BÁO CÁO

KẾT QUẢ GRAYBOX PENETRATION TESTING HỆ THỐNG

Tên tổ chức: Công ty Cổ phần MISA

Tên ứng dụng: QLCB

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://taskgov.misa.vn |
| Hình thức đánh giá: | Graybox |
| Tài khoản sử dụng: | -Quản trị viên  User: admin  Pass: 20202004@Qlcb  -Nhân viên  User: 12345678  Pass: 12345678@Abc |

PHẦN 2: KẾT QUẢ ĐÁNH GIÁ

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

1. **Checklisk danh mục lỗ hổng:**

(File đính kèm qlcb[.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 |
| QLCB-01 | Broken Access Control | Testing Broken Access Control | Mục 2.1 | Critial |

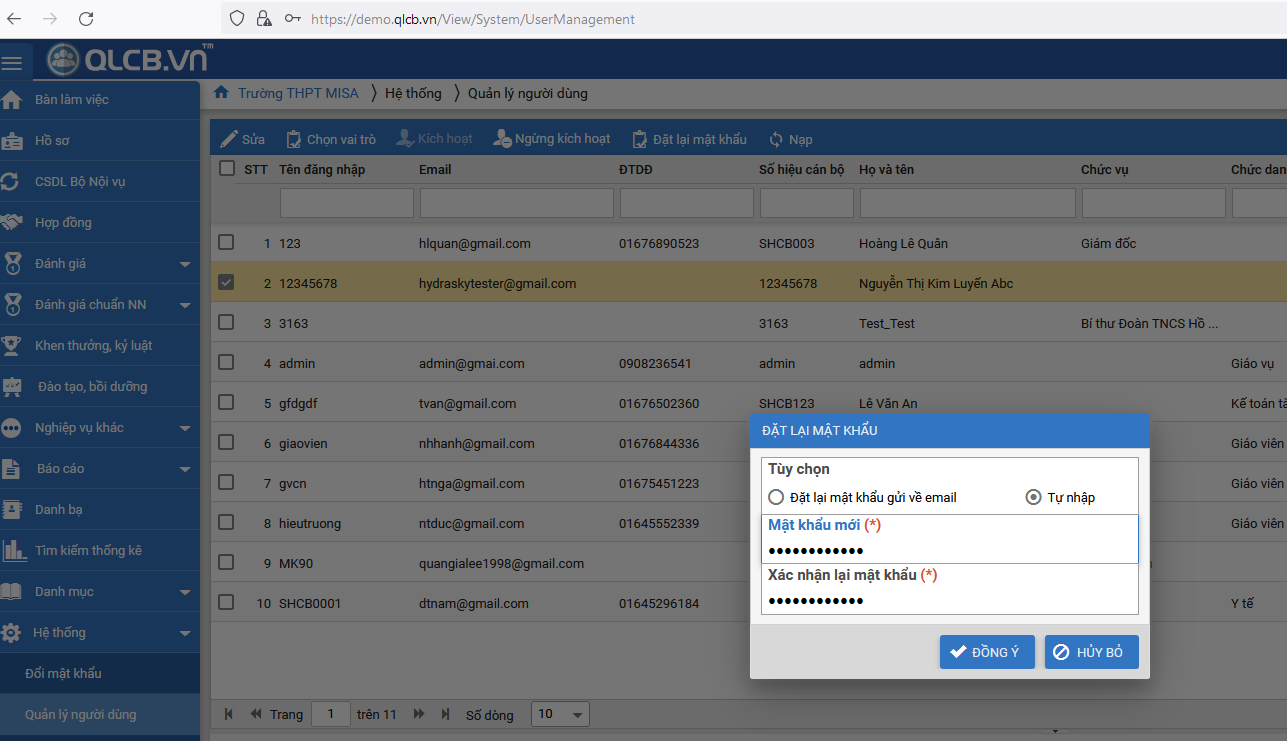
1. *Mô tả chi tiết:*
   1. **Broken Access Control**

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

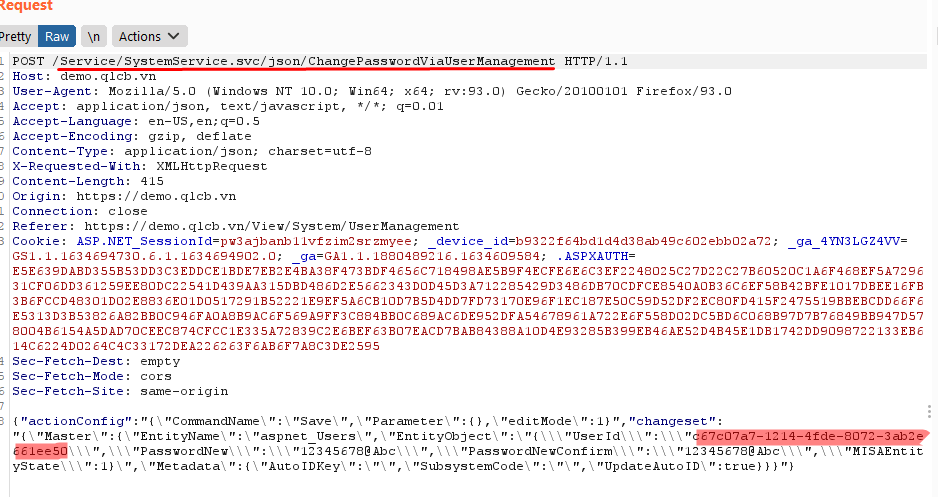
|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /Service/SystemService.svc/json/ChangePasswordViaUserManagement |  |

* **Mô tả**: Tại chức năng đổi mật khẩu của người dùng cho vai trò quản trị, có dính lỗi kiểm soát truy cập , cho phép user không có quyền có thể thực hiện request đổi mật khẩu của bất kì user nào nếu biết được id của người đó.
* **Nguy cơ**: Chiếm tài khoản của người dùng khác
* **Mức độ**: Nguy hiểm
* **Nguyên nhân**: Lỗi kiểm soát truy cập
* **Khắc phục**: Khắc phục kiểm soát truy cập
* **Dựng lại lỗ hổng** :

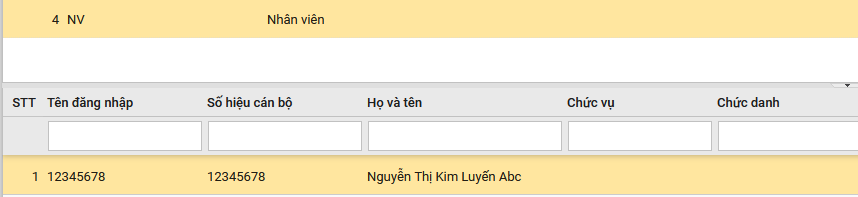
Bước 1: Đăng nhập vào tài khoản admin, vào mục Hệ thống -> Quản lí người dùng -> chọn một user bất kì -> Đặt lại mật khẩu. Sử dụng burpsuite để bắt lại request đổi mật khẩu này.



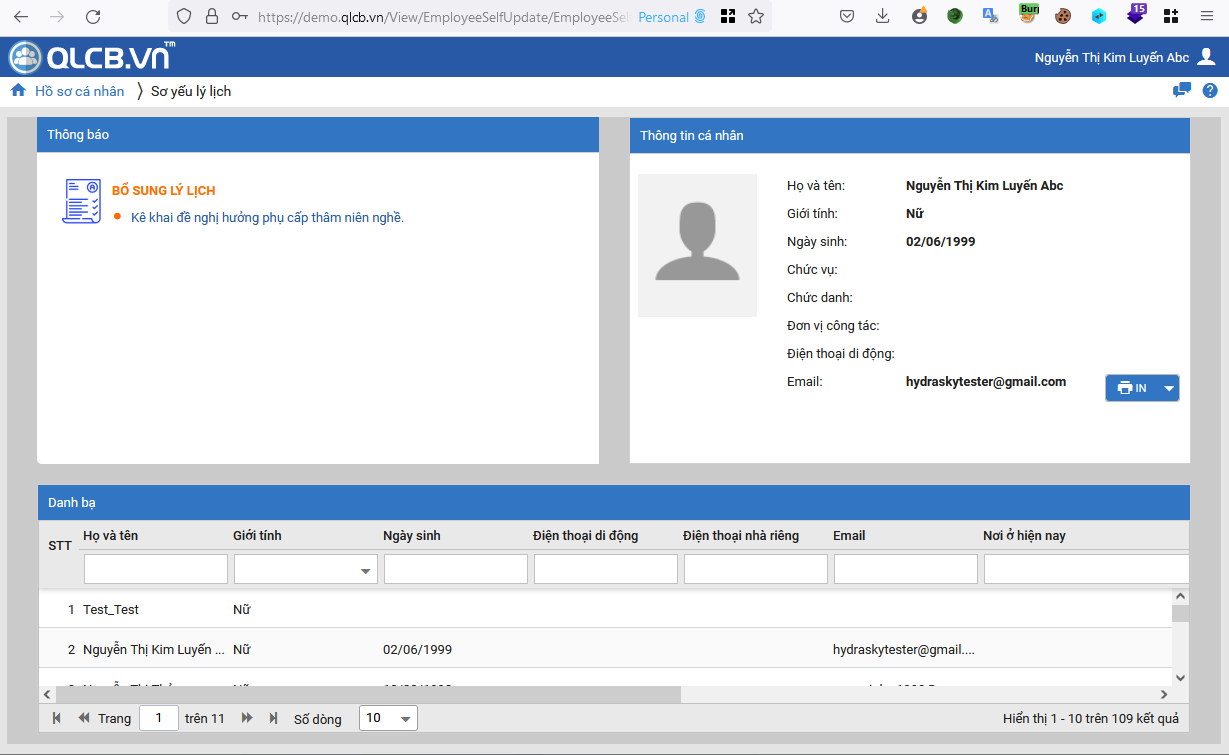
Request bắt lại bằng burpsuite.



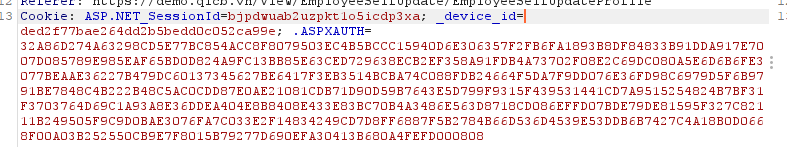
Bước 2: Đăng nhập vào user chỉ có quyền nhân viên (Không có quyền đổi mật khẩu người dùng khác) chỉ có thể xem profile.



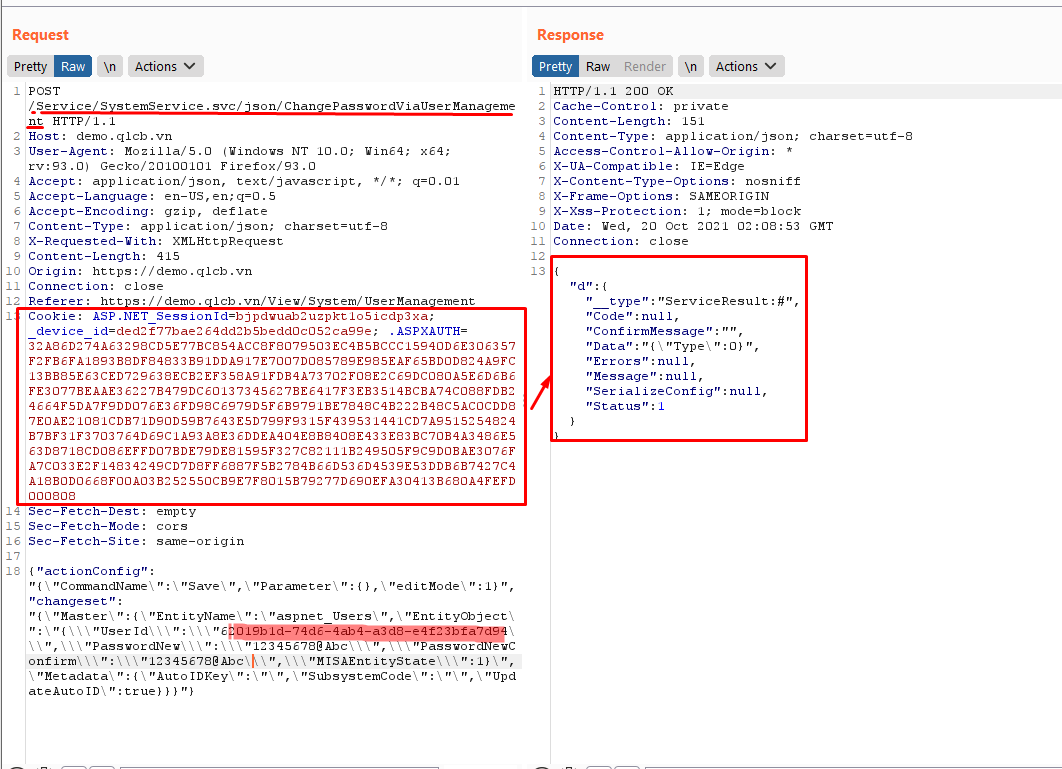
Không có chức năng nào cho vai trò nhân viên



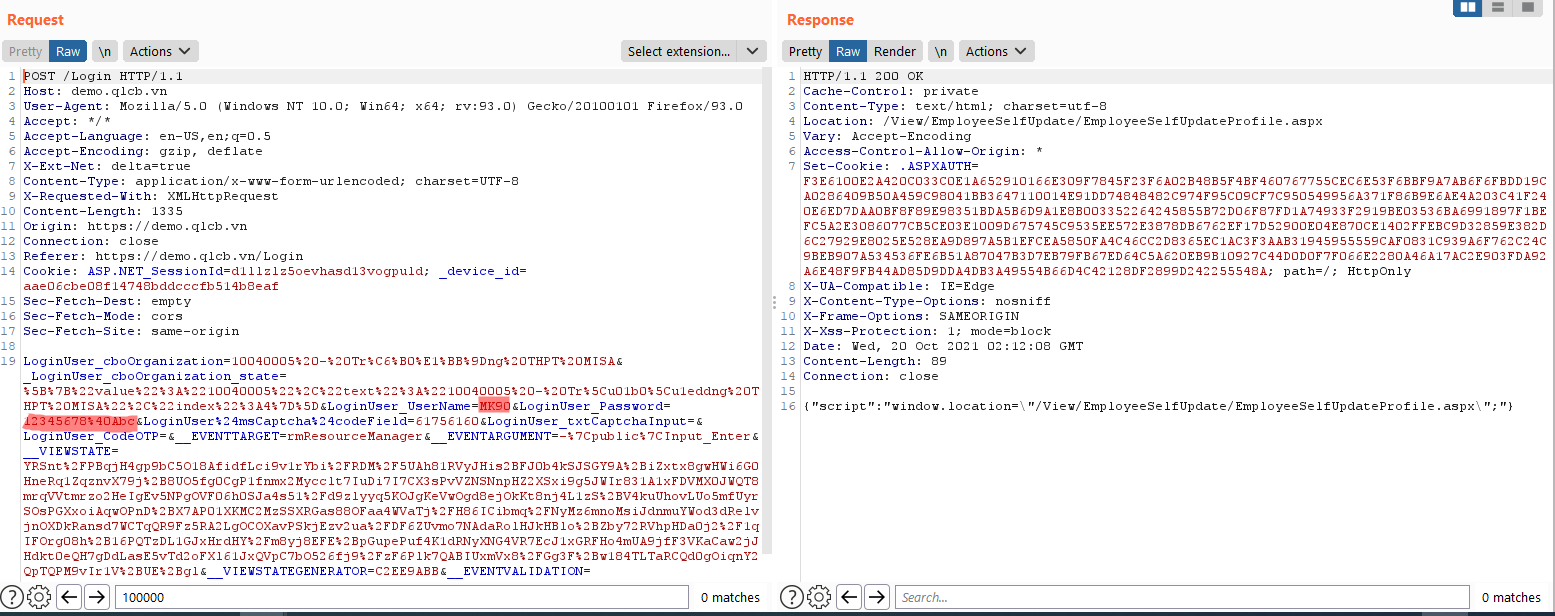
Sử dụng burpsuite bắt request của người dùng này để lấy cookie



Bước 3: Sử dụng cookie của user nhân viên thay vào request Đặt lại mật khẩu bắt được ở bước 1. Có thể thay giá trị UserId bất kì



Bước 4: Kiểm tra lại bằng việc Đăng nhập tài khoản bị đổi bằng mật khẩu.



Có thể đổi được cả tài khoản admin

