**CÔNG TY CP DỊCH VỤ CÔNG NGHỆ TIN HỌC HPT**

**TRUNG TÂM AN TOÀN THÔNG TIN**

**Website: www.hpt.vn**

**---o0o---**

BÁO CÁO KIỂM THỬ XÂM NHẬP

****

**A computer mouse and keyboard

Description automatically generated with medium confidence**

**BÁO CÁO ĐÁNH GIÁ ỨNG DỤNG WEB**

**KHÁCH HÀNG:**

**MỤC LỤC**

[1. THÔNG TIN TÓM LƯỢC 1](#_Toc65225081)

[1.1. PHIÊN BẢN TÀI LIỆU 1](#_Toc65225082)

[1.2. THỜI GIAN THỰC HIỆN 1](#_Toc65225083)

[1.3. NHÂN SỰ TRIỂN KHAI 1](#_Toc65225084)

[1.4. MỤC ĐÍCH ĐÁNH GIÁ 1](#_Toc65225085)

[1.5. PHẠM VI TRIỂN KHAI 1](#_Toc65225086)

[1.6. TIÊU CHUẨN ĐÁNH GIÁ 1](#_Toc65225087)

[1.7. KẾT QUẢ TÓM LƯỢC 2](#_Toc65225088)

[1.8. CÁC KHUYẾN NGHỊ 2](#_Toc65225089)

[2. CHI TIẾT CÁC LỖ HỔNG ỨNG DỤNG WEB 3](#_Toc65225090)

[2.1. DANH SÁCH RỦI RO MỨC NGHIÊM TRỌNG 3](#_Toc65225091)

[2.1.1. ISSUE 3](#_Toc65225092)

[2.2. DANH SÁCH RỦI RO MỨC CAO 3](#_Toc65225093)

[2.2.1. ISSUE 3](#_Toc65225094)

[2.3. DANH SÁCH RỦI RO MỨC TRUNG BÌNH 4](#_Toc65225095)

[2.3.1. ISSUE 4](#_Toc65225096)

[2.4. DANH SÁCH RỦI RO MỨC THẤP 5](#_Toc65225097)

[2.4.1. ISSUE 5](#_Toc65225098)

[3. PHẦN MỞ RỘNG A: THÔNG TIN ĐÁNH GIÁ 7](#_Toc65225099)

[3.1. DANH SÁCH IP THỰC HIỆN ĐÁNH GIÁ 7](#_Toc65225100)

[3.2. DANH SÁCH CÔNG CỤ THỰC HIỆN 7](#_Toc65225101)

[3.3. DANH SÁCH TESTCASE THEO OWASP TOP 10 7](#_Toc65225102)

[4. PHẦN MỞ RỘNG B: PHÂN LOẠI RỦI RO 13](#_Toc65225103)

# THÔNG TIN TÓM LƯỢC

Báo cáo được chia làm nhiều phần bao gồm: báo cáo tổng quát, báo cáo chi tiết lỗ hổng trên ứng dụng

## PHIÊN BẢN TÀI LIỆU

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | NGÀY CẬP NHẬT | PHIÊN BẢN | LOẠI | NGƯỜI CẬP NHẬT |
| [[Version.stt]] | [[Version.update]] | [[Version.version]] | [[Version.type]] | [[Version.author]] |

## THỜI GIAN THỰC HIỆN

* [[Vuln.Name\_Vuln]] Đánh giá bảo mật ứng dụng:

## NHÂN SỰ TRIỂN KHAI

|  |  |  |
| --- | --- | --- |
| STT | TÊN NHÂN SỰ | VAI TRÒ |
| [[Author.stt\_author]] | [[Author.name\_author]] | [[Author.role\_author]] |

## MỤC ĐÍCH ĐÁNH GIÁ

* Kiểm tra bảo mật ứng dụng web.
* Phát hiện sớm các lỗi bảo mật trên ứng dụng web giúp kịp thời ngăn chặn sự can thiệp khai thác các lỗi này từ bên ngoài.

## PHẠM VI TRIỂN KHAI

* Tên ứng dụng:
* Địa chỉ:
* Phương thức thực hiện:
* Kiểm thử xâm nhập Blackbox: kiểm thử xâm nhập ứng dụng từ phía ngoài với các tài khoản như người dùng bình thường
* Đội đánh giá được Whitelist IP trên tường lửa ứng dụng (WAF) để kiểm tra đầy đủ các nhóm lỗ hổng

*[[image-application]:from-resource:maxSize(15)]*

## TIÊU CHUẨN ĐÁNH GIÁ

Kiểm thử xâm nhập theo tiêu chuẩn OWASP Web Top 10 đối với các ứng dụng Web nhằm tìm ra lỗ hổng bảo mật. Danh sách các nhóm đánh giá (phân nhóm Testcase theo OWASP).

* 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

## KẾT QUẢ TÓM LƯỢC

Dưới đây là biểu đồ thống kê các lỗ hổng theo từng cấp độ nghiêm trọng của ứng dụng:

|  |  |
| --- | --- |
| Mức độ | Instances |
| [[pie.name]] | [[pie.value]] |

Danh sách các lỗ hổng tìm thấy trong quá trình đánh giá ứng dụng:

|  |  |  |
| --- | --- | --- |
| STT | MỨC ĐỘ | TÊN LỖ HỔNG |
| [[AllVuln.Table.Id\_Table]] | [[AllVuln.Table.color-Risk\_Table]][[AllVuln.Table.Color]:merge-xml] | [[AllVuln.Table.Namevuln\_Table]] |

## CÁC KHUYẾN NGHỊ

Trong quá trình thực hiện đánh giá/kiểm thử xâm nhập ứng dụng, chúng tôi có một số tổng hợp/nhận xét:

# CHI TIẾT CÁC LỖ HỔNG ỨNG DỤNG WEB

## **Lỗ hổng**: [[critical.Vuln.Name\_Vuln]]

[[Critical.Vuln.Name\_Vuln]]

**Mức độ**: [[Critical.Vuln.Risk\_Vuln]] **Ảnh hưởng**: [[Critical.Vuln.Affect\_Vuln]] **Khả năng**: [[Critical.Vuln.Available\_Vuln]]

**CVSS**:3.0/AV: /AC: /PR: /UI: /S: /C: /I: /A: **CVE:** [[0.Vuln.CVE]]

**Mô tả**

[[0.Vuln.Description\_Vuln]]

**Khuyến nghị**

[[0.Vuln.Suggest\_Vuln]]

**Tham chiếu**

[[0.Vuln.Reference\_Vuln]]

**Chức năng ảnh hưởng:**

[[CriticalVulnDetails.Name]]

[[CriticalVulnDetails.Data]]

**Proof of Concept**

*Request:*

|  |
| --- |
| [[0.Vuln.Request]] |

*Response:*

|  |
| --- |
| [[0.Vuln.Response]] |

*Hình ảnh:*

*[[CriticalVulnDetails.image-Image]:from-resource:maxSize(15)]*

## **Lỗ hổng**: [[High.Vuln.Name\_Vuln]]

[[High.Vuln.Name\_Vuln]]

**Mức độ**: [[High.Vuln.Risk\_Vuln]] **Ảnh hưởng**: [[High.Vuln.Affect\_Vuln]] **Khả năng**: [[High.Vuln.Available\_Vuln]]

**CVSS**:3.0/AV: /AC: /PR: /UI: /S: /C: /I: /A: **CVE:** [[0.Vuln.CVE]]

**Mô tả**

[[High.Vuln.Description\_Vuln]]

**Khuyến nghị**

[[High.Vuln.Suggest\_Vuln]]

**Tham chiếu**

[[High.Vuln.Reference\_Vuln]]

**Chức năng ảnh hưởng:**

[[HighVulnDetails.Name]]

[[HighVulnDetails.Data]]

**Proof of Concept**

*Request:*

|  |
| --- |
| [[0.Vuln.Request]] |

*Response:*

|  |
| --- |
| [[0.Vuln.Response]] |

*Hình ảnh:*

*[[HighVulnDetails.image-Image]:from-resource:maxSize(15)]*

# PHẦN MỞ RỘNG A: THÔNG TIN ĐÁNH GIÁ

## DANH SÁCH IP THỰC HIỆN ĐÁNH GIÁ

|  |  |  |
| --- | --- | --- |
| STT | THỜI GIAN | ĐỊA CHỈ IP |
| 1 |  | 101.99.33.201 |
| 2 |  | 115.165.164.30 |

## DANH SÁCH CÔNG CỤ THỰC HIỆN

|  |  |  |
| --- | --- | --- |
| STT | NHÓM | DANH SÁCH CÔNG CỤ |
| 1 | Công cụ mã nguồn mở/ miễn phí | Nmap, Firefox addons, Grabber, Zed, Sqlmap, WebScarab, Wireshark and other tool in Kali Linux (advanced penetration testing platform) |
| Framework scanner: Drupal, Joomla, WordPress… |
| Software: notepad++, sublime, python, RDP, putty |
| 2 | Công cụ thương mại | Burpsuite – Dò quét ứng dụng, phân tích và chỉnh sửa gói tin |
| Nessus - Dò quét lỗ hổng bảo mật hệ thống Mạng, máy chủ, CSDL, Ứng dụng |
| 3 | Công cụ tự xây dựng (HPT) | HPT Scanner & Tool - Phân tích cấu trúc ứng dụng - Liệt kê chi tiết các thành phần ứng dụng (chức năng, url, tham số,…) - Từ điển mật khẩu và dấu hiệu nhận diện các lỗ hổng nghiêm trọng như XSS, SQL dựa vào trang lỗi - Phát hiện các thành phần nhạy cảm lỗi (GHDB, Module, keyword,tham số, nội dung, email, Ghi chú, backup data….) - Tùy biến khai thác các lỗ hổng nghiêm trọng : SQL Injection, Blind SQLi, XSS, Heartbleed, XPath, XXE, File Upload, File Inclusion, OS Command Injection....và các lỗ hổng khác trong và ngoài Top 10 OWASP - Hỗ trợ tùy biến cho web service |

## DANH SÁCH TESTCASE THEO OWASP TOP 10

|  |  |  |
| --- | --- | --- |
| NHÓM LỖI | TESTCASE | KẾT QUẢ |
| 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 |

# PHẦN MỞ RỘNG B: PHÂN LOẠI RỦI RO

Mỗi rủi ro tìm thấy trong quá trình kiểm thử được tham chiếu việc đánh giá theo OWASP Risk Rating Methodology.

Phương pháp tiếp cận theo OWASP được đề cập trong tài liệu được dùng làm chuẩn tham chiếu/phương pháp tiếp cận và tuỳ biến theo từng ứng dụng để đáp ứng/tinh chỉnh cho phù hợp các test-cases/kịch bản.

Mô hình đánh giá mức độ rủi ro:

**Rủi ro = Khả Năng \* Ảnh hưởng**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mức độ rủi ro (Risk)** | | | | |
| **Mức độ ảnh hưởng**  **(Impact)** | **CAO** | **TRUNG BÌNH** | **CAO** | **NGHIÊM TRỌNG** |
| **TRUNG BÌNH** | **THẤP** | **TRUNG BÌNH** | **CAO** |
| **THẤP** | **GHI CHÚ** | **THẤP** | **TRUNG BÌNH** |
|  | **THẤP** | **TRUNG BÌNH** | **CAO** |
|  | **Khả năng thực hiện (Likelihood)** | | | |

Tài liệu tham khảo:

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