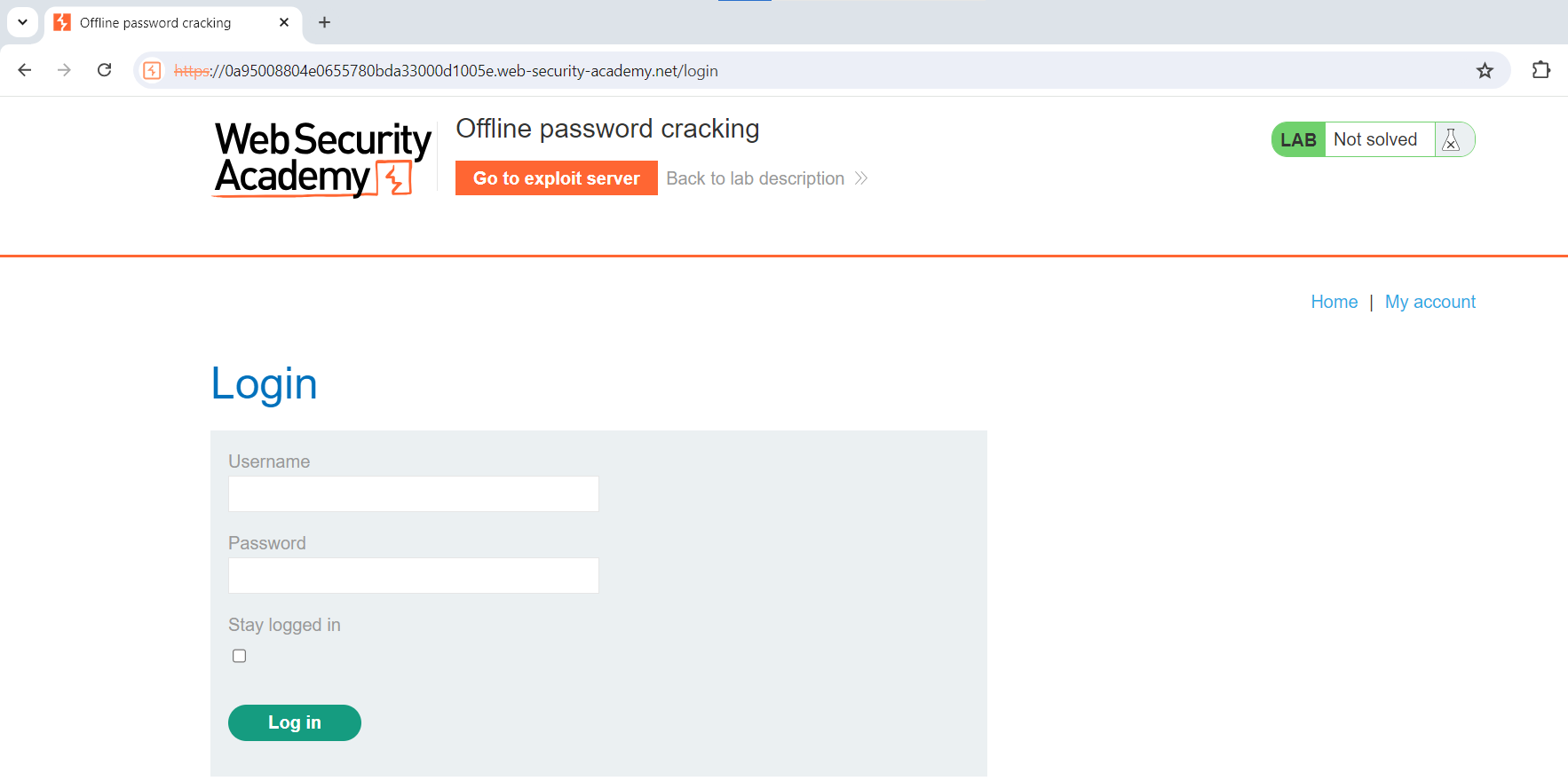
