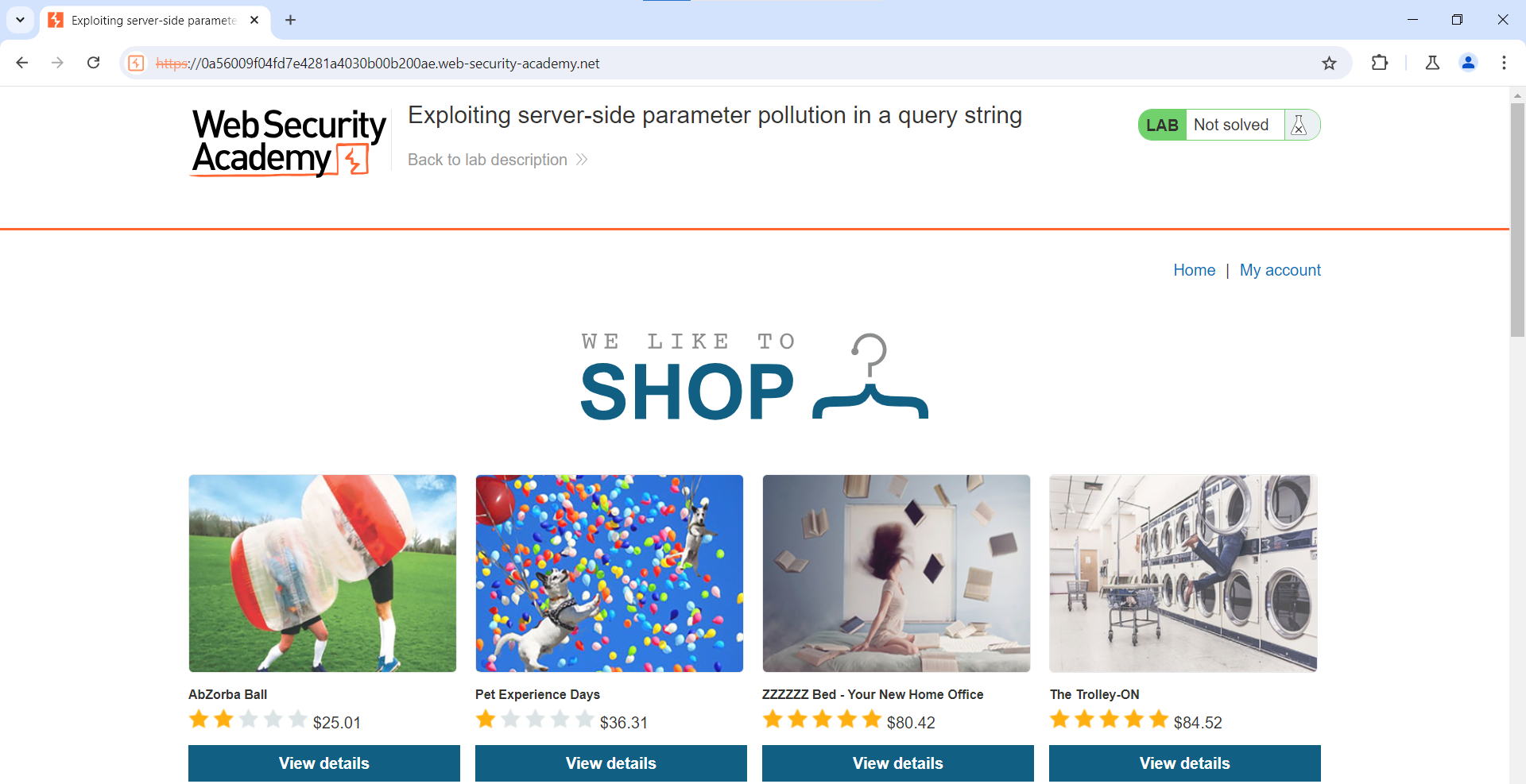
