Lab: JWT authentication bypass via jwk header injection

PRACTITIONER

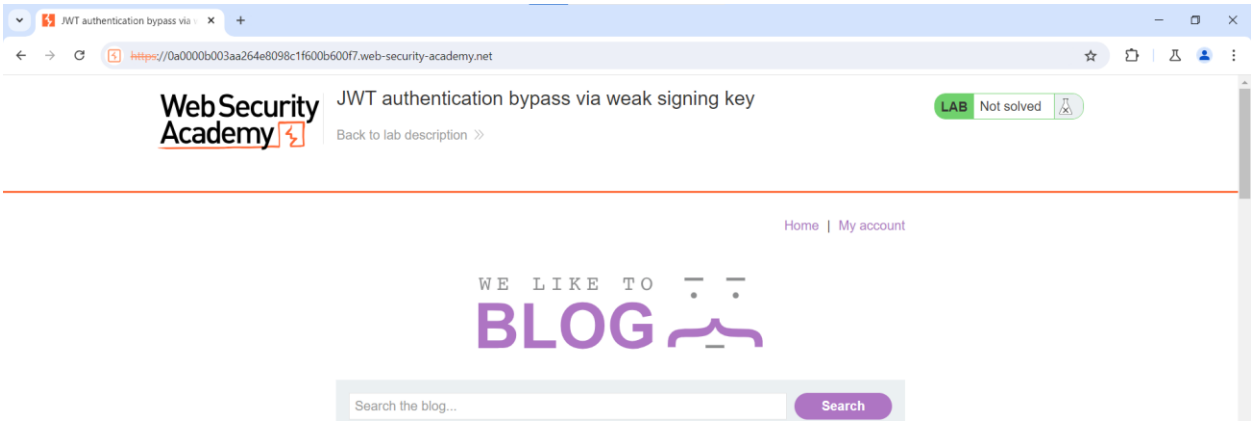
LAB | Not solved

This lab uses a JWT-based mechanism for handling sessions. The server supports the `jwk` parameter in the JWT header. This is sometimes used to embed the correct verification key directly in the token. However, it fails to check whether the provided key came from a trusted source.

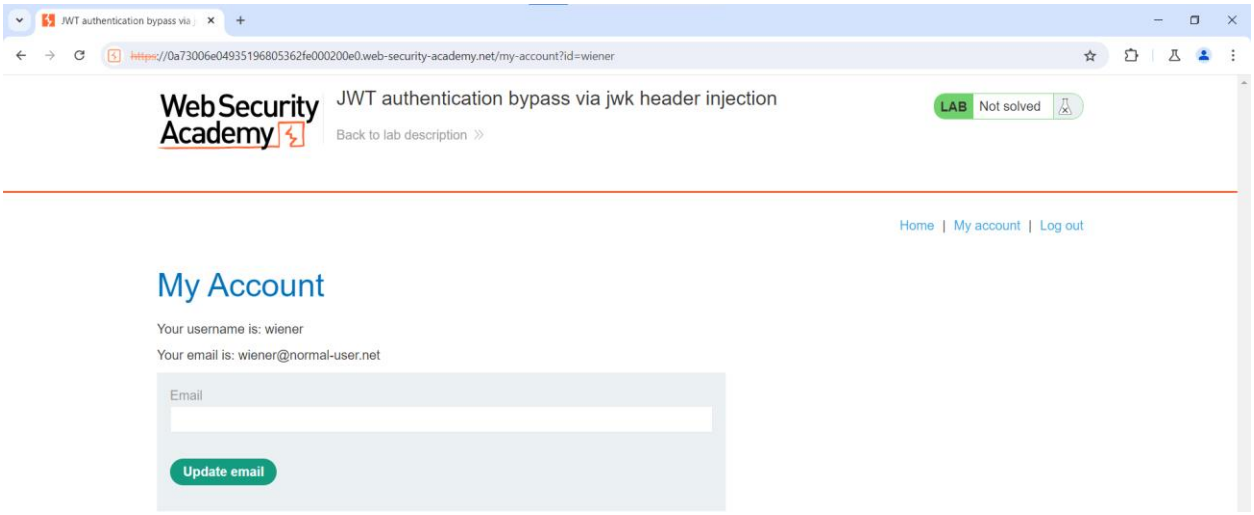
To solve the lab, modify and sign a JWT that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

