Sensitive Data Exposure Lab – Mutillidae (OWASP BWA)

Target: 192.168.29.186

1. Introduction

This lab demonstrates OWASP A6: Sensitive Data Exposure vulnerabilities using the Mutillidae web application inside the OWASP Broken Web Apps VM hosted at 192.168.29.186.

2. Methodology

- Connected to OWASP BWA at http://192.168.29.186/
- Navigated to Mutillidae web application.
- Identified lessons under OWASP 2013 → A6: Sensitive Data Exposure.
- Used Burp Suite to intercept requests and analyze HTTP traffic.
- Inspected phpMyAdmin database to check user credentials storage.
- Forced invalid inputs to observe error messages.

3. Lab Findings

Case 1: Insecure Transmission

Steps Taken: Intercepted login request with Burp Suite.
Impact: Credentials exposed if attacker is on the same network.
Fix: Enforce HTTPS/TLS.

Case 2: Plaintext Password Storage

Steps Taken: Registered a new user and reviewed accounts table in phpMyAdmin.
Impact: Passwords stored in plaintext are easily compromised.
Fix: Implement strong password hashing (bcrypt, Argon2).

Case 3: Information Disclosure

Steps Taken: Forced invalid input to trigger an SQL error.
Impact: Error message revealed database path and schema.
Fix: Use generic error messages without sensitive info.

4. Conclusion

The Mutillidae application at 192.168.29.186 demonstrates common sensitive data exposure vulnerabilities. Encrypting traffic, securely storing credentials, and implementing safe error handling are critical mitigations.

5. References

- OWASP Top 10 – Sensitive Data Exposure
- Mutillidae Documentation
- Burp Suite User Guide