Day 16

Topic: XSS and CSRF

Objective: To study Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF).

Theoretical Concepts:
XSS allows attackers to inject malicious JavaScript into web pages viewed by other users. We differentiated between Stored XSS (persistent), Reflected XSS (non-persistent), and DOM-based XSS. CSRF forces an end user to execute unwanted actions on a web application in which they are currently authenticated.

Practical Work:
On the lab application: 1. Reflected XSS: We input a script *<script>alert('Hacked')</script>* into a search box, causing a popup to appear. 2. Stored XSS: We posted a comment containing a script that stole the session cookie of anyone who viewed the comment section. 3. We analyzed the HTTP headers to see how "SameSite" cookie attributes help prevent CSRF.

Tools Used: Burp Suite, Browser DevTools.

Outcome: Understanding how client-side scripts can be weaponized to steal sessions.