Lab: JWT authentication bypass via flawed signature verification

APPRENTICE

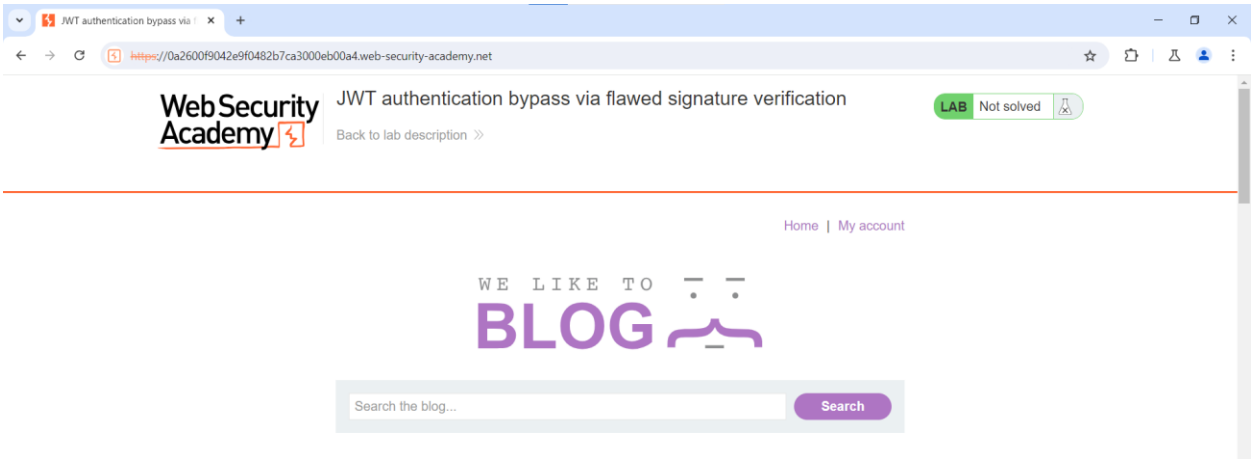
LAB | Not solved

This lab uses a JWT-based mechanism for handling sessions. The server is insecurely configured to accept unsigned JWTs.

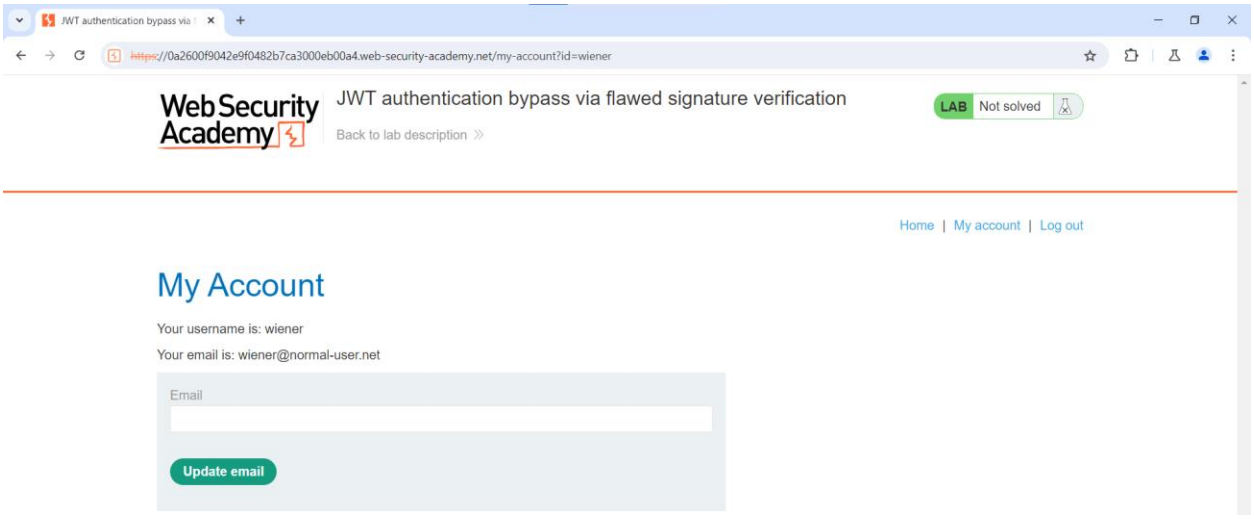
To solve the lab, modify your session token to gain access to the admin panel at `/admin`, then delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

