DAY 7 TASK 7 – WEB APPLICATION VULNERABILITY TESTING

Tools Used :

- Burp suite community edition
- OWASP juice shop (vulnerable website)
- Docker
- Web Browser (Firefox)

Ive understood the common web application vulnerabilities and performed basic vulnerability testing using burpsuite.

ENVIRONMENT SETUP:

- Installed docker
- Deployed OWASP Juice Shop locally
- Installed Burp suite community edition.
- Configured browser proxy to route traffic (127.0.0.1 : 8080)
- Enabled burp suite intercept on to capture HTTP requests
  It stops every request and shows it to us,
  The browser waits for us to forward or drop the request.

SQL Injection:

Used ‘OR 1=1— request to the server and bypass

It logs in as admin account

Vulnerabilities Identified:

- SQL injection
- Cross-Site Scripting(XSS)

Prevention:

Sanitize user inputs

Use CSP (Content security Policy)

Disable inline Js

Use HTTPOnly and secure flags for cookies