6.C. Using Burp Suite to Inspect and Modify Traffic between Browser and Target Application

---

Aim

To intercept, inspect, and modify HTTP/HTTPS traffic using **Burp Suite**.

Tools / Software Used

- Burp Suite
- Web Browser (Chrome / Firefox)

Theory

Burp Suite is a web vulnerability testing tool that acts as a proxy between the browser and web application. It allows interception and modification of requests and responses.

Steps / Procedure

1. Open **Burp Suite**.
2. Go to **Proxy → Intercept**.
3. Turn **Intercept ON**.
4. Open web browser.
5. Configure browser proxy:
    - IP: `127.0.0.1`
    - Port: `8080`
6. Visit any website in browser.
7. HTTP request is intercepted in Burp Suite.
8. Modify request parameters if required.
9. Click **Forward** to send modified request.
10. Observe server response.

Result

Traffic between browser and target application was successfully intercepted and modified using Burp Suite.

⚠ Counter Measures

- User awareness training
- Use CAPTCHA and rate limiting
- Web Application Firewall (WAF)
- DDoS protection services

✅ Overall Result

Thus, social engineering attacks, DDoS attack simulations, and traffic interception were successfully performed using SET, HOIC, LOIC, HULK, and Burp Suite.

🎤 Viva-Ready Line

“Social engineering exploits human trust, while DDoS attacks target system availability.”