Ethical Hacking Report
By Rida Mudassar
DHC-377

1. Test Target:

- Application: OWASP Juice Shop (running locally on `http://localhost:3000`)
- Tools Used: Burp Suite, Browser Developer Tools

2. Vulnerability 1 – SQL Injection

- Test Endpoint:
  `GET /rest/products/search?q=`
- Payload Used:
  `' OR 1=1--`
- Observation:
  Products were returned even with broken SQL logic, indicating a possible SQL injection vulnerability.
- Conclusion:
  The application was vulnerable to basic SQL injection in the product search field.

3. Vulnerability 2 – Cross-Site Request Forgery (CSRF)

- Test Endpoint:
  `GET /rest/user/change-password`

- Test Performed:
  Tried sending a CSRF attack via a crafted HTML page using an `<img>` tag.

- Observation:
  The password did not change. Login failed with new password.

- Conclusion:
  CSRF protection was present on this endpoint. The attack was blocked.

Security Fixes for SQLi and CSRF Implemented in the Code

Security Fixes for SQLi and CSRF

- SQL Injection Fix:
  This vulnerability was already mitigated earlier during Week 1–3 tasks by using parameterized queries in the backend code.

- CSRF Fix:
  CSRF protection is already implemented in the Juice Shop application. No changes were made in this task.

- No new fixes were required as both issues were already handled in the existing codebase.