Lab: JWT authentication bypass via unverified signature

APPRENTICE

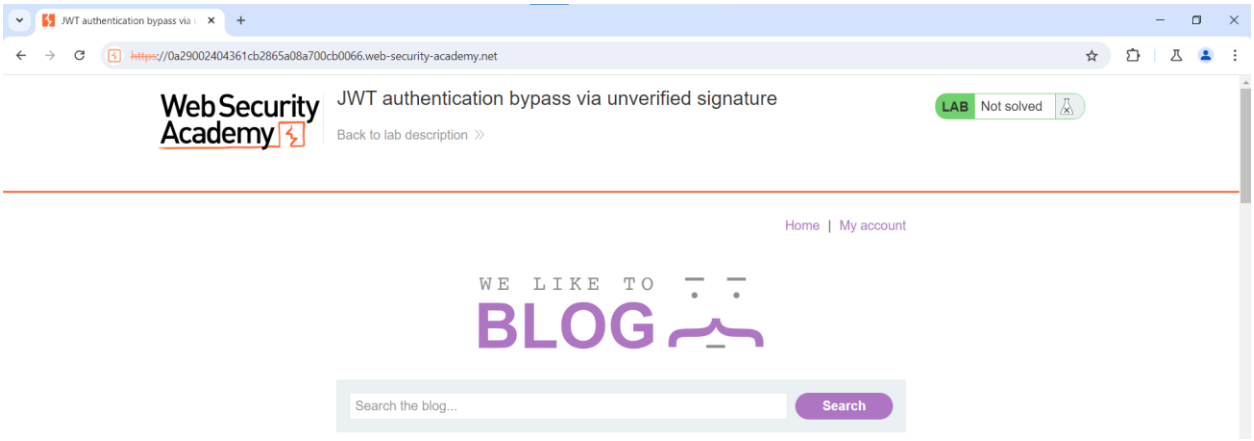
LAB | Not solved

This lab uses a JWT-based mechanism for handling sessions. Due to implementation flaws, the server doesn't verify the signature of any JWTs that it receives.

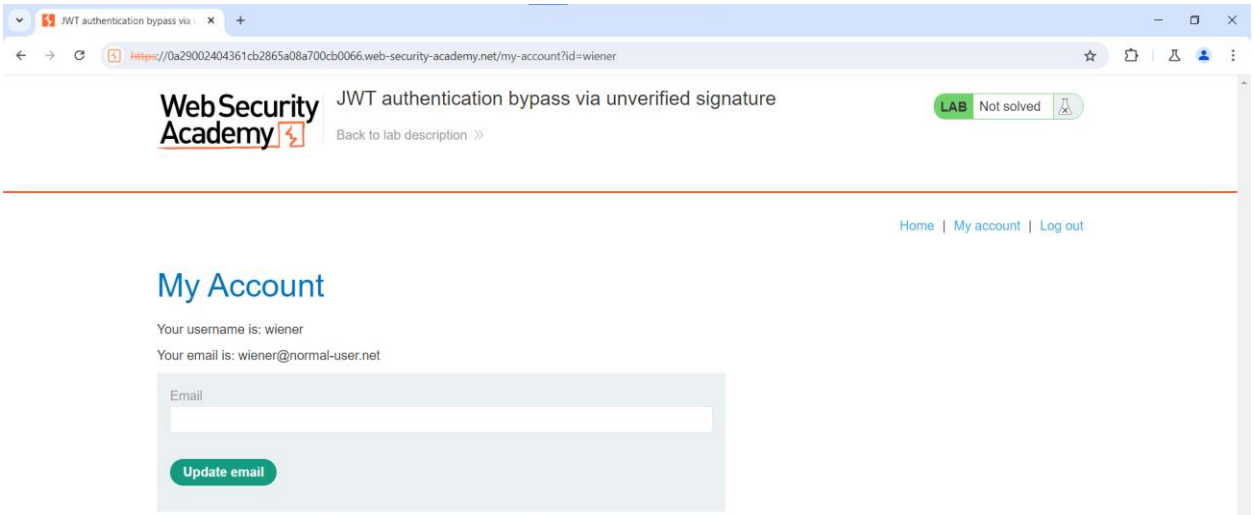
To solve the lab, modify your session token to gain access to the admin panel at `/admin`, then delete the user `carlos`.

