HGAME2019 Week1 题解

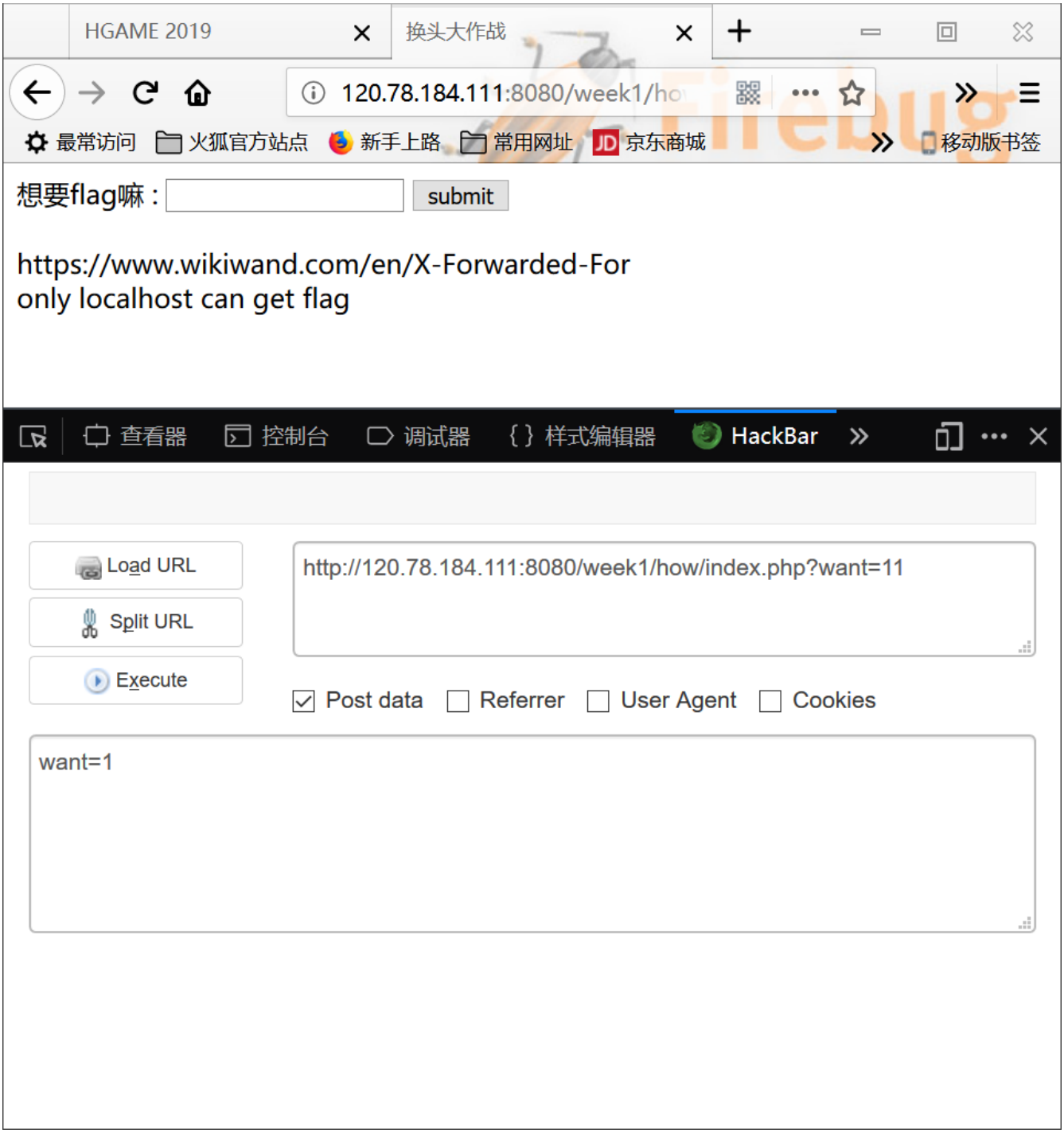
WEB

1.谁吃了我的flag

进去之后一阵分析结果啥也没找到(其实是有提示的seek_disclosure,只是当时脑回路没跟上orz)，最后根据提示'使用Vim编辑器'这一点才想起备份，所以访问'.index.html.bak'即可得到flag。

