CYBERSECURITY DAILY DIARY

DAY-22
DATE- 14 July, 2025

Topics Covered:

- Install Burp Suite Community and configure browser proxy to intercept traffic.

What I Did Today

Installing Burp Suite Community Edition was straightforward using the official `.sh` installer or via package manager (like `snap install burpsuite`). The Community version is free and powerful enough for manual web app testing.

Configuring the browser proxy is key to intercepting traffic:

- Burp listens on `127.0.0.1:8080` by default.
- I set my browser (Firefox) to use a manual proxy: HTTP and HTTPS both pointed to `127.0.0.1:8080`.
- Installed Burp's CA certificate to avoid SSL/TLS warnings and decrypt HTTPS traffic — this allowed full visibility into encrypted requests and responses.

Intercepting traffic felt like peeking behind the curtain:

- Saw raw HTTP headers, cookies, query strings, and form data.
- Paused requests mid-flight, modified parameters, and forwarded them — powerful for testing input validation and authentication flows.
- Realized how many background requests modern websites make — analytics, tracking, and third-party APIs all show up.

Reflections:

- Burp Suite feels like a control room for web traffic — every click in the browser becomes a packet you can inspect and manipulate.
- The proxy setup taught me how browsers communicate under the hood — and how fragile security can be without proper validation.
- Grateful for the clarity this tool brings — it's like Wireshark for the application layer.