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

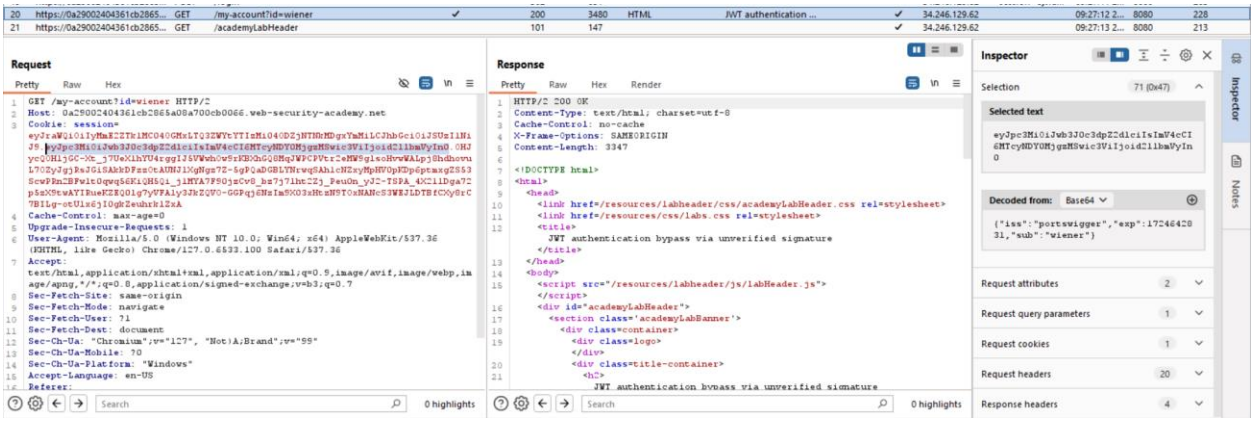
- Mục đích: Truy cập vào trang admin và xóa tài khoản carlos



