BÁO CÁO

KẾT QUẢ GRAYBOX PENETRATION TESTING HỆ THỐNG

Tên tổ chức: Công ty Cổ phần MISA

Tên ứng dụng: Ứng dụng AMIS PLATFORM

( HOME & MARKET)

Thời gian thực hiện: Tháng 11/2020

PHẦN 1: THÔNG TIN CHUNG

|  |  |
| --- | --- |
| Tên tổ chức: | Công ty cổ phần MISA |
| Người đánh giá: | Bùi Đức Trường (bdtruong@software.misa.com.vn)  Sđt: 0396782040 |
| Thời gian đánh giá: | 10/11/2020 – 17/11/2020 |
| Đối tượng đánh giá: | https://testpartnermanager.misa.com.vn |
| Hình thức đánh giá: | Graybox |
| Tài khoản sử dụng: | Tài khoản 1: (Full quyền)  ID: [A05-0002](mailto:giangke1494@gmail.com)  Pass: 12345678@Abc  Tài khoản 2:  ID: C26-0014  Pass: 12345678@Abc |

PHẦN 2: KẾT QUẢ ĐÁNH GIÁ

|  |  |
| --- | --- |
| Kết quả chung | Có 1 lỗi ở mức nghiêm trọng, 1 lỗi mức cao, 2 lỗi mức trung bình |
| Đề xuất khắc phục | 4 |
| Số lỗi nghiêm trọng | 1 |
| Số lỗi cao | 1 |
| Số lỗi trung bình | 2 |
| Số lỗi thấp | 0 |

1. **Checklisk danh mục lỗ hổng:**

(File đính kèm [MISA Partner.xlsx](Kết%20quả%20đánh%20giá%20dự%20án%20MISA%20Partner_2nd.docx))

1. **Thông tin chi tiết và cách khắc phục**
2. *Danh sách lỗi*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mã lỗi | Tên lỗi | Tên lỗ hổng trong danh mục | Mô tả chi tiết | Mức độ |
| MSPA-01 | XSS | Testing for Cross Site Scripting | Mục 2.1 | Trung bình |
| MSPA-02 | Time Based SQLinjection | Testing for SQL injection | Mục 2.2 | Nghiêm trọng |
|  |  |  |  |  |
|  |  |  |  |  |

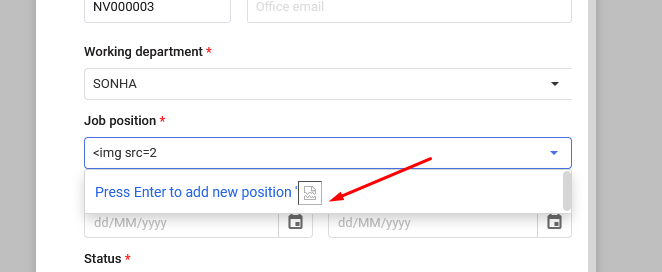
1. *Mô tả chi tiết:*
   1. **XSS**

* Mã lỗi: AMIS-PL-01
* Tên lỗ hổng trong danh mục: QT-INPVAL-001: Testing XSS Reflected
* Vị trí lỗi:

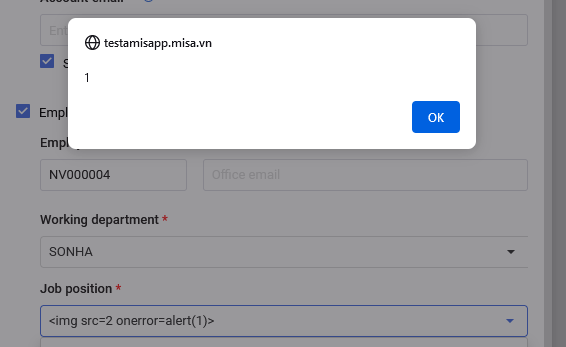
|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | https://testamisapp.misa.vn/system/member |  |
| 2 | https://testamisapp.misa.vn/market |  |

* Mô tả: Thực hiện thay đổi cập nhật một số thông tin ví dụ như địa chỉ khách hàng, vv… và truyền script đơn giản vào.
* Nguy cơ: Bị đánh cắp session và cookie, thông tin người dùng.
* Mức độ: Nghiêm trọng
* Nguyên nhân: Do không lọc các ký tự đầu vào
* Khắc phục: Lọc ký tự đầu vào trước ghi lưu vào database
* Các bước dựng lại lỗi:

**POC1:** Vào mục thêm thành viên (member), Điền vào nội dung thẻ *<img src=1 onerror=alert(1)>* vào trường Job position (Vị trí công việc).

