BÁO CÁO

KẾT QUẢ GRAYBOX PENETRATION TESTING HỆ THỐNG

Tên tổ chức: Công ty Cổ phần MISA

Tên ứng dụng: TaskGo

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: | 6/10/2021 – 12/10/2021 |
| Đối tượng đánh giá: | https://taskgov.misa.vn |
| Hình thức đánh giá: | Graybox |
| Tài khoản sử dụng: | Quản trị viên  User: demotaskgov.misa.vn  Pass:12345678@Abc |

PHẦN 2: KẾT QUẢ ĐÁNH GIÁ

|  |  |
| --- | --- |
| Kết quả chung | Có 3 lỗi |
| Đề xuất khắc phục | 3 |
| Số lỗi nghiêm trọng | 2 |
| Số lỗi cao | 0 |
| Số lỗi trung bình | 1 |
| Số lỗi thấp | 0 |

1. **Checklisk danh mục lỗ hổng:**

(File đính kèm taskgo[.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 |
| TASKGO-01 | Broken Access Control | Testing Broken Access Control | Mục 2.1 | Critial |
| TASKGO-02 | SQL injection | Testing for SQL injection | Mục 2.2 | Critial |
| TASKGO-03 | Disclosure Information | Testing for Sensitive information | Mục 2.3 | Medium |