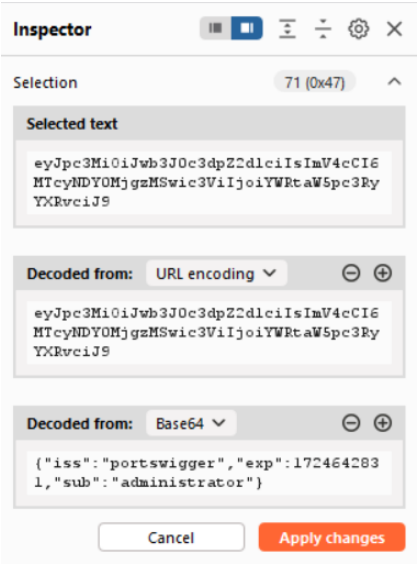
- Đăng nhập tài khoản người dùng wiener



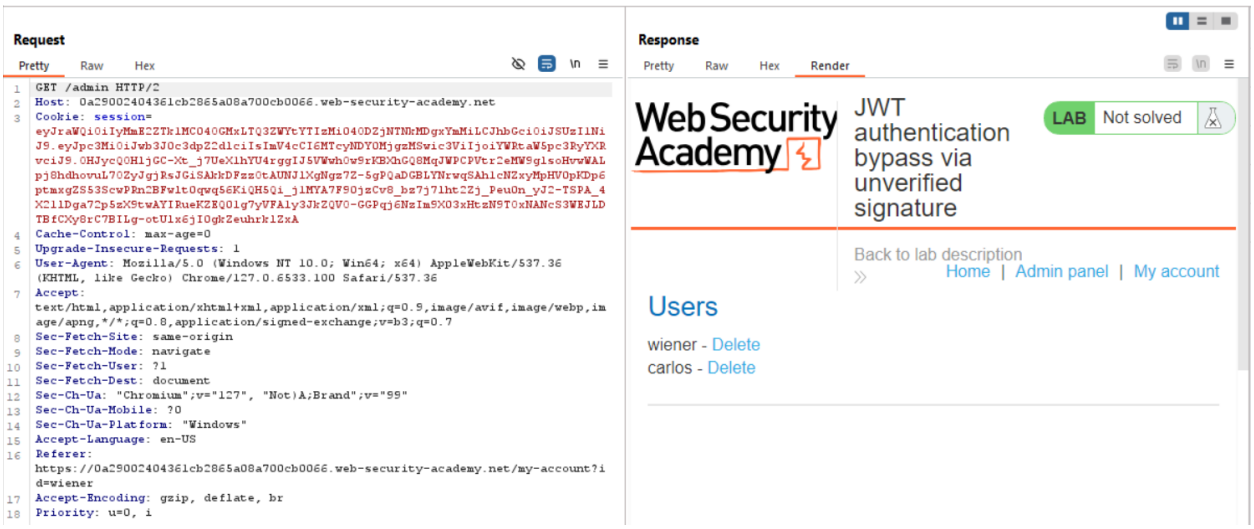
- Bắt gói tin bằng BurpSuite thì ta nhận được Session



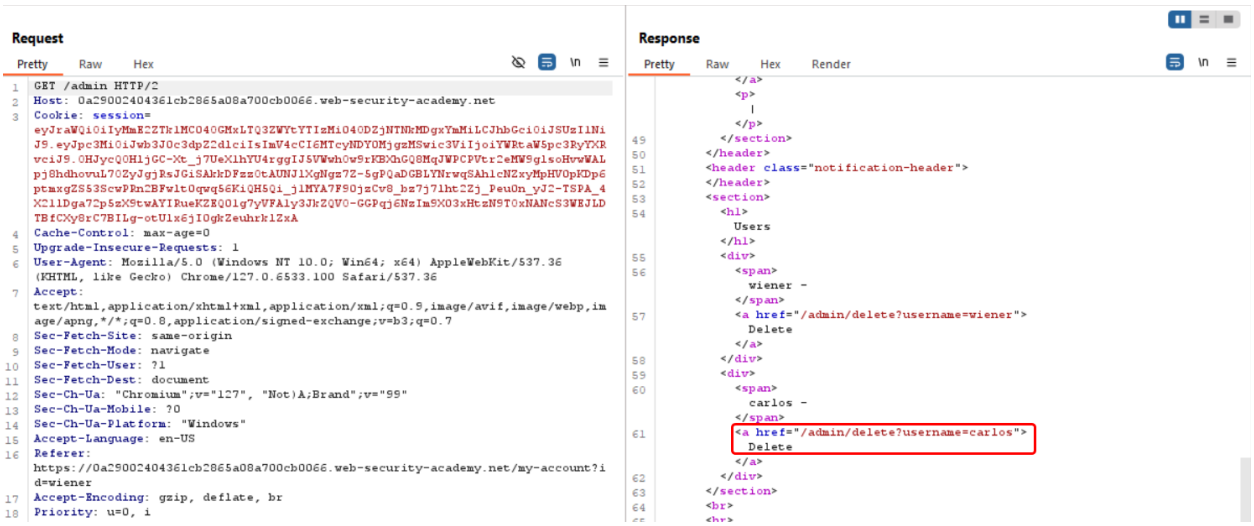
- Chuyển qua Repeater và sửa trường “wiener” thành “administrator”



- Sau đó gửi và xuất hiện “Admin panel”



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



- Xóa tài khoản “carlos”