CYBERSECURITY DAILY DIARY

DAY-24
DATE- 16 July, 2025

Topics Covered:

- Intruder & BApp exploration: basic fuzzing with Intruder and experiment with extensions.

What I Did Today

Intruder Basics Intruder is Burp Suite's automated attack module — perfect for fuzzing input fields, testing for weak credentials, or probing for injection points.

- I captured a login POST request and sent it to Intruder.
- Set the payload position on the `username` field and used a simple wordlist.
- Ran a **Sniper** attack to test one input at a time — saw how response lengths and status codes varied with different usernames.
- Learned that **Battering Ram**, **Pitchfork**, and **Cluster Bomb** offer more complex multi-field fuzzing strategies.

BApp Store Exploration Burp's built-in extension store (BApp Store) offers powerful add-ons.

- Installed **Logger++** to get better visibility into requests/responses.
- Tried **Active Scan++** for deeper vulnerability detection (though limited in Community Edition).
- Explored **Hackvertor** — useful for encoding/decoding payloads and transforming data on the fly.

Reflections

- Intruder taught me how small changes in input can reveal big gaps in validation.
- Extensions expand Burp's capabilities — even in the Community Edition, they add serious value.
- Felt like I was building my own toolkit — customizing Burp to match my workflow and curiosity.