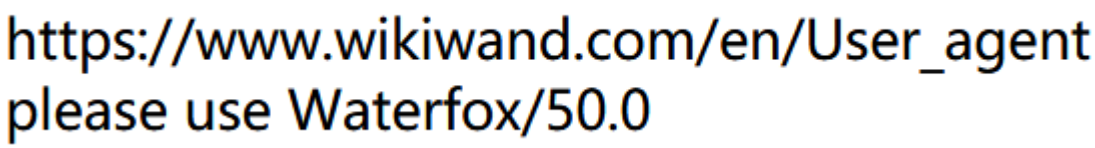
2.换头大作战

一开始submit后会要求使用POST提交，这里直接切出hackbar提交即可,得到如下信息：

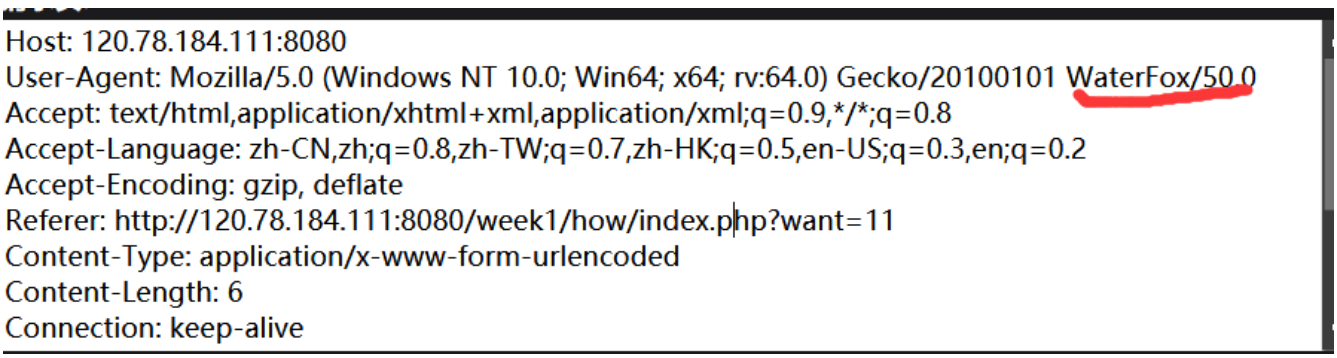


从提示中得知需要本地主机访问，直白点说就是要修改头部的X-Forwarded-For字段，修改如下：

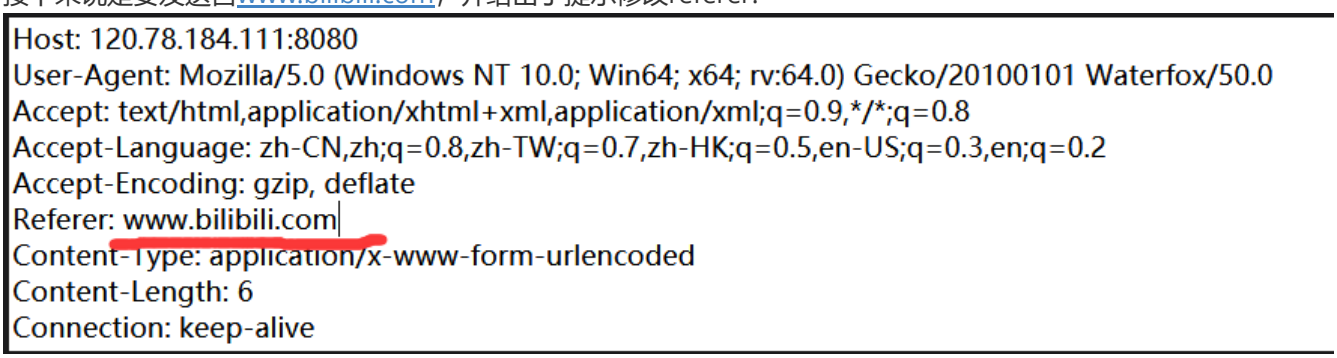
得到结果如下：



那么显然这里要修改的是User-Agent字段，修改如下：



接下来说是要发送自www.bilibili.com，并给出了提示修改referer:



得到相应说you are not admin:

观察可知修改Cookie中的admin选项为1，在此发送即可得到flag

3.Very easy web

上来是一段PHP代码审计。

```php
<?php
error_reporting(0);
include("flag.php");

if(strpos("vidar",$_GET['id'])!==FALSE)
    die("<p>干巴爹</p>");

$_GET['id']  =  urldecode($_GET['id']);
if($_GET['id']  ===  "vidar")
{
    echo  $flag;
}
highlight_file(__FILE__);
?>
```

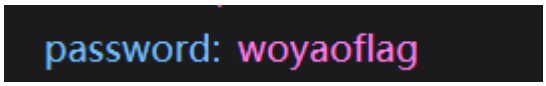
大致意思是提交的id字段经过urldecode之后是vidar,于是只要将'vidar'连续urlencode两次即可。

即最终提交?id=%2576%2569%2564%2561%2572可得到flag

4.can u find me?

首先通过f12看到了隐藏的入口链接'f12.php'

在头中发现了密码信息:



以POST形式提交后出现一个连接，直接点击会出现

aoh,your speed is sososo fast,the flag must have been left in somewhere

使用代理提交后即可得到flag

RE

Pro的Python教室(一)

首先看源代码(原生为Py2，这里改成了Py3):

```python
import base64
import hashlib

enc1 = 'hgame{'
enc2 = b'SGVyZV8xc18zYXN5Xw=='
enc3 = b'Pyth0n}'

print('Welcome to Processor\'s Python Classroom!\n')
print('Here is Problem One.')
print('There\'re three parts of the flag.')

print ('------------------------------------------------')

print ('Plz input the first part:')
first = 'hgame{'
if first == enc1:
    pass
else:
    print ('Sorry , You\'re so vegatable!')
    exit()

print ('Plz input the secend part:')
secend = 'Here_1s_3asy_'
secend = base64.b64encode(secend.encode())
if secend == enc2:
    pass
else:
    print('Sorry , You\'re so vegatable!')
    exit()

print ('Plz input the third part:')
third = input()
third = base64.b32decode(third)
if third == enc3:
    pass
else:
    print ('Sorry , You\'re so vegatable!')
    exit()
```

大致思路比较明显，（最后一段貌似没用，直接拿原始的就可以了）

只需要将中间一段base64解码，在和第一第三部分拼接在一起即可。

MISC

1.Hidden Image in LSB:

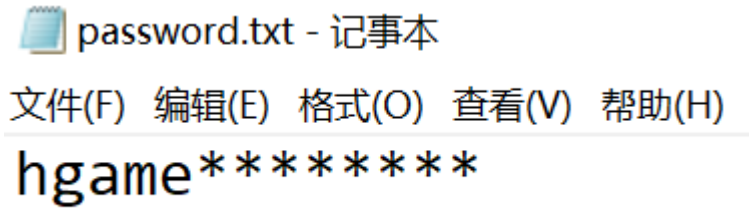
直接暴力上stegsolve，具体的LSB原理我在blog里大致整理了一下，这里就不提及了。

2.Try(~~出题人你过来一下~~):

下载下来是一个流量包，跟踪一下HTTP流可知主要传输了一个解压包

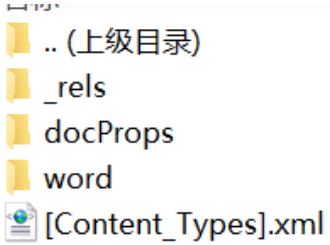
```
HTTP/1.1 200 OK
Date: Thu, 24 Jan 2019 04:35:16 GMT
Server: Apache/2.4.37 (Debian)
Last-Modified: Thu, 24 Jan 2019 04:32:28 GMT
ETag: "152e3-5802cb2b287eb"
Accept-Ranges: bytes
Content-Length: 86755
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/zip

PK.........d8N................dec/PK..
......c8N....*Q..*Q......dec/open-it.zipPK.........c8N.....P..V]......1.jpg...{..2..q.......
36.8.......2Oi`..rX=.f.H....H...?.ic."3....<6T..S.;..-
xf..;.........L{DQ`q.jq.A.j...u..."......*.......U.@.uH...)...9.....
```

