Lab: JWT authentication bypass via jku header injection

PRACTITIONER

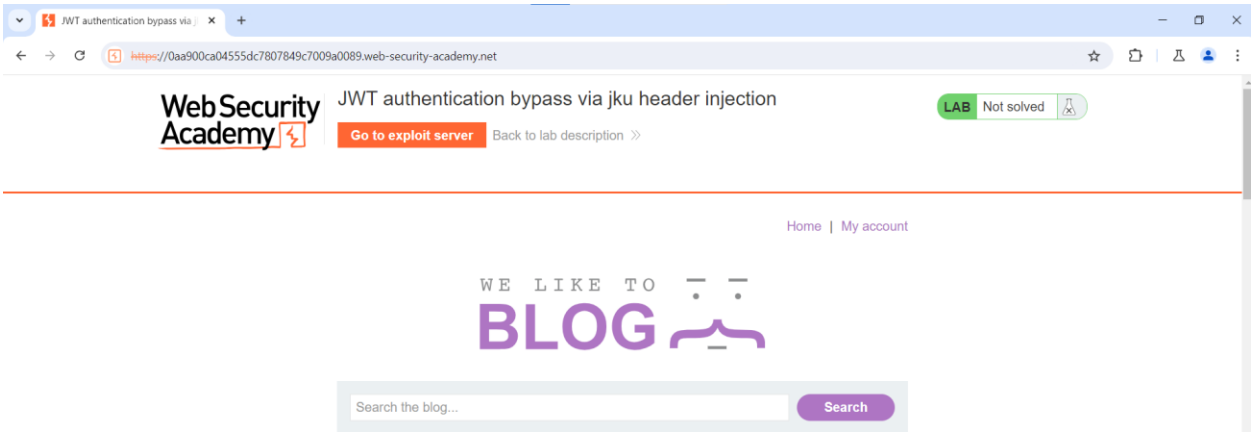
LAB | Not solved

This lab uses a JWT-based mechanism for handling sessions. The server supports the `jku` parameter in the JWT header. However, it fails to check whether the provided URL belongs to a trusted domain before fetching the key.

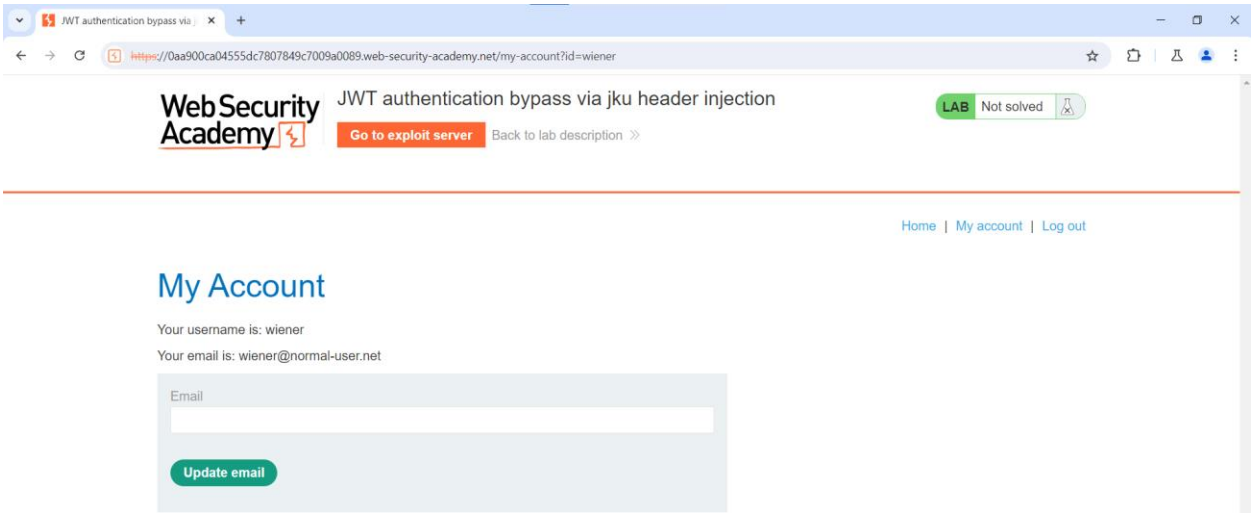
To solve the lab, forge a JWT that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

