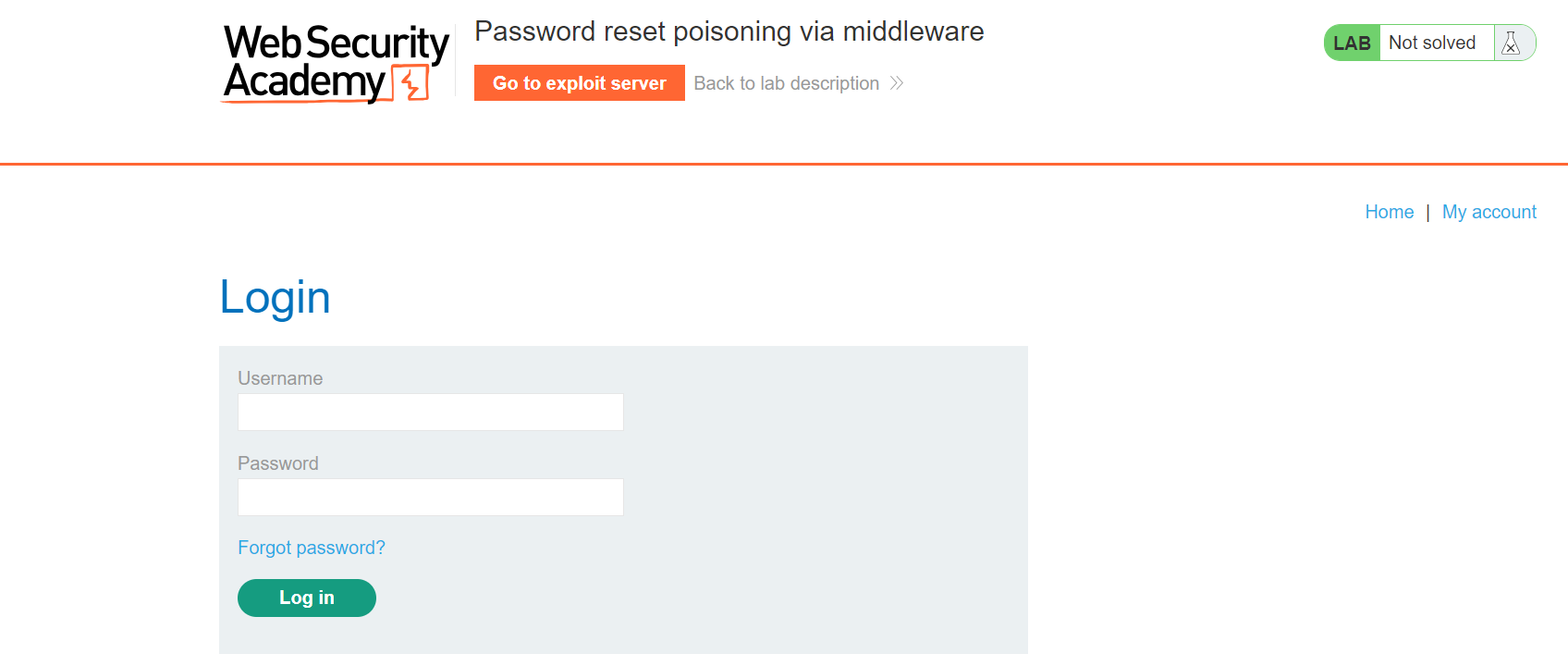


* Bài lab này có lỗ hổng “Forgot password?”
* Carlos sẽ nhấn vào bất kì link nào trong email mà anh ấy nhận được

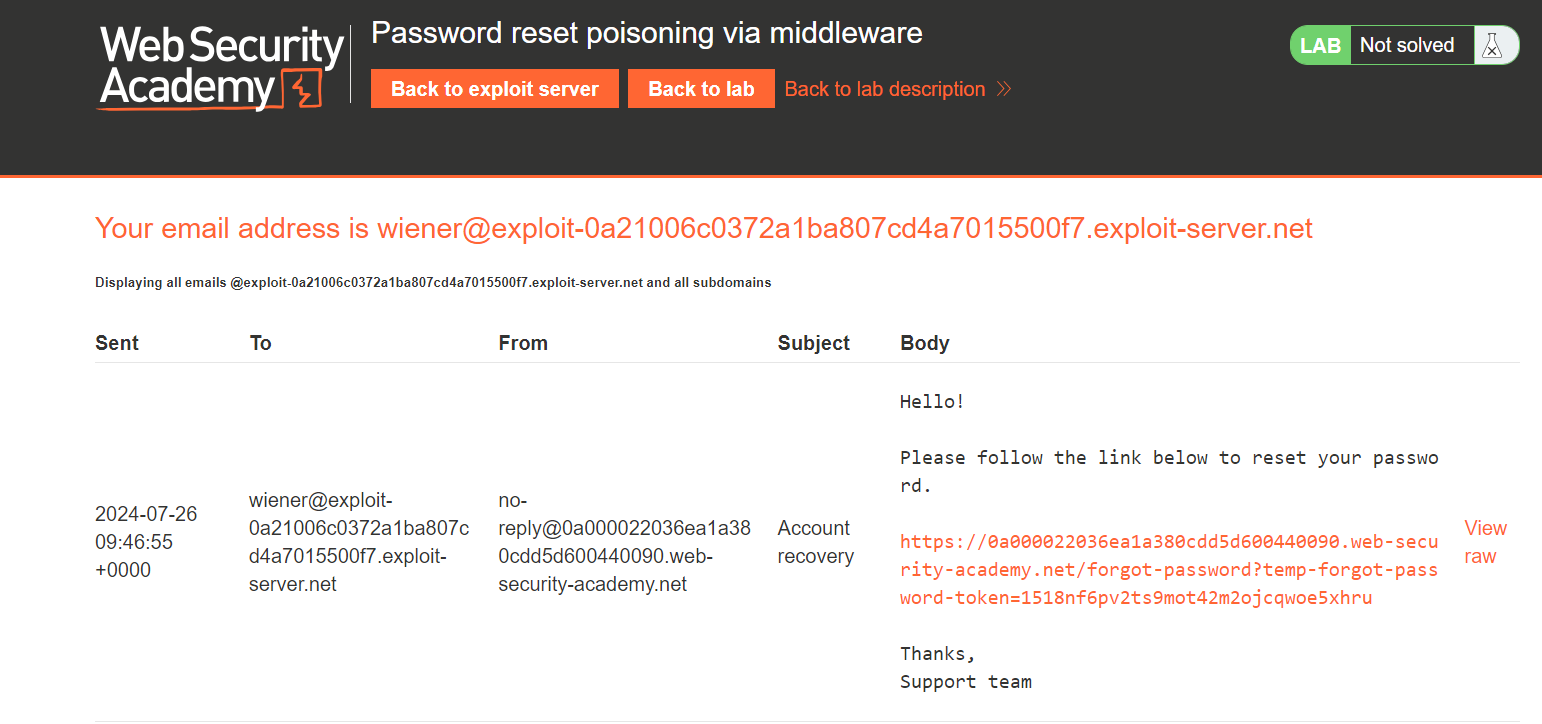
Bước 1: Vào trang Đăng Nhập



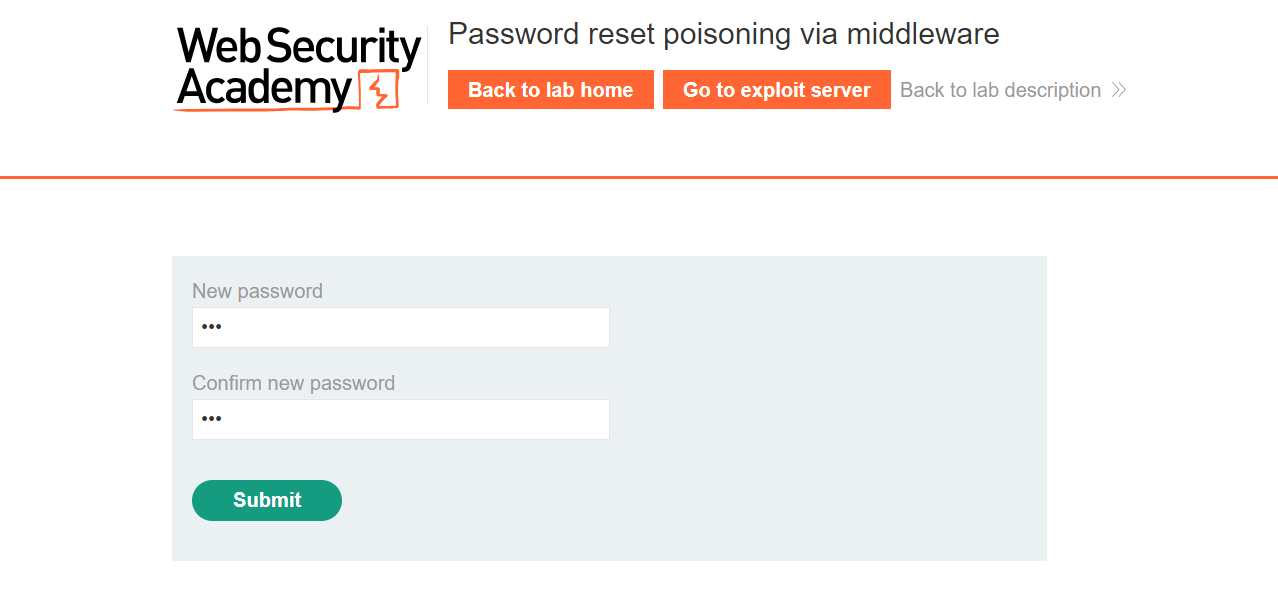
Bước 2: Test thử Forgot password



