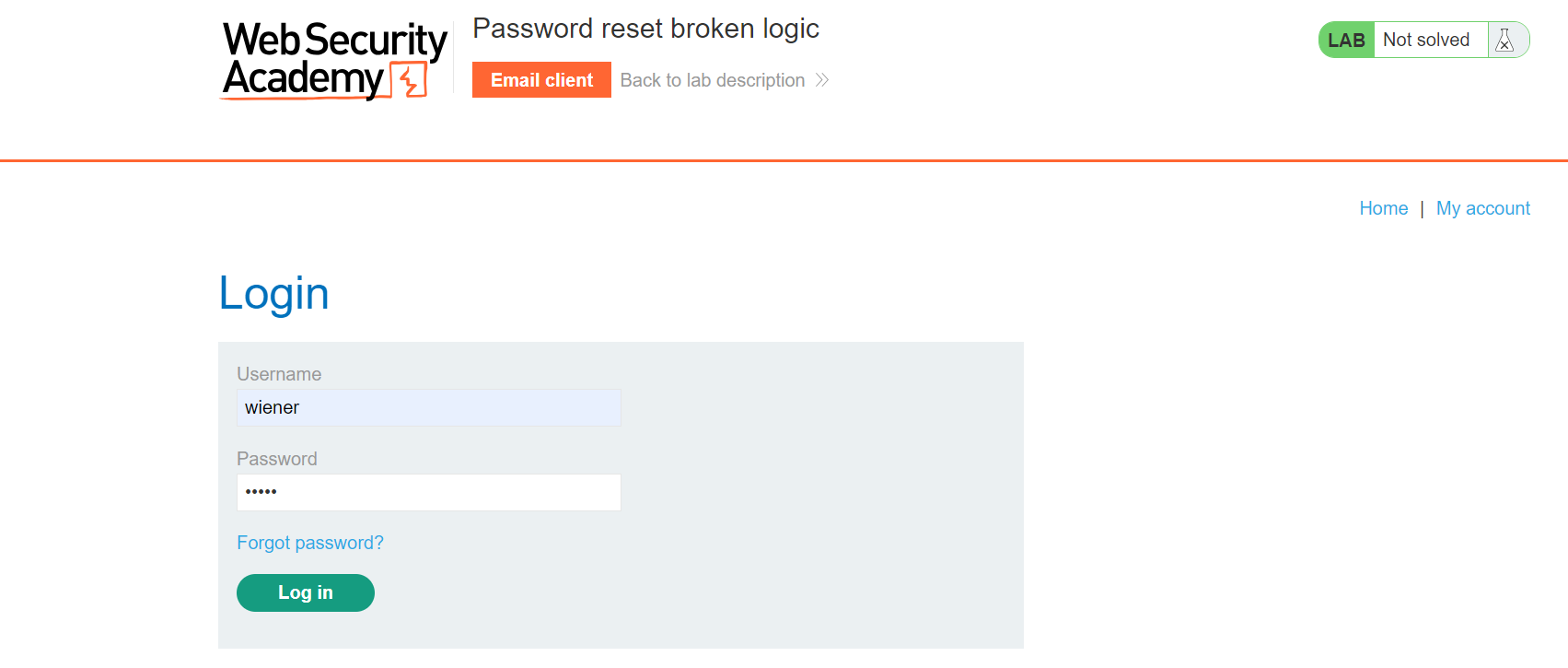
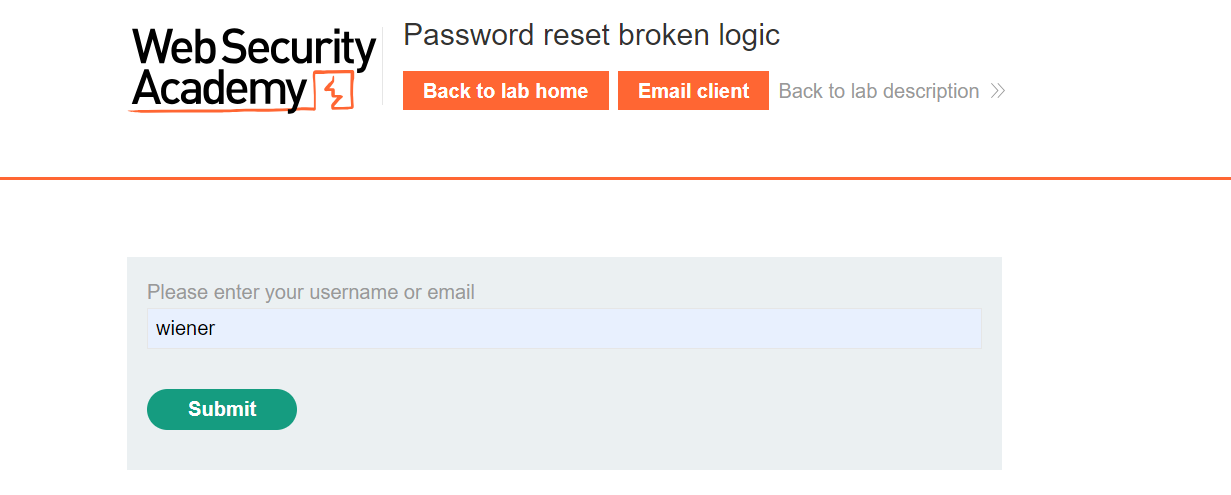


* Bài lab này có lỗ hổng “Forgot password?”

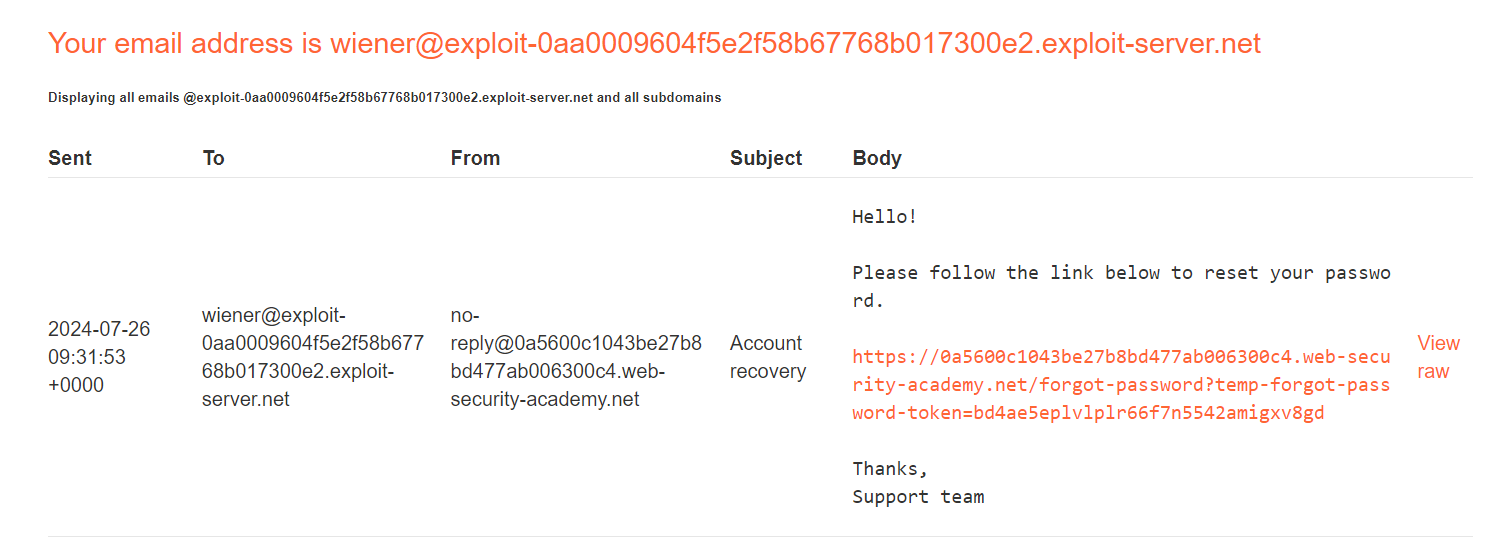
Bước 1: Vào trang Đăng Nhập



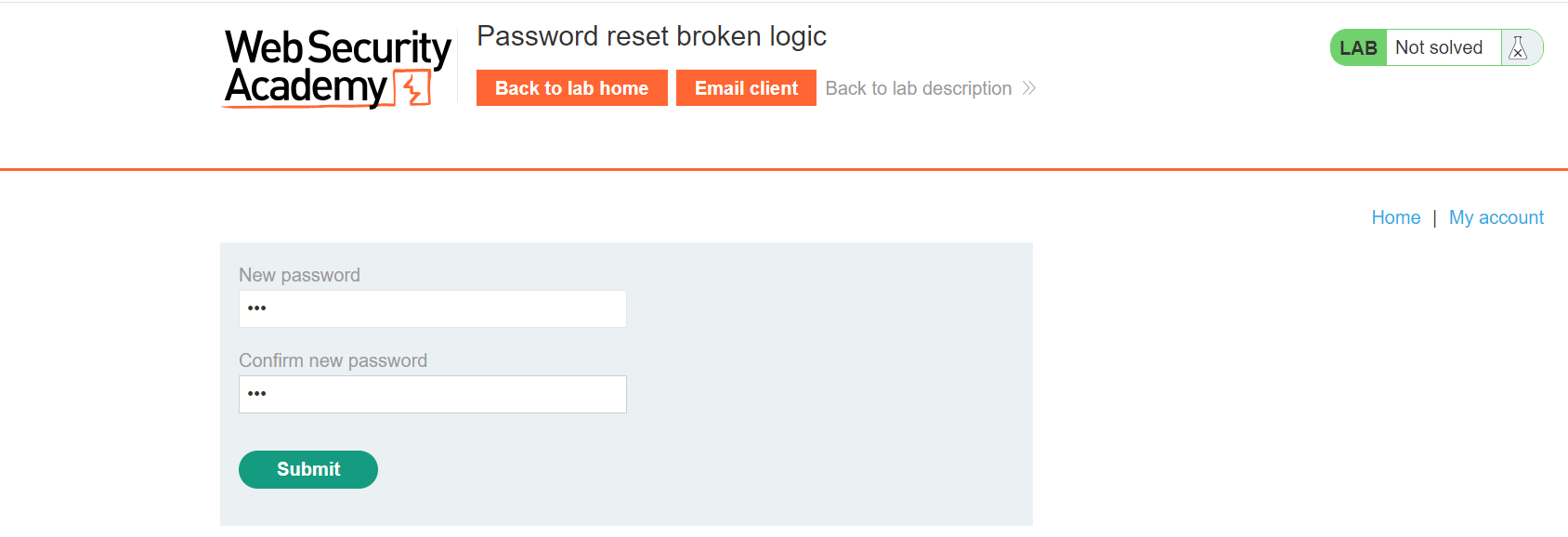
Bước 2: Test thử Forgot password