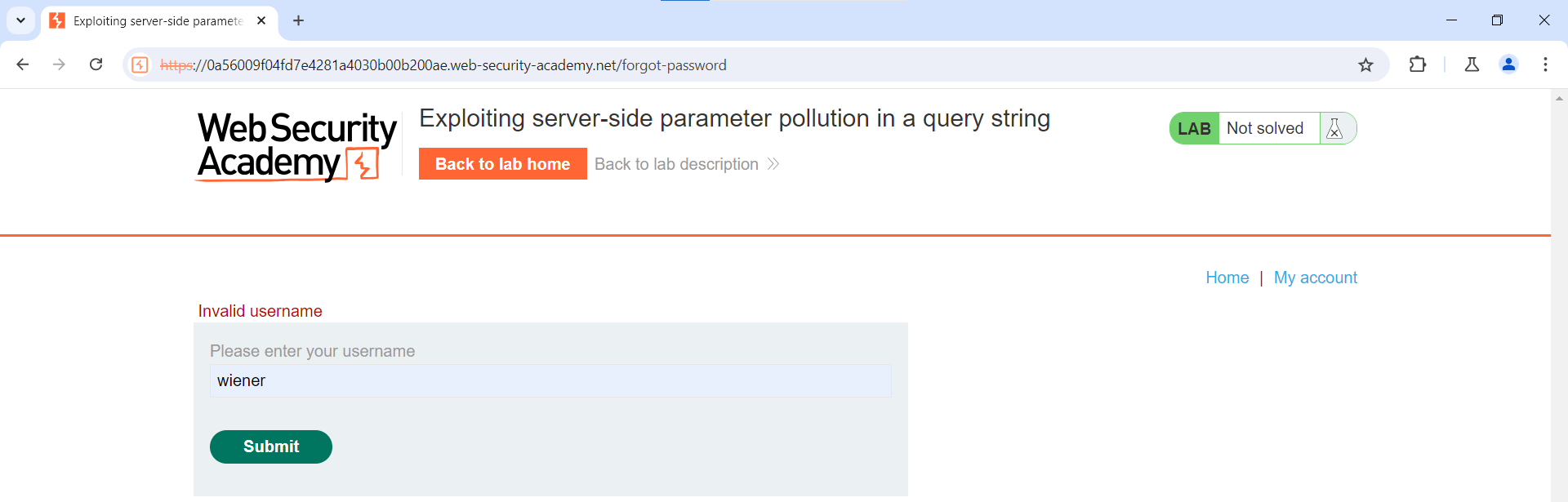


