Web Application Security Assessment Report

Author: Ganesh Rajput
Date: 28-02-2025
Project: Web Security Assessment

---

1. Introduction

This report presents a security assessment conducted on a web application to identify potential vulnerabilities. The goal was to analyze risks, simulate attacks, and recommend security improvements.

2. Tools Used

- **Burp Suite** – Intercepting and analyzing HTTP requests.
- **SQLMap** – Automated SQL injection detection.
- **Nmap** – Network scanning for open ports and services.
- **Nikto** – Web server vulnerability scanning.
- **Kali Linux** – Environment for penetration testing.

3. Vulnerabilities Discovered

3.1 SQL Injection (SQLi)

- **Issue:** A login form was found vulnerable to SQL injection, allowing an attacker to bypass authentication.
- **Impact:** An attacker could extract sensitive user data from the database.
- **Proof of Concept:**
- Input: ' OR '1'='1
- Response: Successfully logged in as admin.
- **Mitigation:** Implement prepared statements and input validation.

3.2 Cross-Site Scripting (XSS)

- **Issue:** The comment section does not sanitize user input.
- **Impact:** An attacker could inject malicious scripts to steal cookies or redirect users.
- **Proof of Concept:**
- <script>alert('XSS')</script>
- **Mitigation:** Sanitize and escape user inputs before rendering.

3.3 Security Misconfigurations

- **Issue:** The application revealed sensitive server information in HTTP headers.
- **Impact:** Attackers can gain insights into the technology stack for further exploitation.

- **Mitigation:** Disable unnecessary headers and configure security policies correctly.

4. Recommendations

1. Implement **input validation** and use **parameterized queries** to prevent SQL injection.
2. Apply **content security policies (CSP)** and escape user inputs to prevent XSS.
3. Disable unnecessary HTTP headers and enforce strong security configurations.

5. Conclusion

This assessment successfully identified critical vulnerabilities in the application. Implementing the recommended security measures will help prevent potential cyberattacks and strengthen overall security.