Report Title: Low-Level SQL Injection Test Report on DVWA

Objective:

To assess the susceptibility of DVWA to low-level SQL injection attacks and analyze the impact on its security.

Test Environment:

Application: DVWA v1.10

Tools Used: Nessus SQL Injection plugins, manual SQL injection techniques

Testing Duration: [Duration of Testing]

Methodology:

1. Initial Analysis: Identified target pages/forms susceptible to SQL injection.
2. Injection Attempts: Executed various SQL injection techniques on vulnerable parameters.
3. Data Retrieval: Attempted to retrieve sensitive data through injections.
4. Impact Assessment: Evaluated the severity and potential impact of successful injections.

Findings:

1. Vulnerable Pages/Forms: Identified [List vulnerable pages/forms] susceptible to SQL injection.
2. Successful Injections: Demonstrated successful low-level SQL injection on [Specific pages/forms].
3. Retrieved Information: Accessed sensitive data (e.g., usernames, passwords) via SQL injection.

Impact:

1. Data Exposure: Demonstrated the risk of unauthorized access to sensitive information.
2. Potential Risks: Highlighted the threat of data theft, unauthorized system access, or data manipulation.

Recommendations:

1. 1Code Sanitization: Implement strict input validation and parameterized queries to prevent SQL injection.
2. Regular Updates: Keep the application updated with security patches to address known vulnerabilities.
3. Security Training: Educate developers and users about SQL injection risks and mitigation strategies.
4. Security Best Practices: Adopt security best practices to safeguard against similar vulnerabilities.

Conclusion:

The test revealed critical vulnerabilities in DVWA, showcasing the risk of low-level SQL injection attacks. Immediate measures are recommended to secure the application and prevent potential exploitation.

HandsOn:

https://drive.google.com/file/d/1m2q8rmkeDL18dQ0m3eMRPdevh0c-w5eH/view?usp=drive_link