



Lecture 24 – Burp Suite (Web Application Penetration Testing)

◆ What is Burp Suite?

Burp Suite is a professional tool used for **web application penetration testing**. It allows ethical hackers or testers to find vulnerabilities like:

- **SQL Injection**
- **Cross-Site Scripting (XSS)**
- **Password Attacks**
- **Session Hijacking**
- **Brute Force Attacks**

Burp Suite acts as a **proxy** between your browser and the target web server. It captures all requests and responses so you can analyze, modify, and resend them for testing security.

◆ Purpose of Burp Suite

Burp Suite helps:

1. Detect vulnerabilities before hackers exploit them.
 2. Analyze how web requests and responses behave.
 3. Automate attacks using built-in tools like **Intruder**, **Repeater**, and **Sequencer**.
 4. Test login forms, cookies, headers, and session tokens safely.
-

◆ HTTP and HTTPS Overview

◆ HTTP (Hypertext Transfer Protocol)

- Used to **transfer data** between a web client (browser) and a web server.
- **Default port:** 80

- **Stateless protocol** → Every request is independent; it does not remember the previous request.

◆ **HTTPS (Hypertext Transfer Protocol Secure)**

- Secure version of HTTP.
 - Uses **SSL/TLS encryption**.
 - **Default port:** 443
 - Provides **confidentiality and integrity** of data during transmission.
-

◆ **Common HTTP Methods**

Method	Function	Example
GET	Request data from the server	Viewing a web page
POST	Send data to the server	Submitting a login form
PUT	Update existing data	Editing profile info
DELETE	Remove data from the server	Deleting user account

◆ **HTTP Response Codes**

Code Range	Type	Description
100–199	Informational	Request is being processed
200–299	Success	Example: 200 OK – Request completed successfully
300–399	Redirection	Example: 301 – Page moved permanently
400–499	Client Error	Example: 400 – Bad request, 401 – Unauthorized, 403 – Forbidden, 404 – Not Found, 408 – Request Timeout
500–599	Server Error	Example: 500 – Internal server error

◆ Starting Burp Suite in Kali Linux

Run this command in terminal:

```
sudo burpsuite
```

Then open your browser and configure the proxy settings.

◆ Setting Up Proxy in Browser

1. Go to **Settings → Search "Proxy" → Manual Configuration**
2. Enter the following:
 - **Address:** 127.0.0.1 (Loopback address)
 - **Port:** 8080
3. Click **OK**

✳ Loopback Address (127.0.0.1):

It refers to your **own system**. Any request sent here will not leave your computer — it's used for local testing.

◆ Proxy and Intercept Feature

After opening Burp Suite:

- Go to **Proxy → Intercept → Turn Intercept ON**
- Open any login form (username & password fields).
- Fill details but **don't click login yet**.
- Turn ON intercept → now click **Login**.
- The request will appear in Burp Suite under **Intercept tab**.

From here, you can:

- **Send to Repeater** (for manual testing)
 - **Send to Intruder** (for automated attack)
-

◆ Repeater (Manual Testing Tool)

The **Repeater** tab is used to test different inputs manually.

Example:

Suppose you capture the login request for a website:

1. Send it to **Repeater**.
2. Try multiple username/password combinations manually.
3. Observe the **response code**:
 - 200 OK → Successful login
 - 302 Found or “Invalid credentials” → Failed login

 **Repeater helps test without reloading the real website every time.**

◆ Intercept Working (Step-by-Step)

1. Go to a login page.
 2. Turn ON intercept in Burp Suite.
 3. Enter credentials and click **Login**.
 4. The request will be captured by Burp before reaching the server.
 5. You can **right-click** → **Send to Repeater or Intruder** to analyze or attack.
-

◆ Intruder (Automated Attack Tool)

Intruder is used for **automating password and input testing**.
It performs **brute-force and dictionary attacks**.

Steps:

1. Capture the login request using Intercept.
2. Send it to **Intruder**.
3. Click **Clear** to remove all preselected parameters.
4. Highlight the username and password fields → click **Add**.

5. Select **Attack Type** → choose the type of attack (explained below).
 6. Load **wordlists (payloads)**.
 7. Click **Start Attack**.
-

◆ **Types of Intruder Attacks**

Type	Description	Use Case
1. Sniper	Attacks one parameter at a time using one payload list.	When you know username and want to test passwords.
2. Battering Ram	Uses one wordlist for all parameters.	When same value needs to be tested in multiple fields.
3. Pitchfork	Tests multiple parameters at the same time using equal-sized lists.	Example: username & password together.
4. Cluster Bomb	Combines multiple payload sets and tests all possible combinations.	Ideal for brute-force username/password testing.

Understanding the Attack Results

After you start the attack:

- Each attempt will show:
 - **Status code**
 - **Response length**

If one result has a **different response length** (e.g., 228 instead of 128), that usually means the **correct credentials** were found.

◆ **How to Create a Wordlist (Dictionary)**

A **wordlist** is a text file containing potential usernames or passwords used in brute-force attacks.

1. Manual Wordlist

Create a .txt file with sample entries:

admin

user

root

password

123456

2. Using Crunch Tool (Kali Linux)

Generates all possible combinations:

crunch 4 6 abcdef123 > wordlist.txt

- ➡ Creates words of length 4 to 6 using letters a-f and numbers 1–3.

3. Using Cewl Tool

Extracts keywords from a target website:

cewl https://example.com -w wordlist.txt

4. Using Pre-Built Wordlists

Use already available wordlists like:

/usr/share/wordlists/rockyou.txt

(pre-installed in Kali Linux)

- ◆ **Sequencer (Testing Session ID Strength)**

- ✿ **What is a Session ID?**

A **session ID** is a unique token generated each time a user logs in.
It helps identify the user's session on the server.

Example:

SessionID=AB12CD34EF56

◆ **Steps to Test Session Strength:**

1. Capture any login request that contains a session ID.
2. Right-click → **Send to Sequencer**.
3. Click **Start Live Capture** → Burp Suite will generate many session tokens.
4. After collecting tokens → click **Stop** → then **Analyze Now**.

Burp Suite will show:

- **Randomness in bits** (called *entropy*).
 - A good session ID should have **128 bits or more entropy**.
-

◆ **Interpretation:**

Bits of Randomness Strength

< 100 bits Weak session ID (easy to predict)

≥ 128 bits Strong session ID (secure)

If a session ID is weak, it can be guessed or reused by attackers — allowing login without credentials.

◆ **Save Tokens Option**

- After capturing, you can use **Save Tokens** in Sequencer to export all collected session IDs.
 - It helps analyze randomness manually later.
-

◆ **Important Notes**

- Burp Suite does **not send requests to the real server** unless you forward them manually.
- All testing (repeater/intruder) happens **within the tool**.
- Always perform testing **ethically** and **with permission**.

- Most **college websites** or small organizations have **poor randomness** and weak session IDs.
-

Summary Table

Component Function

Proxy Captures and modifies requests between browser and server

Repeater Manually modify and resend requests

Intruder Perform brute-force or dictionary attacks

Sequencer Analyze session token randomness

Wordlist List of usernames/passwords used in brute-force attacks

Conclusion

Burp Suite is an essential tool for ethical hackers and cybersecurity professionals.

It provides all-in-one modules to:

- Intercept requests
- Modify parameters
- Test login security
- Analyze session IDs
- Detect vulnerabilities

It is widely used in **penetration testing**, **bug bounty**, and **web security analysis**.