Day 146

Topic: Session Hijacking

Objective: To take over a valid user session to gain unauthorized access without knowing the password.

Theoretical Concepts:
Session Hijacking relies on stealing a valid Session ID (cookie). We discussed methods: XSS, Packet Sniffing (Session Side-Jacking), and Session Fixation. We learned about the importance of the "Secure" and "HttpOnly" flags on cookies.

Practical Work:
Using the XSS vulnerability found in the previous session, we stole a session cookie. We then used a browser extension (Cookie Editor) to inject this stolen cookie into our browser. Upon refreshing the page, we were logged in as the victim user without ever entering a username or password.

Tools Used: Burp Suite, Ettercap, Cookie Editor.

Outcome: Demonstrated how session management flaws allow for account takeover.