Penetration Testing Report – SQL Injection (Lab Environment)

Target Application: DVWA (Damn Vulnerable Web Application)
Test Type: SQL Injection Vulnerability Assessment
Date: 14 Aug 2025
Tester: Waleed Elsmedsey

1. Executive Summary

The objective of this penetration test was to simulate an SQL Injection attack in a controlled lab environment using the DVWA application. The test successfully demonstrated the exploitation of an input validation vulnerability that allowed retrieval of simulated database information.

2. Scope

- **In Scope:** Login and search functionalities in DVWA.
- **Out of Scope:** Any real-world or production applications.
- **Environment:** Localhost installation on Kali Linux with DVWA.

3. Methodology

1. Reconnaissance: Identified vulnerable parameters in the login and search forms.
2. Manual Testing: Injected SQL payloads to test for authentication bypass and data retrieval.
3. Automated Testing: Used SQLmap to confirm and automate the exploitation.
4. Data Extraction: Retrieved simulated user data from the DVWA database.
5. Documentation: Recorded steps, payloads, and recommendations.

4. Findings

Finding ID	Vulnerability	Severity	Description
SQL-001	SQL Injection	High	Unsanitized user input in form fields allowed execution of arbitrar

5. Impact

If present in a real-world application, this vulnerability could allow attackers to retrieve sensitive information, modify database records, or even execute administrative operations on the database server.

6. Recommendations

- Implement server-side input validation and parameterized queries.
- Use ORM frameworks that automatically handle query sanitization.
- Restrict database user privileges to the minimum required.
- Regularly perform security testing and code reviews.

7. Tools Used

- Burp Suite
- SQLmap
- Kali Linux
- DVWA

8. Conclusion

The test confirmed that the DVWA application is vulnerable to SQL Injection in its default configuration. Implementing secure coding practices and regular vulnerability assessments can prevent this type of attack.