Web Application Security Assessment Report

Prepared by: Future Interns  
Project: Cyber Security Task 1

# 1. Executive Summary

This report provides the findings from a security assessment performed on the target web application. The purpose of this assessment was to identify vulnerabilities, evaluate their potential impact, and recommend remediation steps to enhance the application's security posture.

# 2. Methodology

The following tools and methodologies were used during the assessment:  
- OWASP ZAP for automated vulnerability scanning  
- Burp Suite (Community Edition) for manual interception and testing  
- Nikto for web server scanning  
- Manual testing for SQL Injection, XSS, and CSRF  
  
The vulnerabilities were categorized according to the OWASP Top 10 framework.

# 3. Findings

The following vulnerabilities were identified:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability | Severity | Proof (Screenshot Reference) | Impact | Mitigation |
| SQL Injection in Login Form | High | screenshot1.png | Allows bypass of authentication, leading to account takeover. | Use parameterized queries (prepared statements) and ORM. |

# 4. OWASP Top 10 Checklist

|  |  |
| --- | --- |
| OWASP Top 10 Category | Vulnerabilities Identified (Yes/No) |
| 1. Injection | Yes/No |
| 2. Broken Authentication | Yes/No |
| 3. Sensitive Data Exposure | Yes/No |
| 4. XML External Entities (XXE) | Yes/No |
| 5. Broken Access Control | Yes/No |
| 6. Security Misconfigurations | Yes/No |
| 7. Cross-Site Scripting (XSS) | Yes/No |
| 8. Insecure Deserialization | Yes/No |
| 9. Using Components with Known Vulnerabilities | Yes/No |
| 10. Insufficient Logging & Monitoring | Yes/No |

# 5. Conclusion & Recommendations

This assessment highlighted key security vulnerabilities within the application. By addressing the issues identified, the overall security posture of the application can be significantly improved. It is recommended to fix high-severity issues immediately and implement secure coding practices going forward.