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

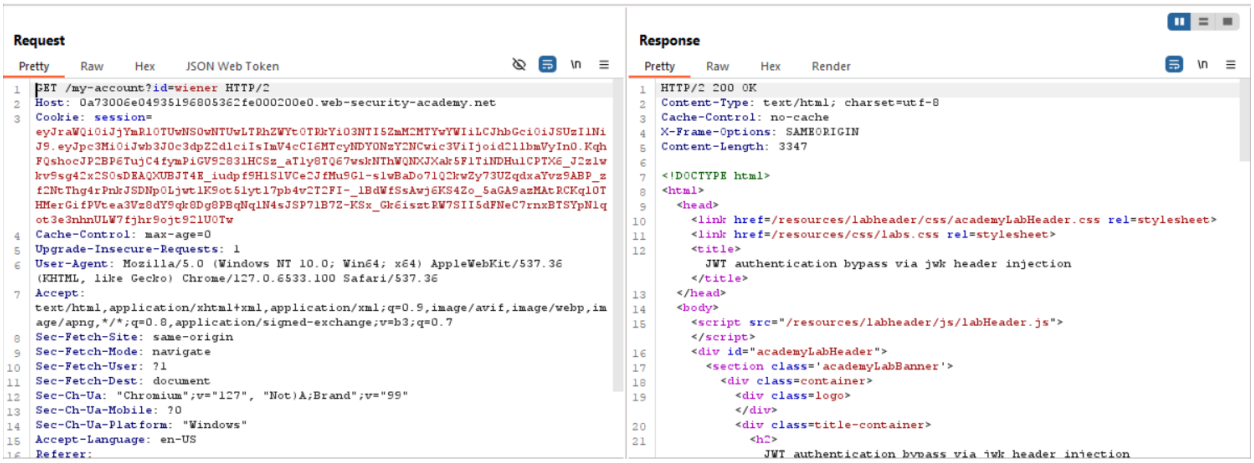
- Mục đích: Sử dụng jwk để nhúng khóa công khai bất kì, sau đó dùng khóa bí mật để thay đổi JWT và truy cập vào trang admin để xóa tài khoản carlos