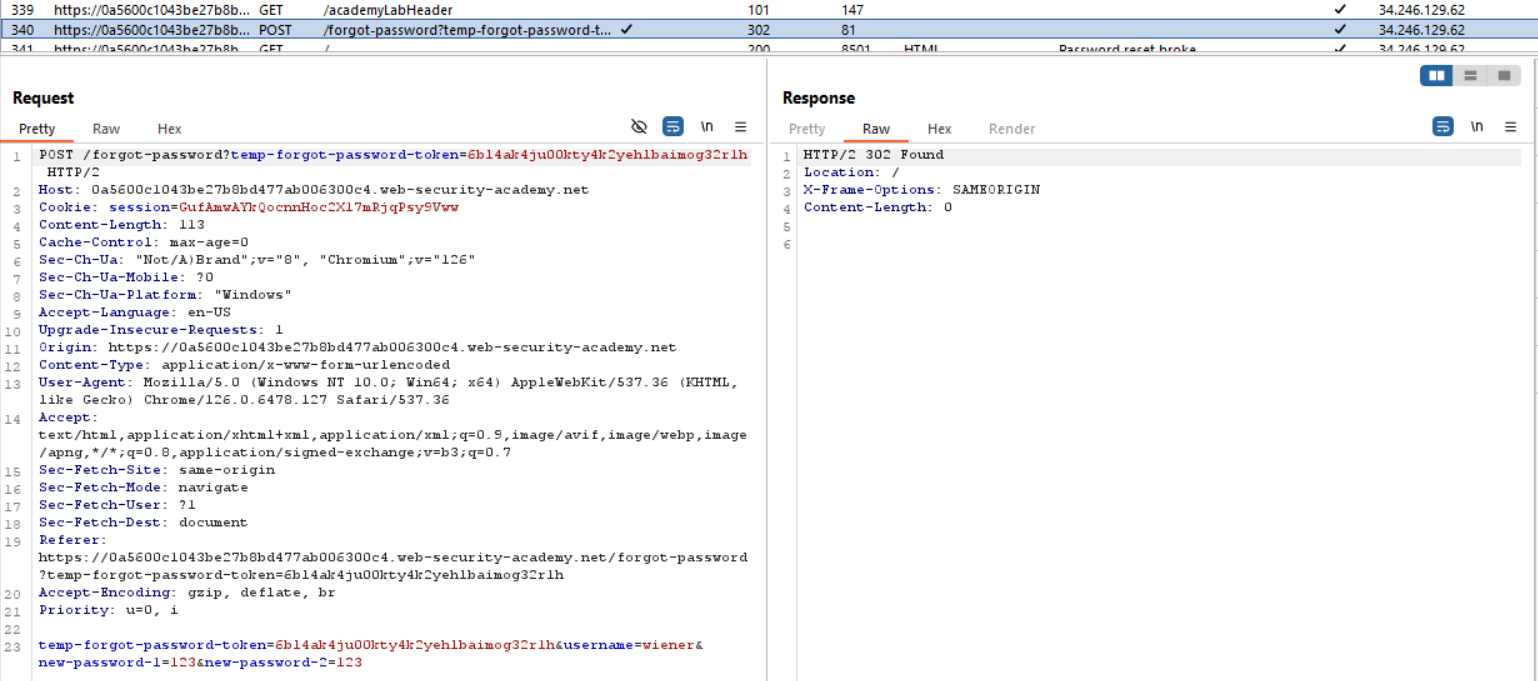
* Có mail được gửi về tài khoản



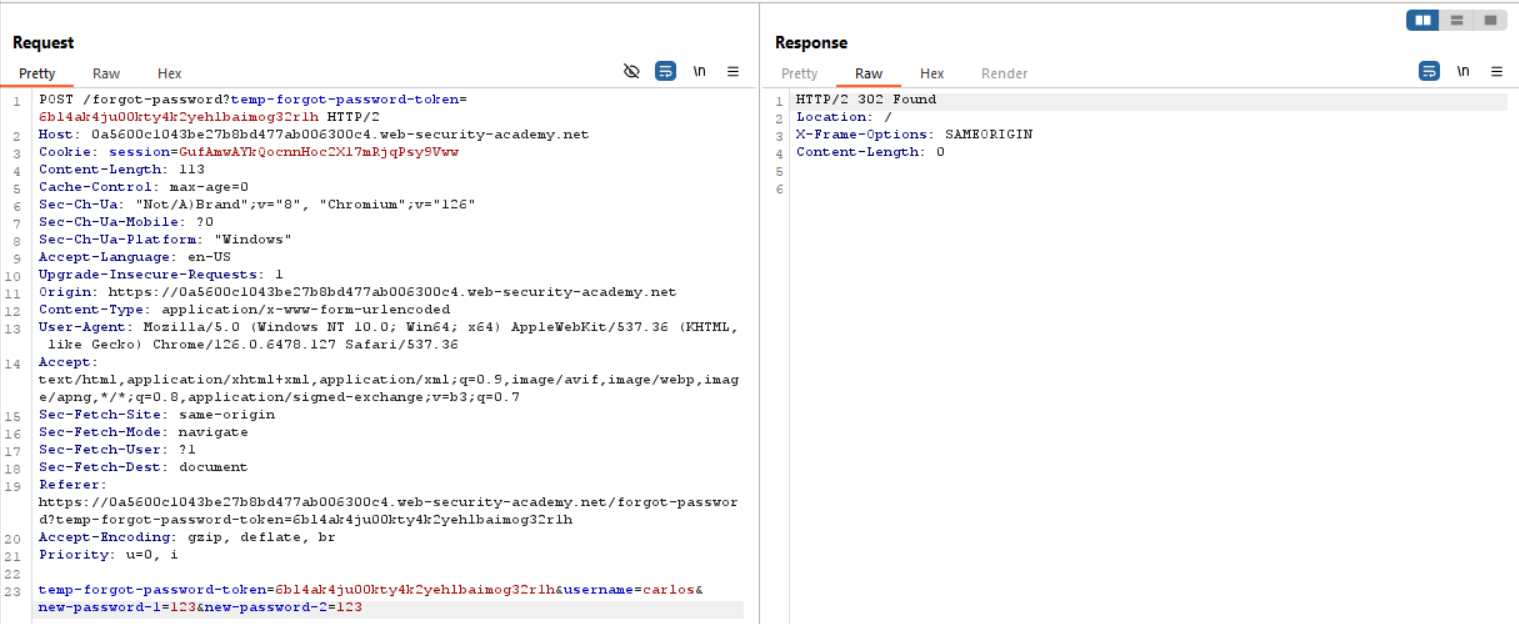
Bước 3: Thực hiện reset password.



* Bắt được gói tin POST có chứa dữ liệu để đổi password



Bước 4: Thử chuyển sang Repeater và thay đổi tài khoản thành caslor



* Phản hồi trả về đã thành công đổi tài khoản
* Đăng nhập thử tài khoản carlos