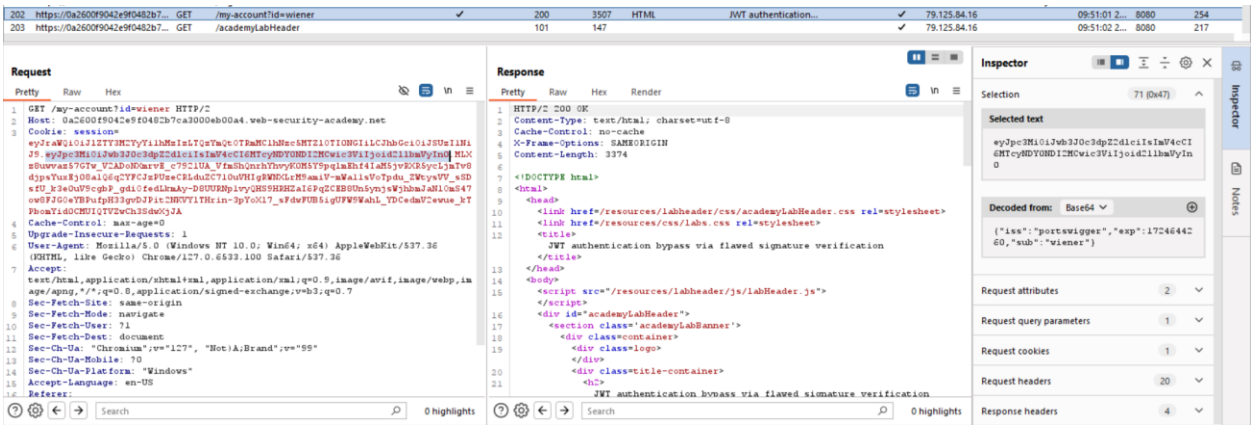
- Mục đích: Truy cập vào trang admin và xóa tài khoản carlos



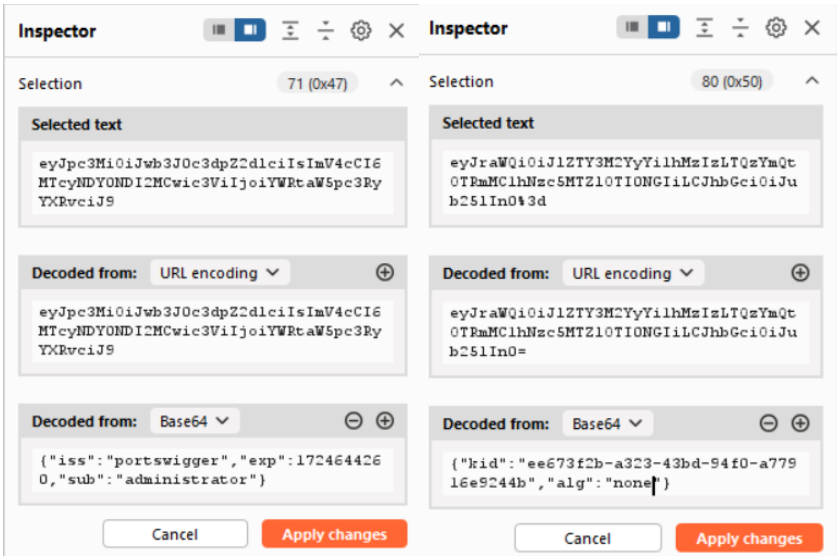
- Đăng nhập tài khoản người dùng wiener

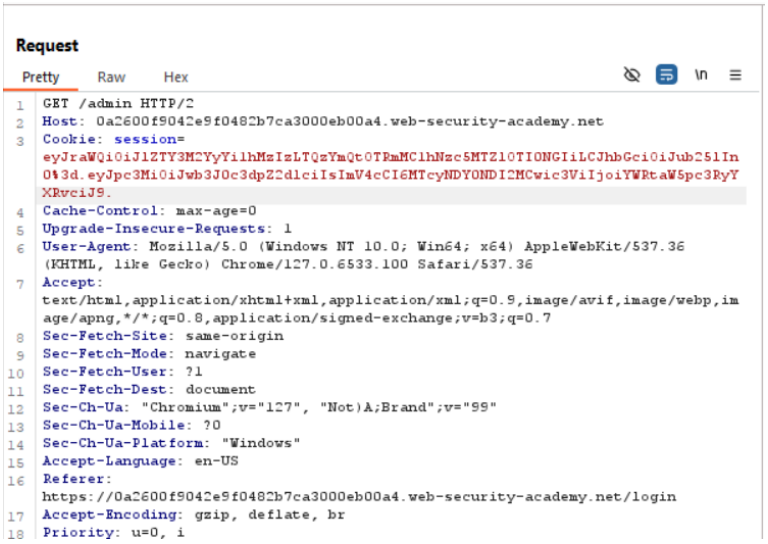


- Bắt gói tin bằng BurpSuite thì ta nhận được Session

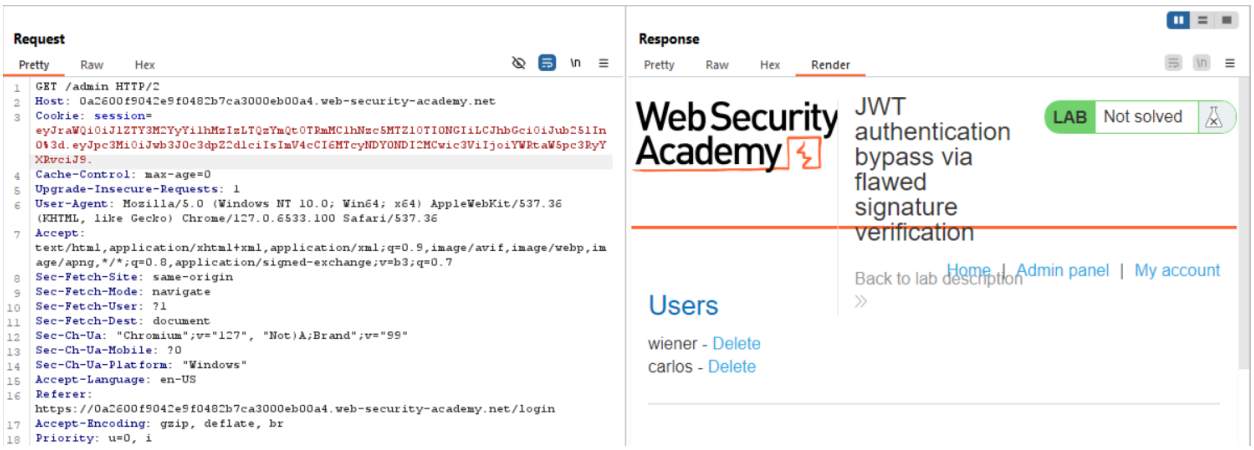


- Chuyển qua Repeater và sửa payload “sub” thành “administrator”, header “alg” thành “none”, cuối cùng xóa chữ ký ở phần session đi.

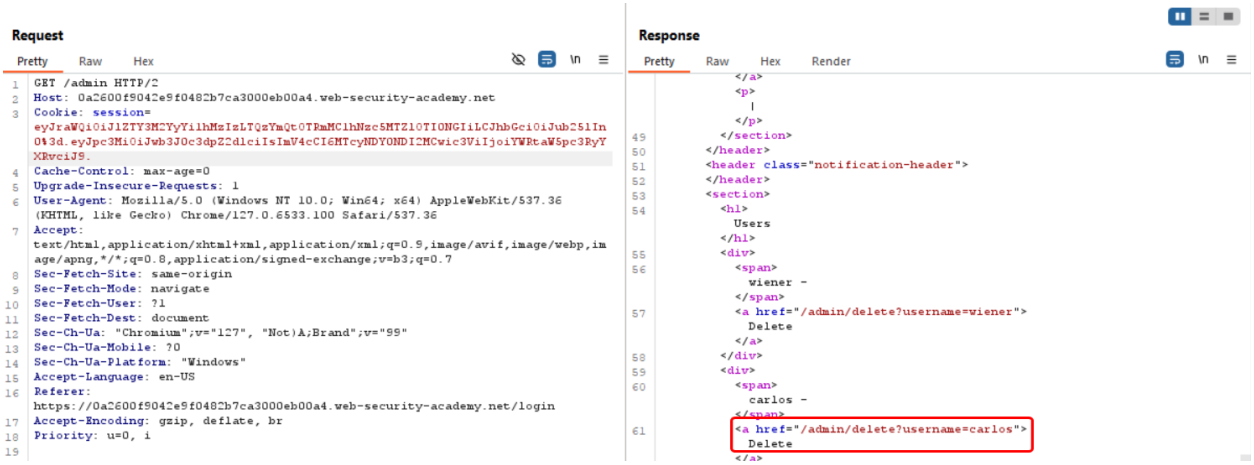




- Sau đó gửi và xuất hiện “Admin panel”



- Đọc code html và thấy đường dẫn để xóa tài khoản carlos



- Xóa tài khoản “carlos”