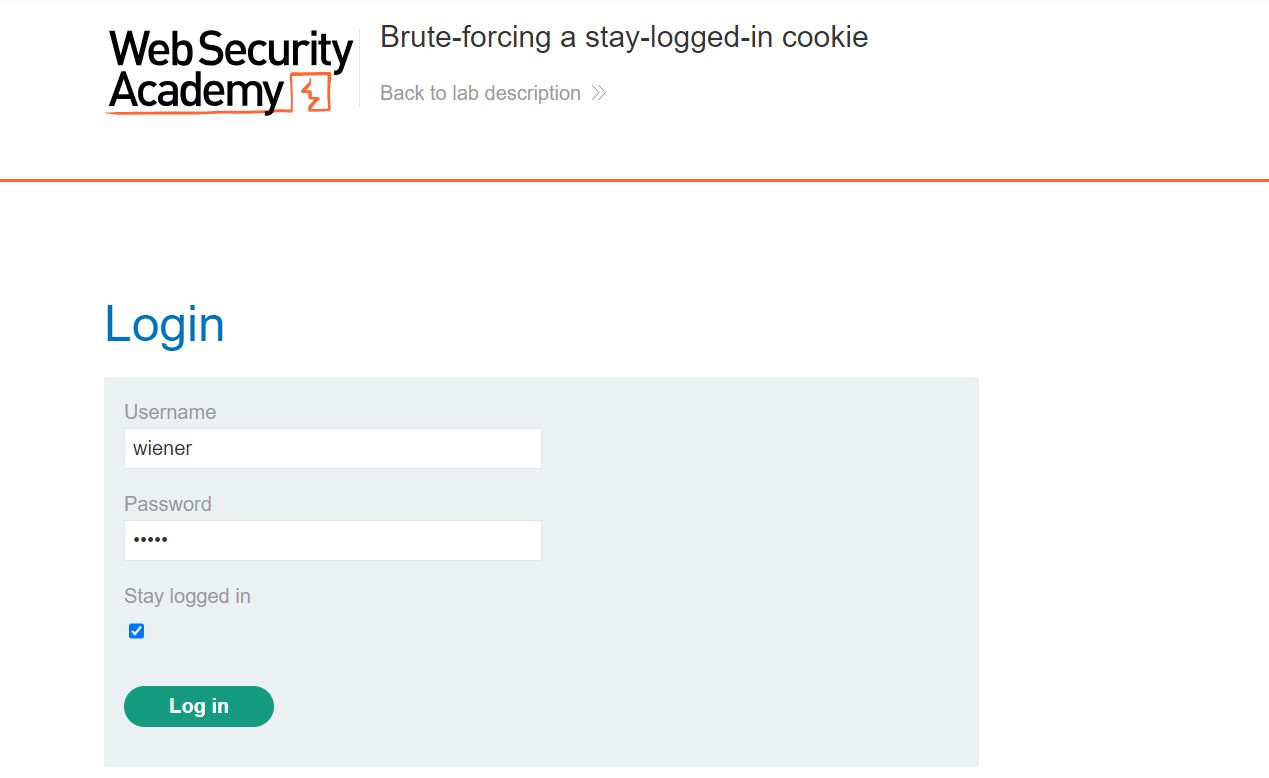
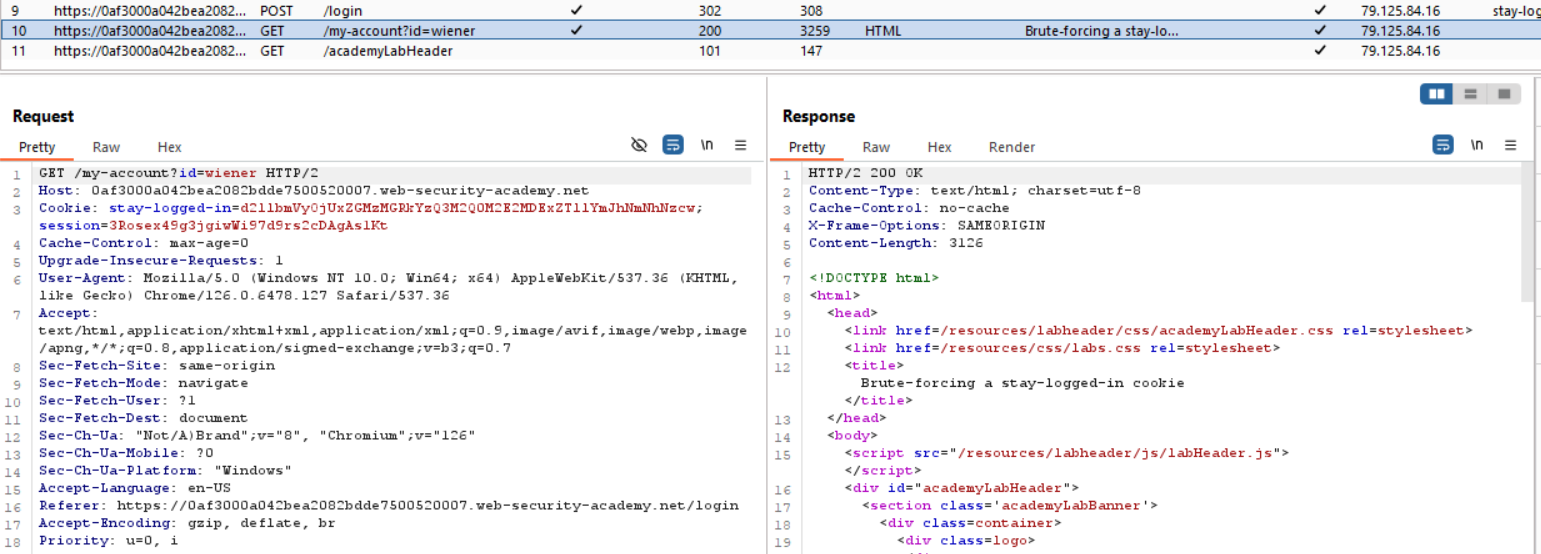


