CYBERSECURITY DAILY DIARY

DAY-23
DATE- 15 July, 2025

Topics Covered:

- Burp basics: proxy interception, Repeater usage, modifying and replaying requests.

What I Did Today

Proxy Interception Burp Suite's proxy acts as a middleman between the browser and the web server. Once configured (usually `127.0.0.1:8080`), it captures every HTTP/S request the browser sends.

- I intercepted login forms, search queries, and even background API calls.
- I learned to toggle "Intercept On/Off" to control flow — keeping it on lets me pause and inspect each request before it reaches the server.

Repeater Usage Repeater is Burp's manual testing playground.

- I sent intercepted requests to Repeater and modified headers, parameters, and payloads.
- Replaying requests helped me test how the server responds to different inputs — like changing a `user_id`, tweaking a `cookie`, or injecting test strings.
- Saw how response codes and body content changed — useful for identifying input validation and authentication logic.

Modifying and Replaying Requests

- Realized how easy it is to manipulate client-side data before it hits the server.
- Replayed a POST request with altered form data and observed how the server handled it — sometimes accepting, sometimes rejecting.
- This reinforced how critical server-side validation is — client-side controls can be bypassed entirely.

Reflections

- Burp Suite feels like a scalpel for web traffic — precise, powerful, and revealing.
- Watching requests unfold and tweaking them gave me a deeper appreciation for how fragile web security can be.
- Grateful for tools like Repeater — they turn passive observation into active testing.