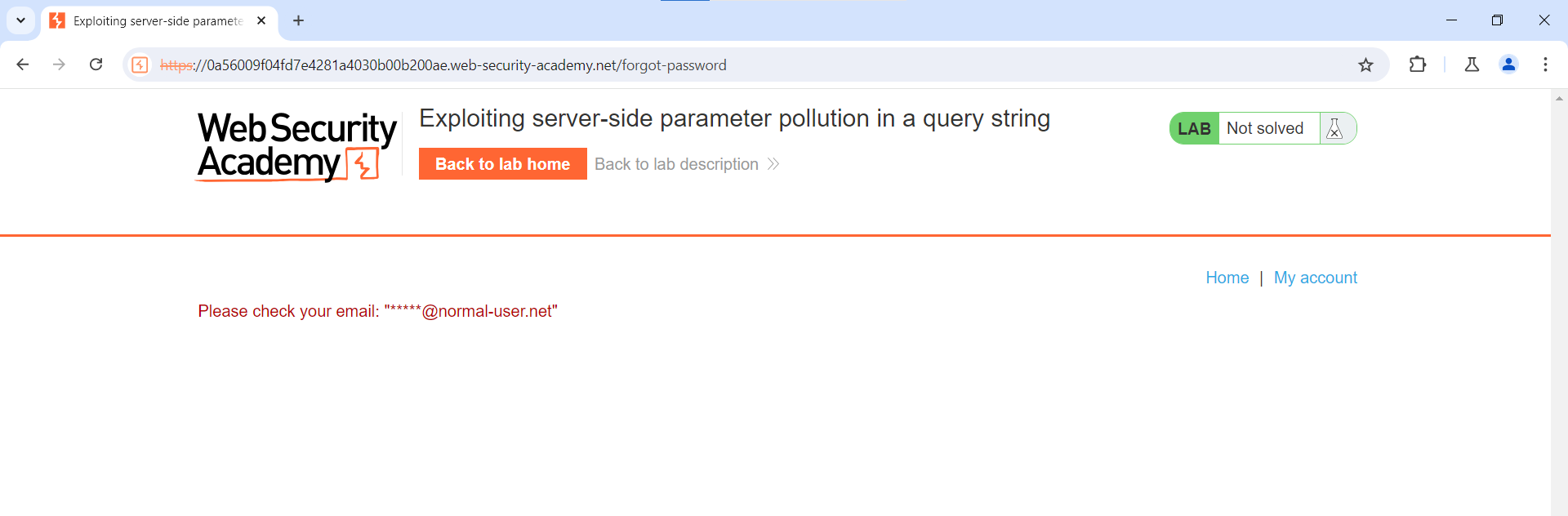
* Mục đích: Xóa tài khoản carlos



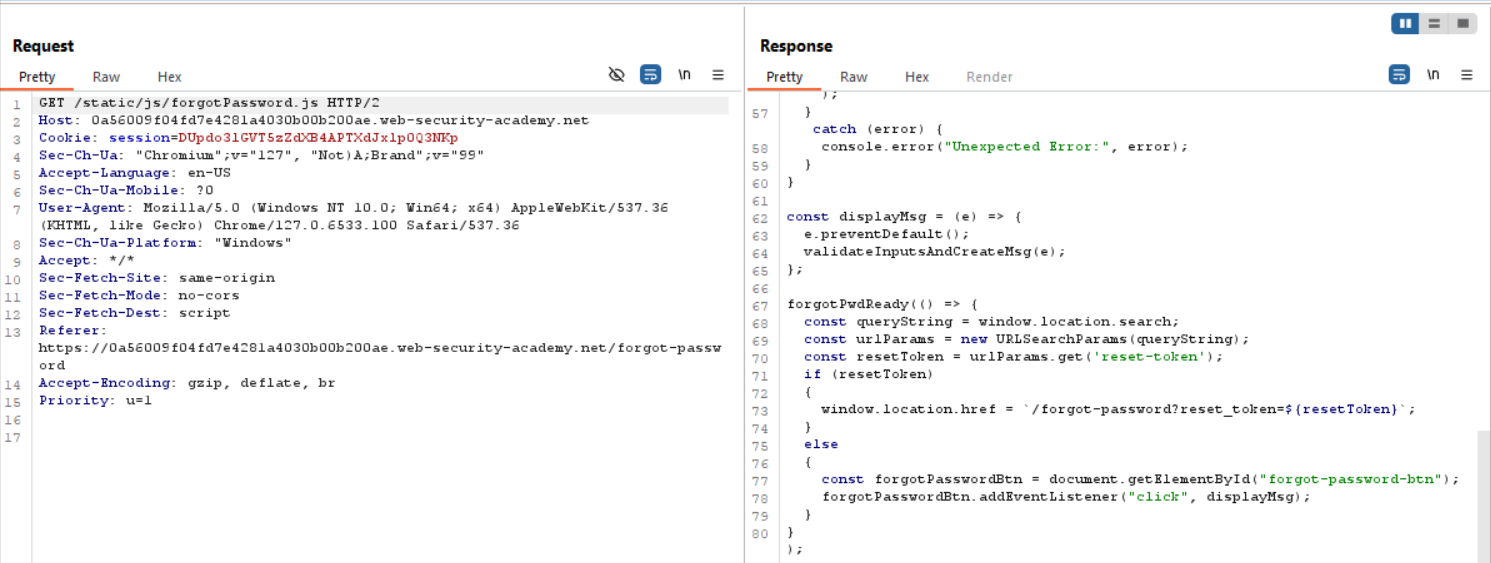
* Vì không có tài khoản nên ta sẽ thử một vài chức năng
* Ta phát hiện ra có chức năng forgot password



* Sau khi thử thì thấy nó sẽ cho biết có tài khoản nào đang tồn tại trên hệ thống
* Ta đã tìm được tài khoản admin là: administrator



