****

**BÁO CÁO**

**Báo cáo**

**ITSD Request ID: xxxxxxx**

**HÀ NỘI, Ngày 28 Tháng 6 Năm 2022**

**MỤC LỤC**

[A. TỔNG QUAN 2](#_Toc107309265)

[**1.** Phương pháp thực hiện 2](#_Toc107309266)

[**2.** Thông tin ứng dụng được đánh giá 3](#_Toc107309267)

[**3.** Kết quả đánh giá 3](#_Toc107309268)

[**4.** Tổng hợp các phát hiện 4](#_Toc107309269)

[B. BÁO CÁO CHI TIẾT 4](#_Toc107309270)

[**1.** Ứng dụng 1 4](#_Toc107309271)

[**2.** Ứng dụng 2 5](#_Toc107309272)

# TỔNG QUAN

## Phương pháp thực hiện

### Phương pháp đánh giá

Thực hiện đánh giá bằng phương pháp graybox/blackbox theo tiêu chuẩn ATTT ứng dụng của MSB và các tiêu chuẩn ATTT quốc tế khác như OWASP, PCI DSS,…

Quá trình đánh giá nhằm mục đích phát hiện các lỗ hổng bảo mật tồn tại trên ứng dụng có thể bị kẻ xấu lợi dụng để tấn công vào hệ thống.

Các lỗ hổng được đánh giá dựa trên tham khảo OWASP top 10 cụ thể bao gồm:

* A1: Injection
* A2: Broken Authentication
* A3: Sensitive Data Exposure
* A4: XML External Entities (XXE)
* A5: Broken Access Control
* A6: Security Misconfiguration
* A7: Cross-Site Scripting XSS
* A8: Insecure Deserialization
* A9: Using Components with Known Vulnerabilities
* A10: Insufficient Logging & Monitoring

### Phân loại rủi ro

Việc phân loại mực độ rủi ro được thực hiện tham khảo theo tiêu chuẩn OWASP căn cứ vào các yếu tố dưới đây:

* Threat Agent Factors
* Vulnerability Factors
* Technical Impact Factors
* Business Impact Factors

Các lỗ hổng bảo mật được phân loại thành 4 cấp độ rủi ro**: Nghiêm trọng, Cao, Trung bình, Thấp** như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Phân loại mức độ rủi ro** | | | | |
| **Mức độ**  **tác động** | CAO | Trung bình | Cao | Nghiêm trọng |
| TRUNG BÌNH | Thấp | Trung bình | Cao |
| THẤP | Ghi chú | Thấp | Trung bình |
|  | THẤP | TRUNG BÌNH | CAO |
|  | **Khả năng xảy ra** | | | |

## Thông tin ứng dụng được đánh giá

### 1231e23123123

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tên ứng dụng** | **Phiên bản** | **Phân loại** | | **Môi trường triển khai** | **Phạm vi triển khai** | **Xử lý dữ liệu thẻ** |
| 1231e23123123 | 3131231 | 312312 | | 313123 | 123123 | Không |
| **Mô tả:**  ádasdasdasd | | | | | | |
| **Đường dẫn truy cập / Link tải file cài đặt:**  1312 | | | | | | |
| **Đường dẫn mã nguồn lưu trữ trên SVN:** | | | | | | |
| **Revision:** | | | **Fixed revision:** | | | |
| **Thời gian thực hiện đánh giá:** Từ ngày …/…/2021 đến ngày …/…/2021 | | | | | | |

## Kết quả đánh giá

Thực hiện đánh giá ứng dụng này trên môi trường UAT/Production phát hiện 1 lỗ hổng bảo mật đang tồn tại cho phép kể tấn công có thể thực hiện chiếm quyền điều khiển, hoặc thực hiện các hành động trái phép thông qua ứng dụng để tác động vào hệ thống.

## Tổng hợp các phát hiện

### Ứng dụng 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Tên lỗ hổng bảo mật** | **Mức độ** | **Số lượng** | **Bắt buộc xử lý** | **Trạng thái** |
| 1 | Broken Authentication | Nguy hiểm |  |  |  |
| 2 |  |  |  |  |  |

# BÁO CÁO CHI TIẾT

## 1231e23123123

### Broken Authentication

|  |
| --- |
| **Mức độ: Nguy hiểm** |
| **Mô tả: Noi dung mo ta loi Authentication** |
| **Kết quả thu được:** |
| **Đường dẫn bị ảnh hưởng:** |
| **Khuyến nghị:** |

|  |  |
| --- | --- |
| **Cán bộ thực hiện** | **GĐ. Phòng An toàn thông tin** |
|  |  |