${asmtName}

Assessment Report



|  |  |  |
| --- | --- | --- |
|  |  |  |
| ${asmtType} Report  Prepared By: FACTION Security  ${today} | | |
|  |  |  |

Assessor: ${asmtAssessor}  
Remediation: ${remediation}  
Phone: 123 123 1234  
Email: [test@yourorg.com](mailto:test@yourorg.com)

${TOC}

# Executive Summary

The ${asmtTeam} was engaged to conduct a web application security assessment of the ${asmtName} application. The scope of the engagement was to identify what exposures an attacker might have access to while using the web application as an authenticated external Internet user. The testing simulated an attacker attempting to gain unauthorized access to data and resources.

Security Findings:

${summary1}

# Objective and Scope

The main objective of our penetration test is to perform due-diligence testing of the ${asmtName} application to ensure it will withstand an attack from an adversary.

The scope included the ${asmtName} site’s gray environment with the most current version at the time of testing. The testing started ${asmtStart} and ended on ${asmtEnd}. The testing was performed against this site in order to cause minimal disruptions to the production site.

${summary2}

# Methodology

The OWASP Testing Guide (<https://www.owasp.org/index.php/OWASP_Testing_Project>) was used as a baseline methodology to follow for the testing. A blended approach was employed to identify application vulnerabilities through manual and automated dynamic testing. The primary focus is on manual efforts and automated scanners are also employed to perform other repetitive tasks such as brute force attacks.

The approach was to begin with an understanding of the application's business logic and map out each dynamic input parameter. From there, manual investigation of the application was performed looking for security exposures. Communications between the client and server are inspected for each request using a local proxy. This “man-in-the-middle” position allows all traffic to be inspected and modified both to and from the server. No denial-of-service testing was performed during the assessment.

Premier commercial and open-source toolsets are used when performing application security assessments. A sampling of tools available includes Burp Suite Professional Edition, IBM AppScan Black Box Edition, Acunetix Application Security Scanner, Metasploit Pro, NeXpose, Nessus, and Checkmarx source code analyzer. The effort is focused on quality identification of vulnerabilities and ensuring a comprehensive approach to the detection of application flaws.

# Findings

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ${vulnTable} | ${color Critical=8064a2,High=c0504d,Medium=e68e00,Low=33D7FF,Recommended=081417,Informational=657376} | | | |
| # | Vulnerability | Tracking Id | Likelihood | Impact | Severity |
| ${count} | ${loop} ${vulnName} | ${tracking} | ${likelihood} | ${impact} | ${severity} |

# Technical Findings

${fiBegin}

${fill Critical=8064a2,High=c0504d,Medium=e68e00,Low=33D7FF,Recommended=081417,Informational=657376}

## ${vulnName} - ${severity}

Description:

${desc}

Recommendation:

${rec}

${details}

${fiEnd}

# Technical Findings Network Section

${fiBegin Network\_Security}

${fill Critical=8064a2,High=c0504d,Medium=e68e00,Low=33D7FF,Recommended=081417,Informational=657376}

## ${vulnName} - ${severity}

Description:

${desc}

Recommendation:

${rec}

${details}

${fiEnd Network\_Security}

# Conclusion

All findings reported are based on Corporate Standards and Compliance. Please review all findings for similar code and functionality that may have been missed by the assessor.

All vulnerabilities must be remediated in PRODUCTION before the due date to prevent escalation. The vulnerabilities begin tracking on the date of the report-out meeting. All vulnerabilities must be verified by a member of the assessment team before moving the changes to production. Below is a table describing the timelines for each of the vulnerability Severity Ratings.

|  |  |
| --- | --- |
| Critical | Critical Findings have a 100 day SLA to production. All vulnerabilities must be verified first in the LLE before moving to production. |
| High | High Findings have a 150 data SLA to production. All vulnerabilities must be verified first in the LLE before moving to production. |
| Medium | Medium Findings are recommended to be mitigated in production by 200 days. The Information Security Team does not track issues below a High Severity Rating. |
| Low | Low Findings are recommended to be mitigated in production by 360 days. The Information Security Team does not track issues below a High Severity Rating. |
| Recommended | Recommended Items do not have a timeline in which they need to be mitigated. These are usually recommendations that could improve your security posture but are not required. |