poker

发表于 2021-01-21 分类于 Challenge， 2017， HCTF， Web
Challenge | 2017 | HCTF | Web | poker

点击此处获得更好的阅读体验

WriteUp 来源

https://xz.aliyun.com/t/1589

题目考点

解题思路

这次想以游戏安全出一些题目，但是又担心出的太难，大家没做过类似的游戏漏洞挖掘(其实是为了偷懒)，就出了一道战斗频率没有限制的刷级漏洞。这是一个去掉充值功能以外完整的游戏，我去掉了后台对于加速器的检测机制。 提示给的很明显，在flag.php里提示了

```
getFlag when you are at level 100!!!
```

升到一百级就可以拿到flag，但是比赛时间的48个小时正常情况下不吃不喝也是升不到100级的，ctf本来就是一个hack game，所以需要分析他的游戏机制。这个版本的poker2没有战斗频率限制，可以高速无限战斗，脚本很简单，但是还需要分析游戏的细节。众多野怪地图里有一个叫圣诞小屋的挂机地图，伤害低经验高，写好挂机脚本还是很简单的。

```
import requests
import re
from time import sleep
host = "petgame.2017.hctf.io"

headers = {
    "Cookie":"PHPSESSID=c4gn8hav06nsv43bo65tlfkto3"
}
def getFight(host, headers):
    url = "http://"+host+"/function/Fight_Mod.php?p=37&bid=5226&rd=0.5365947475076844"
    req = requests.get(url = url, headers = headers)
    html = req.content
    gid = re.findall("gg=[.*,(.*)]",html)
    if len(gid)>0:
        gid = gid[0]
        attack(gid, 4, host, headers)
    else:
        return False

def attack(gid, times, host, headers):
    url = "http://"+host+"/function/FightGate.php?id=1&g="+str(gid)+"&checkwg=checked&rd=0.34966725314993186"
    for i in xrange(0,times-1):
        req = requests.get(url = url, headers = headers)
        html = req.content
        print html

while True:
    getFight(host,headers)
#    sleep(0.1)

#attack(86,url,headers)
```

其实还有其他解法，就是在poker-poker一题中找到注入点，如果有一百级的玩家的密码是弱口令(md5可查)则可以进入其他人账号获得flag。我特意把poker2一题放在第二层，poker-poker在第三层，但是还是有人找到了非预期的注入点(注册处)，提前获取了别人的session，在我删除一百级账号前获得flag。

Flag

```
无
```

- *本文作者： CTFHub*
- *本文链接： https://writeup.ctfhub.com/Challenge/2017/HCTF/Web/4gutq9F276kVGCoxXTK2YY.html*

 # Challenge # Web # 2017 # HCTF
babycrack
poker-poker