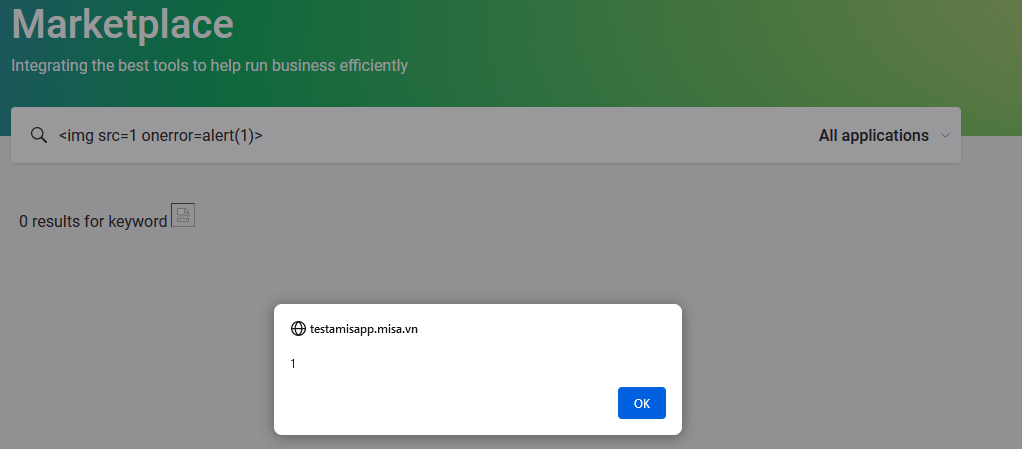


Kết quả :



**POC2:**

**Truy cập vào chợ ứng dụng và Điền vào nội dung thẻ <img src=1 onerror=alert(1)> vào ô tìm kiếm -> Nhấn Enter**



* 1. **Time based SQL injection**
* Mã lỗi: AMIS-PL-02
* Tên lỗ hổng trong danh mục: Vị trí lỗi: Diện rộng

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /APIS/PlatformAPI/api/JobPositions/paging |  |
| 2 | /APIS/EmployeesContactAPI/api/Employee/data-paging/ |  |
| 3 | /APIS/PlatformAPI/api/User/userNotPermissionInApp/null |  |

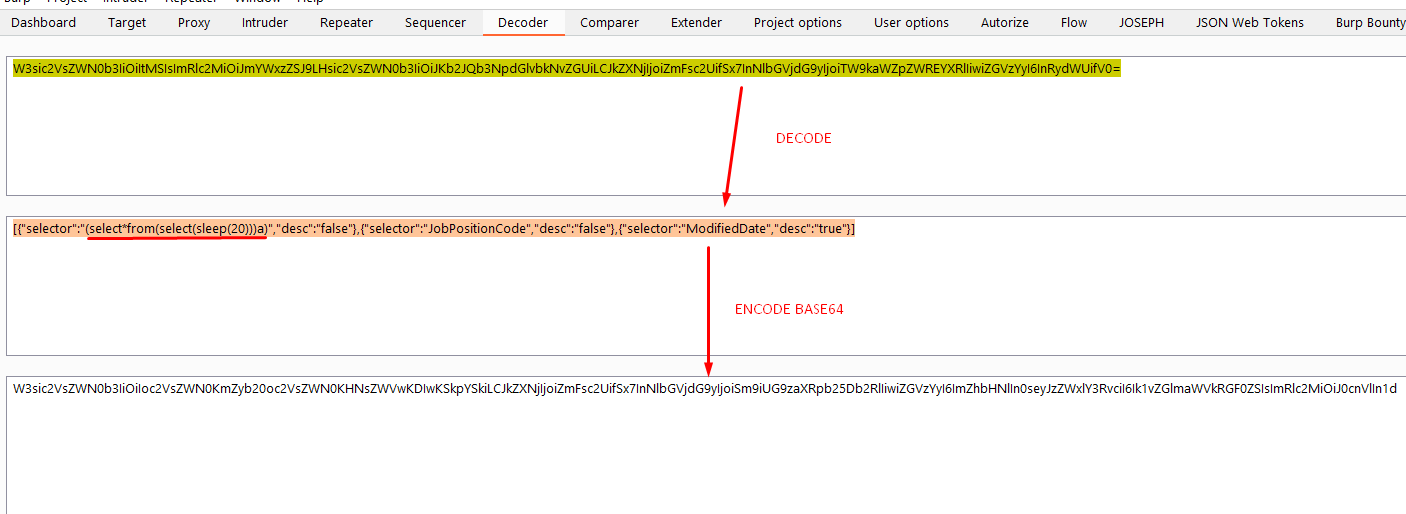
* Mô tả: Tại tham số Sort cho phép chèn câu truy vấn SQL dẫn đến lỗ hổng SQL injection. API nào sử dụng đầu vào là thame số Sort đều bị ảnh hưởng
* Nguy cơ: Kể tấn công có thể khai thác và drop cơ sở dữ liệu
* Mức độ: Nghiêm trọng
* Nguyên nhân: Không kiểm soát dữ liệu đầu vào
* Khắc phục: Lọc các kí tự đặc biệt, tham số hóa và sử dụng thủ tục (procedure)
* Các bước dựng lại lỗi:

Bước 1: Truy cập vào ứng dụng AMIS , Sử dụng burpsuite chặn bắt API request



Tiến hành decode giá trị của tham số Sort , chèn payload (select\*from(select(sleep(20)))a) – Delay reponse 20s

vào giá trị của tham số selector



Thay lại vào giá trị Sort và kiểm tra kết quả:

