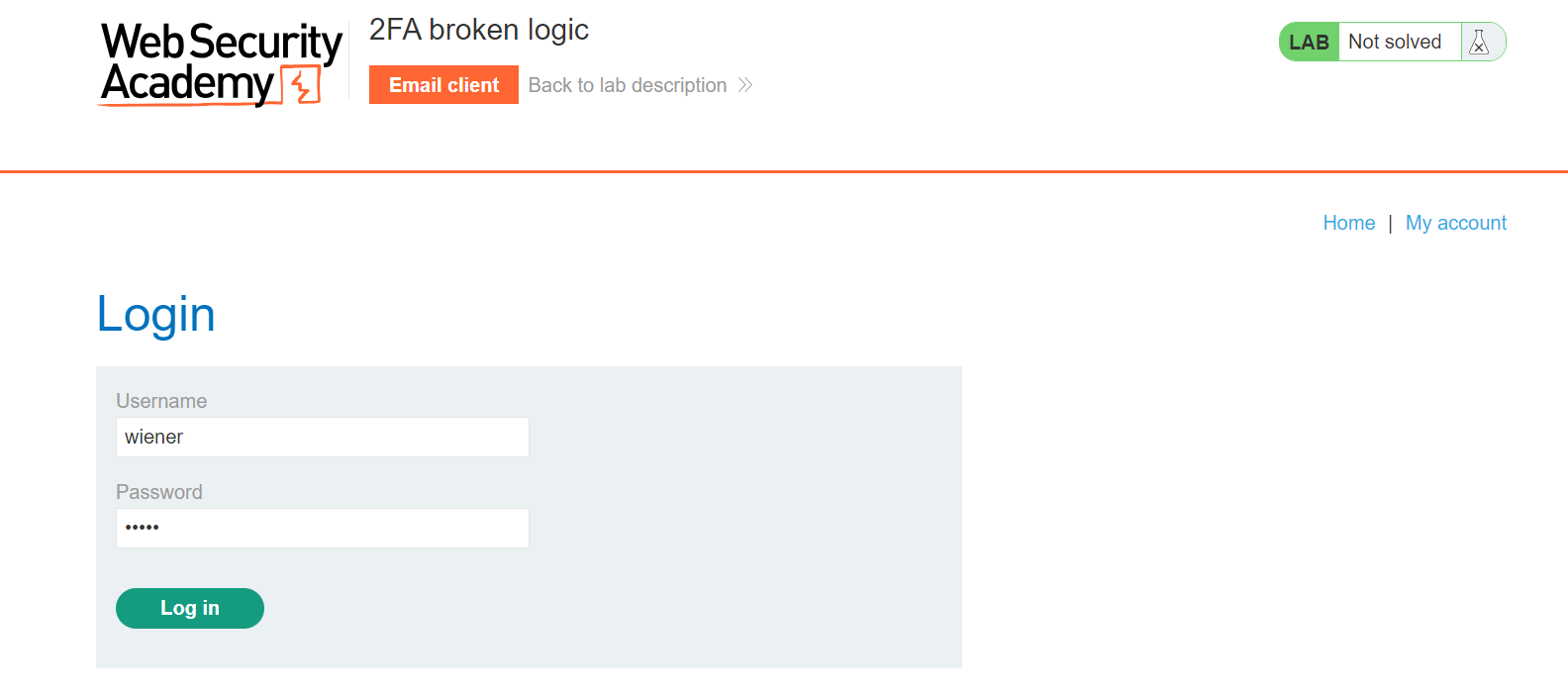
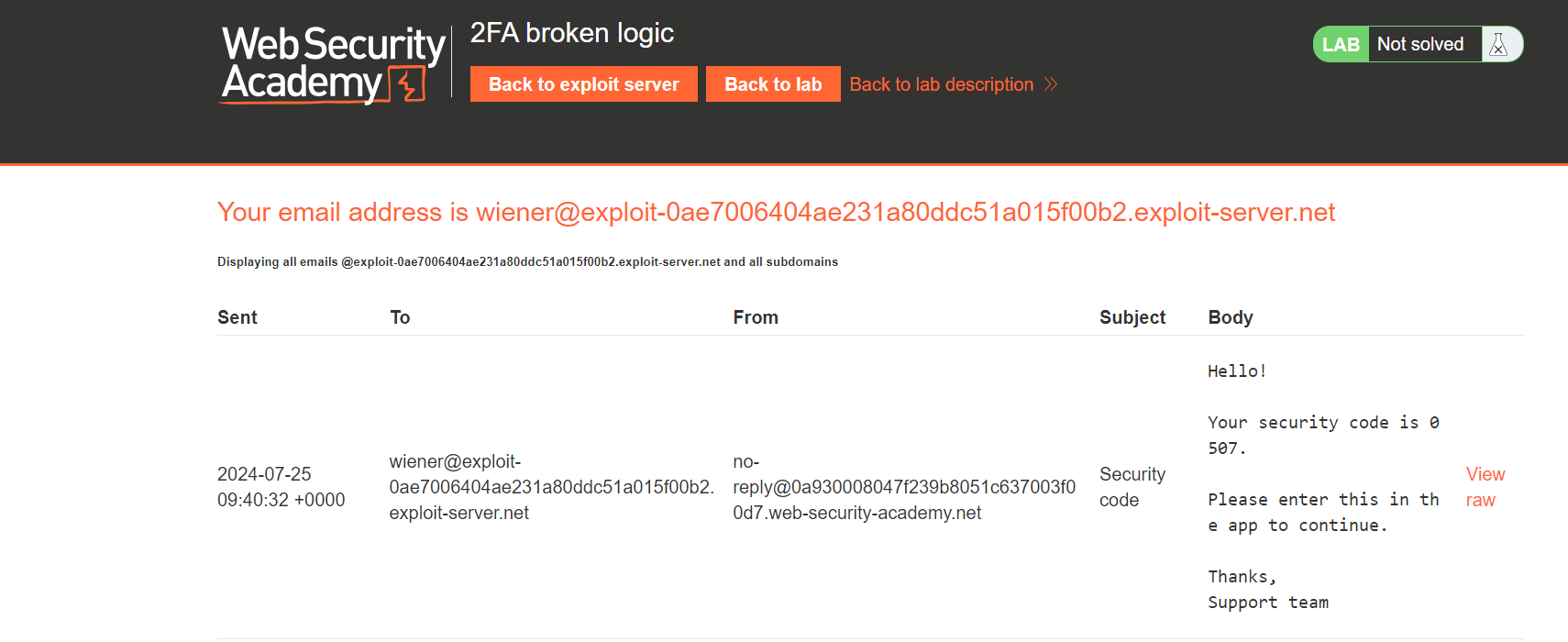
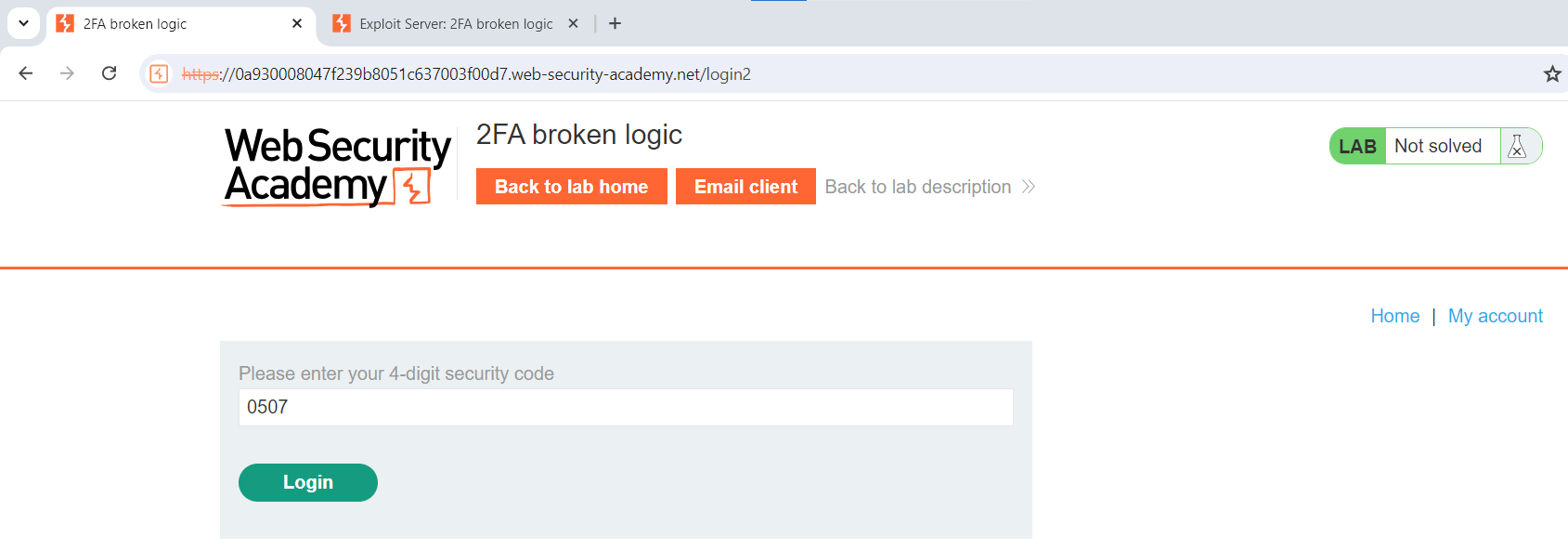