* Bài lab này có lỗ hổng “stay-logged-in”, chỉ cần có trường này trong cookie thì sẽ bypasss được tài khoản và mật khẩu đăng nhập
* Phải tìm được dữ liệu phù hợp để đăng nhập tài khoản carlos

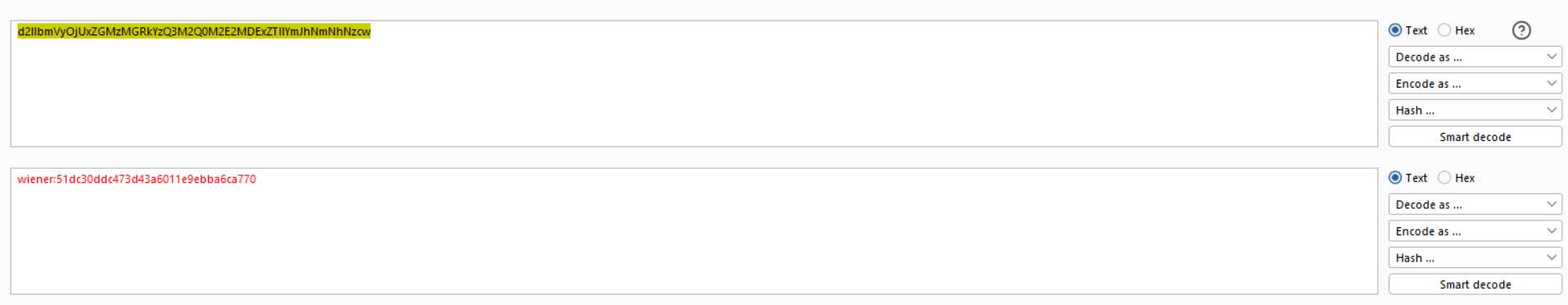
Bước 1: Vào trang Đăng Nhập



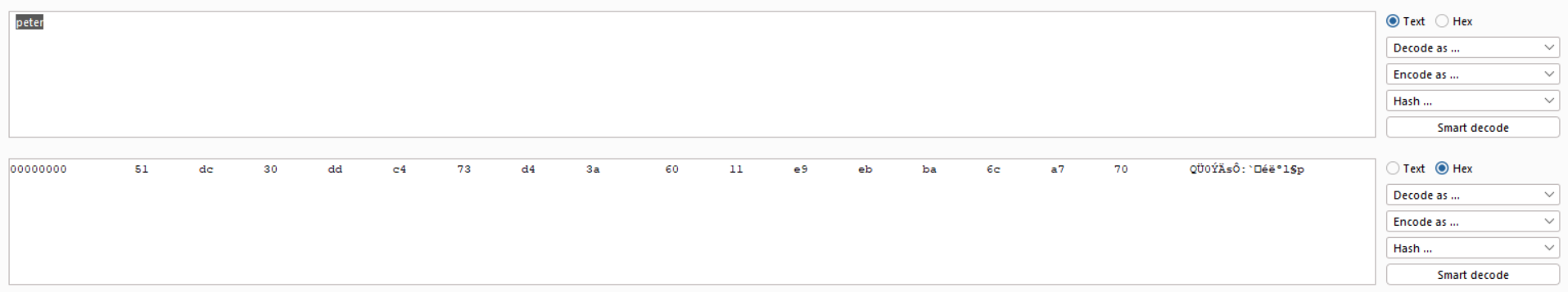
Bước 2: Đăng nhập xong thì cookie hiện thêm một trường là stay-logged-in



