SQL Injection Practical Exploitation – Lab Report

Student Name: Gayathri
Course: MCA
Lab Title: SQL Injection Practical Exploitation

1. Objective

The objective of this lab is to understand SQL Injection vulnerabilities, analyze their impact on database security, and study defensive techniques to prevent such attacks in web applications.

2. Tools Used

- SQLMap (conceptual use in lab environment)
- Manual testing techniques

3. Theory

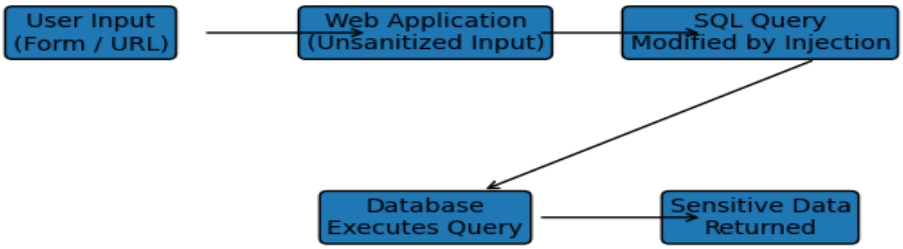
SQL Injection is a web security vulnerability that allows attackers to interfere with database queries by injecting malicious SQL statements through user inputs. This can lead to unauthorized access, data leakage, and data manipulation.

4. Methodology

1. Identify input parameters accepting user data.
2. Analyze input handling mechanisms.
3. Test parameters in a controlled lab environment.
4. Observe database responses.
5. Analyze the security impact.

5. SQL Injection Attack Flow

The following diagram explains the logical flow of an SQL Injection attack:



6. Impact Analysis

- Unauthorized access to database records
- Exposure of sensitive user information
- Risk of data manipulation or deletion
- Legal and reputational consequences

7. Security Fixes

- Use prepared statements and parameterized queries
- Validate and sanitize all user inputs
- Apply least privilege principle to database users
- Disable verbose database error messages

8. Conclusion

This lab demonstrates the seriousness of SQL Injection vulnerabilities and emphasizes the importance of secure coding practices in modern web applications.

9. Result

The lab successfully demonstrated SQL Injection concepts and reinforced database security best practices.