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

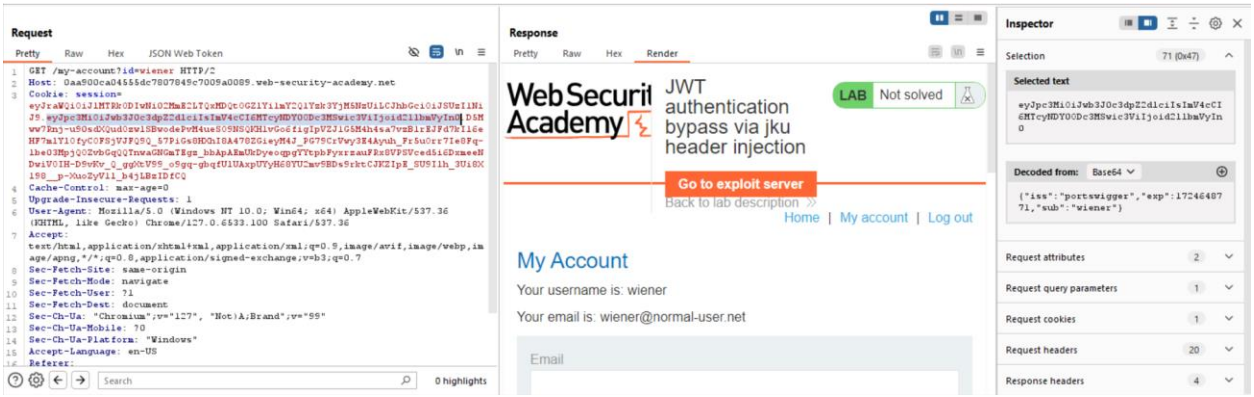
- Mục đích: Sử dụng jku để lấy khóa từ tên miền không tin cậy và truy cập vào trang admin để xóa tài khoản carlos