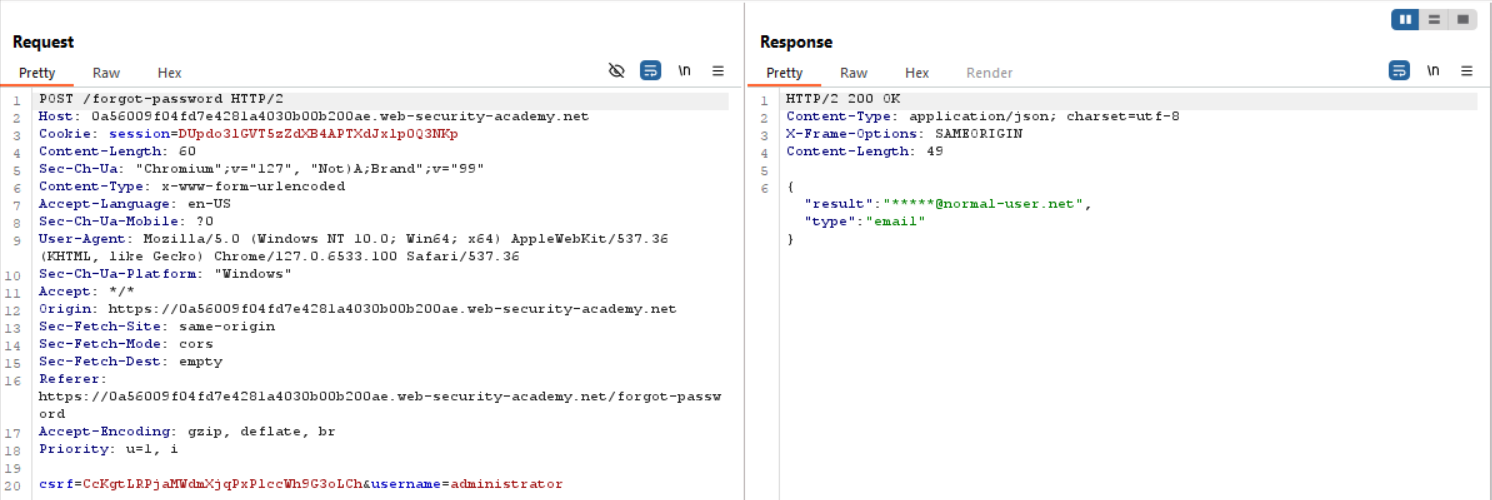
* Sau đó, có một mail reset password được gửi về email của tài khoản của administrator.
* Bắt gói tin bằng BurpSuite, ta phát hiện được một gói tin javascript. Gói tin này có chứa chức năng hoạt động của reset password khi được gửi về email.



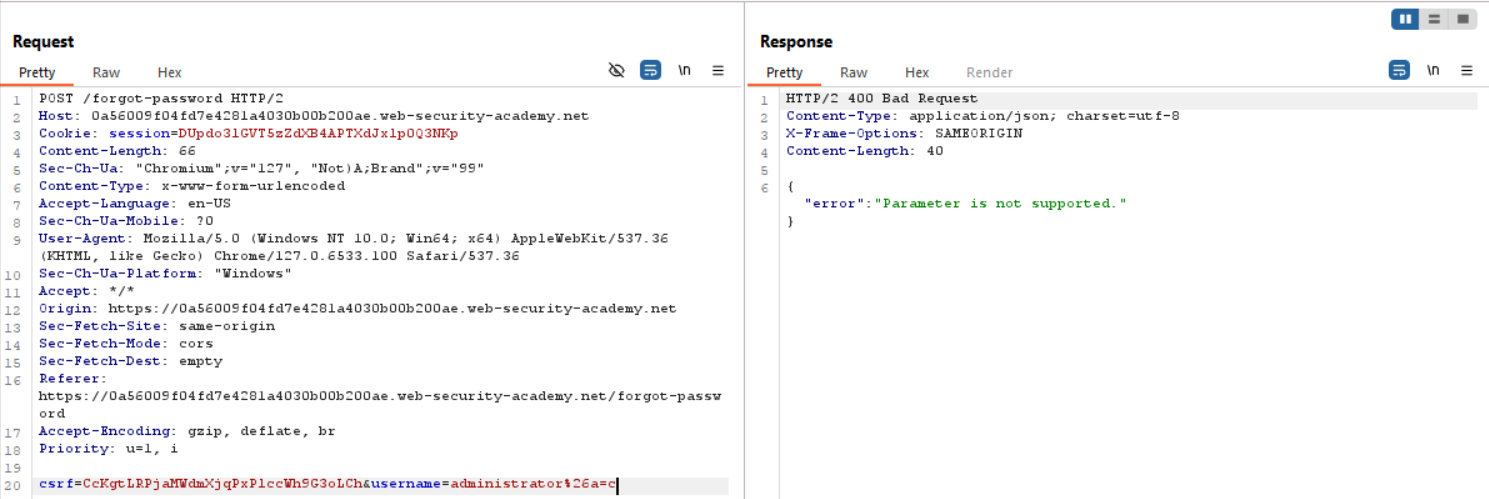
* Ta đã biết được đường dẫn tiếp theo để reset password là

