BÁO CÁO

KẾT QUẢ GRAYBOX PENETRATION TESTING HỆ THỐNG

Tên tổ chức: Công ty Cổ phần MISA

Tên ứng dụng: CUKCUK

Thời gian thực hiện: Tháng 11/2021

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: | 29/10/2021 – 10/11/2021 |
| Đối tượng đánh giá: | https://test01.cukcuk.vn |
| Hình thức đánh giá: | Graybox |
| Tài khoản sử dụng: | -Quản trị viên  User: ntyen  Pass: 123456aA  -Nhân viên  User: nv01  Pass: 123456aA |

PHẦN 2: KẾT QUẢ ĐÁNH GIÁ

|  |  |
| --- | --- |
| Kết quả chung | Có 4 lỗi |
| Đề xuất khắc phục |  |
| Số lỗi nghiêm trọng | 1 |
| Số lỗi cao | 1 |
| Số lỗi trung bình | 1 |
| Số lỗi thấp | 1 |

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 |
| CUKCUK-01 | Broken Access Control | Testing Broken Access Control | Mục 2.1 | Critial |
| CUKCUK-02 | Bypass password authentication in data maintenance feature | Bypass authentication schema | Mục 2.2 | High |
| CUKCUK-03 | API unauthenticated | Bypass authentication schema | Mục 2.3 | Medium |
| CUKCUK-04 | Error information disclosure | Testing for sensitive information disclosure | Mục 2.4 | Low |

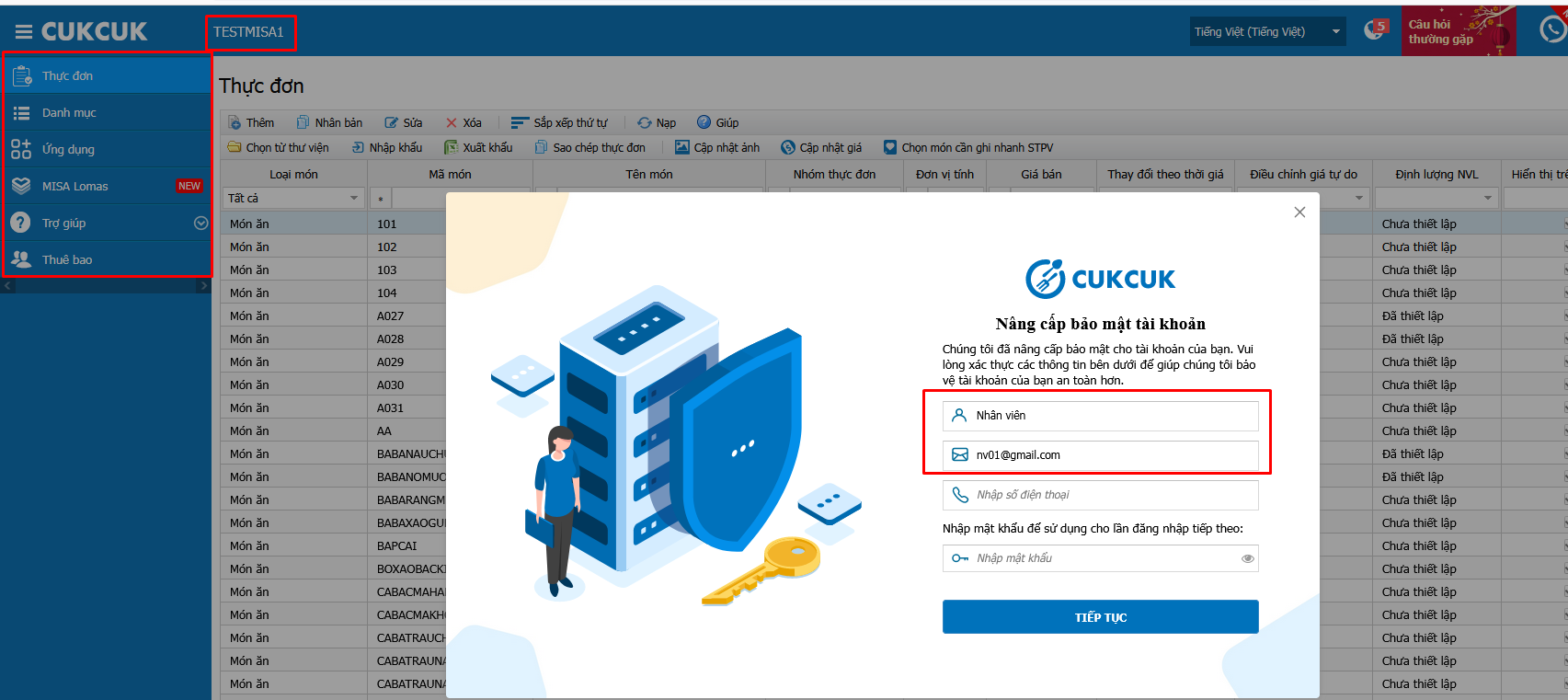
1. *Mô tả chi tiết:*
   1. **Broken Access Control**

* **Mã lỗi**: CUKCUK-01
* **Tên lỗ hổng trong danh mục**: Testing broken access control
* **Vị trí lỗi**: Diện rộng (Yêu cầu check lại toàn bộ các endpoint)

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /Service/SettingService.svc/GetAllAuditingLogPaging |  |
| 2 | /Service/SettingService.svc/GetAllMSC\_RolePaging |  |
| 3 | Service/SettingService.svc/GetPermissionsOfRoleInSubSytem |  |
| 4 | /Service/SettingService.svc/CheckDelete |  |
| 5 | /Service/DictionaryService.svc/SubmitChanges |  |
| … | … |  |

* **Mô tả**: Người dùng không được phân quyền vẫn có thể truy cập được vào dữ liệu thông qua các endpoint trên
* **Nguy cơ**: Lấy thông tin của shop khác, thực thi các chức năng không được phân quyền dẫn đến leo thang đặc quyền.
* **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 nhân viên “nv01” , bắt request và lấy cookie của user này. (User chỉ có quyền quản lí thực đơn)



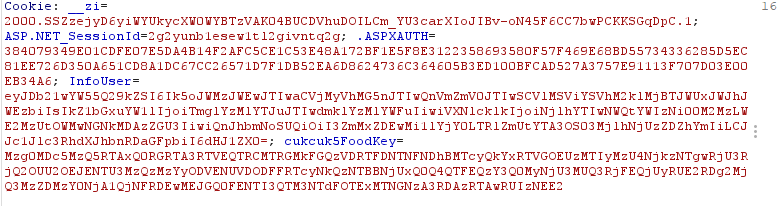
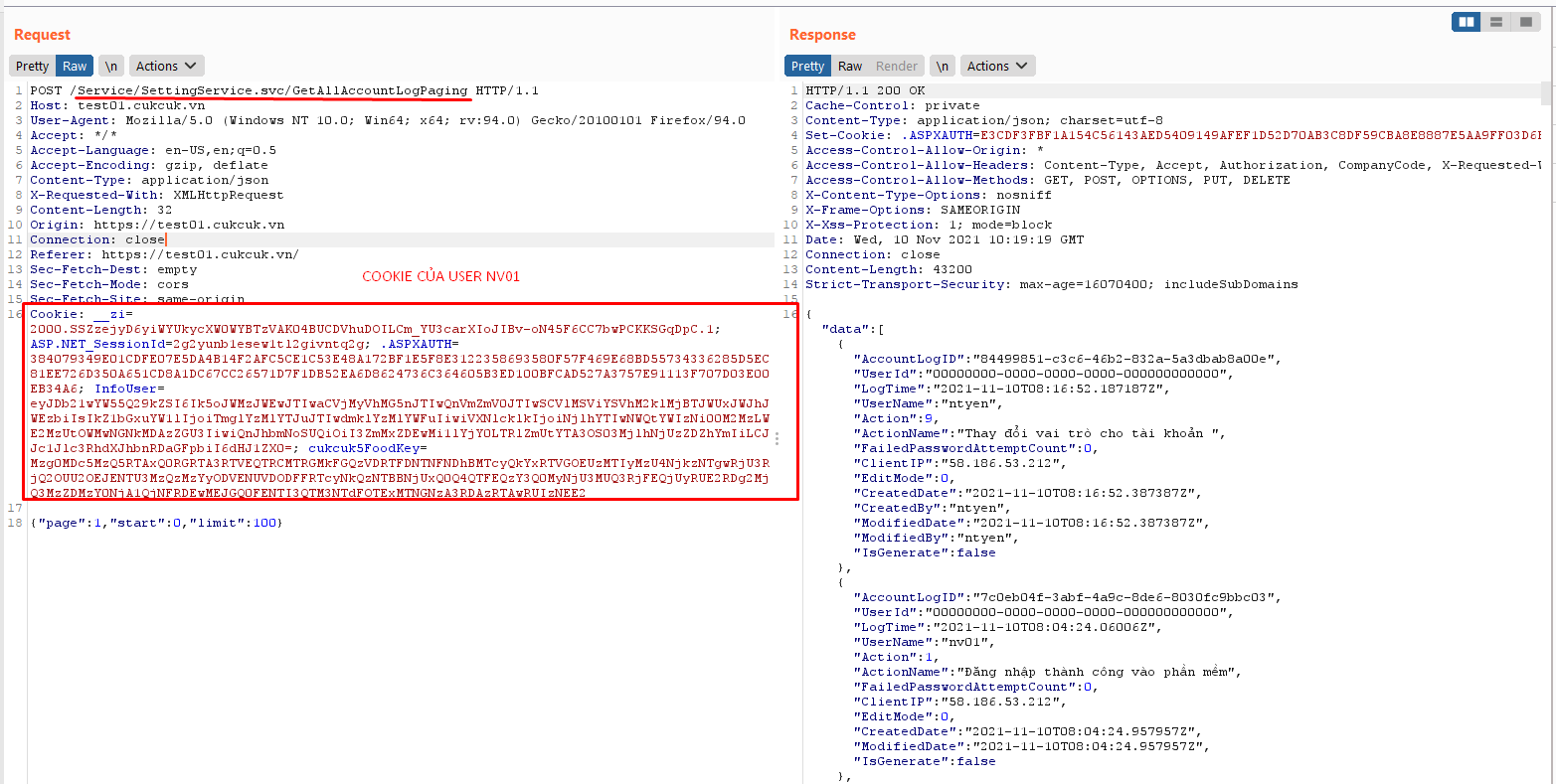
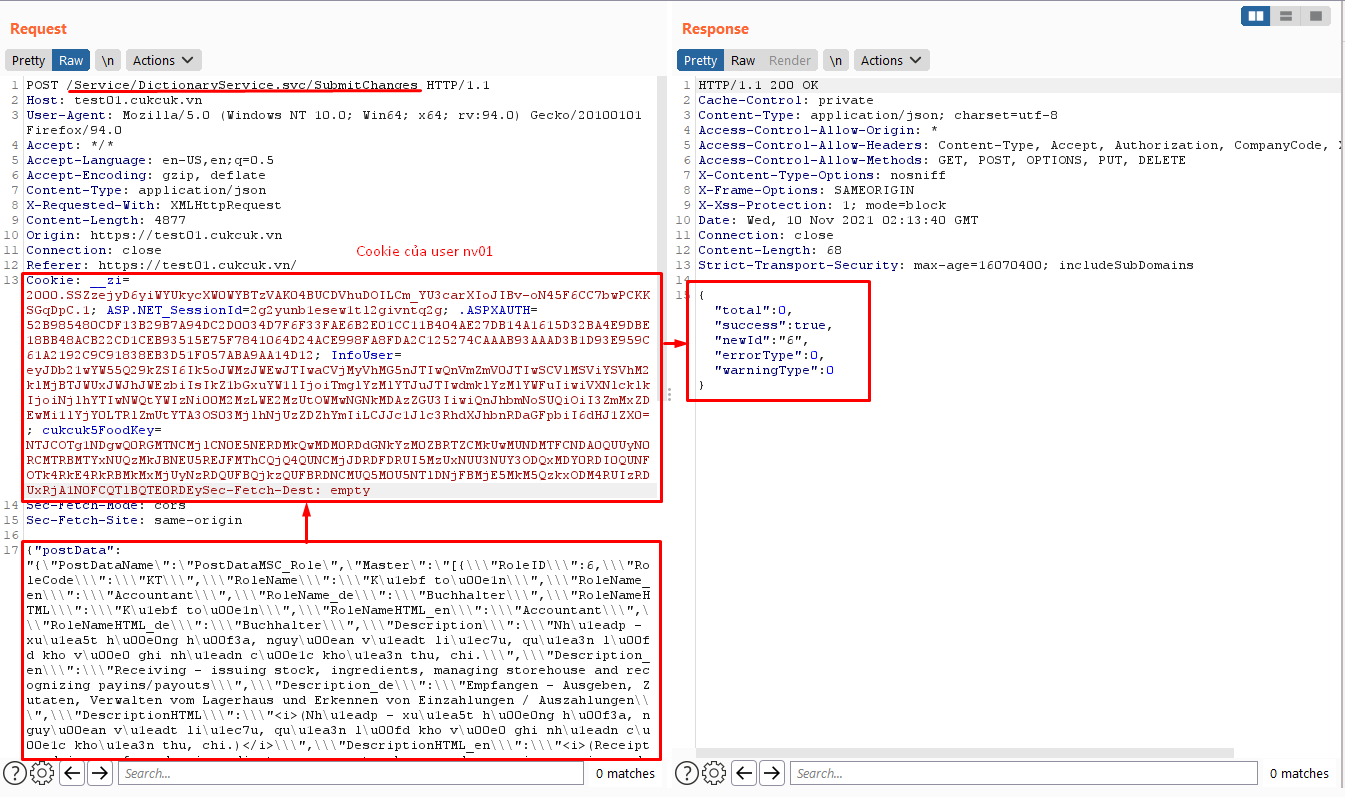


Figure 1: Cookie của user nv01

Bước 2: Lấy cookie thay thế vào các request đọc nhật kí truy cập chỉ admin có thể thực hiện để kiểm tra việc kiểm soát truy cập. Dữ liệu vẫn trả về



Bước 3. Thực hiện tự thêm vai trò cho tài khoản (leo thang đặc quyền).

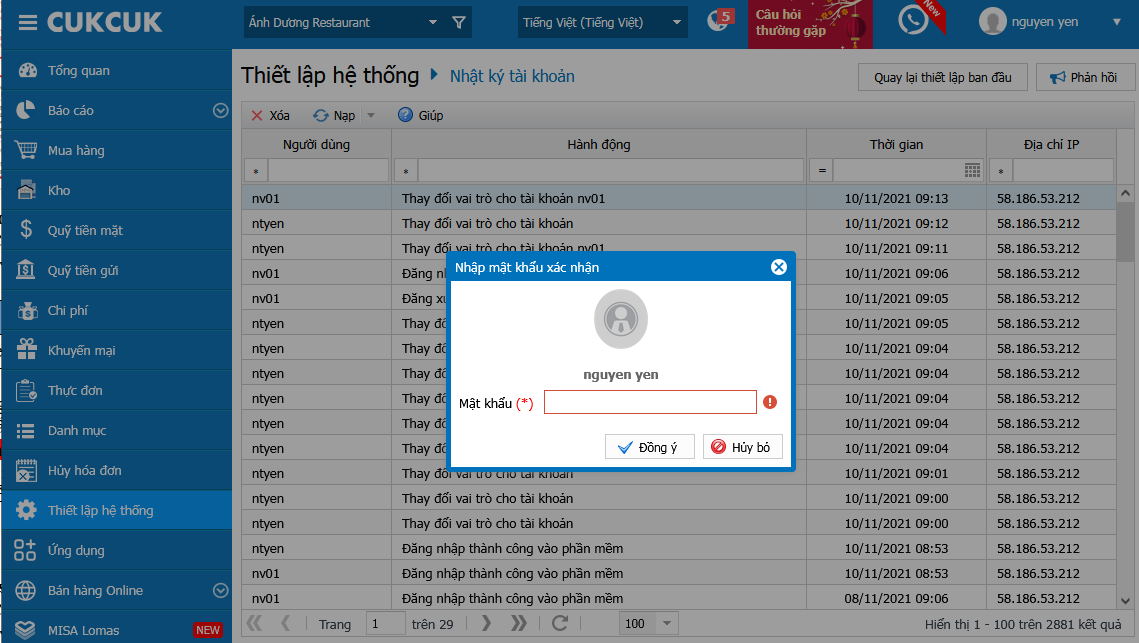


* 1. **Bypass password authentication in data maintenance feature**
* **Mã lỗi**: CUKCUK-02
* **Tên lỗ hổng trong danh mục**: Testing bypass authentication schema
* **Vị trí lỗi**:

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /Service/SettingService.svc/CheckOldPassword |  |

* **Mô tả**: Có thể bỏ qua yêu cầu xác thực bằng mật khẩu tại chức năng bảo trì dữ liệu trong mục thiết lập hệ thống mà không cần biết mật khẩu.
* **Nguy cơ**: Kẻ tấn công có thể thực hiện chức năng không được phép
* **Mức độ** : High
* **Nguyên nhân** : Thực hiện xác thực phản hồi ở phía client
* **Tái dựng lỗ hổng** :

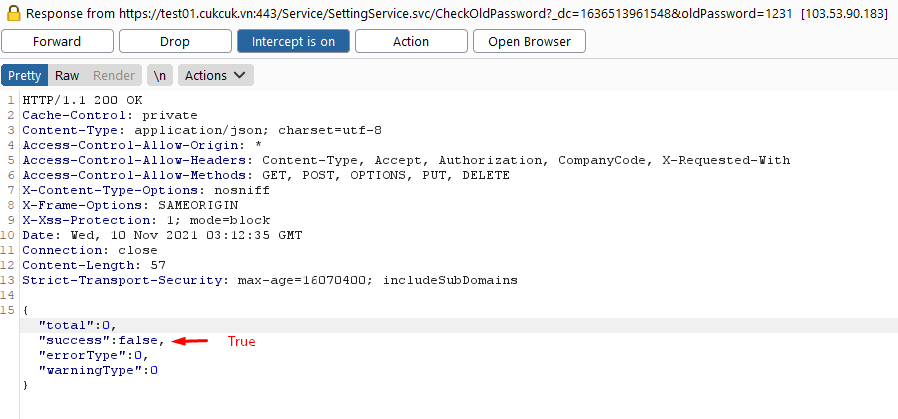
Bước 1: Vào mục Thiếp lập hệ thống -> Bảo trì dữ liệu -> Nhập password bất kì



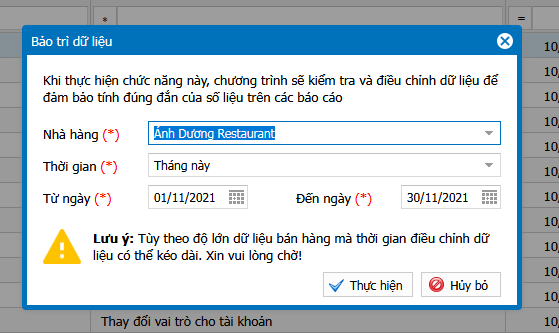
Bước 2: Sử dụng burpsuite để gửi request và chặn response trả về trình duyệt



Bước 3: Sửa message trong phản hồi (response) từ server về -> “success”:false thành “success”: true



Kết quả



Ngoài ra , nên thay request bằng phương thước POST bởi vì dùng phương thức GET để gửi tham số oldpassword cũng có thể là lỗ hổng . Kẻ tấn công có thể crawl hoặc lạm dụng cache để thu thập các giá trị oldpassword trên url.

* 1. **API unauthenticated**
* **Mã lỗi**: CUKCUK-03
* **Tên lỗ hổng trong danh mục**: Testing bypass authentication schema
* **Vị trí lỗi**:

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /Service/LicenseServiceClient.svc/GetLicenseObjectInfo |  |
| 2 | /Service/LicenseServiceClient.svc/GetLicenseObjectInfo\_Payment |  |

* **Mô tả**: Bất kì ai cũng có thể truy cập 2 endpoint này đẻ xem thông tin host đã đăng kí với bên CUKCUK
* **Nguy cơ**: Kẻ tấn công có thể kiểm tra được ngày tháng đăng kí và hết hạn của cửa hàng với bên CUKCUK. Từ có thể thực chiếm đoạt, lừa đảo lấy tên miền con
* **Mức độ**: Medium
* **Nguyên nhân**: Không có cơ chế xác thực
* **Khắc phục**: Bổ sung cơ chế xác thực bằng cookie cho endpoint
* **Dựng lại lỗ hổng** :

Bước 1: Bắt request bằng burpsuite, Không cần dùng cookie trong request



Bước 2: Có thể xem bất kì của hàng nào chỉ cần thay trường HOST header:

test01 -> test



* 1. **Error information disclosure**
* **Mã lỗi**: CUKCUK-04
* **Tên lỗ hổng trong danh mục**: Testing for sensitive information disclosure
* **Vị trí lỗi**: Diện rộng (Yêu cầu check lại toàn bộ các endpoint)

|  |  |  |
| --- | --- | --- |
| STT | Url | Ghi chú |
| 1 | /Service/CAService.svc/GetAllCAReceiptPaymentPaging |  |
| 2 | /Service/DictionaryService.svc/GetAllKitchenbyBranch |  |
| 3 | /Service/CostService.svc/GetAllCostPaging |  |
| 4 | /Service/DictionaryService.svc/GetInventoryItemMateriaType\_ByLoadType |  |
| 5 | /Service/DictionaryService.svc/GetCustomerCategory |  |
| .. | … |  |

* **Mô tả**: Khi truyền các giá trị không hợp lệ vào các tham số đầu vào thì app đều bắn trực tiếp exception về phía người dùng.
* **Nguy cơ**: Kẻ tấn công có thể lạm dụng các thông tin lỗi để thu thập và thực hiện các kiểu tấn công khác
* **Mức độ**: Low
* **Nguyên nhân**: Không trả về trang custem thông báo lỗi
* **Khắc phục**: Trả về trang custom thông báo lỗi
* **Dựng lại lỗ hổng** :

Bước 1: Sử dụng burpsuite để bắt request và chuyền các giá trị không hợp lệ vào các tham số đầu vào dể bắt exception