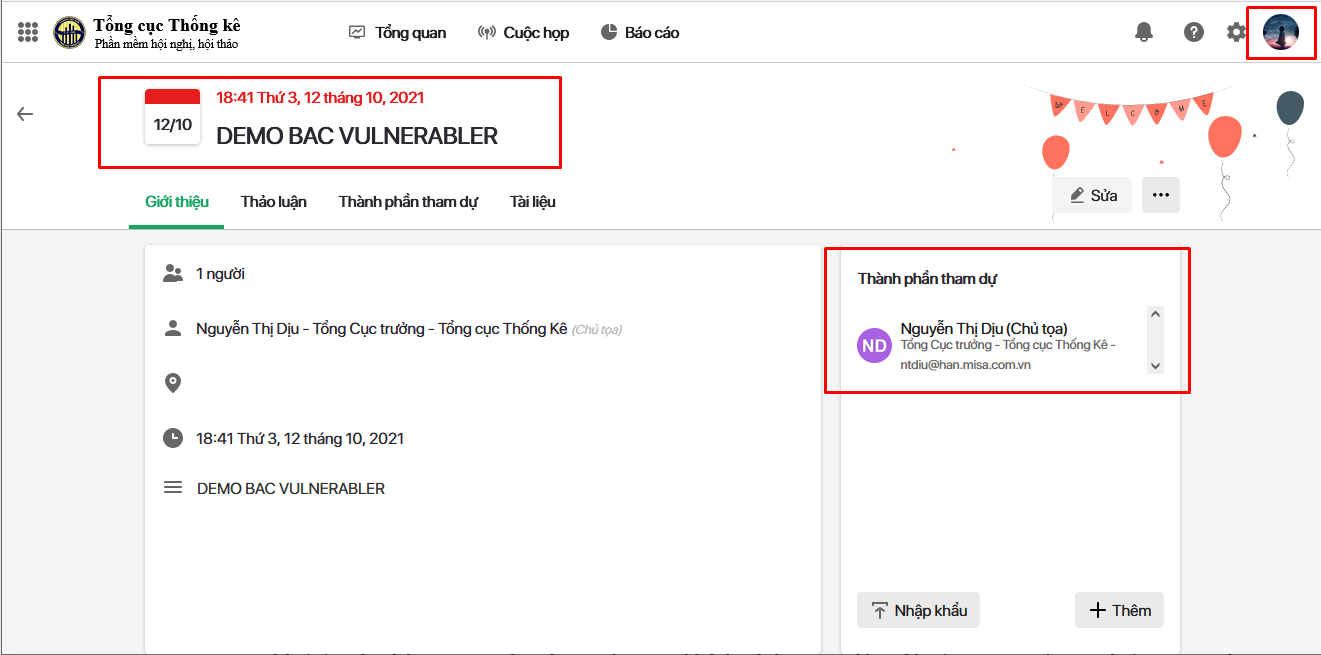
1. *Mô tả chi tiết:*
   1. **IDOR**

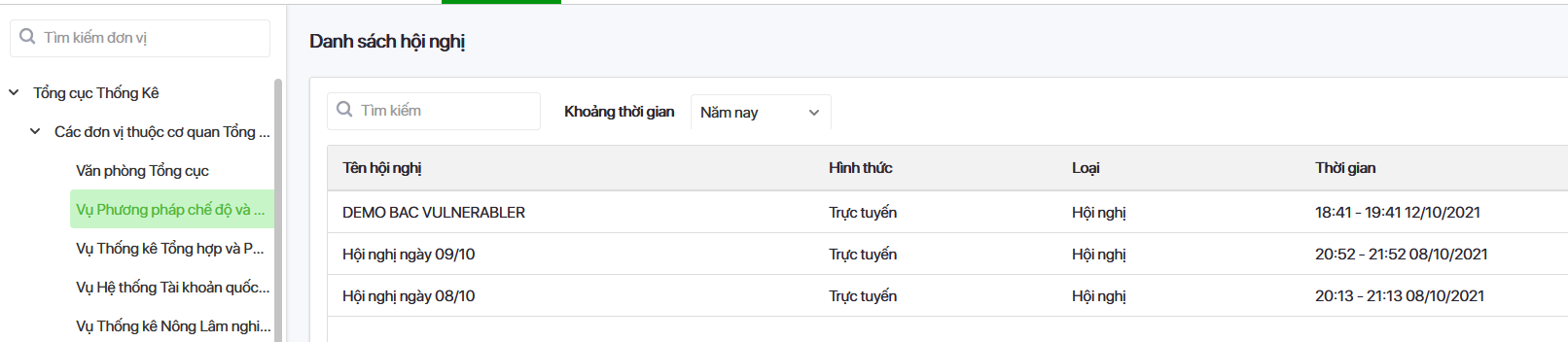
* **Mã lỗi**: TASKGO-01
* **Tên lỗ hổng trong danh mục**: Testing broken access control
* **Vị trí lỗi**: App Hội Nghị

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /APIS/EventAPI/api/event/deleteDataByID/X | X là EventID |
| 2 | /APIS/EventAPI/api/event/save |  |
| 3 | /event/meeting?eventId=438 | IDOR |

* **Mô tả**: Trong App Hội Nghị , lỗi kiểm soát truy cập ở các API , cho phép người dùng không có quyền có thể xem,sửa và xóa thông tin của các hội nghị chỉ cần biết giá trị EventID
* **Nguy cơ**: Kẻ tấn công có thể xem,sửa và xóa thông tin của các hội nghị bất kì
* **Mức độ**: Nguy hiểm
* **Nguyên nhân**: Lỗi kiểm soát truy cập
* **Khắc phục**: Khắc phục kiểm soát truy cập
* **Dựng lại lỗ hổng** :

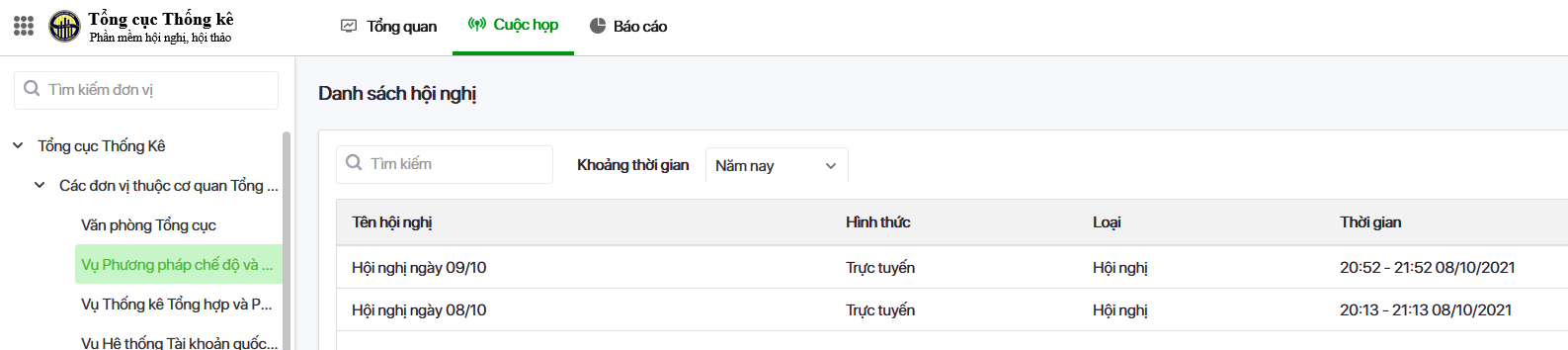
Bước 1: Đăng nhập tài khoản demotaskgo.misa.vn tạo hội nghị .