/forgot-password?reset\_token=${resetToken}

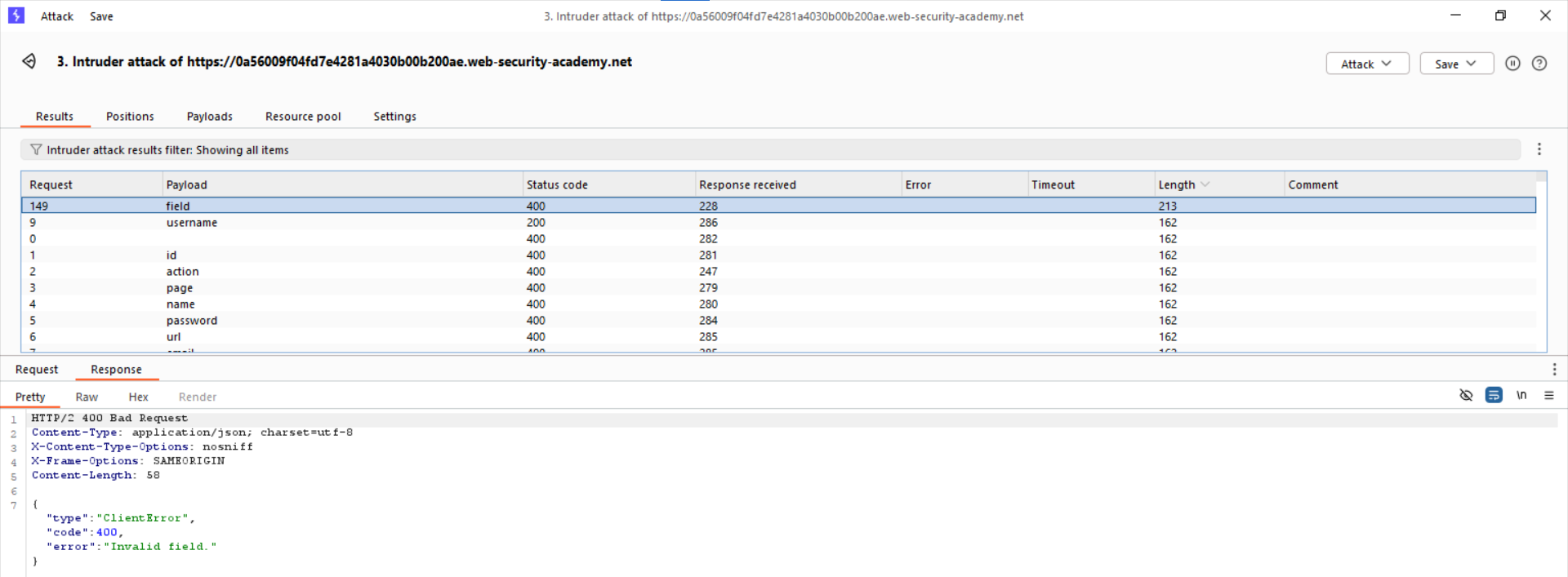
* Tuy nhiên, ta lại không biết resetToken là gì
* Ta còn phát hiện thêm một gói tin được dùng để lấy thông tin tài khoản



