BÁO CÁO

KẾT QUẢ GRAYBOX PENETRATION TESTING HỆ THỐNG

Tên tổ chức: Công ty Cổ phần MISA

Tên ứng dụng: EMIS SAS

Thời gian thực hiện: Tháng 10/2021

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: | 13/10/2021 – 19/10/2021 |
| Đối tượng đánh giá: | https://emisapp.misa.vn |
| Hình thức đánh giá: | Graybox |
| Tài khoản sử dụng: | -Quản trị viên  User: admin  Pass: 12345678@Abc  -Nhân viên  User: qlthietbi  Pass: 12345678@Abc |

PHẦN 2: KẾT QUẢ ĐÁNH GIÁ

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

1. **Checklisk danh mục lỗ hổng:**

(File đính kèm emis-sas[.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 |
| EMIS-SAS-01 | SQL injection in sort, customFilter param | Testing SQL injection | Mục 2.1 | Critial |
| EMIS-SAS-02 | SQLServerException information disclosure | Testing for sensitive information | Mucj 2.2 | Low |

1. *Mô tả chi tiết:*
   1. **SQL injection in sort, customFilter param (Equipment)**

* **Mã lỗi**: EMIS-SAS-01
* **Tên lỗ hổng trong danh mục**: Testing SQL injection
* **Vị trí lỗi**: Diện rộng

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /rc/equipment/api/ShoppingRegistration/GetShoppingRegistration |  |
| 2 | /rc/equipment/api/ShoppingRegistration/Paging |  |
| 3 | /rc/equipment/api/ClassRoom/Paging |  |
| … | … |  |

* **Mô tả**: Trong app Thiết bị, tại tham số **sort** và **customFilter** trong body paload , cho phép chèn các câu truy vấn SQL làm thay đổi cấu trúc câu truy vấn của ứng dụng dẫn đến lỗ hổng SQL injection
* **Nguy cơ**: Kẻ tấn công có thể khai thác cơ sở dữ liệu, leo thang đặc quyền
* **Mức độ**: Nguy hiểm
* **Nguyên nhân**: Lỗi kiểm soát dữ liệu đầu vào
* **Khắc phục**: Kiểm soát dữ liêu đầu vào, sử dụng library của MISA
* **Dựng lại lỗ hổng** :