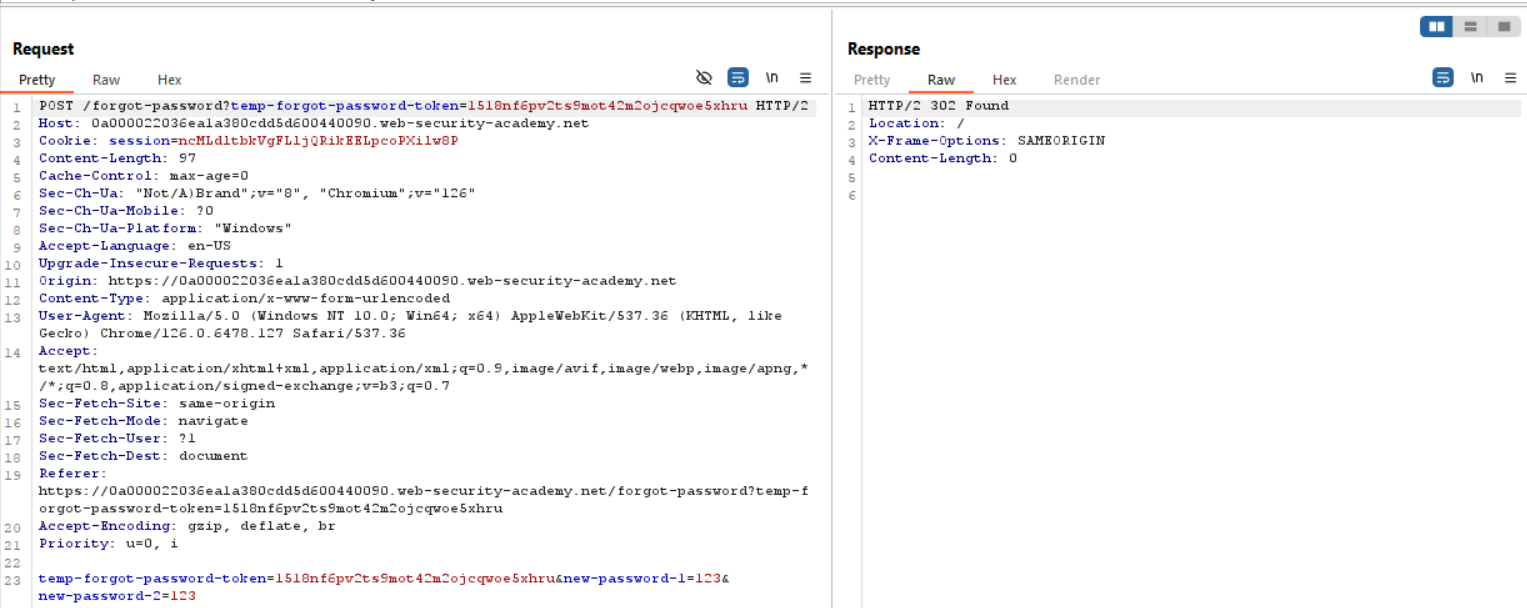
* Có mail được gửi về tài khoản email của người dùng



Bước 3: Thực hiện reset password.