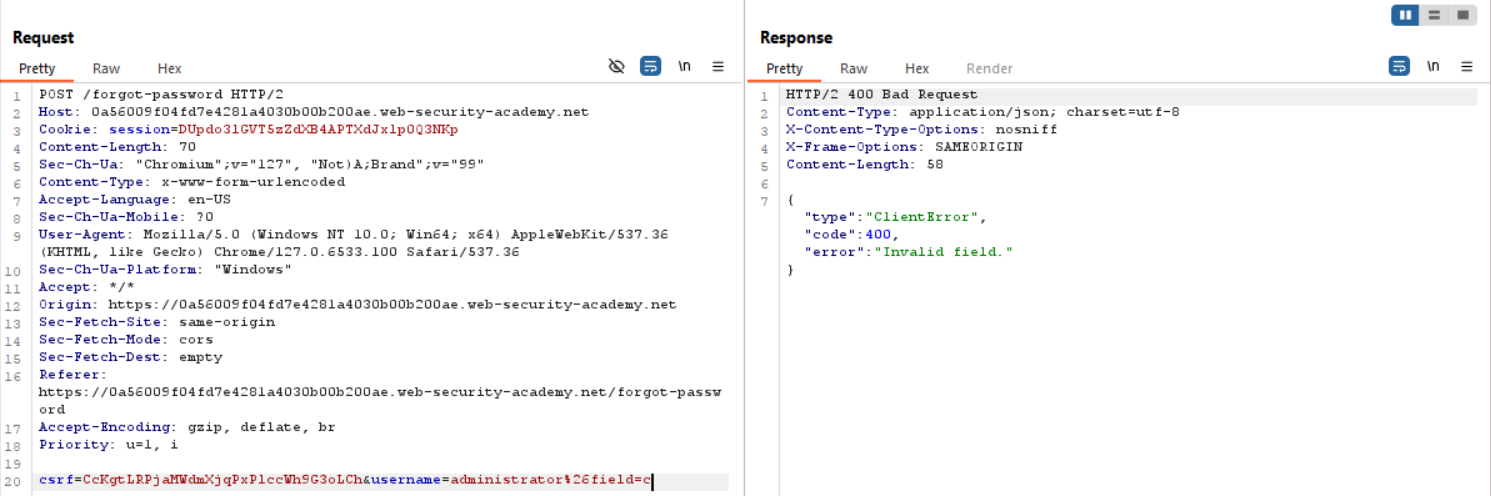
* Ta có thể dựa vào gói tin này để lấy thông tin khác của người dùng
* Sau khi gửi repeater và thử vài lần, ta phát hiện rằng server có xử lý trường dữ liệu khác



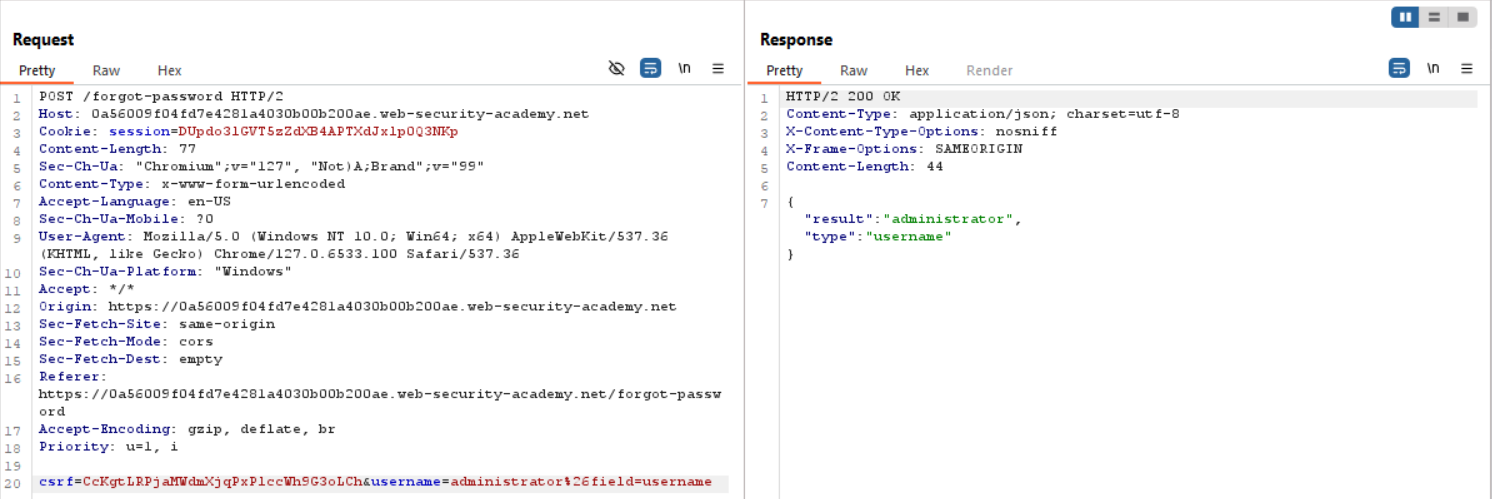
* Ta sẽ gửi qua intruder để tìm kiếm trường ẩn này là gì