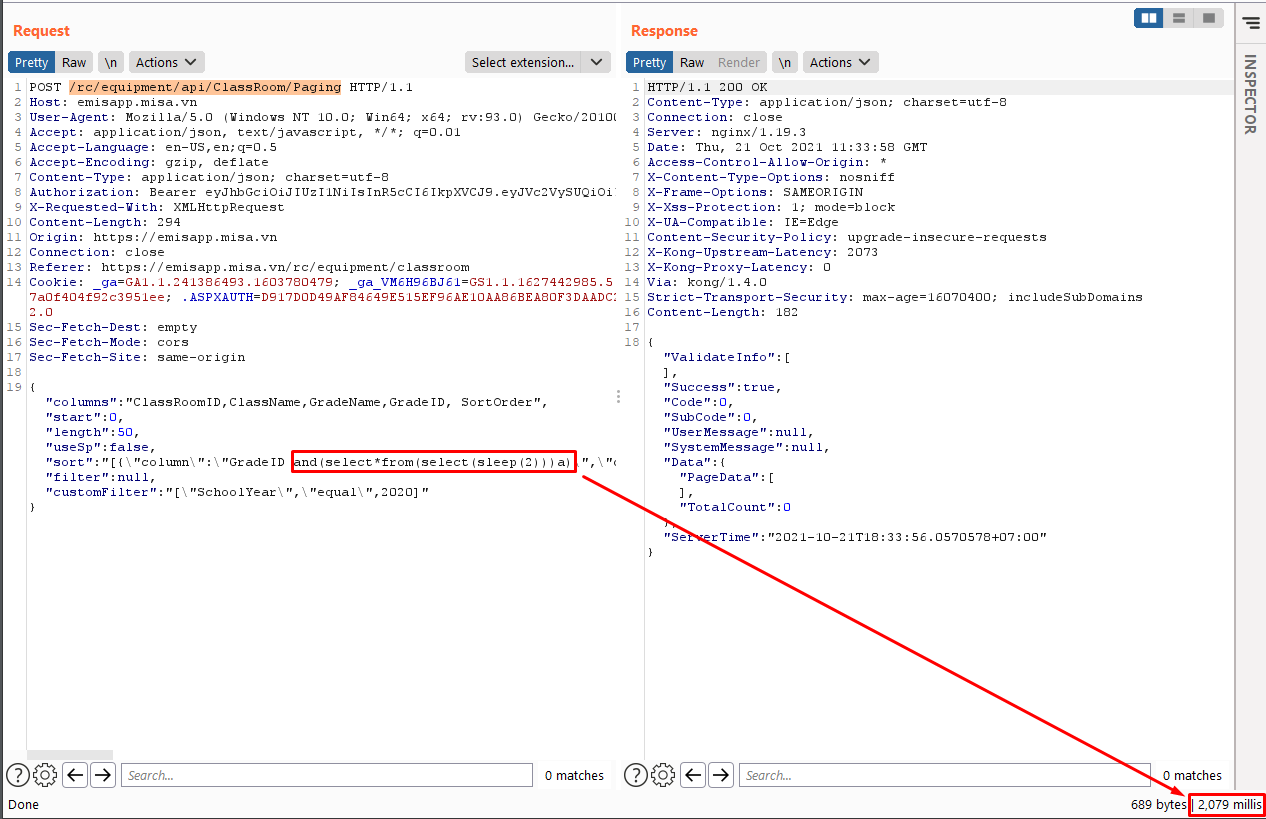
Sử dụng burpsuite để bắt request có tham số sort và custemFilter



Tại tham số sort, chèn payload để xác định có thể sql injection

and (select\*from(select(sleep(2)))a) -> 2s

and (select\*from(select(sleep(4)))a) -> 4s



Lưu ý thời gian phản hồi tùy thuộc vào DB thực thi comment chứ không phải theo thời gian của sleep() nhưng nó sẽ tỉ lệ với time được set cho hàm sleep().

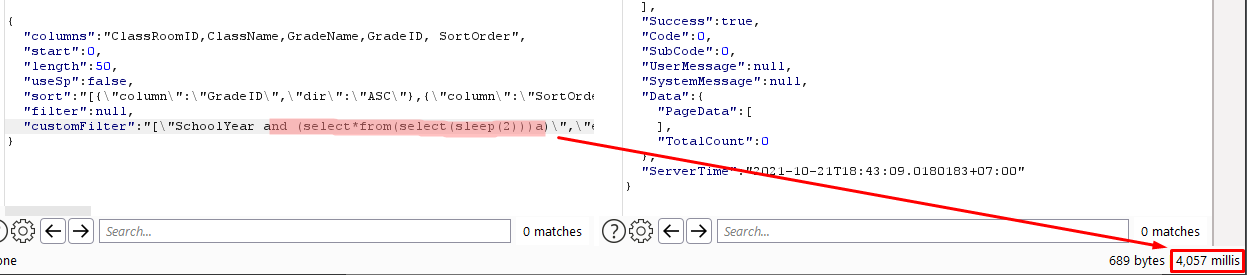
* Tương tự tại tham số custemFilter , chèn payload:

and(select\*from(select(sleep(2)))a) để kiểm tra .