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



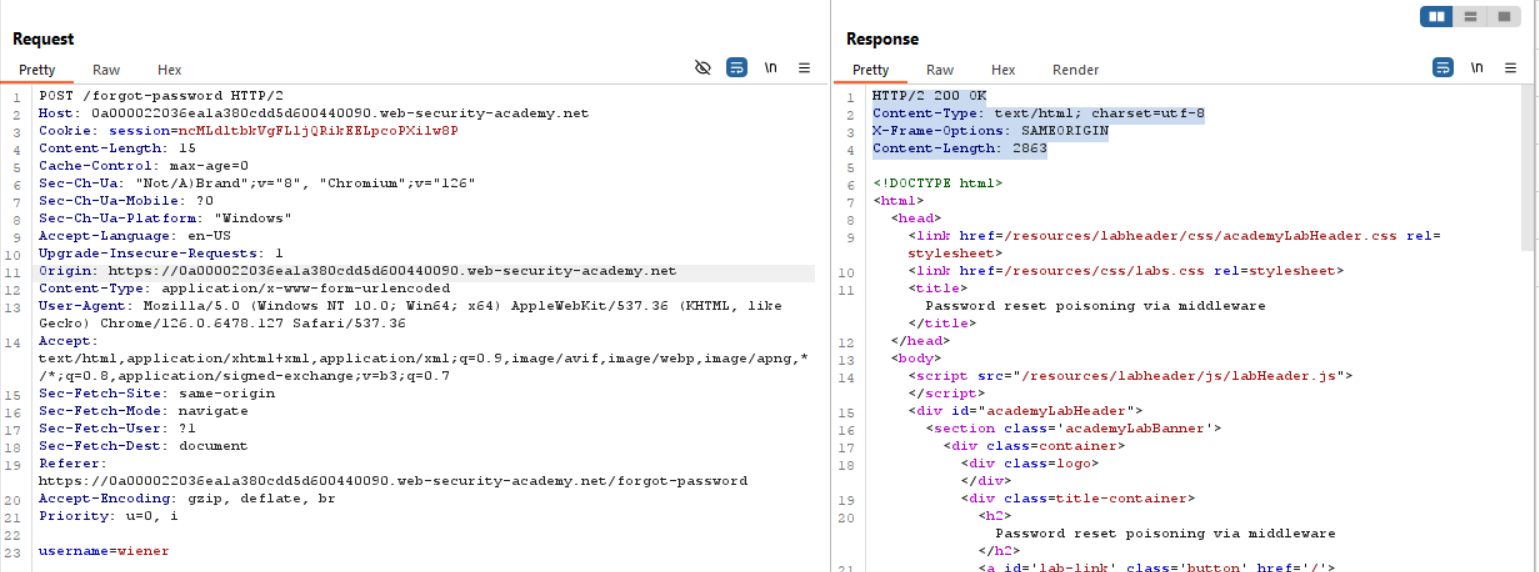
* Không có trường username nữa mà tài khoản xác nhận được đổi thông qua temp-forgot-password-token

Bước 4: Thử chuyển sang Repeater và thay đổi mật khẩu



* Token chỉ được sử dụng một lần, sau đó sẽ bị hủy

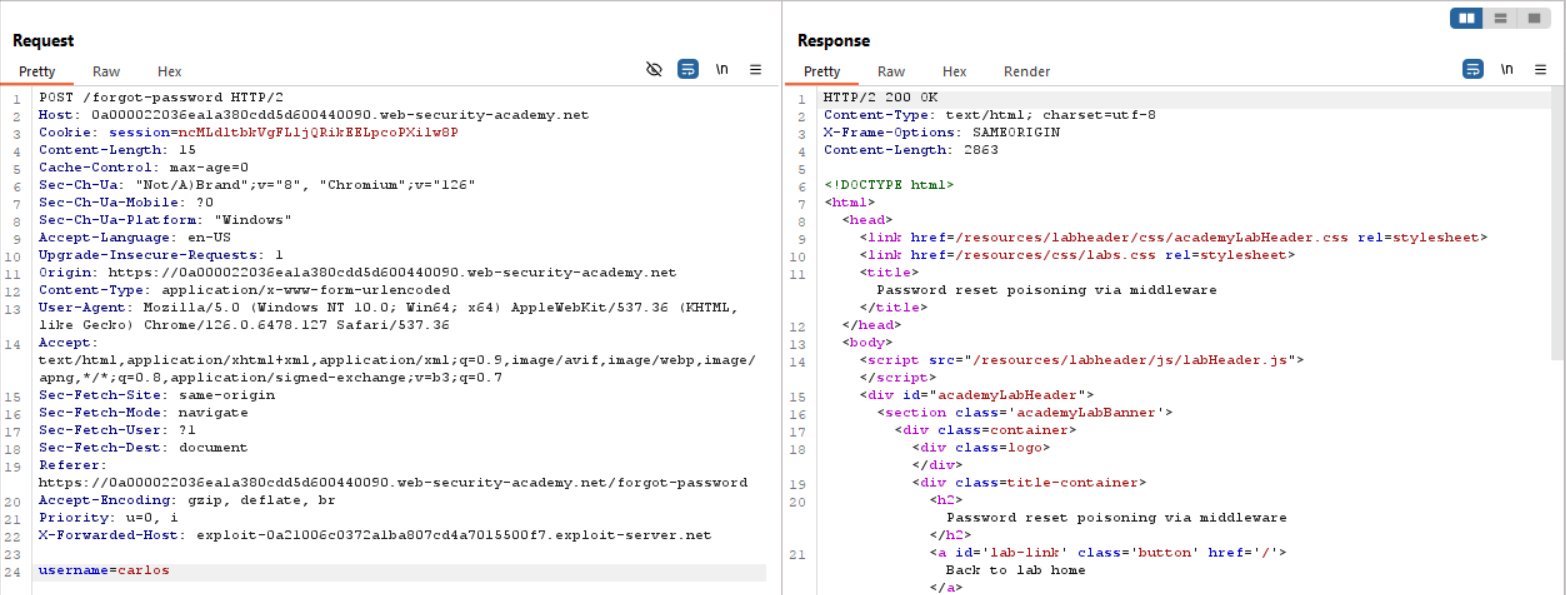
Bước 5: Lục lại gói tin POST /forgot-password



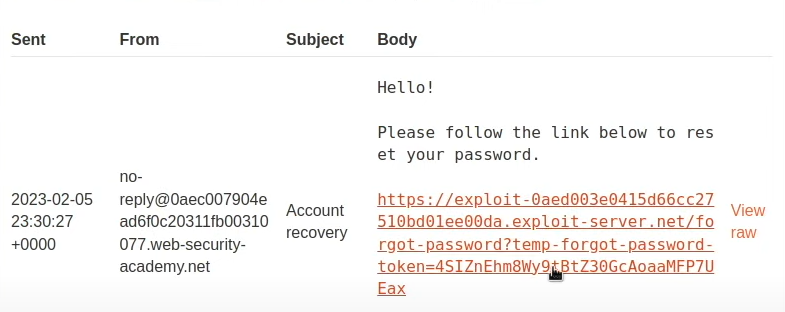
* Gói tin này sẽ gửi token đến email của người muốn reset password

Bước 6: Chuyển đến Repeater và thêm X-Forwarded-Host

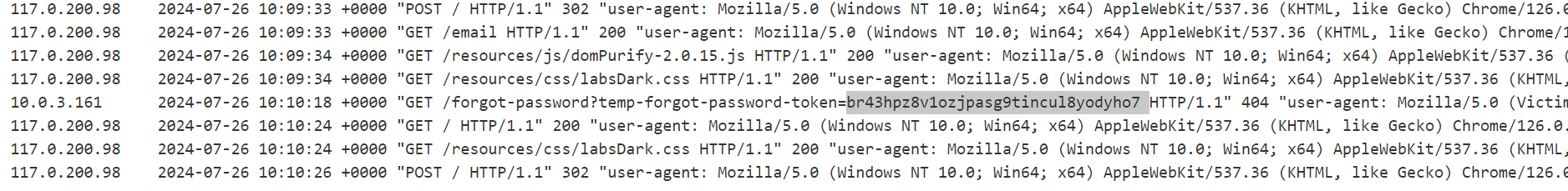
* Tại đây, ta sẽ sửa username thành carlos
* X-Forwarded-Host thêm URL của Exploit Server
* Nếu thành công thì đường dẫn đổi mật khẩu sẽ trở thành đường dẫn của Exploit Server vì URL của X-Forwarded-Host đã thay thế URL của Origin



* Khi gửi Request này đi thì Email của Carlos sẽ nhận được một mail “Reset Password” với đường dẫn là đến Exploit Server (Khác với đường dẫn thông thường ở bước 2)



* Bởi vì Carlos nhấn vào đường dẫn này nên sẽ chuyển hướng đến Exploit Server
* Vì vậy nên ta đọc được Log của Server có chứa yêu cầu GET /forgot-password



Bước 7: Gói tin đổi mật khẩu đến Repeater và sửa password



* Đăng nhập thành công