* Chuyển Cookie stay-logged-in sang Decoder

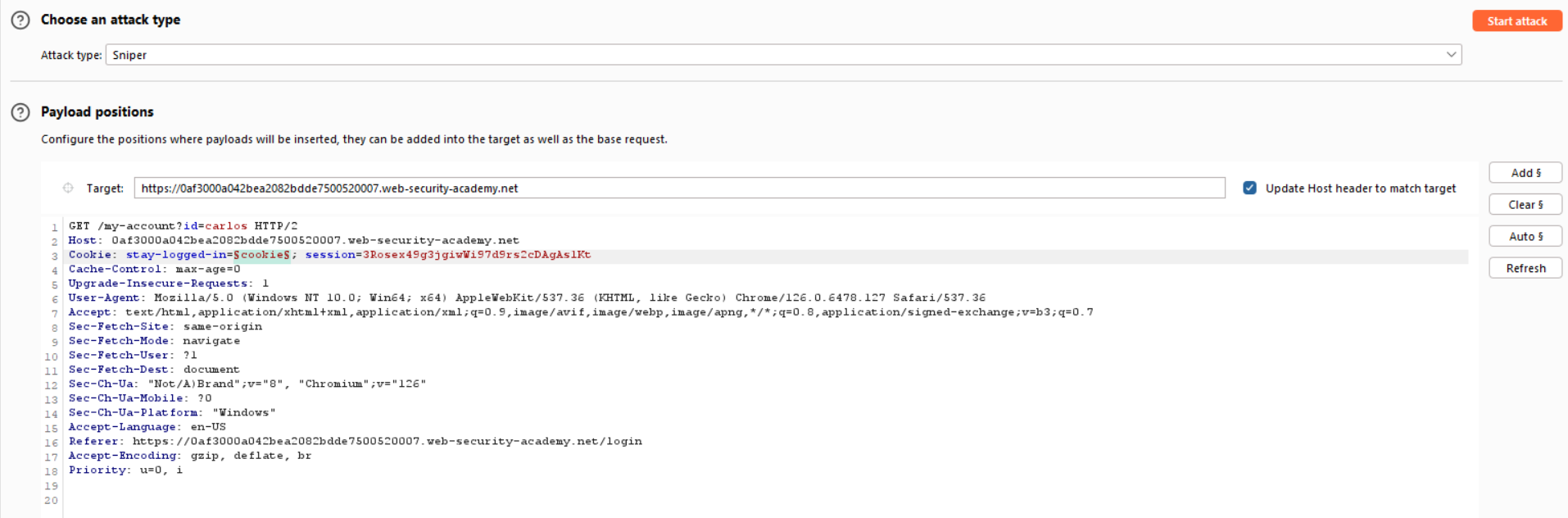


* Cookie được mã hóa bằng Base64

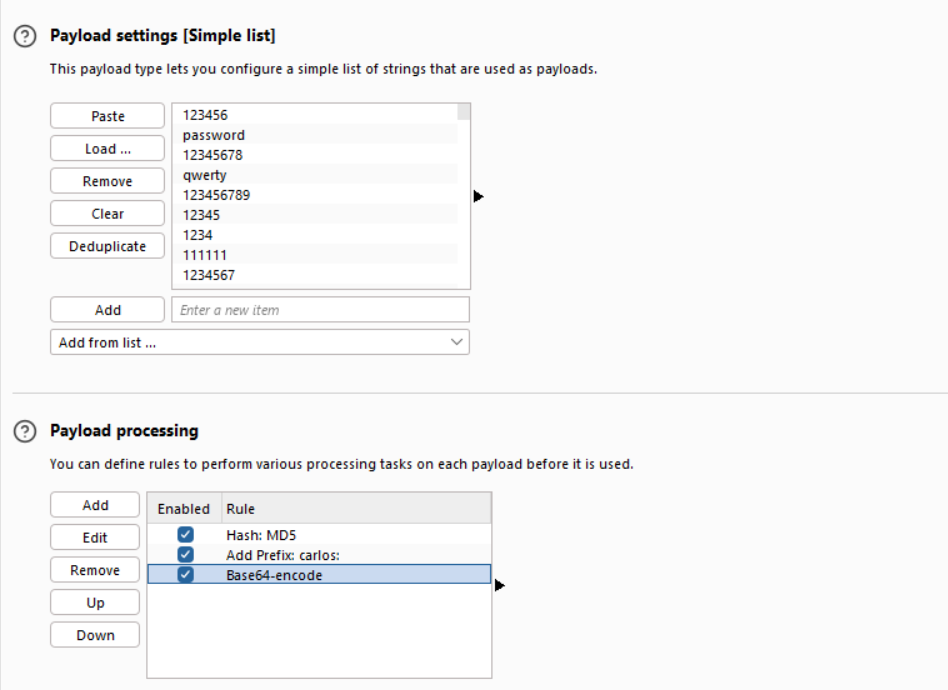


* Mật khẩu được mã hóa bằng hàm băm MD5
* Cookie = Base64(Username:MD5(Password))

