

🔥 Day 6: Burp Suite और Traffic Interception – पूरा हिंदी में

🌀 Burp Suite क्या है?

Burp Suite एक पावरफुल ethical hacking टूल है जिसका इस्तेमाल web applications की vulnerabilities (कमज़ोरियाँ) निकालने के लिए किया जाता है। यह web traffic को intercept करके modify करने देता है।

◇ Burp Suite से आप:

- वेबसाइट के login system को test कर सकते हो
- Cookies और Sessions को capture कर सकते हो
- Hidden URLs और forms निकाल सकते हो
- XSS, SQLi, CSRF जैसे attacks को perform कर सकते हो

💻 Burp Suite कैसे install करें?

☑ Kali Linux में:

```
sudo apt update
sudo apt install burpsuite
```

☑ Windows/Linux में:

Download करें: 🔗 <https://portswigger.net/burp>

🌐 Browser को Burp के साथ Connect करना

☑ Step 1: Proxy सेटअप करें

- Burp Suite खोलो → Proxy → Options
- Default Proxy: 127.0.0.1 : 8080

☑ Step 2: Browser में Proxy सेट करें

- Firefox → Settings → Manual Proxy:

```
HTTP Proxy: 127.0.0.1
Port: 8080
```

- ☑ "Use this proxy for all protocols" पर टिक करें

HTTPS Sites Intercept करने के लिए Certificate Install करें

कैसे करें:

- Browser में जाओ: <http://burp>
- "CA Certificate" डाउनलोड करो
- Firefox → Settings → Certificates → Import
- इसे "Trusted Root CA" में Add करो

Burp से Traffic Intercept कैसे करें?

Step-by-Step:

1. Burp Suite खोलो → Proxy → Intercept → Intercept ON करो
2. अब browser में कोई site खोलो (<http://testphp.vulnweb.com>)
3. Burp उस request को पकड़ लेगा
4. Request को देखो, edit करो, या forward करो

Request को Modify करना

Example:

```
POST /login.php HTTP/1.1
Host: testphp.vulnweb.com
username=admin&password=1234
```

- Admin को बदलो → `admin' OR '1'='1`
- इसे **Repeater** में भेजो और Response चेक करो

Repeater Tab क्या करता है?

- Intercept की गई request को Right-click → "Send to Repeater"
- Repeater tab में जाकर:
 - Request modify करो
 - "Send" दबाओ
 - Response देखो

Cookies और Session ID चेक करना

Headers में देखो:

```
Cookie: PHPSESSID=abcd123
```

Try:

- Cookie delete करके logout चेक करो
- किसी और की session ID लगाओ (lab environment में)

💡 Burp Suite के Tabs और उनके काम

Tab	काम
Proxy	Live traffic intercept करता है
Target	Site structure दिखाता है
Repeater	Requests modify करके बार-बार भेज सकते हो
Decoder	Payloads को encode/decode करना
Intruder	Brute force या fuzzing करना
Logger	सारे HTTP logs देख सकते हो

🧐 Burp Practical – Real Practice

☑ Target Site:

<http://testphp.vulnweb.com>

Try These:

- Login request पकड़ो
- Username/password बदलो
- Burp से SQLi payload भेजो
- Cookie modify करके session hijack try करो
- HTML form को fuzz करो Intruder से

📋 Cheat Sheet – Burp Shortcut Guide

Action	Shortcut
Intercept On/Off	Proxy → Intercept Tab
Request को modify करना	Repeater में भेजो
Cookie change करना	Headers edit करो
Brute Force	Intruder में Payloads लगाओ
Traffic log देखना	HTTP History / Logger

📄 Summary




Tool	काम
Burp Proxy	Request पकड़ता है
Repeater	Response analyze करता है
Cookie	Session test करने में उपयोग
Certificate	HTTPS decrypt करने में ज़रूरी
Test Site	http://testphp.vulnweb.com

Recommended Labs for Practice:

Lab	Link
DVWA	http://127.0.0.1/DVWA
bWAPP	GitHub पर Available
WebGoat	https://owasp.org/www-project-webgoat/
TryHackMe	"Burp Suite: The Basics" Room

Practice Checklist

- ☐ DevTools में cookies और headers analyze करो
- ☐ Burp से Intercept करके POST request modify करो
- ☐ Session cookie को edit करो
- ☐ SQLi payloads try करो
- ☐ Burp Repeater से response compare करो

 **Save this file as:** `day6_burp_suite.md`  Open in any markdown editor like VS Code or Obsidian 
Use with Kali Linux or test labs like DVWA/WebGoat