Bước 1: Vào trang Đăng Nhập

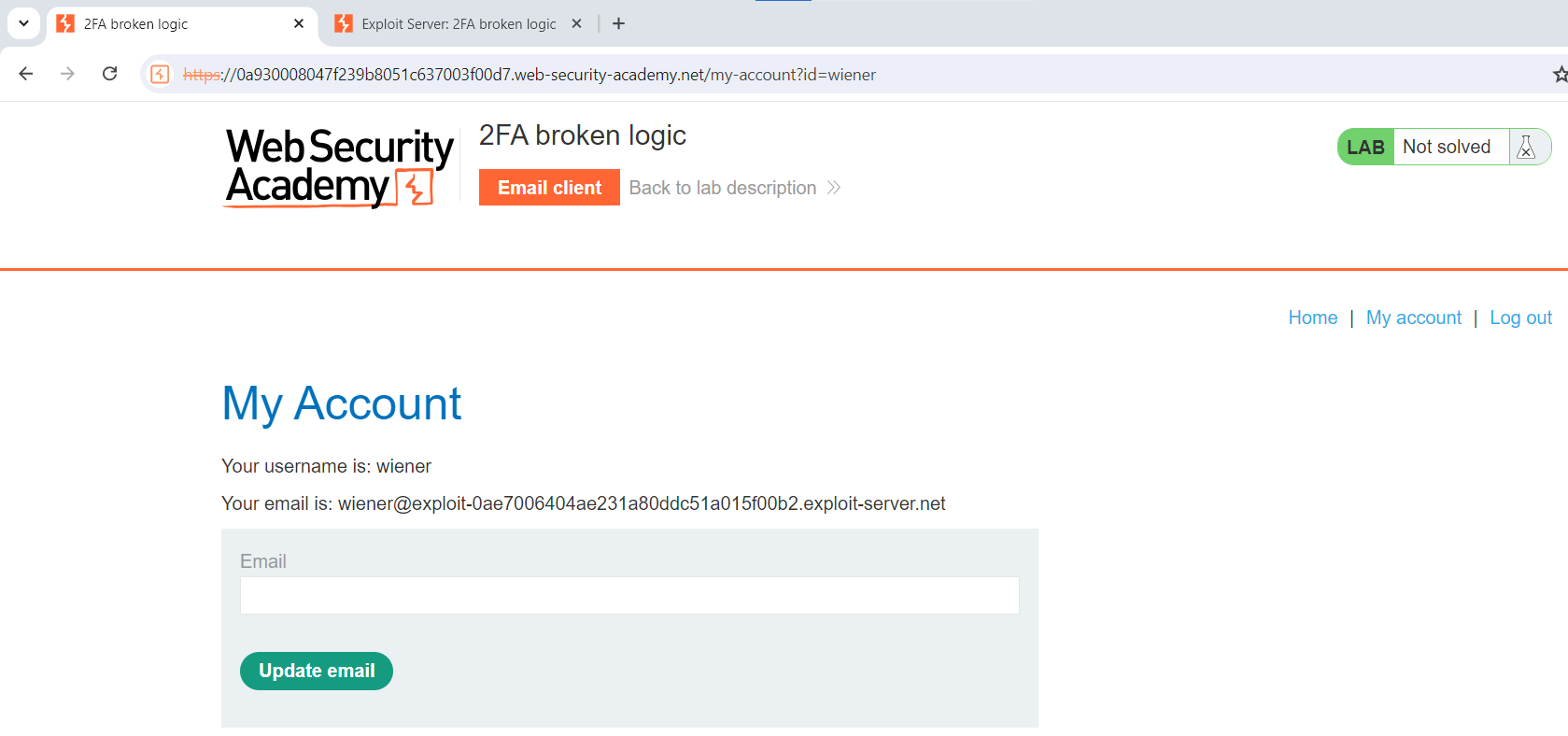


Bước 2: Đăng nhập thì yêu cầu mã được gửi về email

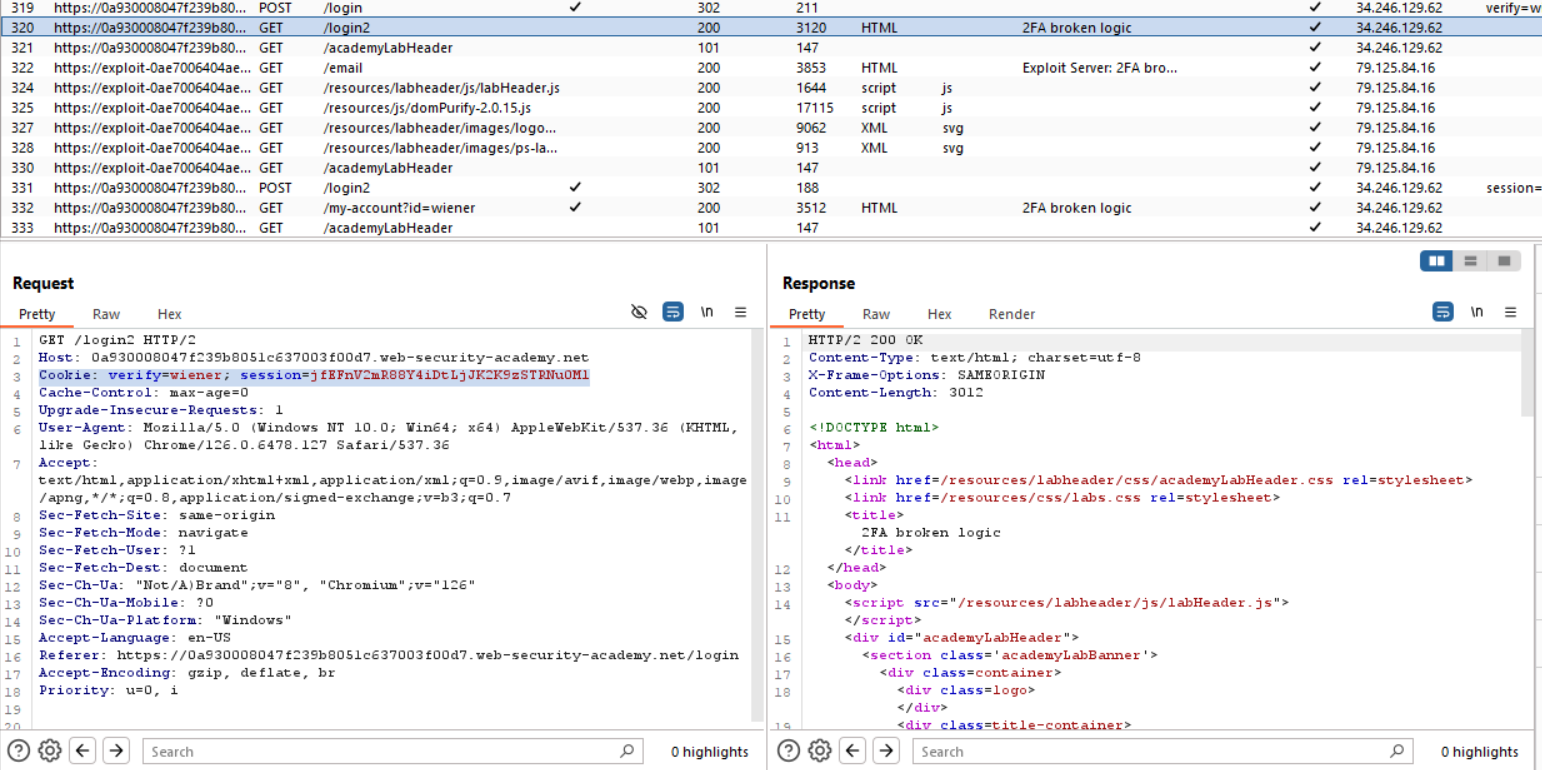




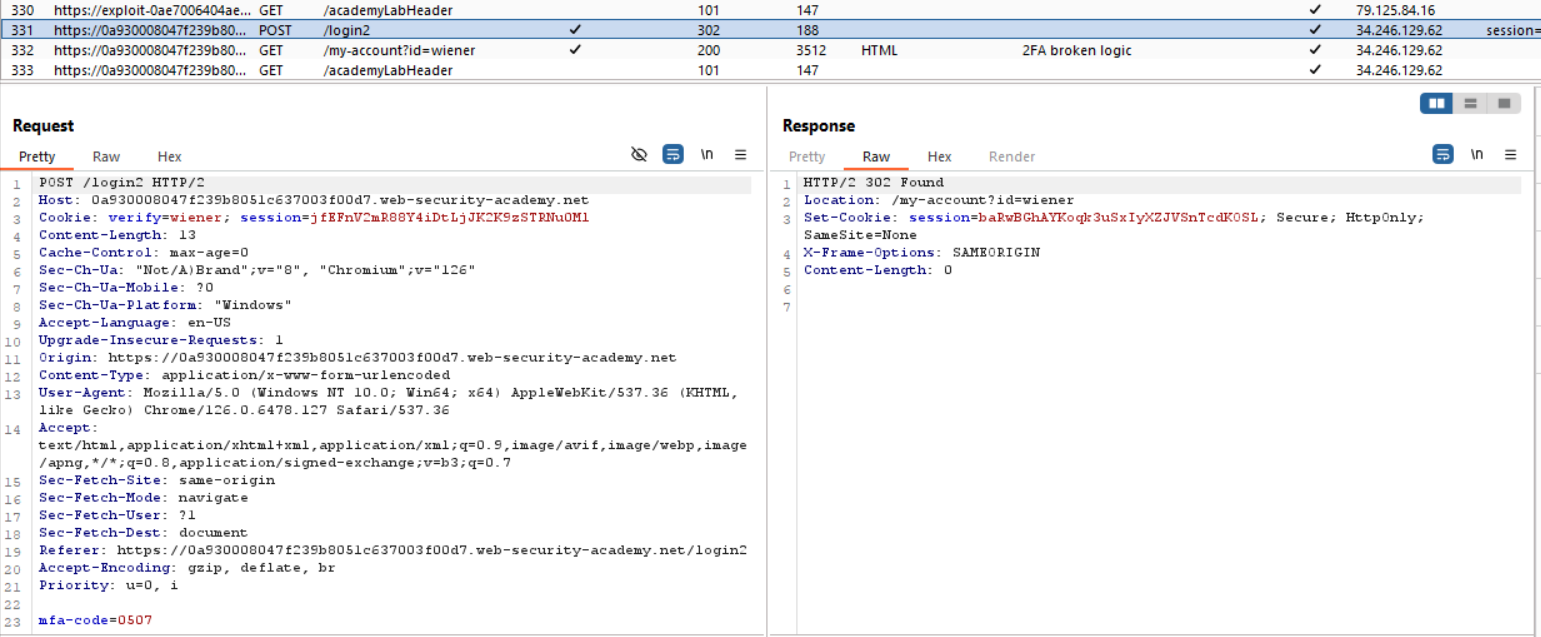
* Đăng nhập thành công



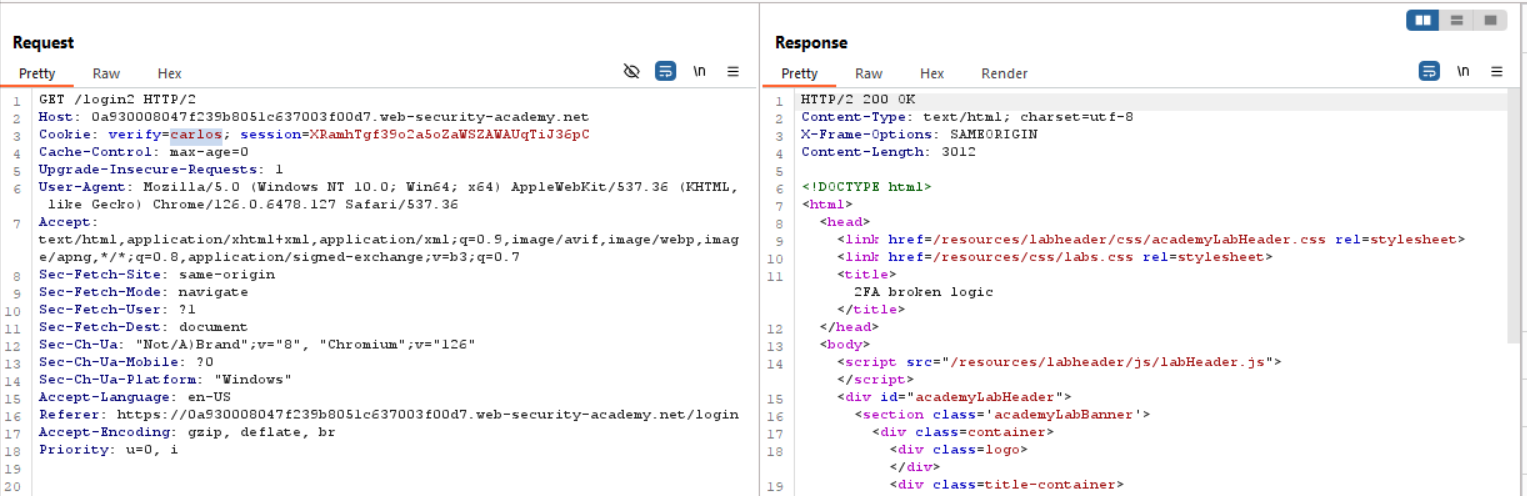
Bước 3: Bắt gói tin bằng BurpSuite, ta thấy sau khi nhập tài khoản và mật khẩu thành công sẽ chuyển sang /login2.



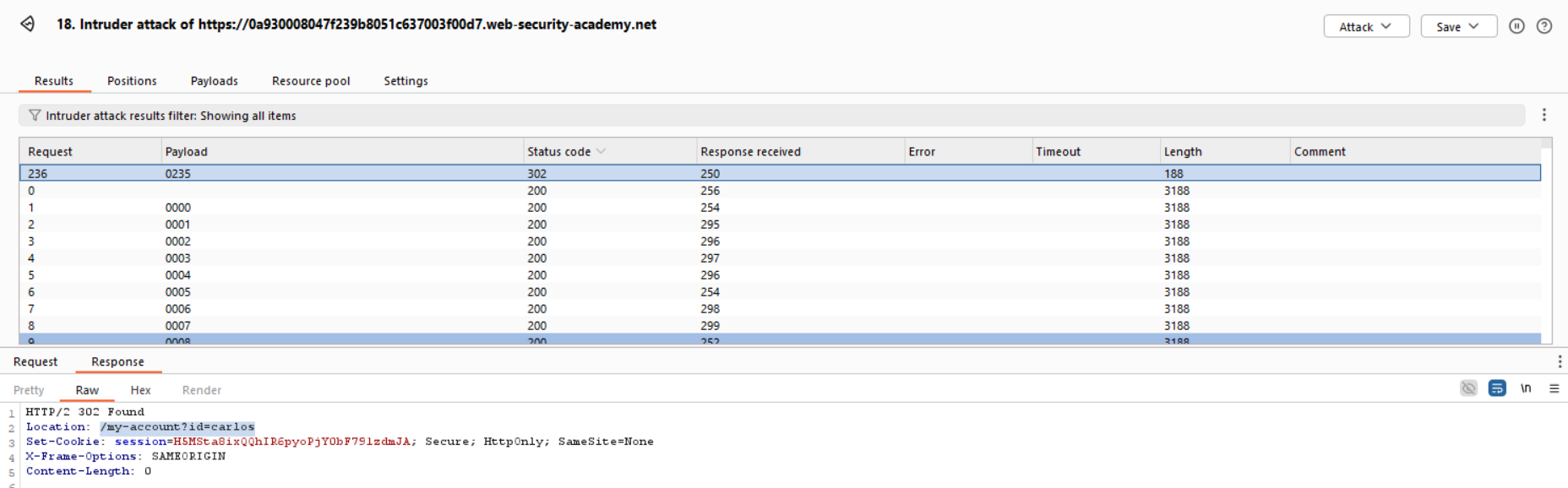
* Tại đây, ta thấy được Cookie thêm một trường là “verify=wiener”
* Sau khi nhập mã code từ email thì sẽ được chuyển qua /my-account?id=wiener



Bước 4: Gửi GET /login2 đến Repeater và sửa cookie thành tài khoản Carlos để lấy email xác nhận code



Bước 5: Gửi POST /login2 đến Intruder để Brute-Force code của tài khoản Carlos



* Code: 0235

Bước 6: Chuyển Respone sang bên web để vào tài khoản Carlos