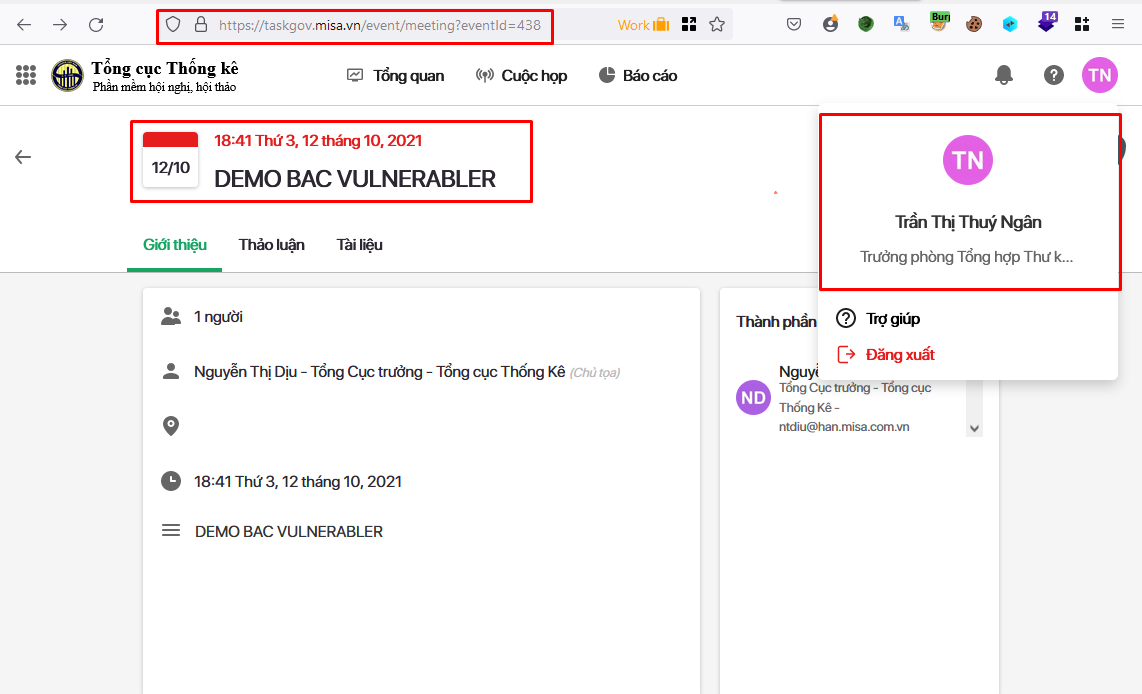
Bước 2: Đăng nhập vào tài khoản user chỉ có quyền thêm hội nghị 

Usser này không thể xem được hội nghị “DEMO BAC VULNERABLE”

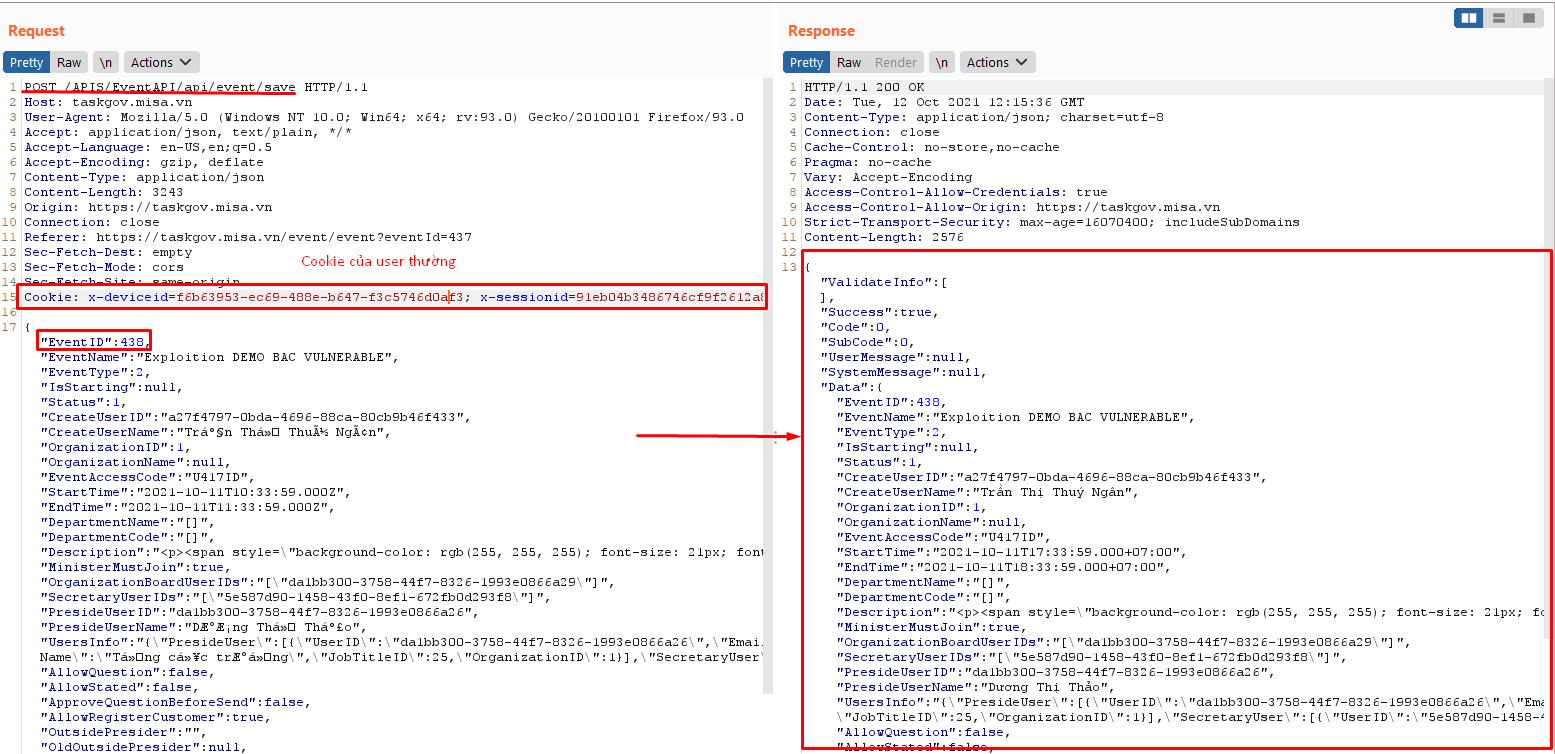


Bước 3: Sử dụng các Endpoint (Các vị trí lỗ hổng) trên để xem các thông tin trái phép :

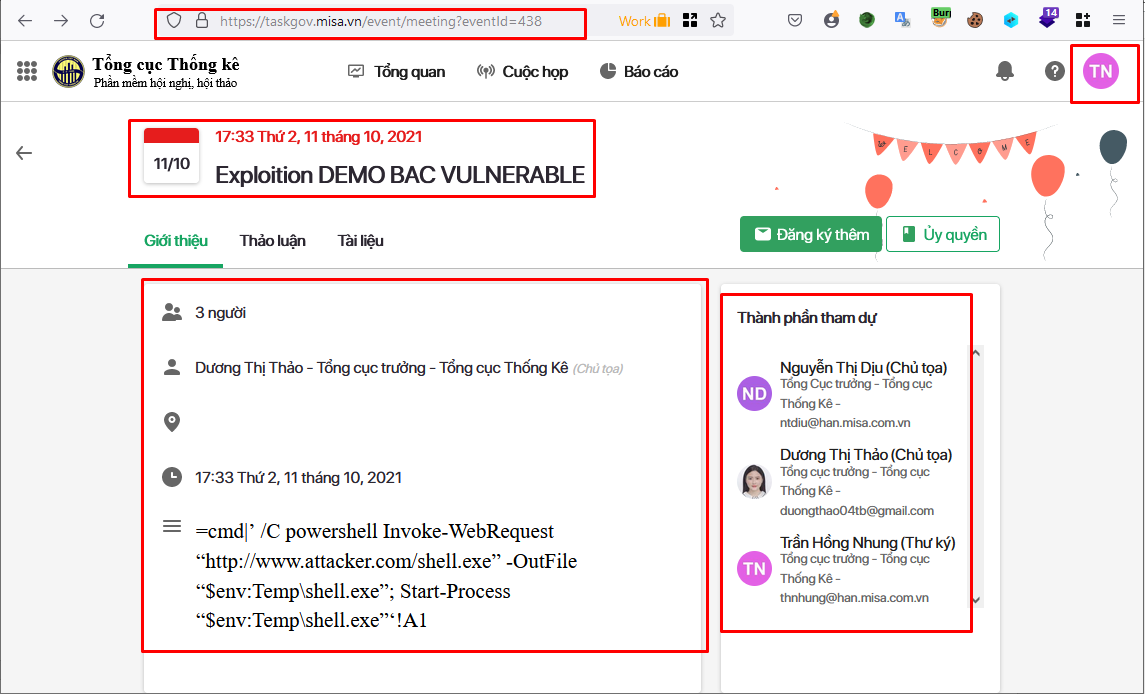
* Gõ đường dẫn trên trình duyệt



Trên trình duyệt có thể xem nhưng không thể sửa và xóa. Để Sửa và xóa cần burpsuite để bắt request và xác định được EventID cần sửa xóa.



Như vậy là có thể chỉnh sửa tùy ý

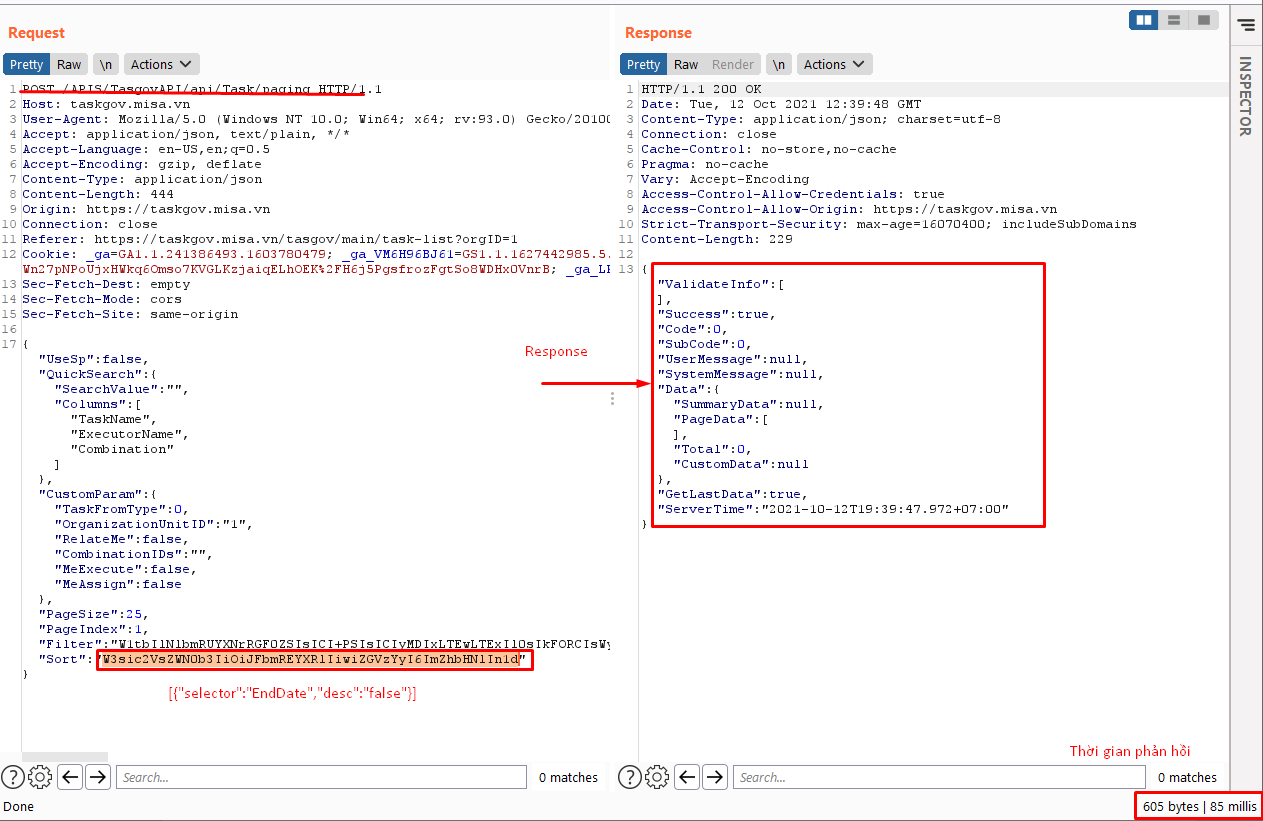


* Xóa lịch hội nghị cũng tương tự.
  1. **SQL injection**
* **Mã lỗi**: TASKGO-02
* **Tên lỗ hổng trong danh mục**: Testing for SQL injection
* **Vị trí lỗi**: Diện rộng – App Công Việc

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /APIS/TasgovAPI/api/Task/paging |  |
| 2 | /APIS/TasgovAPI/api/GroupCombination/paging |  |
| … | …. |  |

* **Mô tả**: Tại các tham số Sort và Filter trong data cho phép chèn các câu truy vấn SQL.
* **Nguy cơ**: Kẻ tấn công có thể đánh cắp dữ , thay đổi và xóa dữ liệu trong DB
* **Mức độ**: Critical
* **Nguyên nhân**: Chưa kiểm sát dữ liệu đầu vào.
* **Khắc phục**: Kiểm soát dữ liệu đầu vào từ client, lọc các kí tự đặc biệt. Đối với các toán tử nên harden hoặc không cho phép kiểm soát bởi phía client.
* **Dựng lại lỗ hổng** :
* **Tại tham số Sort**

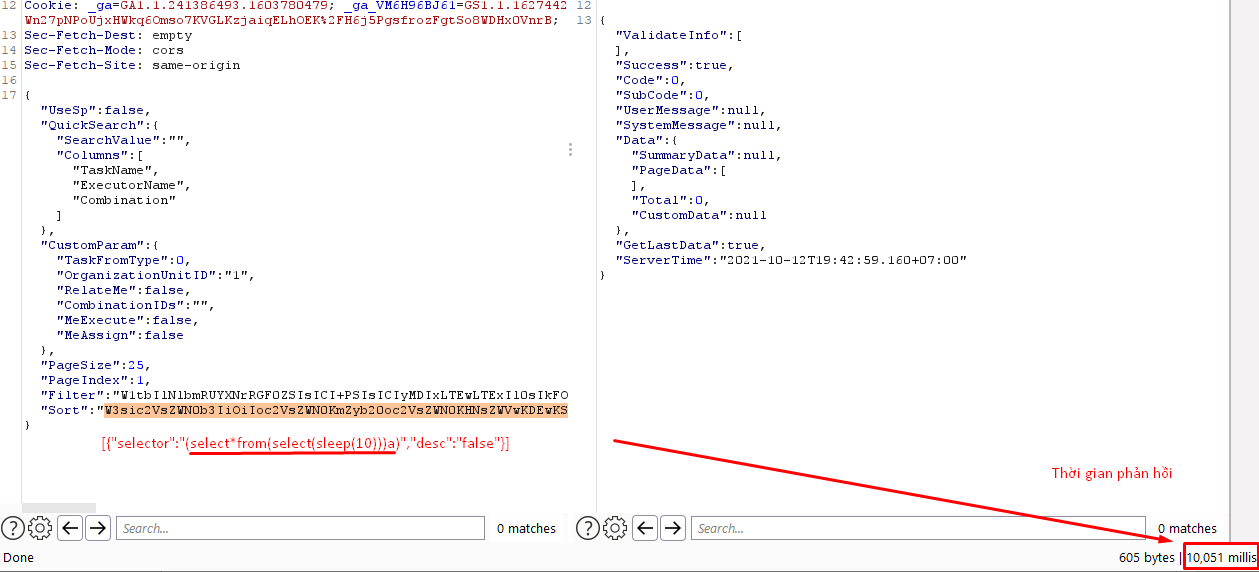
Bước 1: Đăng nhập tài khoản và bắt request.



