CYBERSECURITY DAILY DIARY

DAY-28
DATE- 20 July, 2025

Topics Covered:

- Weekly review & documentation: capture screenshots, write vulnerability descriptions and remediation.

What I Did Today

Capturing Screenshots

- Used tools like the browser's built-in screenshot feature and `gnome-screenshot` to capture key moments: intercepted requests, XSS payloads triggering alerts, and Burp Suite Repeater responses.
- Learned to annotate screenshots with arrows and highlights using tools like Flameshot — made reports clearer and more professional.
- Realized the importance of naming files descriptively (e.g., `dvwa_xss_reflected_alert.png`) for easy reference in documentation.

Writing Vulnerability Descriptions

- Followed a structured format:
  - **Title**: Clear and concise (e.g., *Reflected XSS in Search Parameter*)
  - **Description**: What the issue is, where it occurs, and how it was discovered
  - **Impact**: What an attacker could do (e.g., steal cookies, deface UI)
  - **Steps to Reproduce**: Step-by-step with payloads and screenshots
- Practiced writing in a tone that's technical but accessible — useful for both devs and stakeholders.

Remediation Guidance

- Suggested fixes tailored to each issue:
  - For XSS: Use output encoding libraries (e.g., OWASP ESAPI), validate input, apply Content Security Policy (CSP)
  - For session issues: Regenerate tokens on login, set `HttpOnly` and `Secure` flags, enforce timeouts
  - For weak authentication: Implement rate limiting, strong password policies, and MFA
- Learned to cite OWASP recommendations and link to relevant documentation — adds credibility and clarity.

Reflections

- Documentation isn’t just a chore — it’s how you translate technical insight into actionable change.
- Screenshots tell a story; clear writing makes it stick.
- Grateful for the discipline of weekly reviews — they turn scattered notes into a portfolio of progress.