater, and request analysis.

03

PortSwigger Web Security Academy

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

Questions?

Bring them to the CTF group