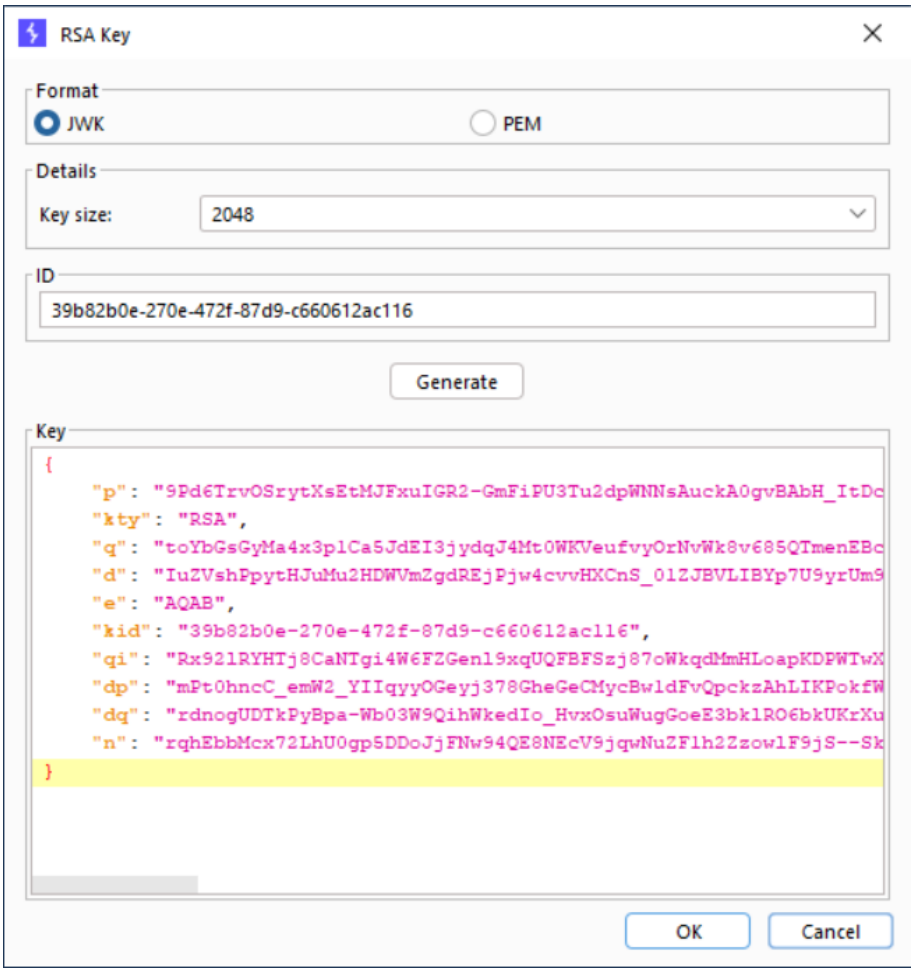
- Đăng nhập tài khoản người dùng wiener



- Bắt gói tin bằng BurpSuite thì ta nhận được Session

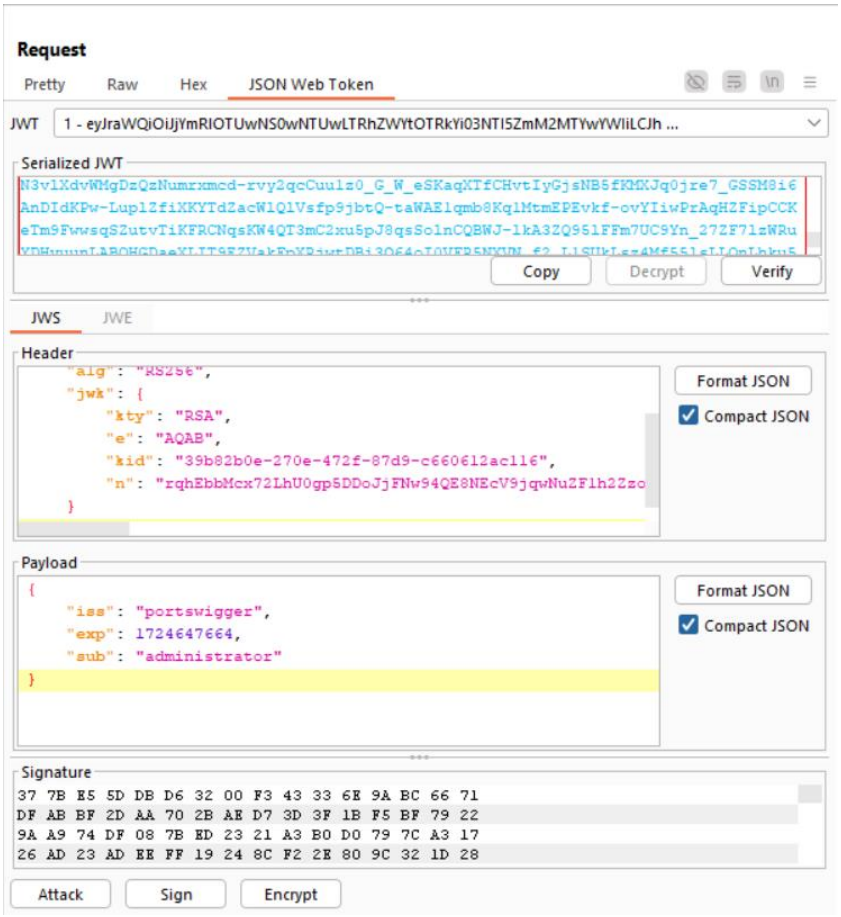


- Theo như bài lab, server có hỗ trợ jwk nên ta sẽ lợi dụng điều này để bypass chữ ký trong JWT
- Tạo mã RSA 2048: JWT Editor => New RSA Key

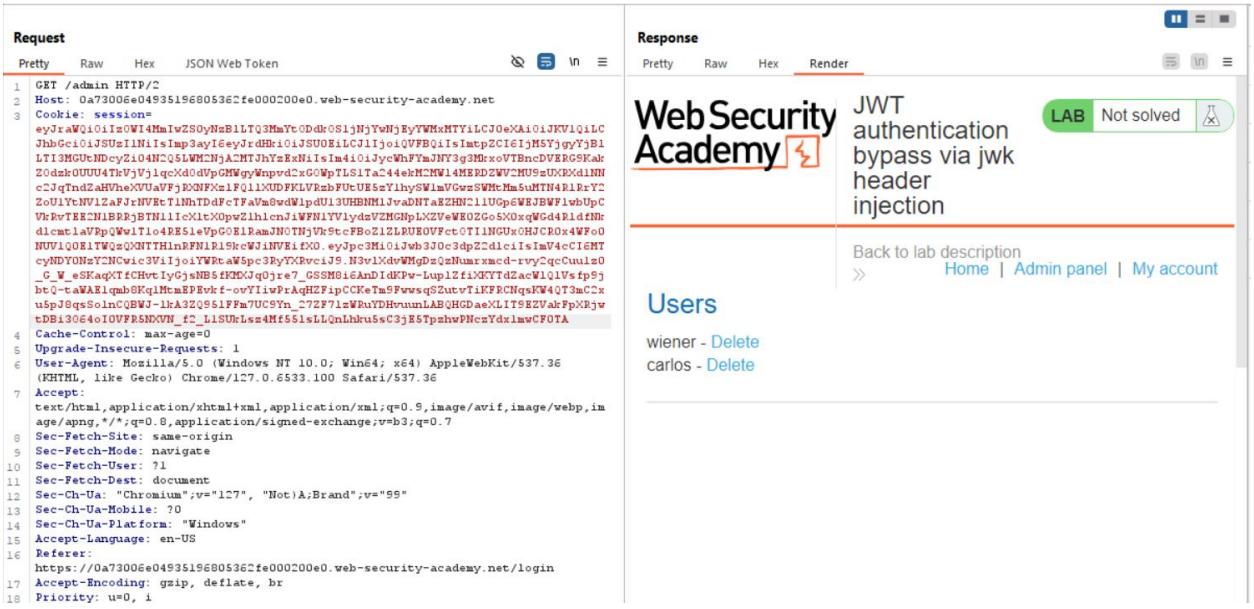


- Chuyển gói tin GET đã bắt được vào Repeater

- Chuyển sang tab JSON Web Token => Sửa “wiener” thành “administrator” => Attack => Embedded JWK



- Nhấn Send để gửi đi thì ta đã thành công vào “/admin”



- Xóa tài khoản “carlos”