CYBERSECURITY DAILY DIARY

DAY-25
DATE- 17 July, 2025

Topics Covered:

- Authentication & session testing: inspect cookies, modify session tokens, and test for weaknesses.

What I Did Today

Inspecting Cookies Using Burp Suite's Proxy and Repeater, I intercepted login responses and examined `Set-Cookie` headers.

- Saw session identifiers like `JSESSIONID`, `PHPSESSID`, and custom tokens.
- Noted attributes like `HttpOnly`, `Secure`, and `SameSite` — crucial for preventing XSS and CSRF attacks.
- Realized how cookie scope (domain/path) affects access and persistence.

Modifying Session Tokens Sent authenticated requests to Repeater and manually altered session tokens.

- Changing a valid token to a random string triggered `401 Unauthorized` — confirming token validation.
- Tried session fixation by injecting a known token before login — some apps accepted it, revealing a potential flaw.
- Learned that predictable or weak tokens (e.g., sequential IDs) are vulnerable to brute-force or replay attacks.

Testing for Weaknesses

- Checked if tokens expired properly after logout — some didn't, allowing reuse.
- Verified if session timeout was enforced — idle sessions stayed active too long.
- Explored token reuse across accounts — tested horizontal privilege escalation by swapping tokens between users.

Reflections

- Authentication isn't just about logging in — it's about how identity is maintained and protected.
- Session management is a fragile bridge — one misconfigured cookie or token can expose the entire app.
- Felt empowered seeing how small tweaks in Burp revealed deep flaws — like peeling layers off a security onion.