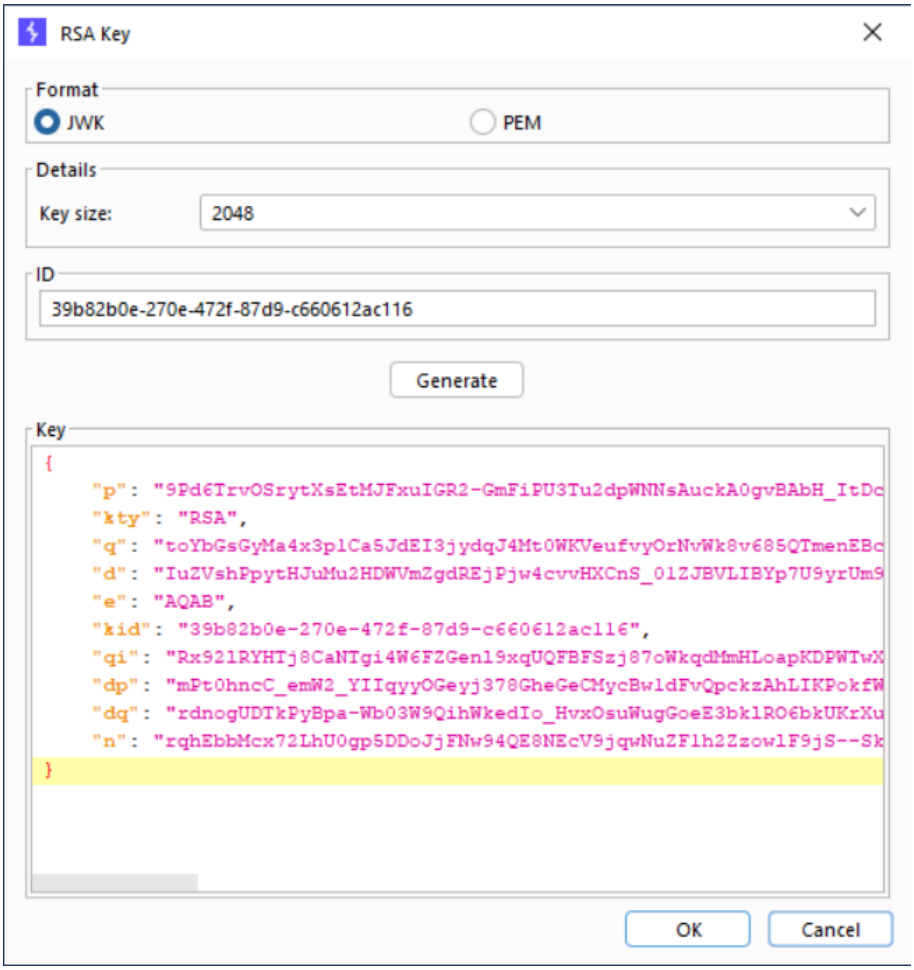
- Đăng nhập tài khoản người dùng wiener



- Bắt gói tin bằng BurpSuite thì ta nhận được Session



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



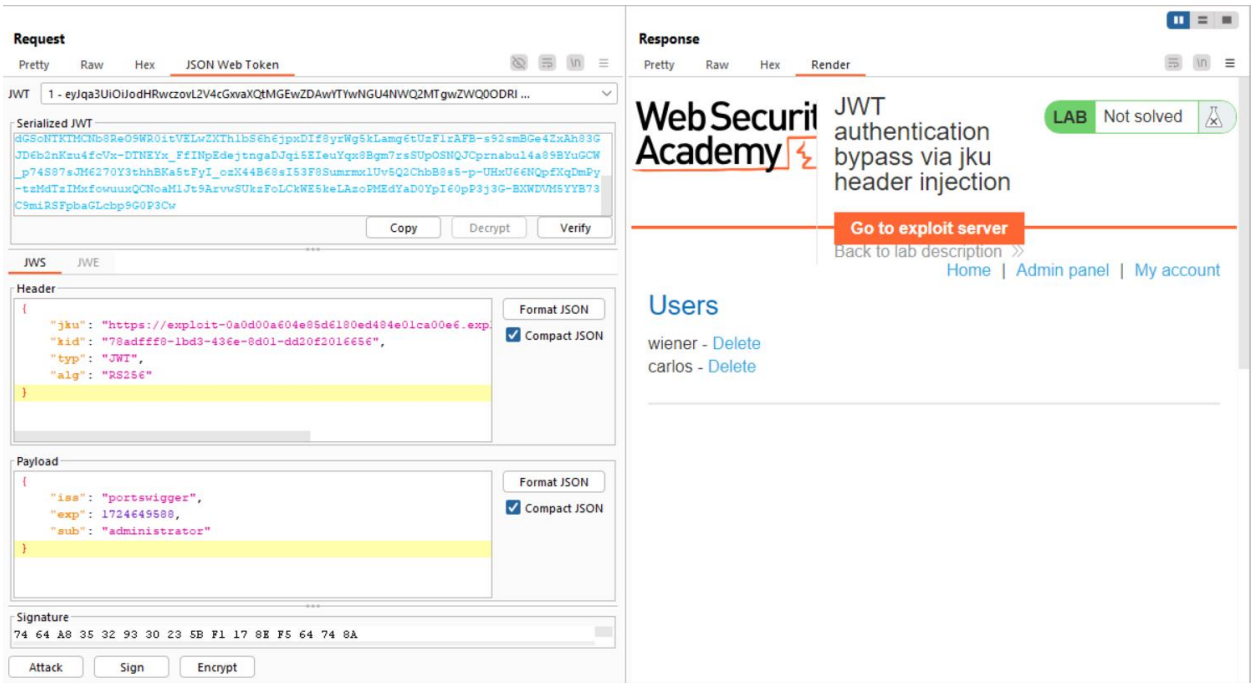
- Mở Exploit Server và viết code JSON chứa mã công khai RSA

Body:


```
{
   "keys": [
      {
   "kty": "RSA",
   "e": "AQAB",
   "kid": "39b82b0e-270e-472f-87d9-c660612ac116",
   "n": "rqhEbbMcx72LhU0gp5DDoJjFNw94QE8NEcV9jqwNuZF1h2ZzowlF9jS--Skn8zC61ix0DCeev1OsQtWwSMsbjNwYhuayuTiQcEsE_9EBYWP1J-TslU-PNscXrlmfTl3Ic-2nn13xFTkcfhSV-5YYhRk5Q-OSaL7Eq1ZVo0uiiuMwPpM2Roh3ShFG7iuPjzXBAXYpmJBVDoLA67PQF0S7YHqym_JpfXerrbXSuaYrw5Y0ci-vUya4dj9_LjXgxFW_6GerkeiTiAl5OZ8DNuyZF8IQjbM93cVOmpPhgVKEA4TW-9254e18rBGLxXZ45EuCA5Md3AsSLygDSuG_dqbb5Q"
}
   ]
}
```


- Chuyển gói tin GET đã bắt được vào Repeater
- Chuyển sang tab JSON Web Token => Sửa “wiener” thành “administrator” => Thêm trường “jku” với URL là web exploit => Sign

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



- Xóa tài khoản “carlos”