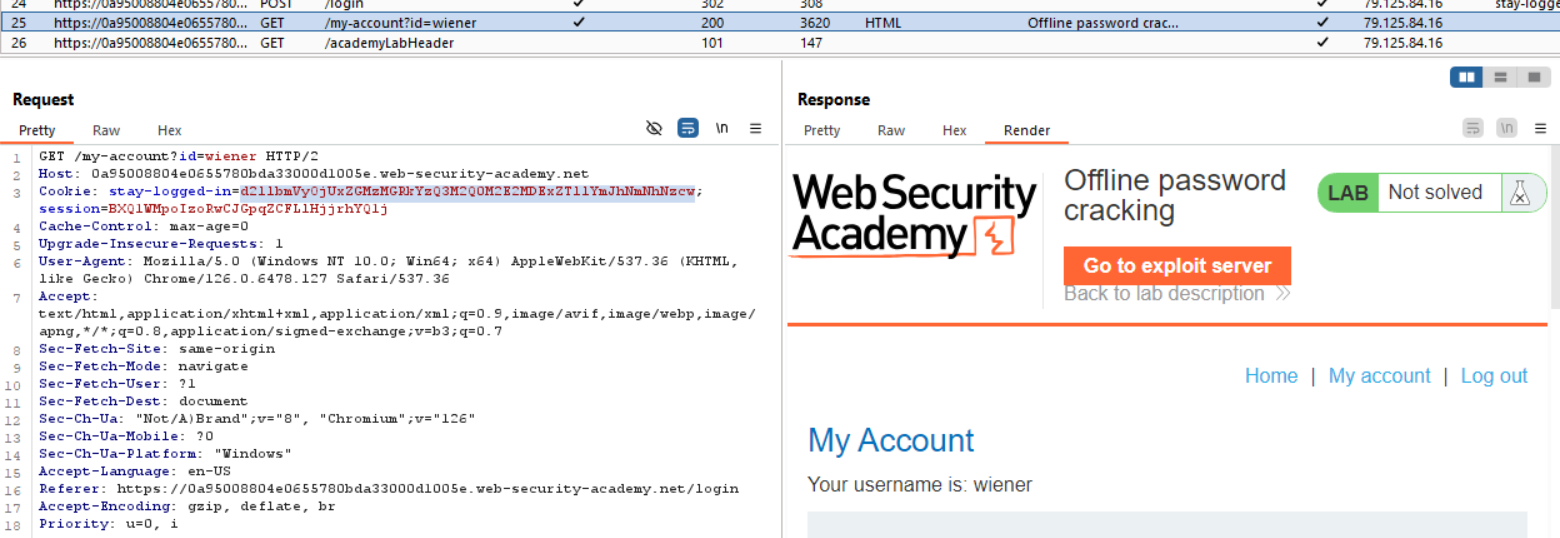


