|  |  |
| --- | --- |
|  |  |
|  | **BÁO CÁO KIỂM THỬ XÂM NHẬP**  **ABC COMPANY**  *Version 1.1*  Soạn bởi: ***CÔNG TY CỔ PHẦN DỊCH VỤ CÔNG NGHỆ TIN HỌC HPT – TRUNG TÂM AN TOÀN THÔNG TIN***  Ngày: 07.06.2020 |



**BÁO CÁO ĐÁNH GIÁ AN TOÀN THÔNG TIN**

**Khách hàng:**

**DỊCH VỤ KIỂM THỬ XÂM NHẬP**

**MỤC LỤC**

[1. BÁO CÁO TÓM TẮT 5](#_Toc55857913)

[1.1. THỐNG KÊ LỖ HỔNG 5](#_Toc55857914)

[1.2. DANH SÁCH LỖ HỔNG 5](#_Toc55857915)

[1.3. KHUYẾN NGHỊ 6](#_Toc55857916)

[2. THÔNG TIN DỰ ÁN 7](#_Toc55857917)

[2.1. PHẠM VI THỰC HIỆN 7](#_Toc55857918)

[2.2. ENGAGEMENT SUMMARY 7](#_Toc55857919)

[3. BÁO CÁO CHI TIẾT 8](#_Toc55857920)

[3.1. LỖ HỔNG 1 8](#_Toc55857921)

[3.2. LỖ HỔNG 2 9](#_Toc55857922)

[4. PHỤ LỤC A: PHÂN LOẠI RỦI RO 10](#_Toc55857923)

**Priority Key**

|  |  |  |
| --- | --- | --- |
| **Priority** | **Impact** | **Example Vulnerability Types** |
| P1 – Critical | Vulnerabilities that cause a privilege escalation from unprivileged to admin or allow for remote execution, financial theft, etc. | * Remote Code Execution * Vertical Authentication Bypass * XML External Entities Injection * SQL Injection * Insecure Direct Object Reference for a critical function |
| P2 – High | Vulnerabilities that affect the security of the platform including the processes it supports | * Lateral authentication bypass * Stored Cross-Site Scripting * Cross-Site Request Forgery for a critical function * Insecure Direct Object Reference for an important function * Internal Server-Side Request Forgery |
| P3 – Medium | Vulnerabilities that affect multiple users and require little or no user interaction to trigger | * Reflected Cross-Site Scripting with limited impact * Cross-Site Request Forgery for an important function * Insecure Direct Object Reference for an unimportant function * URL redirect |
| P4 – Low | Vulnerabilities that affect singular users and require interaction or significant prerequisites to trigger (MitM) to trigger | * Cross-Site Scripting with limited impact * Cross-Site Request Forgery for an unimportant function * External Server-Side Request Forgery |

# BÁO CÁO TÓM TẮT

## THỐNG KÊ LỖ HỔNG

|  |  |  |
| --- | --- | --- |
| Mức độ | Lỗ hổng | Instances |
| NGHIÊM TRỌNG | 1 | 1 |
| CAO | 1 | 1 |
| TRUNG BÌNH | 1 | 1 |
| THẤP | 1 | 1 |

## DANH SÁCH LỖ HỔNG

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Mức độ** | **Lỗ hổng** | **Instances** |
|  | NGHIÊM TRỌNG | Test Business Logic Data Validation | 1 |
|  | CAO | Testing for Local File Inclusion | 1 |
|  | TRUNG BÌNH | Tesing for Authentication Missing | 1 |
|  | THẤP | Testing for Stored Cross Site Scripting | 1 |

## KHUYẾN NGHỊ

# THÔNG TIN DỰ ÁN

## PHẠM VI THỰC HIỆN

|  |  |
| --- | --- |
| Mục tiêu 1 | |
| Ứng dụng | [[InfoVuln.AreaAction.Application]] |
| Đối tượng | [[InfoVuln.AreaAction.Target]] |
| Nền tảng | [[InfoVuln.AreaAction.Platform]] |
| Mục tiêu 2 | |
| Ứng dụng | ABC |
| Đối tượng | https://abc.xyz |
| Nền tảng | Web |

## ENGAGEMENT SUMMARY

|  |  |
| --- | --- |
| Thời gian | 1/1/2020 – 31/1/2020 |
| Phương thức | Blackbox |
| Số lượng nhân sự | 3 |

# BÁO CÁO CHI TIẾT

## LỖ HỔNG 1

**Mức độ**: Nghiêm Trọng **Ảnh hưởng**: Cao **Khả năng**: Cao

**CVSS**:3.0/AV: /AC: /PR: /UI: /S: /C: /I: /A: **CVE:** CVE-2020-1234

**Mô tả**

abcxyz

**Khuyến nghị**

abcxyz

**Tham chiếu**

abcxyz

**Chức năng ảnh hưởng:** Cập nhật tên – https://abc.xyz/update

**Proof of Concept**

*Request:*

|  |
| --- |
|  |

*Response:*

|  |
| --- |
|  |

*Hình ảnh:*

**Chức năng ảnh hưởng:** Thêm – https://abc.xyz/add

**Proof of Concept**

*Request:*

|  |
| --- |
|  |

*Response:*

|  |
| --- |
|  |

*Hình ảnh:*

## LỖ HỔNG 2

**Mức độ**: Nghiêm Trọng **Ảnh hưởng**: Cao **Khả năng**: Cao

**CVSS**:3.0/AV: /AC: /PR: /UI: /S:z /C: /I: /A: **CVE:** CVE-2020-1234

**Mô tả**

abcxyz

**Khuyến nghị**

abcxyz

**Tham chiếu**

abcxyz

**Chức năng ảnh hưởng:** Cập nhật tên – https://abc.xyz/update

**Proof of Concept**

*Request:*

|  |
| --- |
|  |

*Response:*

|  |
| --- |
|  |

*Hình ảnh:*

**Chức năng ảnh hưởng:** Thêm – https://abc.xyz/add

**Proof of Concept**

*Request:*

|  |
| --- |
|  |

*Response:*

|  |
| --- |
|  |

*Hình ảnh:*

# PHỤ LỤC A: 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 testcase/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://owasp.org/www-community/OWASP_Risk_Rating_Methodology>

A picture containing text

Description automatically generated

Lô E2a-3 Đường D1, Khu Công nghệ cao, P.Long Thạnh Mỹ, Q.9, TP.HCM

Tel: +(84 28) 38 266 206 • Fax: +(84 28) 54 108 801

www.hpt.vn