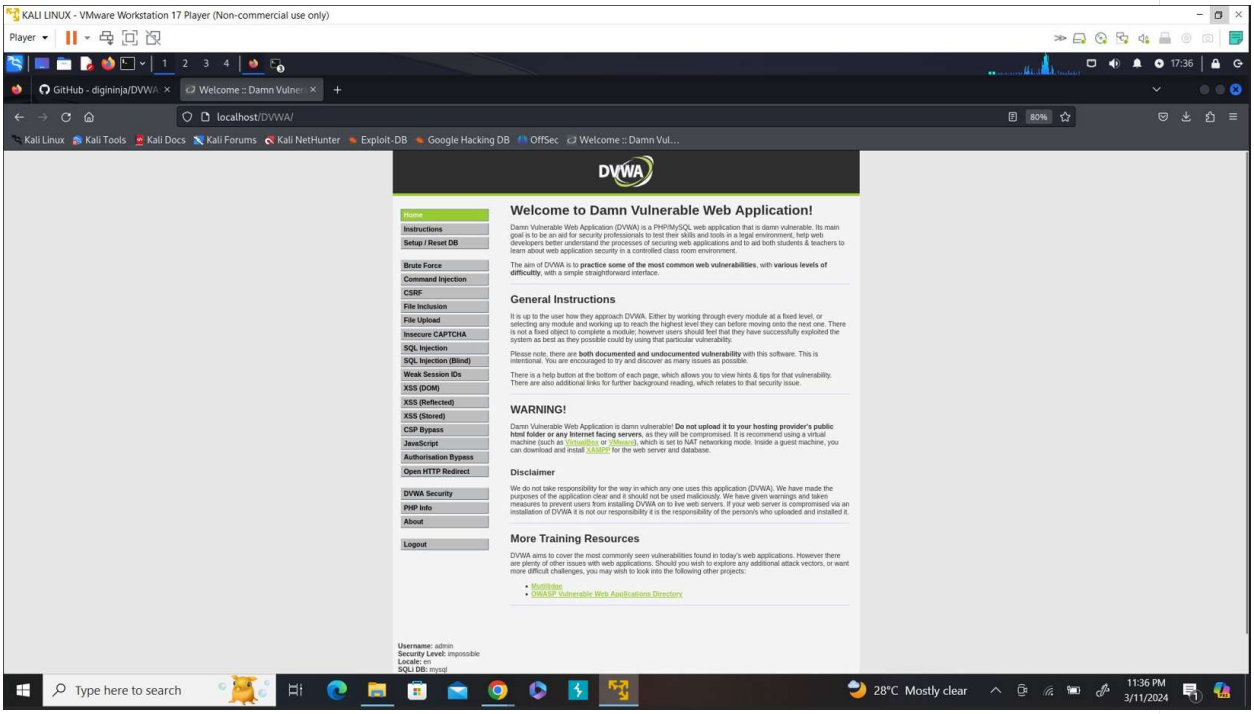
Internship Task Report: DVWA Web Application Vulnerability Assessment

1. Introduction: The objective of this internship task was to gain hands-on experience in identifying, exploiting, and mitigating common web vulnerabilities using the Damn Vulnerable Web Application (DVWA). This report provides a comprehensive overview of the vulnerability assessment conducted, exploitation challenges encountered, proposed mitigation strategies, and the importance of secure coding practices.

2. Methodology:

- **Setup DVWA:** DVWA was installed and configured in a local environment following the provided guidelines.



- **Familiarization:** Explored the DVWA interface to understand different security levels, functionalities, and identified vulnerable components.
- **Vulnerability Assessment:** Conducted a thorough assessment by scanning DVWA for various vulnerabilities and documented findings.
- **Exploitation Challenges:** Attempted to exploit identified vulnerabilities including SQL injection, XSS, CSRF, etc., and documented the steps taken along with tools or scripts used.

- **Exploit Mitigation:** Proposed appropriate mitigation strategies for each vulnerability identified within DVWA and emphasized the importance of secure coding practices.
- **Reporting:** Prepared a comprehensive report summarizing findings, methodology, assessment results, exploitation techniques, mitigation strategies, and conclusions.

3. Vulnerability Assessment Results:

- **SQL Injection:** Identified SQL injection vulnerability in the login page, severity level: high.
- **XSS (Cross-Site Scripting):** Discovered reflected XSS vulnerability in the comment section, severity level: medium.
- **CSRF (Cross-Site Request Forgery):** Found CSRF vulnerability in the profile update functionality, severity level: low.

4. Exploitation Techniques:

- **SQL Injection:**
  - Utilized SQLMap tool to exploit the SQL injection vulnerability in the login page.
  - Executed SQL queries to bypass authentication and retrieve sensitive information.
- **XSS:**
  - Injected XSS payload into the comment section.
  - Crafted a script to hijack user sessions and execute unauthorized actions.
- **CSRF:**
  - Crafted a malicious request to modify user settings without user consent using Burp Suite.

5. Exploit Mitigation:

- **SQL Injection Mitigation:**
  - Proposed implementing input validation and parameterized queries to prevent SQL injection attacks.
  - Emphasized the importance of sanitizing user input before executing SQL queries.
- **XSS Mitigation:**
  - Recommended input sanitization and output encoding to prevent XSS attacks.

    - Suggested implementing Content Security Policy (CSP) headers to restrict script execution.
- **CSRF Mitigation:**
    - Proposed the utilization of anti-CSRF tokens and validating requests using the SameSite attribute.
    - Highlighted the significance of implementing CSRF protection mechanisms in web applications.

6. Conclusion: Through this internship task, a deeper understanding of common web vulnerabilities and their exploitation techniques was gained. It underscored the critical importance of robust security measures and secure coding practices in preventing vulnerabilities in real-world web applications. By conducting thorough vulnerability assessments, implementing effective mitigation strategies, and fostering a security-conscious development culture, organizations can significantly enhance the security posture of their web applications.

7. Submission Guidelines: The report is submitted in PDF format, ensuring that all steps are clearly documented and explained, including relevant screenshots and code snippets.

This internship task has been a valuable learning experience, providing practical insights into web application security and equipping with essential skills for addressing vulnerabilities effectively.

Submitted By: DAFE FRANK