BÁO CÁO

KẾT QUẢ GRAYBOX PENETRATION TESTING HỆ THỐNG

Tên tổ chức: Công ty Cổ phần MISA

Tên ứng dụng: AMIS NHÂN VIÊN

Thời gian thực hiện: Tháng 9/2021

PHẦN 1: THÔNG TIN CHUNG

|  |  |
| --- | --- |
| Tên tổ chức: | Công ty cổ phần MISA |
| Người đánh giá: | Lê Bình An (lban@software.misa.com.vn)  Sđt: 0979700145 |
| Thời gian đánh giá: | 1/10/2021 – 5/10/2020 |
| Đối tượng đánh giá: | https://demosalagovapp.misa.vn |
| Hình thức đánh giá: | Graybox |
| Tài khoản sử dụng: | Admin/20212004@misa |

PHẦN 2: KẾT QUẢ ĐÁNH GIÁ

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

1. **Checklisk danh mục lỗ hổng:**

(File đính kèm galagov[.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 |
| SALAGOV  -01 | XSS Stored | Testing for XSS Stored | Mục 2.1 | High |

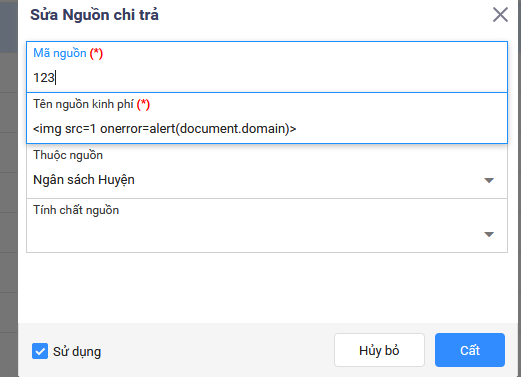
1. *Mô tả chi tiết:*
   1. **XSS Stored**

* **Mã lỗi**: SALAGOV-01
* **Tên lỗ hổng trong danh mục**:
* **Vị trí lỗi**: Diện rộng

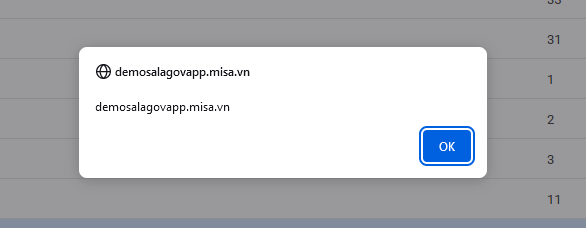
|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /View/Dictionary/OrganizationUnitESB |  |
| 2 | /APIS/EmployeeCnBAPI/api/Note/paging |  |
| 3 | /APIS/EmployeeCnBAPI/api/Attendance/getAttendanceStatistic |  |

* **Mô tả**: Tại tất các trường điền thông tin đều không được kiểm soát giá trị truyền vào của người dùng, cho phép chèn cả script dẫn đến lỗ hổng XSS
* **Nguy cơ**: Kẻ tấn công có thể chèn script độc hại để ăn cắp thông tin người dùng khác,tạo keylogger, nội dung giả mạo trang web.
* **Mức độ**: Cao
* **Nguyên nhân**: Không kiểm soát dữ liệu đầu vào
* **Khắc phục**: Ap dụng các bộ lọc, khử kí tự đặc biệt và encode dữ liệu đầu ra. Nên sử dụng encode để đảm bảo không bỏ sót bất cứ bộ lọc nào.
* **Dựng lại lỗ hổng** :

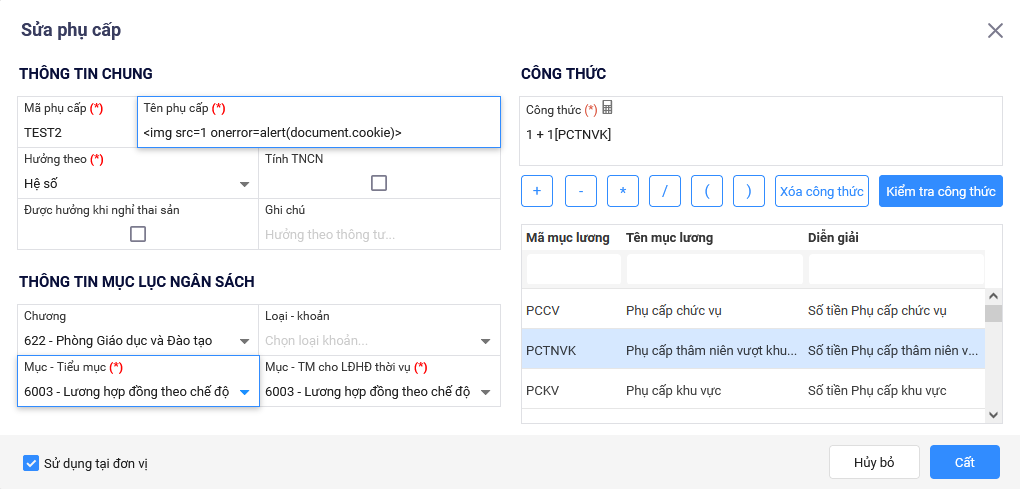
Tại các trường thông tin được kiểm soát bởi người dùng, có thể chèn tuy ý muốn



Kết quả



Còn nữa.



Script đã được thực thi

