**HPTVIETNAM CORPORATION**

**HPT Cyber Security Center**

**Website: www.hpt.vn**

**---o0o---**

SECURITY ASSESSMENT REPORT

****

**A computer mouse and keyboard

Description automatically generated with medium confidence**

**PENETRATION TESTING REPORT   
WEB APPLICATION**

**CUSTOMER:**

**TABLE OF CONTENTS**

[1. EXECUTIVE SUMMARY 1](#_Toc34146486)

[1.1. VERSION OF DOCUMENT 1](#_Toc34146487)

[1.2. IMPLEMETATION TIME 1](#_Toc34146488)

[1.3. TECHNICAL TEAM 1](#_Toc34146489)

[1.4. MỤC ĐÍCH ĐÁNH GIÁ 1](#_Toc34146490)

[1.5. SCOPE OF ASSESSMENT 1](#_Toc34146491)

[1.6. ASSESSMENT STANDARD 1](#_Toc34146492)

[1.7. VULNERABILITIES STATISTICS 2](#_Toc34146493)

[1.8. RECOMMENDATION 3](#_Toc34146494)

[2. TECHNICAL DETAIL REPORT 4](#_Toc34146495)

[2.1. CRITICAL RISK FINDINGS 4](#_Toc34146496)

[2.1.1. ISSUE 4](#_Toc34146497)

[2.2. HIGH RISK FINDINGS 4](#_Toc34146498)

[2.2.1. ISSUE 4](#_Toc34146499)

[2.3. MEDIUM RISK FINDINGS 5](#_Toc34146500)

[2.3.1. ISSUE 5](#_Toc34146501)

[2.4. LOW RISK FINDINGS 6](#_Toc34146502)

[2.4.1. ISSUE 6](#_Toc34146503)

[3. APPENDIX A: ASSESSMENT INFORMATION 8](#_Toc34146504)

[3.1. LIST OF IP DOING ASSESSMENT 8](#_Toc34146505)

[3.2. LIST OF TOOLS 8](#_Toc34146506)

[3.3. LIST OF OWASP TESTCASE 8](#_Toc34146507)

[4. APPENDIX B: RISK CLASSIFICATION 13](#_Toc34146508)

# PROJECT INFORMATION

The report is divided into several sections including executive report and detail report for findings of application

## VERSION OF DOCUMENT

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | UPDATE DATE | VERSION | TYPE | AUTHOR |
| [[Doc.ID]] | [[Doc.Update\_Date]] | [[Doc.Version]] | [[Doc.Type]] | [[Doc.Author]] |

## IMPLEMETATION TIME

* Web Application Assessment: [[Project.time]]

## TECHNICAL TEAM

|  |  |  |
| --- | --- | --- |
| ID | TECHNICIAN | ROLE |
| [[Team.stt]] | [[Team.name]] | [[Team.role]] |

## PURPOSE OF ASSESSMENT

* Security test for web application.
* Determine vulnerabilities in application in scope of assessment early to prevent exploitation.

## SCOPE OF ASSESSMENT

* Name: [[Project.Name]]
* Domain/URL: [[Project.Target]]
* Scope of assessment:
* BlackBox: Perform pentest without any information of Web application
* GreyBox: Perform using normal user, registered user

## ASSESSMENT STANDARD

The assessment method is based on OWASP Top 10 Web Category which defines top common category and vulnerablities in Web Appilcation.

* A1 Injection
* A2 Broken Authentication and Session Management
* A3 Cross-Site Scripting (XSS)
* A4 Insecure Direct Object References
* A5 Security Misconfiguration
* A6 Sensitive Data Exposure
* A7 Missing Function Level Access Control
* A8 Cross-Site Request Forgery (CSRF)
* A9 Using Components with Known Vulnerabilities
* A10 Unvalidated Redirects and Forwards

# EXECUTIVE SUMMARY

## VULNERABILITIES STATISTICS

Below is statistics chart of vulnerabilities categorized by severity level in application:

|  |  |  |
| --- | --- | --- |
| ID | SEVERITY | VULNERABILITY |
| [[Table.Id\_Table]] | [[Table.color-Risk\_Table]][[Table.Color]:merge-xml] | [[Table.Namevuln\_Table]] |

## RECOMMENDATION

After performing security assessment for application, we have some general summary/comment:

# TECHNICAL DETAIL REPORT

## CRITICAL RISK FINDINGS

## [[Critical.Vuln.Name\_Vuln]]

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Critical.Vuln.Category\_Vuln]] | | |
| **DESCRIPTION** | [[Critical.Vuln.Description\_Vuln]] | | |
| **SEVERITY** | **[[Critical.Vuln.Risk\_Vuln]]** | | |
| **IMPACT** | **[[Critical.Vuln.Affect\_Vuln]]** | **LIKELIHOOD** | **[[Critical.Vuln.Available\_Vuln]]** |
| **RECOMMENDATION** | [[Critical.Vuln.Suggest\_Vuln]] | | |
| **REFERENCE** | [[Critical.Vuln.Reference\_Vuln]] | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | [[Critical.Vuln.Name\_Function]] | | |
| **AFFECTED URL** | [[Critical.Vuln.Url]] | | |
| **PARAMETER** | [[Critical.Vuln.Parameter]] | | |
| **CONDITION** | [[Critical.Vuln.Condition]] | | |

|  |
| --- |
| **[[Critical.Vuln.Details.Name]]:**  [[Critical.Vuln.Details.Data]]  [[Critical.Vuln.Details.image-Image]:from-resource:maxSize(15)] |

## HIGH RISK FINDINGS

## [[Critical.Vuln.Name\_Vuln]]

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Critical.Vuln.Category\_Vuln]] | | |
| **DESCRIPTION** | [[Critical.Vuln.Description\_Vuln]] | | |
| **SEVERITY** | **[[Critical.Vuln.Risk\_Vuln]]** | | |
| **IMPACT** | **[[Critical.Vuln.Affect\_Vuln]]** | **LIKELIHOOD** | **[[Critical.Vuln.Available\_Vuln]]** |
| **RECOMMENDATION** | [[Critical.Vuln.Suggest\_Vuln]] | | |
| **REFERENCE** | [[Critical.Vuln.Reference\_Vuln]] | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | [[Critical.Vuln.Name\_Function]] | | |
| **AFFECTED URL** | [[Critical.Vuln.Url]] | | |
| **PARAMETER** | [[Critical.Vuln.Parameter]] | | |
| **CONDITION** | [[Critical.Vuln.Condition]] | | |

|  |
| --- |
| **[[Critical.Vuln.Details.Name]]:**  [[Critical.Vuln.Details.Data]]  [[Critical.Vuln.Details.image-Image]:from-resource:maxSize(15)] |

## MEDIUM RISK FINDINGS

## [[Critical.Vuln.Name\_Vuln]]

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Critical.Vuln.Category\_Vuln]] | | |
| **DESCRIPTION** | [[Critical.Vuln.Description\_Vuln]] | | |
| **SEVERITY** | **[[Critical.Vuln.Risk\_Vuln]]** | | |
| **IMPACT** | **[[Critical.Vuln.Affect\_Vuln]]** | **LIKELIHOOD** | **[[Critical.Vuln.Available\_Vuln]]** |
| **RECOMMENDATION** | [[Critical.Vuln.Suggest\_Vuln]] | | |
| **REFERENCE** | [[Critical.Vuln.Reference\_Vuln]] | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | [[Critical.Vuln.Name\_Function]] | | |
| **AFFECTED URL** | [[Critical.Vuln.Url]] | | |
| **PARAMETER** | [[Critical.Vuln.Parameter]] | | |
| **CONDITION** | [[Critical.Vuln.Condition]] | | |

|  |
| --- |
| **[[Critical.Vuln.Details.Name]]:**  [[Critical.Vuln.Details.Data]]  [[Critical.Vuln.Details.image-Image]:from-resource:maxSize(15)] |

## LOW RISK FINDINGS

## [[Critical.Vuln.Name\_Vuln]]

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Critical.Vuln.Category\_Vuln]] | | |
| **DESCRIPTION** | [[Critical.Vuln.Description\_Vuln]] | | |
| **SEVERITY** | **[[Critical.Vuln.Risk\_Vuln]]** | | |
| **IMPACT** | **[[Critical.Vuln.Affect\_Vuln]]** | **LIKELIHOOD** | **[[Critical.Vuln.Available\_Vuln]]** |
| **RECOMMENDATION** | [[Critical.Vuln.Suggest\_Vuln]] | | |
| **REFERENCE** | [[Critical.Vuln.Reference\_Vuln]] | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | [[Critical.Vuln.Name\_Function]] | | |
| **AFFECTED URL** | [[Critical.Vuln.Url]] | | |
| **PARAMETER** | [[Critical.Vuln.Parameter]] | | |
| **CONDITION** | [[Critical.Vuln.Condition]] | | |

|  |
| --- |
| **[[Critical.Vuln.Details.Name]]:**  [[Critical.Vuln.Details.Data]]  [[Critical.Vuln.Details.image-Image]:from-resource:maxSize(15)] |

# APPENDIX A: ASSESSMENT INFORMATION

## LIST OF IP DOING ASSESSMENT

|  |  |  |
| --- | --- | --- |
| ID | TIMELINE | IP ADDRESS |
| 1 | [[Project.time]] | 101.99.33.201 |
| 2 | [[Project.time]] | 115.165.164.30 |

## LIST OF TOOLS

|  |  |  |
| --- | --- | --- |
| No. | CATEGORY | TOOLS |
| 1 | Open-Source tools | Nmap, Firefox addons, Grabber, Zed, Sqlmap, WebScarab, Wireshark and other tool in Kali Linux (advanced penetration testing platform) |
| Framework scanner: Microsoft ASP.NET |
| Software: notepad++, sublime, python, RDP, putty |
| 2 | Commercial tools | Burpsuite – Proxy for application scanning, analyzing and modifying requests, responses |
| Nessus - Vulnerability scanner for servers, databases, applications and network devices |
| 3 | Self-developed tools (HPT) | HPT Scanner & Tool - Analyzing application structure - Enumerate application components (functions, url, parameters, …) - Password dictionary and signs of critical vulnerabilities, for example XSS, SQL based on errors  - Sensitive components detection (GHDB, Module, keyword, parameters, contents, email, notes, backup data, …) - Customized exploit for critical vulnerabilities: SQL Injection, XSS, Heartbleed, XPath, XXE, File Upload, File Inclusion, OS Command Injection, … and others vulnerabilities in and out of OWASP Top 10  - Customization support for web service |

## LIST OF OWASP TESTCASES

|  |  |  |
| --- | --- | --- |
| CATEGORY | TESTCASE | RESULT |
| Information Gathering | Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001) | Pass |
| Fingerprint Web Server (OTG-INFO-002) | Pass |
| Review Webserver Metafiles for Information Leakage (OTG-INFO-003) | Pass |
| Enumerate Applications on Webserver (OTG-INFO-004) | Pass |
| Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005) | Pass |
| Identify application entry points (OTG-INFO-006) | Pass |
| Map execution paths through application (OTG-INFO-007) | Pass |
| Fingerprint Web Application Framework (OTG-INFO-008) | Pass |
| Fingerprint Web Application (OTG-INFO-009) | Pass |
| Map Application Architecture (OTG-INFO-010) | Pass |
| Configuration and Deployment Management Testing | Test Network/Infrastructure Configuration (OTG-CONFIG-001) | Pass |
| Test Application Platform Configuration (OTG-CONFIG-002) | Pass |
| Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003) | Pass |
| Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004) | Pass |
| Enumerate Infrastructure and Application Admin Interfaces (OTG-CONFIG-005) | Pass |
| Test HTTP Methods (OTG-CONFIG-006) | Pass |
| Test HTTP Strict Transport Security (OTG-CONFIG-007) | Pass |
| Test RIA cross domain policy (OTG-CONFIG-008) | Pass |
| Identity Management Testing | Test Role Definitions (OTG-IDENT-001) | Pass |
| Test User Registration Process (OTG-IDENT-002) | Pass |
| Test Account Provisioning Process (OTG-IDENT-003) | Pass |
| Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004) | Pass |
| Testing for Weak or Unenforced Username Policy (OTG-IDENT-005) | Pass |
| Authentication Testing | Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001) | Pass |
| Testing for Default Credentials (OTG-AUTHN-002) | Pass |
| Testing for Weak Lock Out Mechanism (OTG-AUTHN-003) | Pass |
| Testing for Bypassing Authentication Schema (OTG-AUTHN-004) | Pass |
| Test Remember Password Functionality (OTG-AUTHN-005) | Pass |
| Testing for Browser Cache Weakness (OTG-AUTHN-006) | Pass |
| Testing for Weak Password Policy (OTG-AUTHN-007) | Pass |
| Testing for Weak Security Question/Answer (OTG-AUTHN-008) | Pass |
| Testing for Weak Password Change or Reset Functionalities (OTG-AUTHN-009) | Pass |
| Testing for Weaker Authentication in Alternative Channel (OTG-AUTHN-010) | Pass |
| Authorization Testing | Testing Directory Traversal/File Include (OTG-AUTHZ-001) | Pass |
| Testing for Bypassing Authorization Schema (OTG-AUTHZ-002) | Pass |
| Testing for Privilege Escalation (OTG-AUTHZ-003) | Pass |
| Testing for Insecure Direct Object References (OTG-AUTHZ-004) | Pass |
| Session Management Testing | Testing for Bypassing Session Management Schema (OTG-SESS-001) | Pass |
| Testing for Cookies Attributes (OTG-SESS-002) | Pass |
| Testing for Session Fixation (OTG-SESS-003) | Pass |
| Testing for Exposed Session Variables (OTG-SESS-004) | Pass |
| Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005) | Pass |
| Testing for Logout Functionality (OTG-SESS-006) | Pass |
| Test Session Timeout (OTG-SESS-007) | Pass |
| Testing for Session Puzzling (OTG-SESS-008) | Pass |
| Input Validation Testing | Testing for Reflected Cross Site Scripting (OTG-INPVAL-001) | **Fail** |
| Testing for Stored Cross Site Scripting (OTG-INPVAL-002) | Pass |
| Testing for HTTP Verb Tampering (OTG-INPVAL-003) | Pass |
| Testing for HTTP Parameter Pollution (OTG-INPVAL-004) | Pass |
| Testing for SQL Injection (OTG-INPVAL-005) | Pass |
| Oracle Testing | Pass |
| MySQL Testing | Pass |
| SQL Server Testing | Pass |
| Testing PostgreSQL (from OWASP BSP) | Pass |
| MS Access Testing | Pass |
| Testing for NoSQL injection | Pass |
| Testing for LDAP Injection (OTG-INPVAL-006) | Pass |
| Testing for ORM Injection (OTG-INPVAL-007) | Pass |
| Testing for XML Injection (OTG-INPVAL-008) | Pass |
| Testing for SSI Injection (OTG-INPVAL-009) | Pass |
| Testing for XPath Injection (OTG-INPVAL-010) | Pass |
| IMAP/SMTP Injection (OTG-INPVAL-011) | Pass |
| Testing for Code Injection (OTG-INPVAL-012) | Pass |
| Testing for Local File Inclusion | Pass |
| Testing for Remote File Inclusion | Pass |
| Testing for Command Injection (OTG-INPVAL-013) | Pass |
| Testing for Buffer overflow (OTG-INPVAL-014) | Pass |
| Testing for Heap overflow | Pass |
| Testing for Stack overflow | Pass |
| Testing for Format string | Pass |
| Testing for Incubated Vulnerabilities (OTG-INPVAL-015) | Pass |
| Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016) | Pass |
| Testing for HTTP Incoming Requests (OTG-INPVAL-017) | Pass |
| Testing for Error Handling | Analysis of Error Codes (OTG-ERR-001) | Pass |
| Analysis of Stack Traces (OTG-ERR-002) | Pass |
| Testing for Weak Cryptography | Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001) | Pass |
| Testing for Padding Oracle (OTG-CRYPST-002) | Pass |
| Testing for Sensitive Information Sent via Unencrypted Channels (OTG-CRYPST-003) | Pass |
| Business Logic Testing | Test Business Logic Data Validation (OTG-BUSLOGIC-001) | Pass |
| Test Ability to Forge Requests (OTG-BUSLOGIC-002) | Pass |
| Test Integrity Checks (OTG-BUSLOGIC-003) | Pass |
| Test for Process Timing (OTG-BUSLOGIC-004) | Pass |
| Test Number of Times a Function Can be Used Limits (OTG-BUSLOGIC-005) | Pass |
| Testing for the Circumvention of Workflows (OTG-BUSLOGIC-006) | Pass |
| Test Defenses Against Application Misuse (OTG-BUSLOGIC-007) | Pass |
| Test Upload of Unexpected File Types (OTG-BUSLOGIC-008) | **Fail** |
| Test Upload of Malicious Files (OTG-BUSLOGIC-009) | Pass |
| Client Side Testing | Testing for DOM based Cross Site Scripting (OTG-CLIENT-001) | Pass |
| Testing for JavaScript Execution (OTG-CLIENT-002) | Pass |
| Testing for HTML Injection (OTG-CLIENT-003) | Pass |
| Testing for Client Side URL Redirect (OTG-CLIENT-004) | Pass |
| Testing for CSS Injection (OTG-CLIENT-005) | Pass |
| Testing for Client Side Resource Manipulation (OTG-CLIENT-006) | Pass |
| Test Cross Origin Resource Sharing (OTG-CLIENT-007) | Pass |
| Testing for Cross Site Flashing (OTG-CLIENT-008) | Pass |
| Testing for Clickjacking (OTG-CLIENT-009) | Pass |
| Testing Web Sockets (OTG-CLIENT-010) | Pass |
| Test Web Messaging (OTG-CLIENT-011) | Pass |
| Test Local Storage (OTG-CLIENT-012) | Pass |

# APPENDIX B: RISK CLASSIFICATION

Each risk and possible threat is assigned a severity level base on the OWASP Risk Rating Methodology

The OWASP approach presented here is based on these standard methodologies and is customized for application security.

The standard risk model:

**Risk = Likelihood \* Impact**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **OVERALL RISK SEVERITY** | | | | |
| **IMPACT** | HIGH | Medium | High | Critical |
| MEDIUM | Low | Medium | High |
| LOW | Note | Low | Medium |
|  | LOW | MEDIUM | HIGH |
|  | **LIKELIHOOD** | | | |

For the detail of the rating method, please refer at:

<https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology>