Report eProfile

Tổng số lỗi: 4

1. iDOR: user x có thể xem được thông tin của user y nào đó.

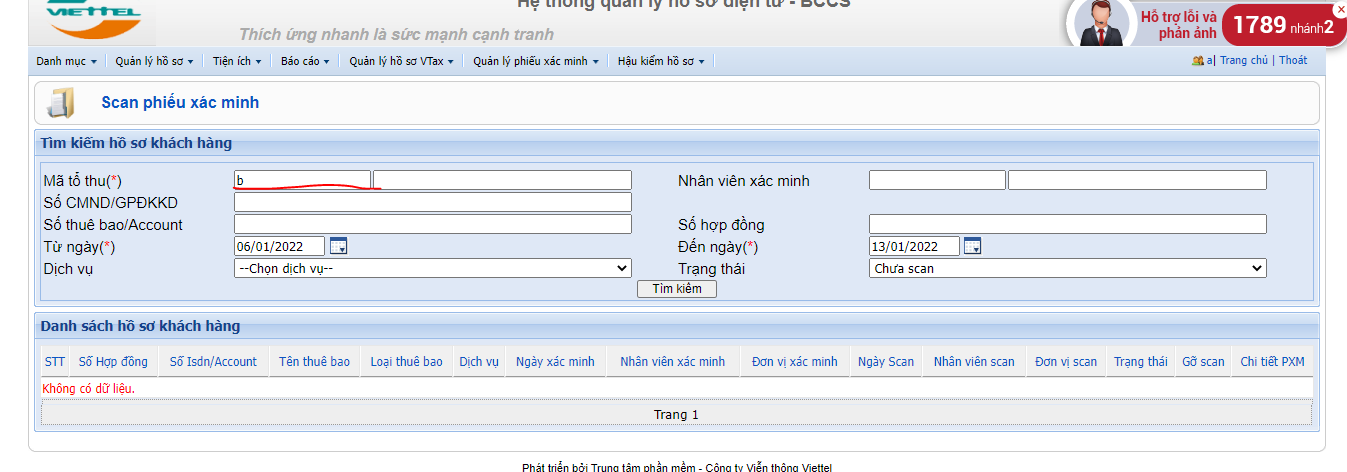
Mức độ: thấp

Ảnh hưởng: kẻ tấn công có thể lấy được thông tin của user mà họ không có quyền.

Fix: Kiểm tra quyền trước khi thực hiện lấy thông tin.

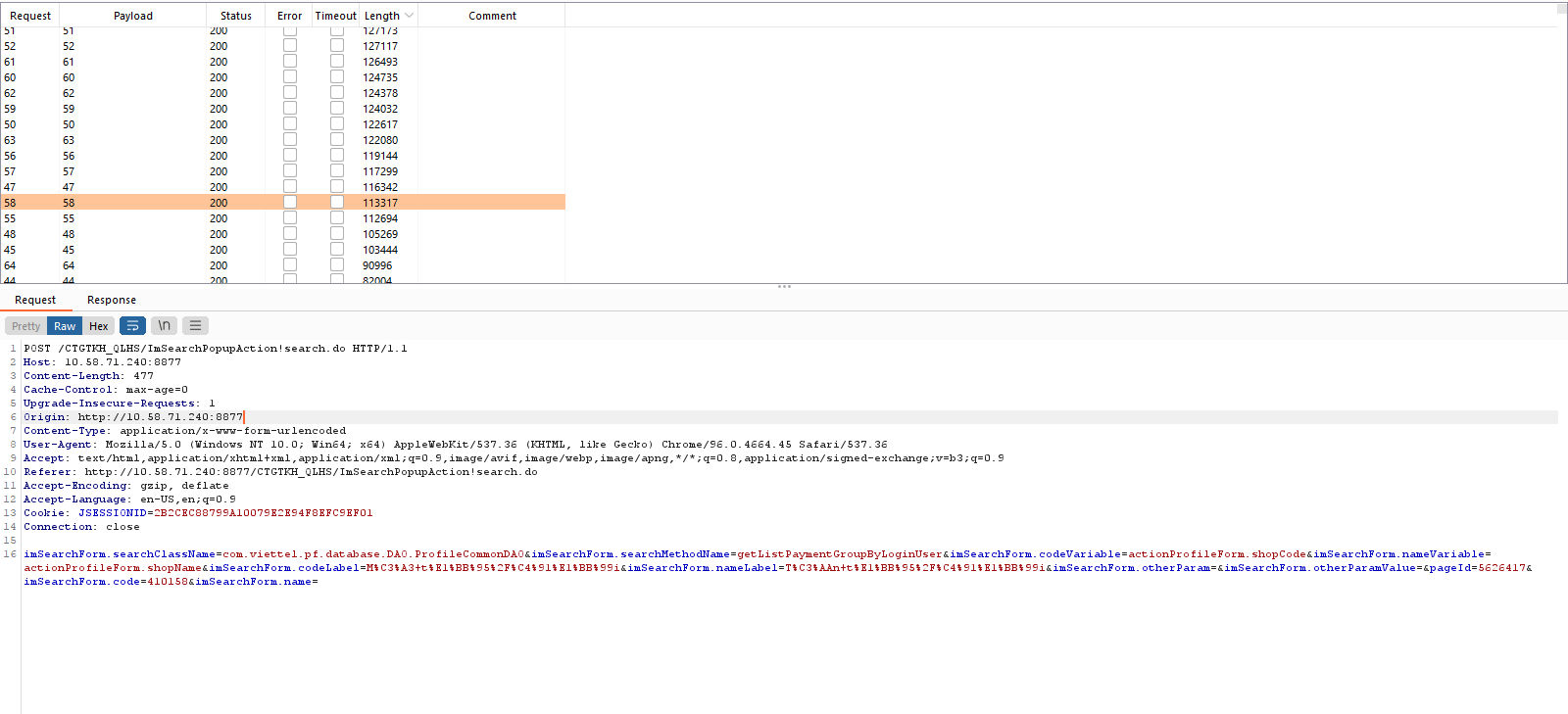
PoC:

* Chức năng Scan phiếu xác minh

Bước 1: đăng nhập vào user tiendc\_test vào chức năng Scan phiếu xác minh: 

Bước 2: tìm kiếm mã tổ thu, sau đó bắt request.

Bước 3: thay đổi giá trị imSearchForm.code, ta sẽ list được danh sách của user khác

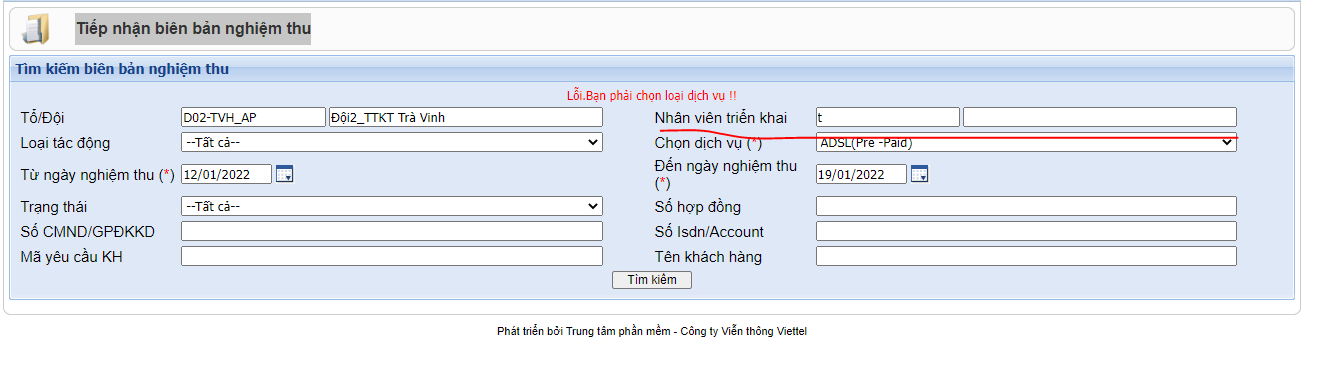


Bước 3: lấy chọn một số selectedShopId bất kỳ và thay thế ở chức năng displayShop để nhìn thông tin cụ thể của từng kênh bán hàng.

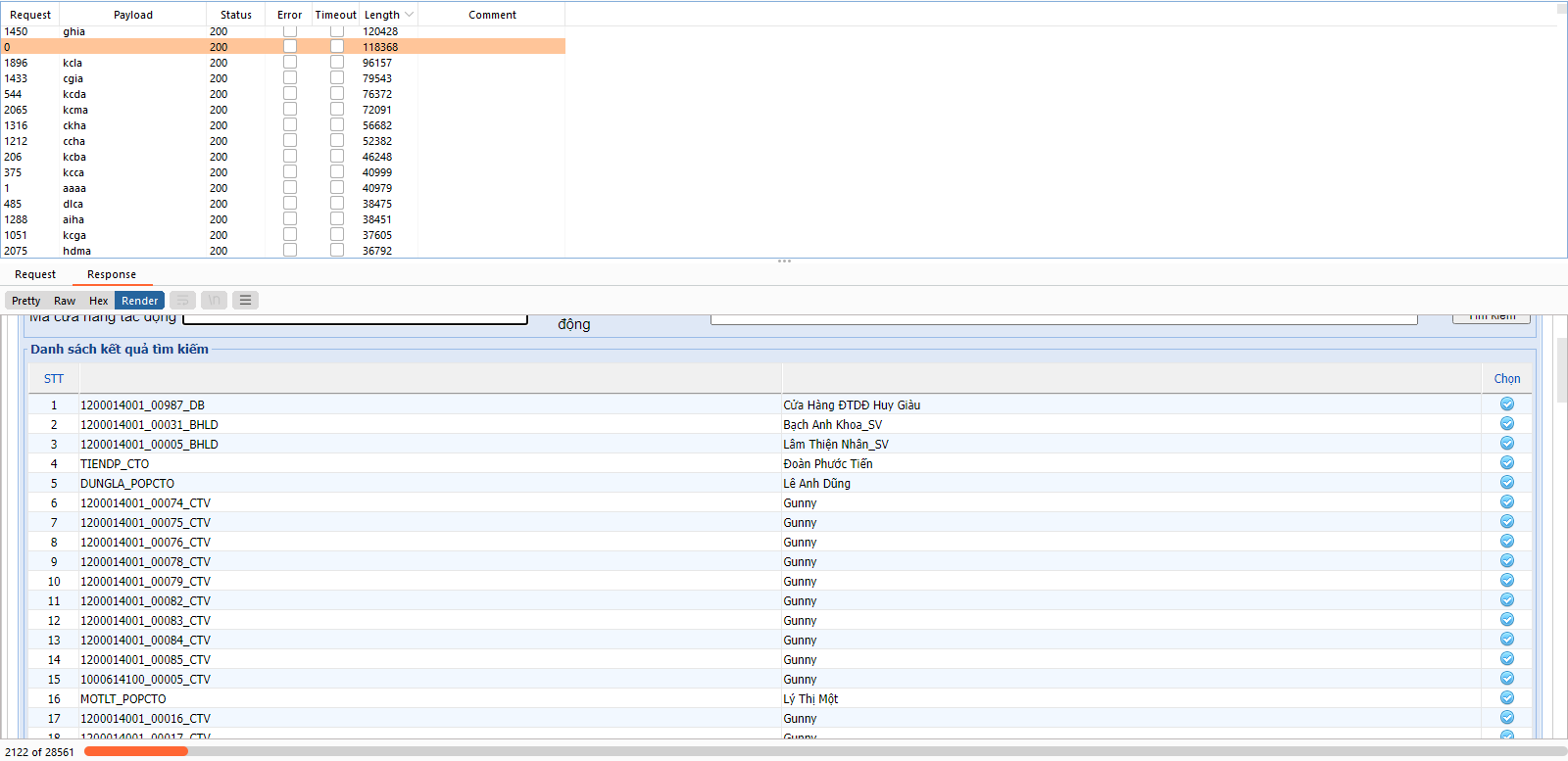


* Chức năng Tiếp nhận biên bản nghiệm thu

Bước 1: chọn tìm kiếm nhân viên triển khai



Bước 2: bắt request tìm kiếm và sử dụng các mẫu tìm kiếm khác nhau sẽ cho ra các kết quả của cửa hàng khác.



1. DOS

Mức độ: Thấp.

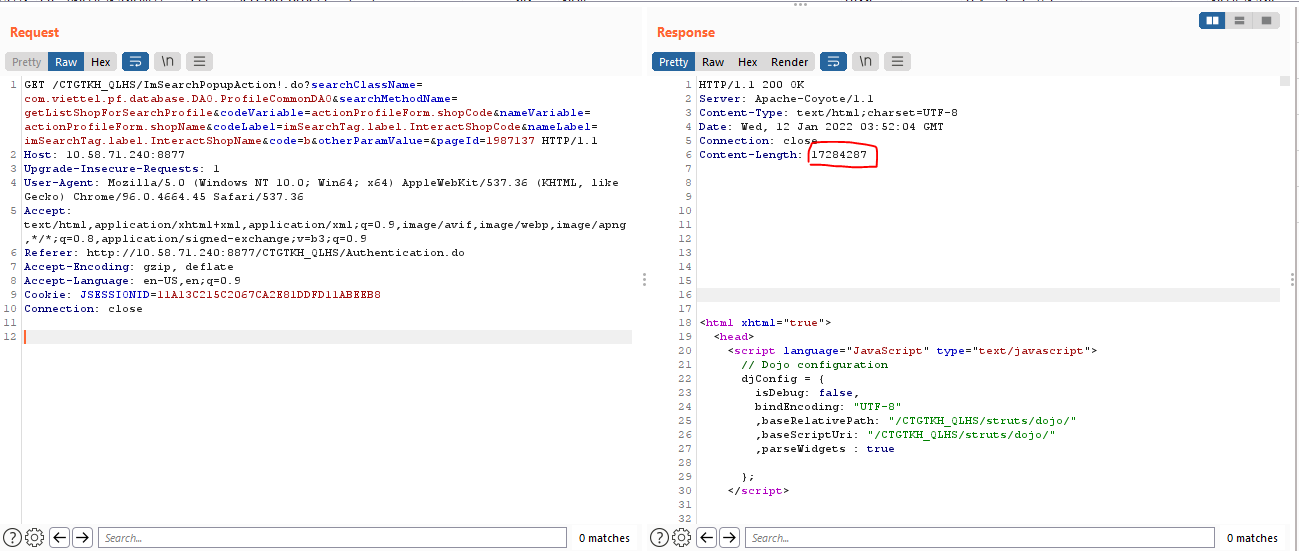
Nguyên nhân: trả về quá nhiều dữ liệu.

Ảnh hưởng: gây chậm dịch vụ.

Fix: thực hiện phân trang.

PoC

Endpoint: ImSearchPopupAction!.do



1. CSRF

Mức độ: yếu

Nguyên nhân: không kiểm tra token người dùng.

Ảnh hưởng: người dùng vô tình click vào đường dẫn, dẫn tới việc xóa mất một record.

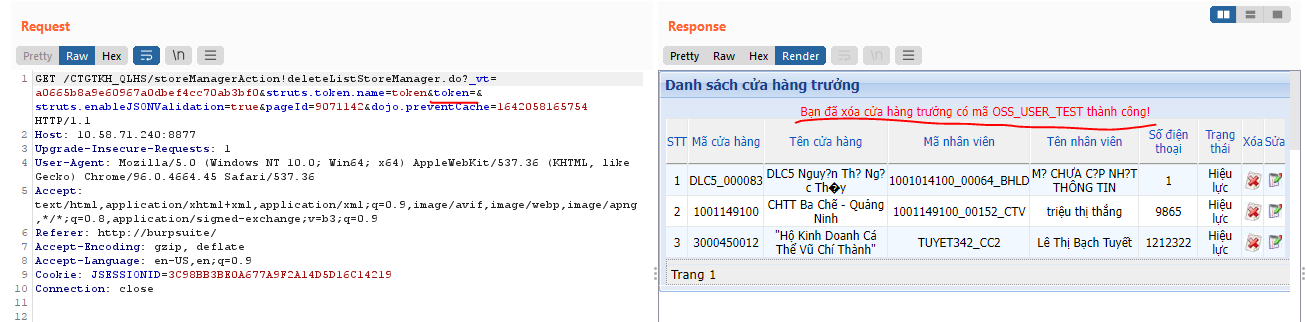
Fix: kiểm tra token người dùng gửi lên

PoC:

* Endpoint ảnh hưởng.

/CTGTKH\_QLHS/cusTypeGroupAction!deleteListStoreManager.do

/CTGTKH\_QLHS/configRegionByProvince!deleteListRegionByProvince.do





1. XSS stored

Mức độ: Cao.

Chức năng: thêm mới thông báo.

Nguyên nhân: không encode dữ liệu đầu ra.

Ảnh hưởng: kẻ tấn công có thể thực hiện những hành động trên trình duyệt mà người dùng không hay biết.

Fix: encode dữ liệu do người dùng nhập vào trước khi lưu vào DB.

PoC:

