Day 14

Topic: Web Application Attacks

Objective: To understand the architecture of web apps and the OWASP Top 10 security risks.

Theoretical Concepts:
Web applications are the most common attack vector today. We studied the HTTP request/response cycle in depth using **Burp Suite**. We reviewed the OWASP Top 10 list, focusing on Broken Access Control, Injection, and Security Misconfiguration.

Practical Work:
We configured our browser to route traffic through Burp Suite (Proxy). We intercepted requests and modified parameters on the fly before sending them to the server. We performed a "Parameter Tampering" attack, changing the price of an item in a shopping cart from $100 to $1 before checkout. We also used OWASP ZAP to crawl the application structure.

Tools Used: Burp Suite (Community), OWASP ZAP.

Outcome: Understanding how to intercept and manipulate web traffic to bypass client-side controls.