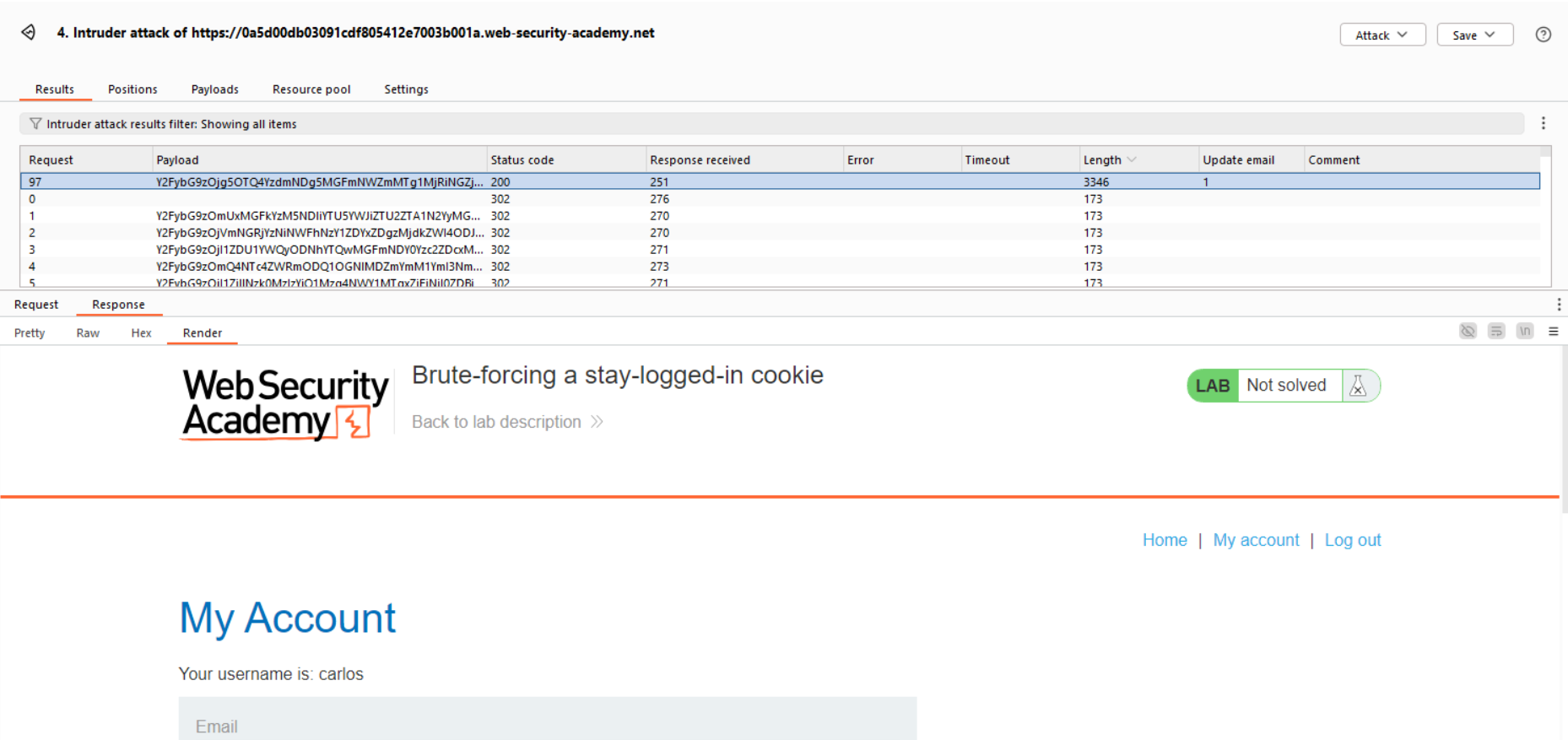
Bước 3: Chuyển gói tin GET /my-account sang Intruder và tạo payload ở Cookie



* Thêm wordlist mật khẩu và thêm mã hóa Base64, hàm băm MD5 và trường username ở trước.



Bước 4: Thực hiện tấn công



* Đã vào được tài khoản của carlos và hoàn thành bài lab