sleep(2) -> 4s

sleep(3) -> 6s

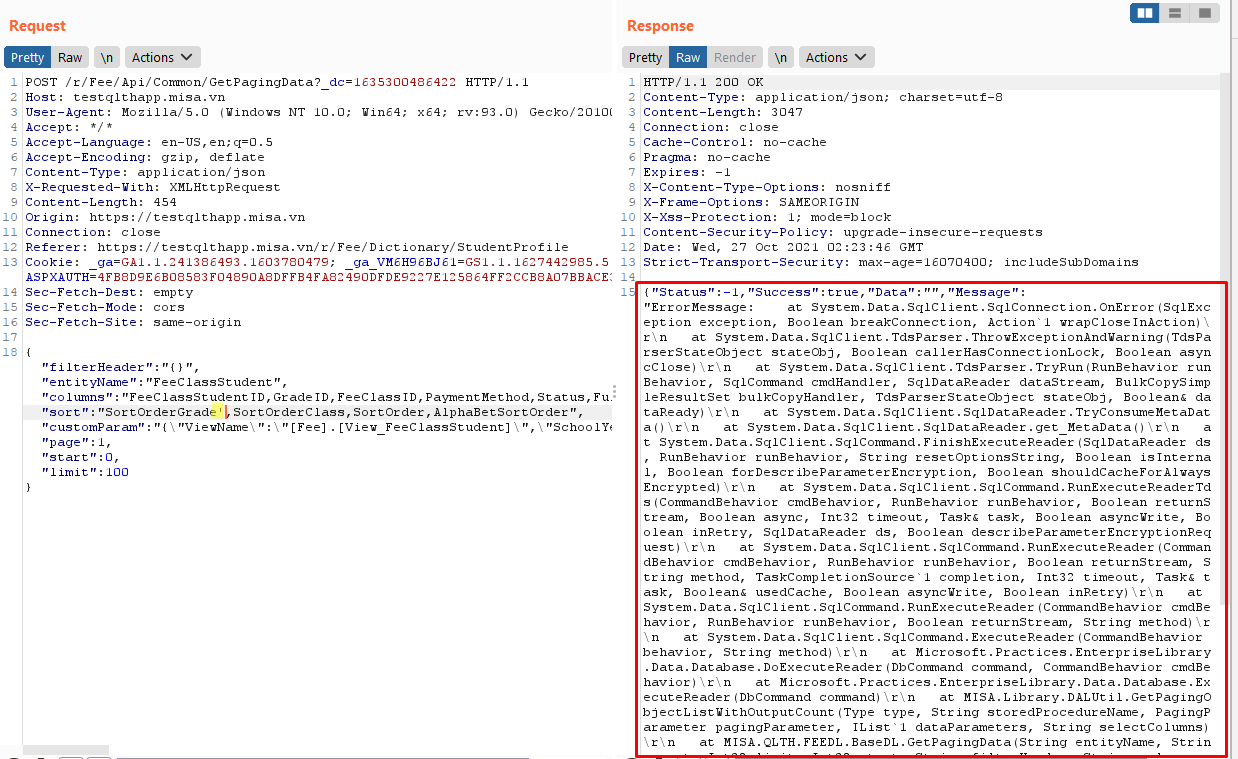
…



* 1. **SQLServerException information disclosure**
* **Mã lỗi**: EMIS-SAS-02
* **Tên lỗ hổng trong danh mục**: Testing for sensitive information
* **Vị trí lỗi**: Diện rộng ( Thu phí V2)

|  |  |
| --- | --- |
| Url | Ghi chú |
| /r/Fee/Api/Common/GetPagingData |  |
| /rc/equipment/api/ShoppingRegistration/Paging |  |
| /rc/equipment/api/ClassRoom/Paging |  |
| … |  |

* **Mô tả**: Trong app Thu phí V2, Nếu truyền các kí tự đặc biệt như ‘, - ,; vào các tham số đầu vào đều bắn trực tiếp SQLexception về cho người dùng
* **Nguy cơ**: Lộ lọt thông tin trong DB, kẻ tấn công có thể lạm dụng để khai thác các lỗ hổng khác
* **Mức độ**: Low
* **Nguyên nhân**: Lỗi kiểm soát dữ liệu đầu vào
* **Khắc phục**: Kiểm soát dữ liêu đầu vào, sử dụng library của MISA
* **Dựng lại lỗ hổng** :
* **Chèn kí tự ‘ vào sau tên column trong tham số sort**



* Chèn kí tự ‘ vào sau ViewName trong tham số customParam