* Bài lab này có lỗ hổng “stay-logged-in”, chỉ cần có trường này trong cookie thì sẽ bypasss được tài khoản và mật khẩu đăng nhập.
* Lỗ hổng XSS trong comment nên ta có thể dùng Stored XSS để lấy được cookie của tài khoản carlos.

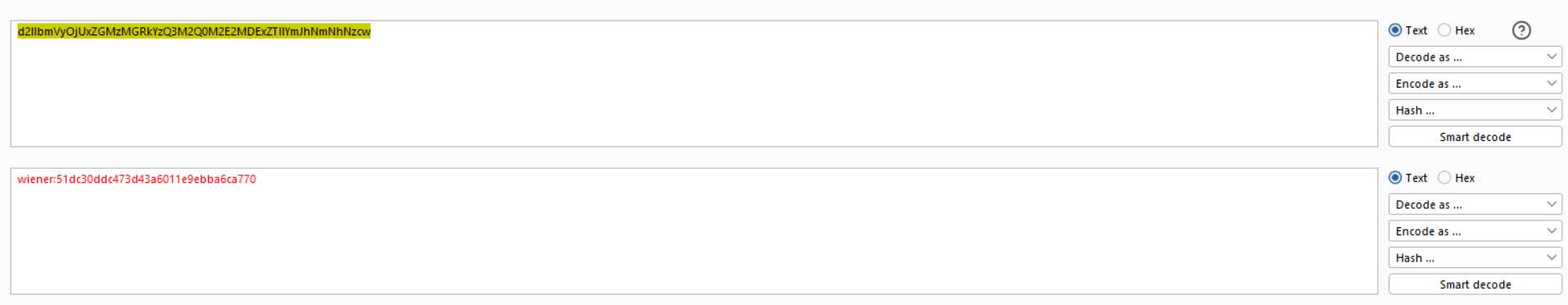
Bước 1: Vào trang Đăng Nhập



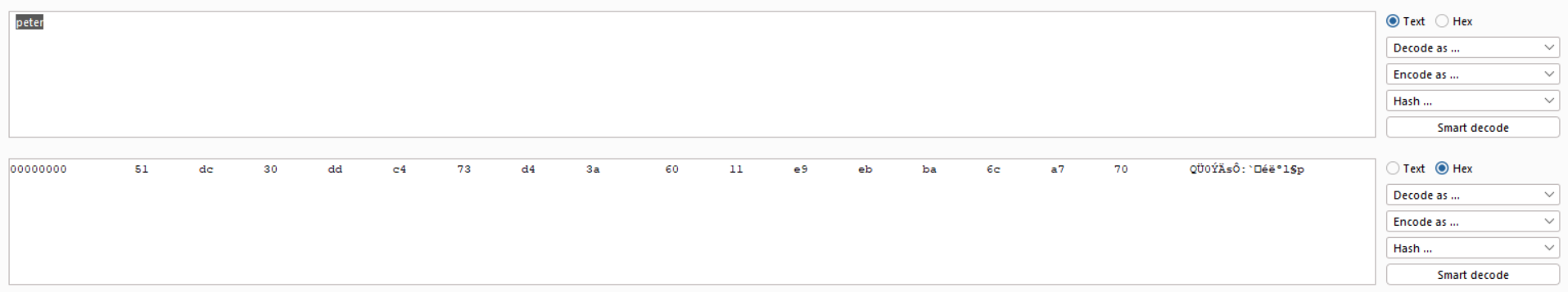
Bước 2: Đăng nhập xong thì cookie hiện thêm một trường là stay-logged-in



* Chuyển Cookie stay-logged-in sang Decoder

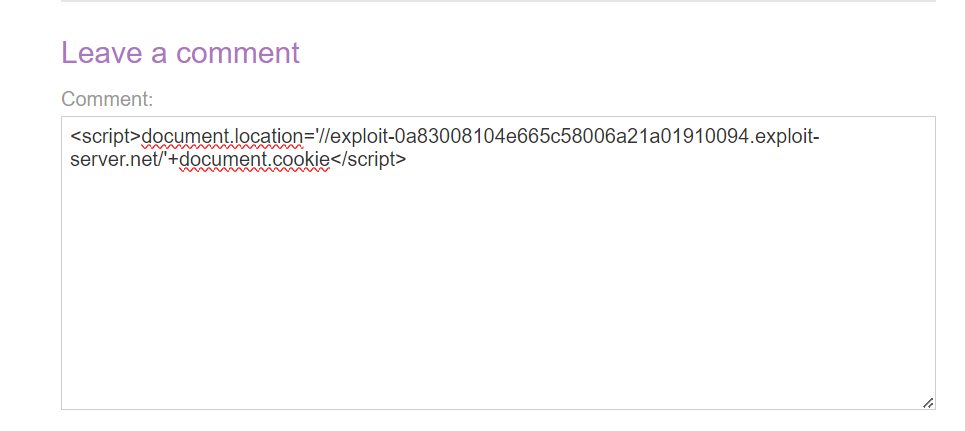


* Cookie được mã hóa bằng Base64

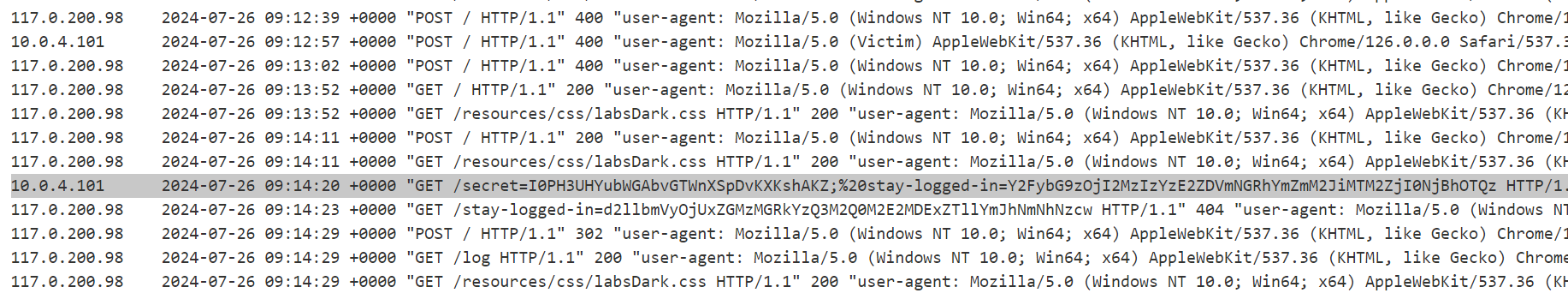


* Mật khẩu được mã hóa bằng hàm băm MD5
* Cookie = Base64(Username:MD5(Password))