Bước 2: Decode giá trị , chèn các câu query sql và encode lại để gửi lên server

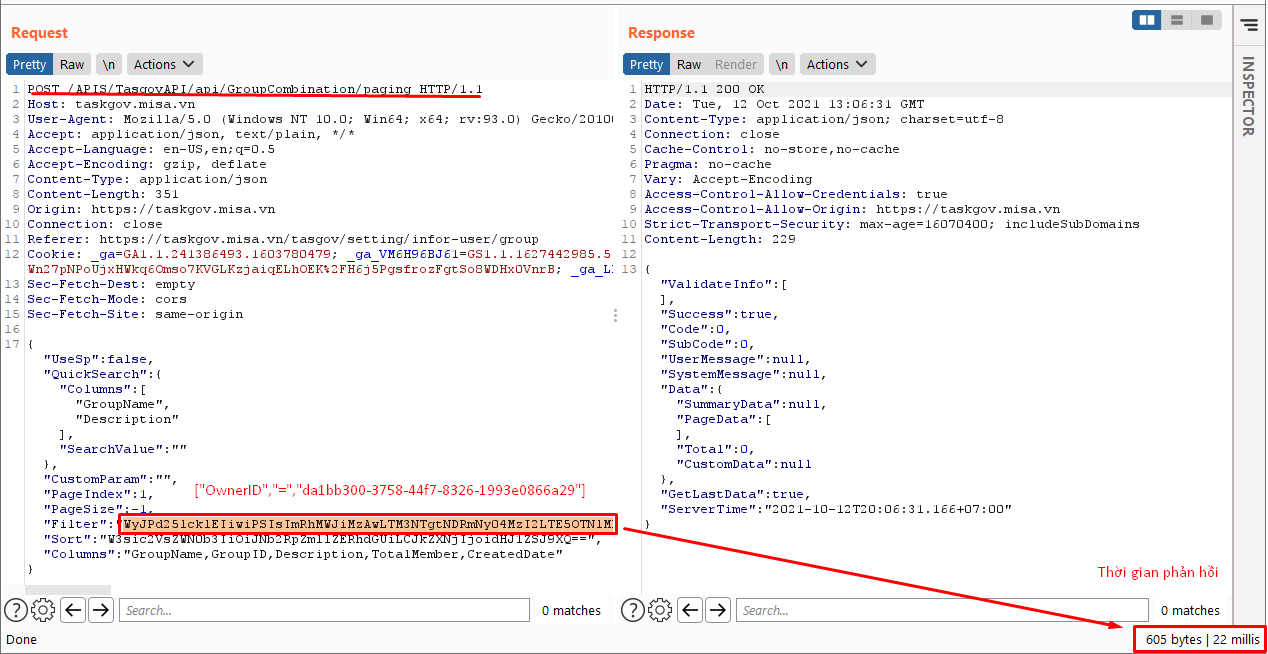
Payload: (select\*from(select(sleep(10)))a) -> true -> delay 10s mới phản hồi

Thay thể 5,15,20s để kiểm tra.



* **Tại tham số Filter**

Bước 1: Đăng nhập tài khoản và bắt request.



Bước 2: Decode giá trị , chèn các câu query sql và encode lại để gửi lên server

Payload: (select\*from(select(sleep(10)))a) -> true -> delay 10s mới phản hồi

Thay thể 5,15,20s để kiểm tra.



* 1. **SQL injection**
* **Mã lỗi**: TASKGO-02
* **Tên lỗ hổng trong danh mục**: Testing for Sensitive information
* **Vị trí lỗi**: Diện rộng – App Công Việc

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /APIS/TasgovAPI/api/Task/paging |  |
| 2 | /APIS/TasgovAPI/api/GroupCombination/paging |  |
| … | …. |  |

* **Mô tả**: Query DB trả về trong phản hồi phía người dùng do lỗi câu truy vấn.
* **Nguy cơ**: Kẻ tấn công có thể phân tích, lạm dụng query đến DB để khai thác lỗ hổng SQL injection như lỗi tại tham số Filter bên trên
* **Mức độ**: Medium
* **Nguyên nhân**: Trả về trực tiếp ngoại lệ trong phản hồi
* **Khắc phục**: Bắt các exception xảy ra và trả về trang thiết lập sẵn cho các lỗi như 400 – exception xảy ra.
* **Dựng lại lỗ hổng** :

Tại các vị trí có thể SQL injection, khi chèn các query không hợp lệ thì server đều trả về dòng code thực thi bị lỗi, trong đó có chứa câu query.