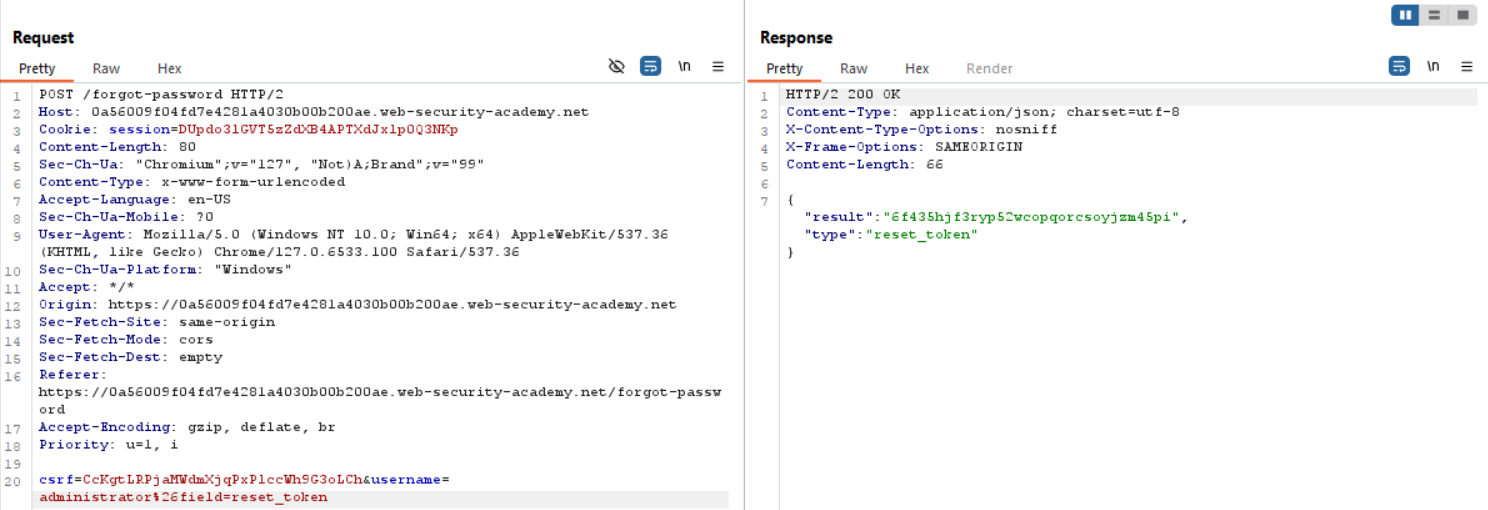
* Ta phát hiện một trường khả nghi là “field” và “username”. Trường “username” thì ta đã biết sẵn rồi nên ta sẽ test thử trường còn lại



* Server trả về phản hồi trường field không đúng. Tuy nhiên, ta đã biết có một trường đúng là “username” mà ta đã bruteforce được ở trên kia

