undefined

**BÁO CÁO**

**KẾT QUẢ ĐÁNH GIÁ AN TOÀN THÔNG TIN ỨNG DỤNG**

****

**MỤC LỤC**

[**TỔNG QUAN**](#_heading=h.gjdgxs) **[2](#_heading=h.gjdgxs)**

[Phương pháp thực hiện](#_heading=h.30j0zll) [2](#_heading=h.30j0zll)

[Phương pháp đánh giá](#_heading=h.vzy11agl5tt3) [2](#_heading=h.vzy11agl5tt3)

[Phân loại rủi ro](#_heading=h.1fob9te) [2](#_heading=h.1fob9te)

[Thông tin ứng dụng được đánh giá](#_heading=h.3znysh7) [3](#_heading=h.3znysh7)

[Kết quả đánh giá](#_heading=h.3dy6vkm) [3](#_heading=h.3dy6vkm)

[Tổng hợp các phát hiện](#_heading=h.4d34og8) [4](#_heading=h.4d34og8)

[Ứng dụng 1](#_heading=h.b58flh82ds67) [4](#_heading=h.b58flh82ds67)

[ứng dụng 2](#_heading=h.3mjbeaevimas) [5](#_heading=h.3mjbeaevimas)

[**BÁO CÁO CHI TIẾT**](#_heading=h.2s8eyo1) **[5](#_heading=h.2s8eyo1)**

[Ứng dụng 1](#_heading=h.17dp8vu) [5](#_heading=h.17dp8vu)

[Lỗ hổng 1](#_heading=h.y2o9s6het51o) [5](#_heading=h.y2o9s6het51o)

[Lỗ hổng 2](#_heading=h.o9askk7u0hc4) [5](#_heading=h.o9askk7u0hc4)

[Ứng dụng 2](#_heading=h.3rdcrjn) [5](#_heading=h.3rdcrjn)

[Lỗ hổng 1](#_heading=h.wtuum02yplnr) [5](#_heading=h.wtuum02yplnr)

[Lỗ hổng 2](#_heading=h.26in1rg) 5

# 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

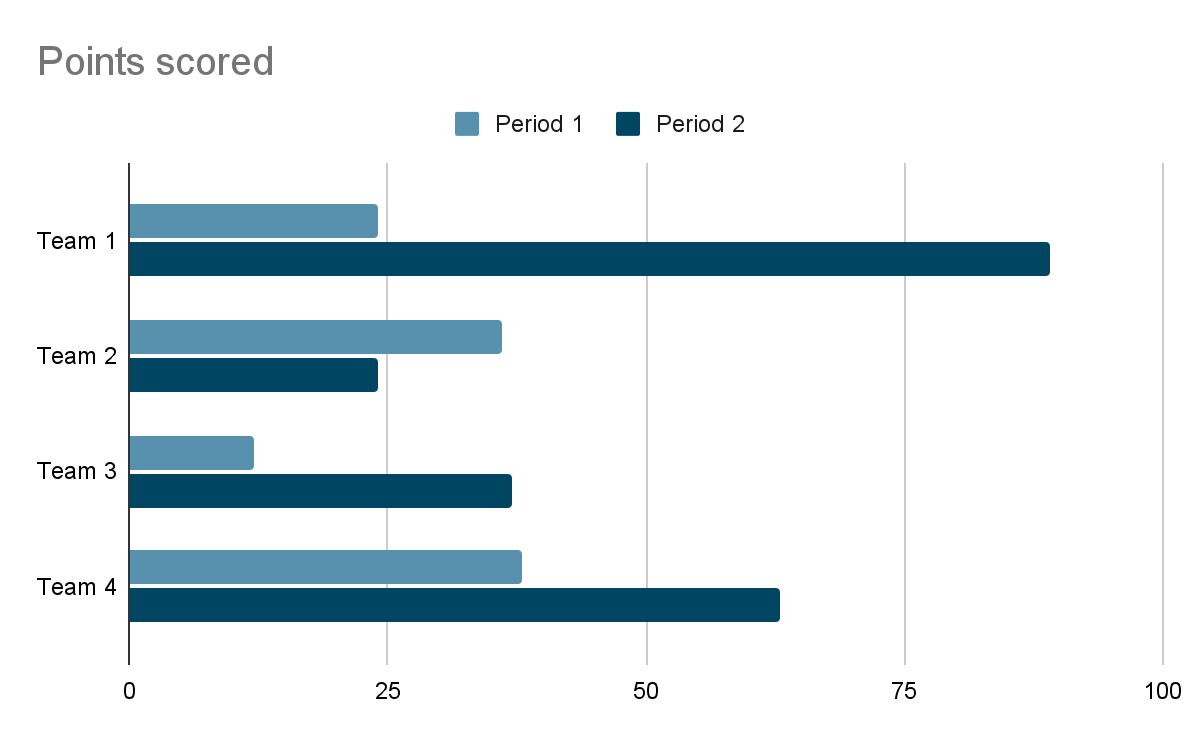
### 0

| **Tên ứng dụng** | **Phiên bản** | **Phân loại** | | **Môi trường triển khai** | **Phạm vi triển khai** | **Xử lý dữ liệu thẻ** |
| --- | --- | --- | --- | --- | --- | --- |
| 0 | 3131231 | 312312 | | 313123 | 123123 | Không |
| **Mô tả:**  (Thông tin chung về ứng dụng, tên các chức năng, API cần đánh giá)  Xây dựng luồng xử lý ở IB server cho tính năng Hiển thị số dư trái phiếu trên Mobile App | | | | | | |
| **Đường dẫn truy cập / Link tải file cài đặt:**  1312 | | | | | | |
| **Đường dẫn mã nguồn lưu trữ trên SVN:**  0 | | | | | | |
| **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 4 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



ok

undefined

### 0

| **STT** | **Tên lỗ hổng bảo mật** | **Mức độ** | **Số lượng** | **Bắt buộc xử lý** | **Trạng thái** |
| --- | --- | --- | --- | --- | --- |
| 1 | Injection | Nguy hiểm | undefined | undefined | undefined |
| 2 | Broken Authentication | Nguy hiểm | undefined | undefined | undefined |
| 3 | Injection | Nguy hiểm | undefined | undefined | undefined |
| 4 | Injection | Nguy hiểm | undefined | undefined | undefined |

# BÁO CÁO CHI TIẾT

+++FOR app IN getApplications()+++

### +++$app.name+++

+++FOR vulnerability IN getAllVulnerabilities($app.index)+++

### +++$vulnerability.name+++

| **Mức độ: +++=$vulnerability.level +++** |
| --- |
| **Mô tả: +++=$vulnerability.dsscription +++** |
| **Kết quả thu được:** |
| **Đường dẫn bị ảnh hưởng:** |
| **Khuyến nghị:** |

+++END-FOR vulnerability+++

+++END-FOR app+++

### 

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