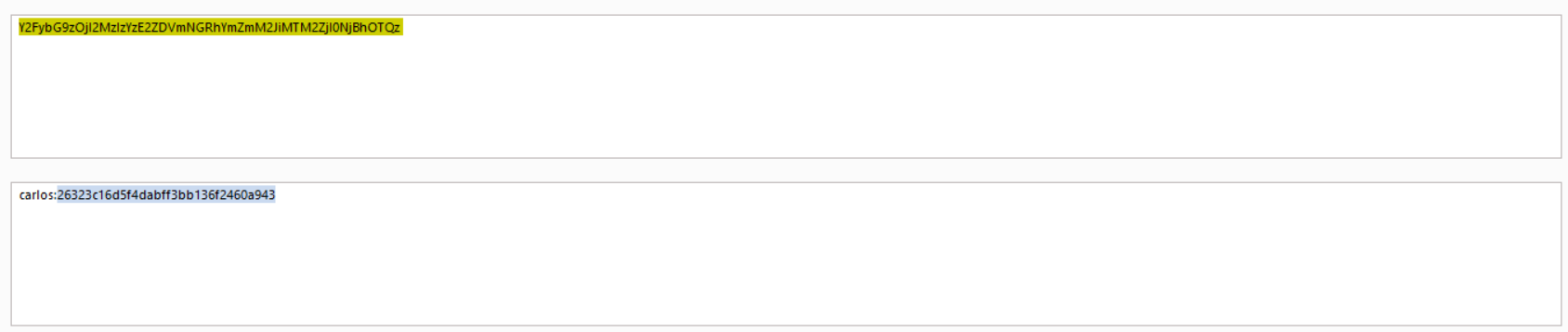
Bước 3: Viết payload tấn công XSS gửi về Exploit-Server và gửi comment lên bài post.



Bước 4: Thực hiện tấn công



* Bắt được gói tin có IP khác
* Thử giải mã xem có phải của Carlos không

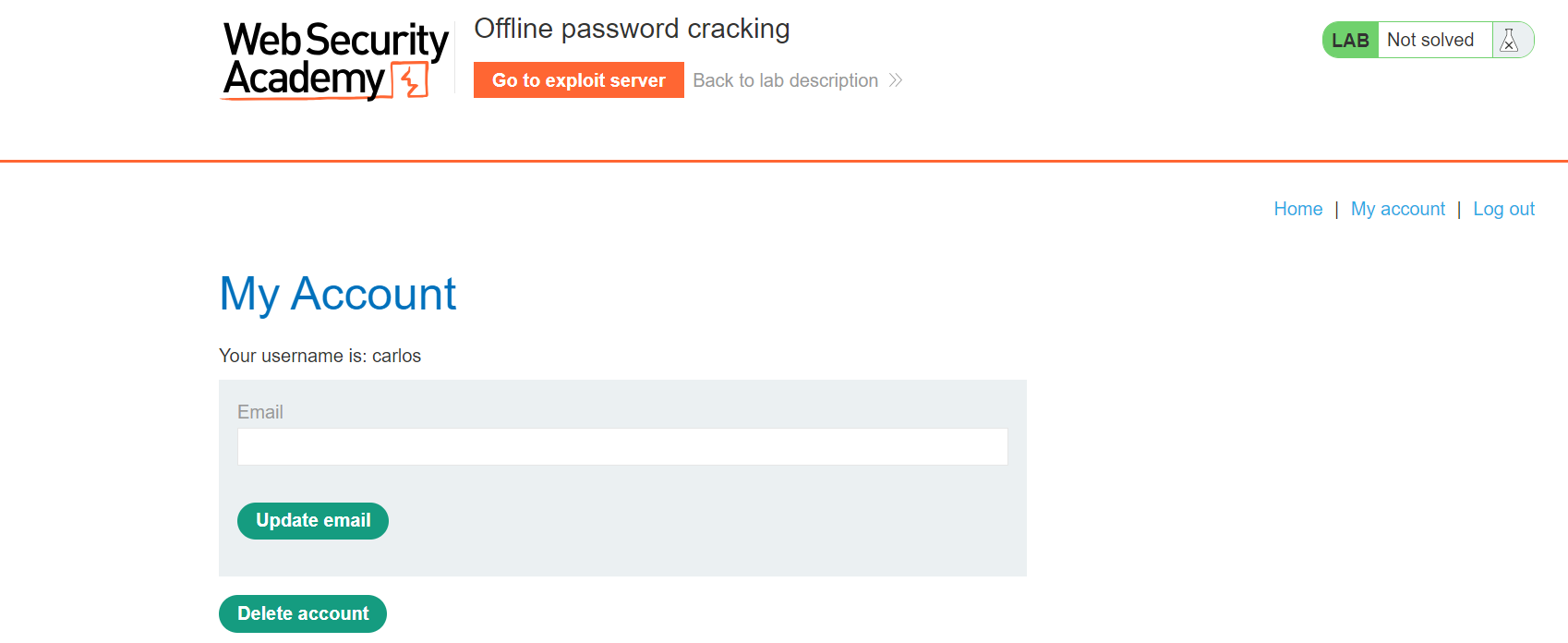


* Đúng là của Carlos
* Thử giải mã hash MD5



* Username: carlos
* Password: onceuponatime

Bước 5: Đăng nhập vào tài khoản carlos



* Xóa tài khoản của carlos và hoàn thành bài lab