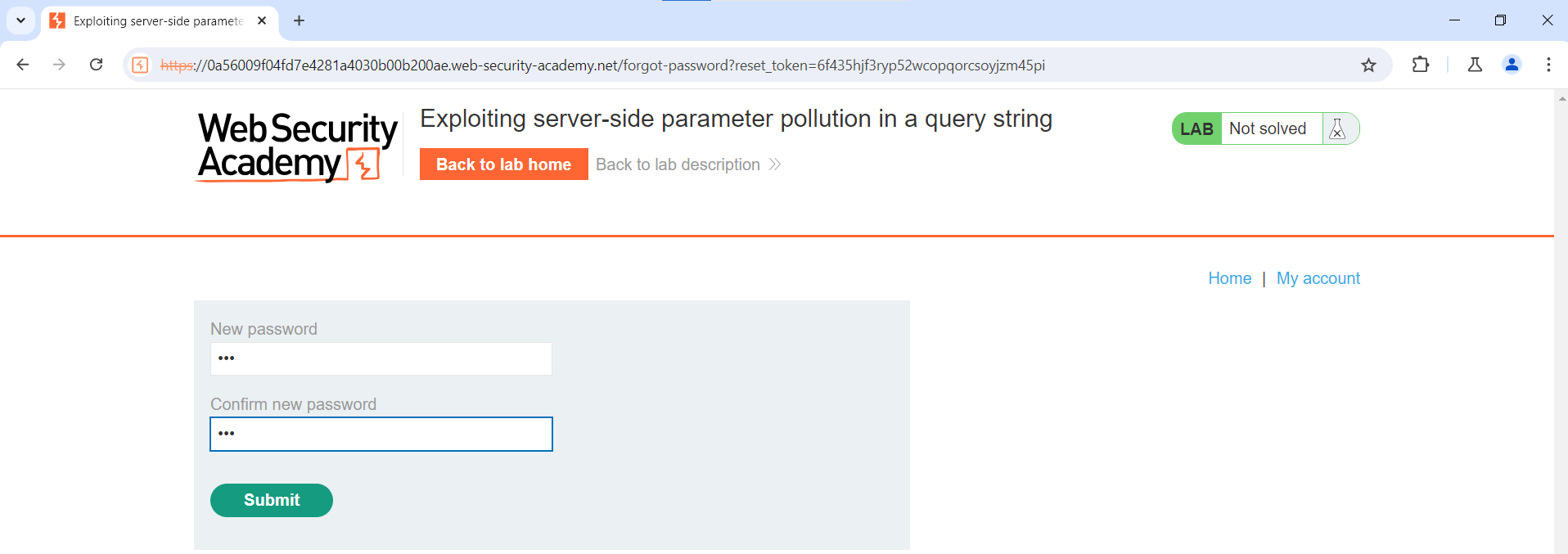


* Ta sẽ thử lấy reset-token của tài khoản này xem được không

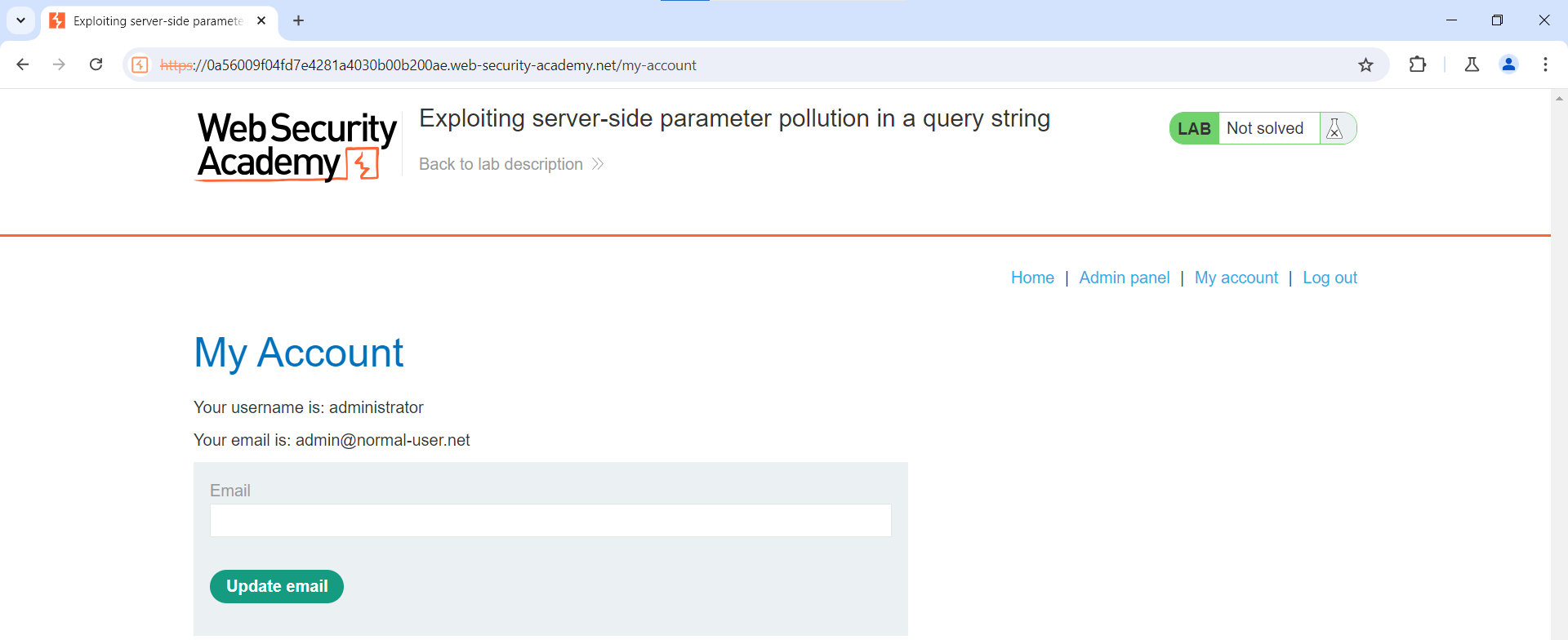


* Giờ đây ta đã có thể truy cập đường dẫn reset password

/forgot-password?reset\_token=6f435hjf3ryp52wcopqorcsoyjzm45pi



* Đăng nhập tài khoản admin thành công



* Xóa tài khoản carlos và hoàn thành lab

