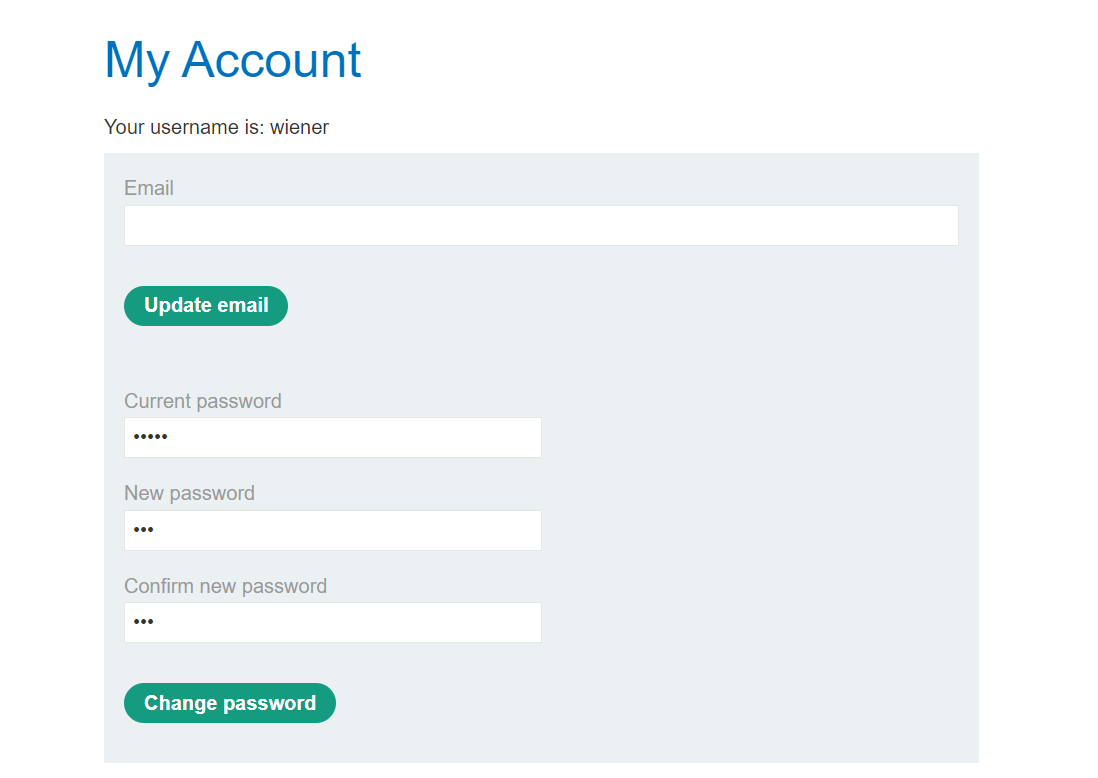
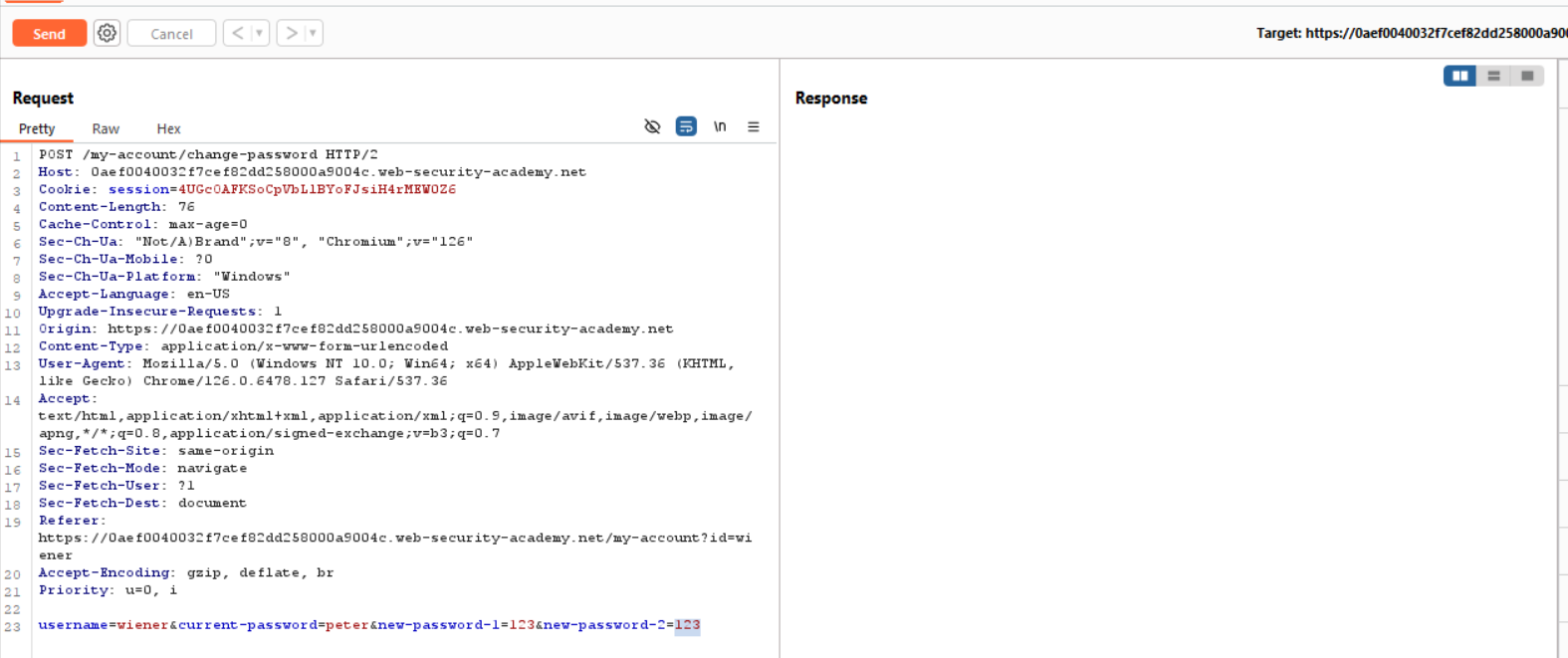


* Bài lab này có lỗ hổng trong Thay đổi mật khẩu

Bước 1: Đăng nhập và thay đổi mật khẩu



Bước 2: Bắt gói tin đổi mật khẩu bằng BurpSuite.



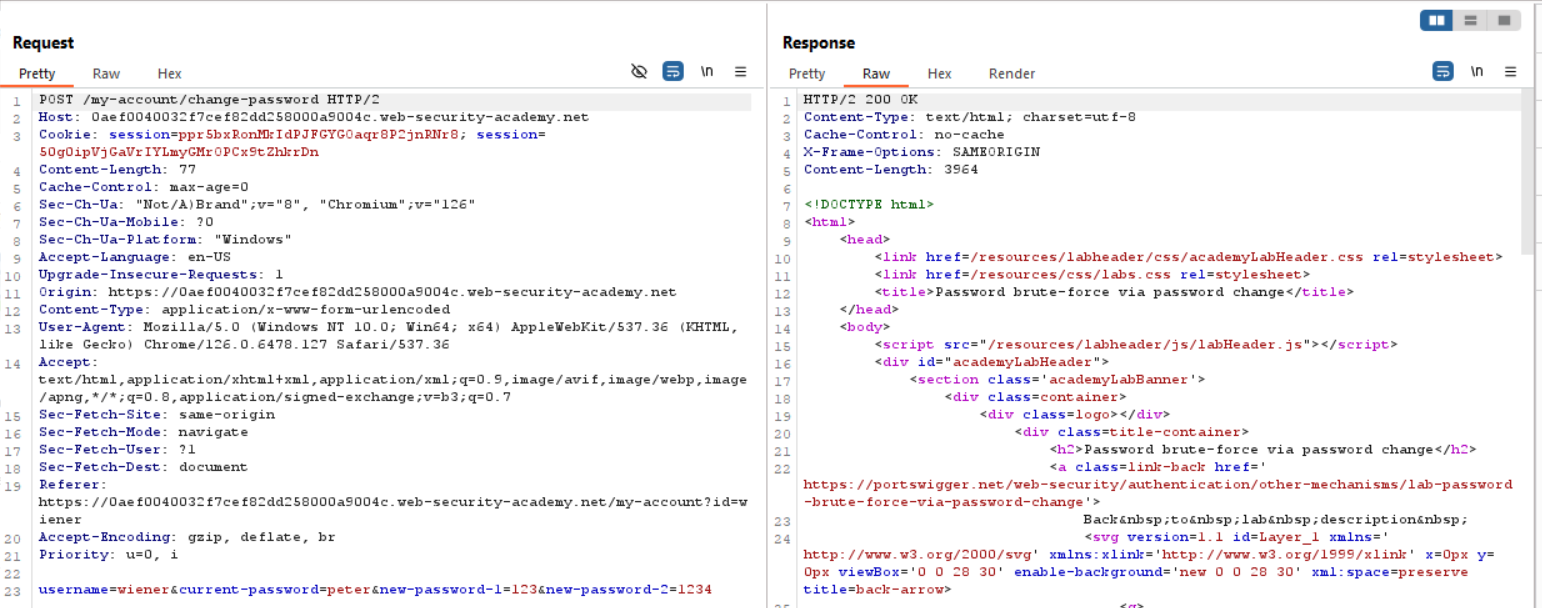
* Bắt được gói tin POST có chứa dữ liệu để đổi password

Bước 4: Thử nhập sai mật khẩu và đúng 2 trường mật khẩu còn lại

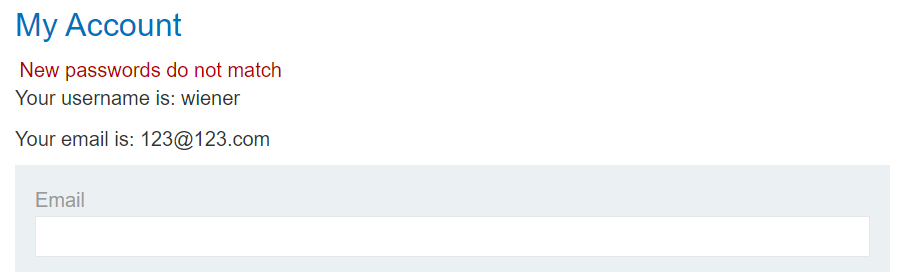


* Tự động đăng xuất và chuyển về trang login

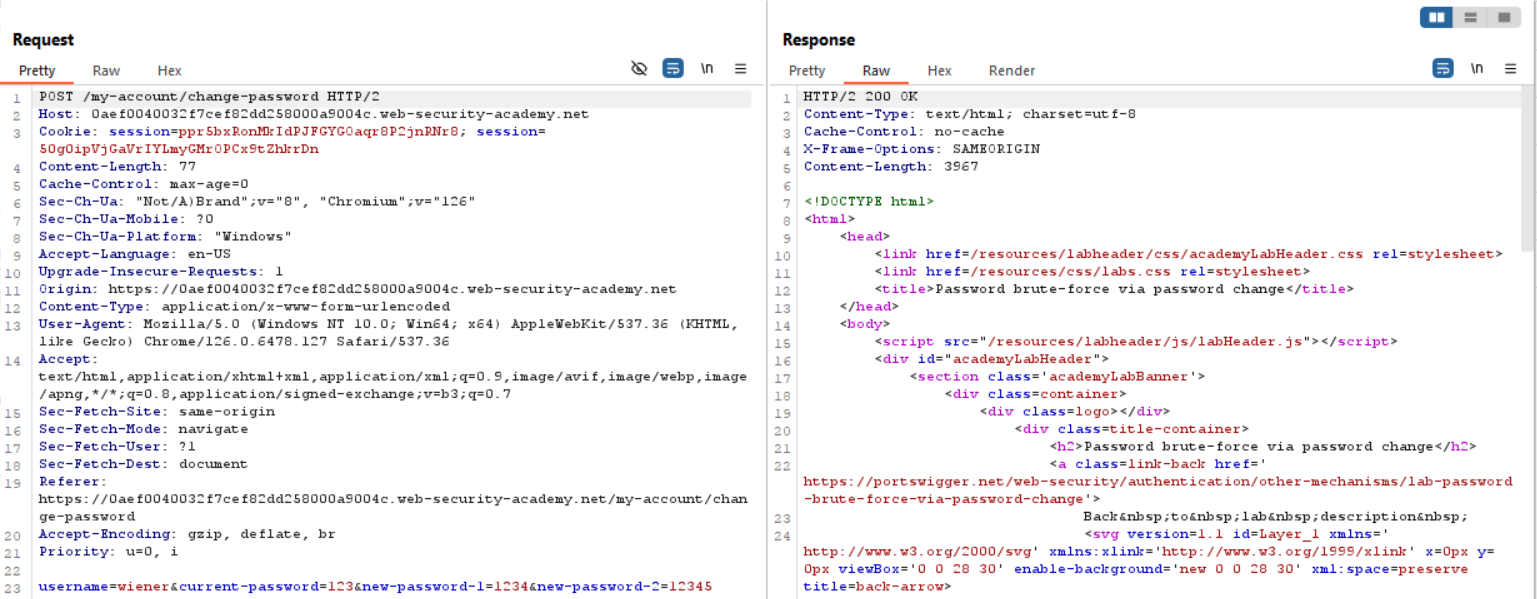
Bước 5: Thử nhập đúng mật khẩu và sai 2 trường mật khẩu còn lại



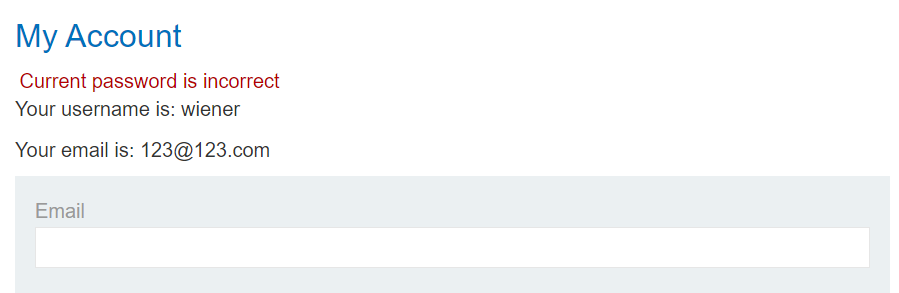
* Có xuất hiện thông báo: New passwords do not match



Bước 6: Thử nhập sai toàn bộ 3 trường mật khẩu

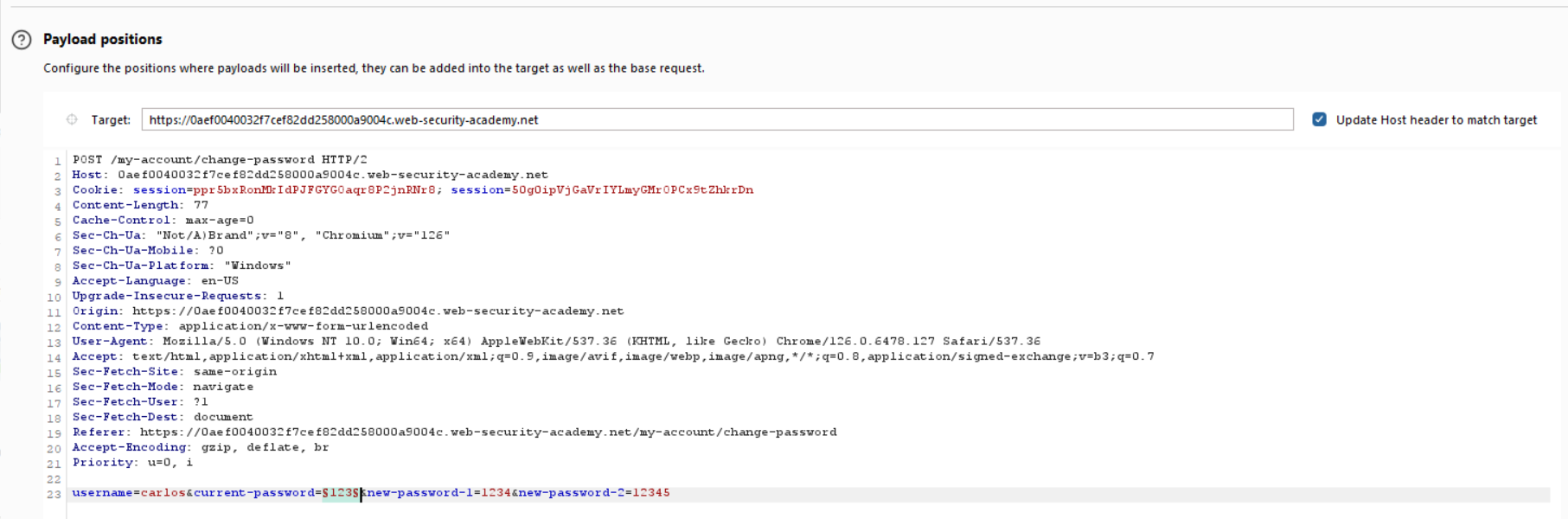


* Xuất hiện thông báo: Current password is incorrect

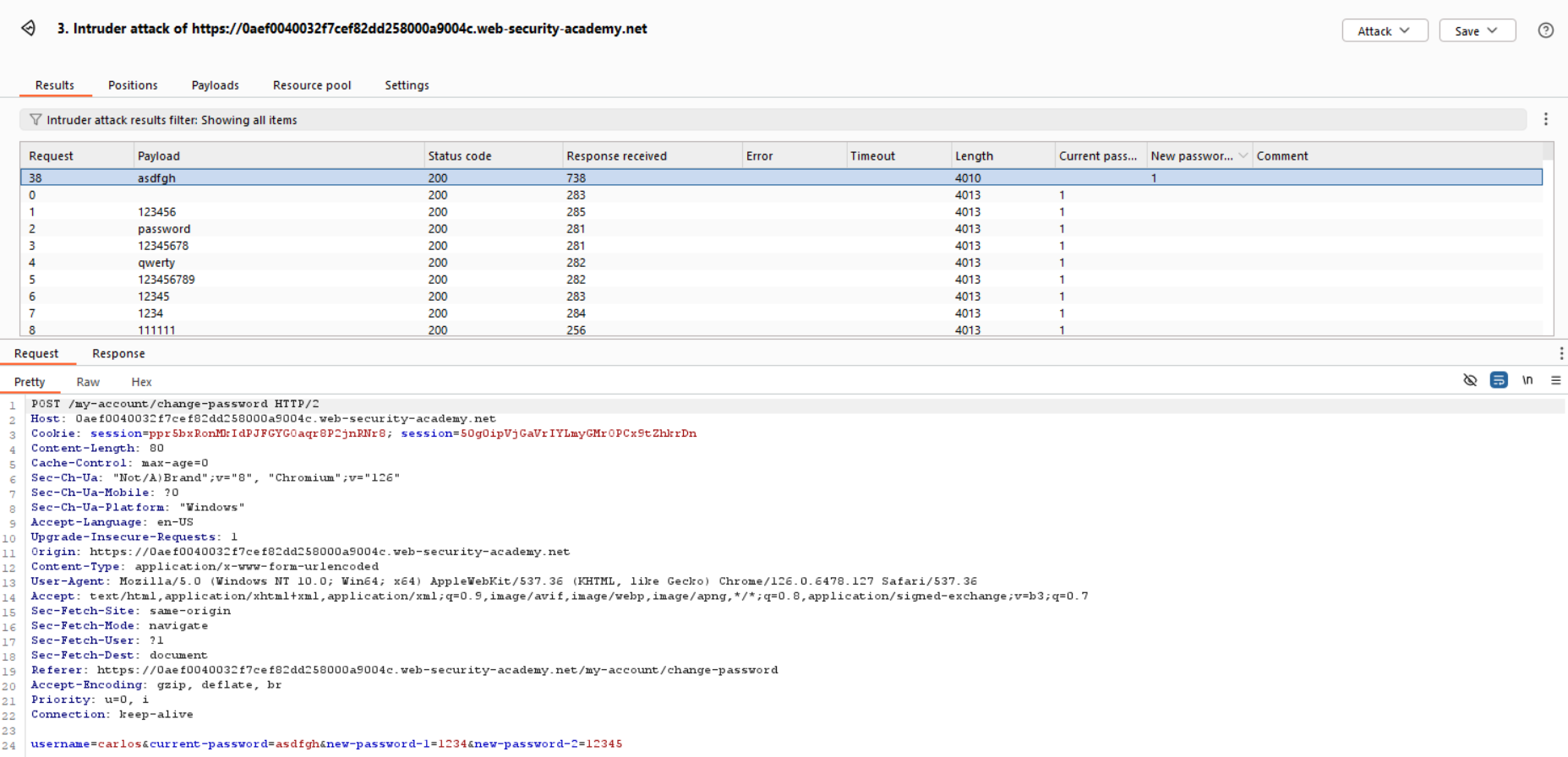


* Ý tưởng: ta sẽ Brute-Force thay đổi mật khẩu của tài khoản carlos với payload ở phần mật khẩu cho đến khi xuất hiện thông báo “New passwords do not match”

Bước 7: Chuyển gói tin về Intruder và tấn công



* Tìm được mật khẩu của carlos: asdfgh



Bước 8: Đăng nhập tài khoản và hoàn thành lab