下载下来得到一张图片(需要密码)以及一份txt(密码)，提示为：



来了，Week1最令我受苦的地方。显然到这里的意思就是去破解这个密码的后8位，然而我一下子有反应不过来去哪里照这个密码，花了将近一天时间分析原来的流量包以及附加的一些无关紧要的文件，各种研究zip格式，伪加密，明文攻击之类的花东西。最终竟然无意间发现只需要暴力破解数字即可orz(最开始排除的就是暴力破解，8位的排列数是在太多了，谁知道只由数字组成)。

解开后得到一张图片，binwalk后发现存在隐藏文件，提取出来后又是一份解压包，如下：



最终在word\document.xml中得到flag。

CRYPTO

Base全家

一打开是一个极其庞大的文本:

TXpNek5ETXpNemN6TXpNMU16TXpNak16TXpRek16TXhNek16T1RNek16UXpNek0wTXpRek1qTXpNe1V6TXpNeE16TXpOR
E0wTXpFek16TTFNek16T1RNek16UXpNek0zTXpNek5ETTBNe1F6TXpNek16TXpNak16TXpVek16TTBNek16TkRNME16UX
pNek0wTXpRek5UTXpNe1F6TXpNeU16TXpOVE16TXpRek16TTBNek16TnpNek16VXpNek15TXpNek5ETXpNek16TXpNME1
6TXpORE16TXpRek16TTNNek16TkRNME16UXpNek0xTXpNek1qTXpNe1V6TXpNMk16TXpORE16TXpjek16TTBNek16T1RN
ek16TXpNek15TXpNek5ETXpNe1V6TXpNME16TXpOVE16TXpRek5ETTFNek16TkRNME16RXpNek0xTXpNek16TXpNe1F6T
XpNM016TXpOVE16TXpJek16TTBNek16TVRNek16VXpNek0wTXpNek5ETXpNemt6TXpNME16UXpOVE16TXpRek5ETXhNek
16T1RNek16VXpNek0wTXpNek9UTXpNe1F6TXpNNU16TXpNek16TXpJek16TTFNek16TkRNek16UXpNek01TXpNek5ETTB
Ne1V6TXpNME16UXpNVE16TXpVek16TXpNek16TkRNek16Y3pNek0xTXpNek5UTXpNe1V6TXpNNU16TXpOVE16TXpRek16
TTBNek16T1RNek16UXpORE0yTXpNek5ETTBNekV6TXpNMU16TXp0ak16TXpRek16TTNNek16T1RNek16VXpNek16TXpNe
k1qTXpNe1V6TXpNME16TXpOVE16TXpNek16TTBNe1F6T1RNek16UXpNek15TXpNek5UTXpNemN6TXpNME16TXp0ek16TX
pVek16TXhNek16TXpNek16SXpNek0xTXpNek5ETXpNe1F6TkRNeU16TXpORE0wTXpRek16TTFNek16TWpNek16VXpNek0
xTXpNek5ETXpNemN6TXpNMU16TXpNVE16TXpNek16TXlNek16TkRNek16UXpNek0wTXpRek1qTXpNe1F6TkRNMU16TXp0
RE16TXpJek16TTFNe1F6TVRNek16UXpNek0zTXpNek5UTXpNek16TXpNME16TXpNVE16TXpVek16TTBNek16TkRNek16a
3pNek0wTXpRek5qTXpNe1F6TXpNeU16TXpOVE16TXpVek16TTBNek16TnpNek16VXpNek0xTXpNek16TXpNek16TXpNME
16TXpOVE16TXpRek16TTFNek16TkRNME16VXpNek0wTXpRek1UTXpNe1V6TXpNMk16TXpORE16TXpjek16TTFNek16TWp
Nek16UXpNek14TXpNek5UTXpNe1F6TXpNME16UXpNak16TXpRek5ETTFNek16TkRNek16SXpNek0xTXpNek5UTXpNe1F6
TXpNNU16TXpORE16TXprek16TXpNek16TWpNek16UXpNek0wTXpNek5ETTBNe1F6TXpNME16UXpOVE16TXpRek16TXpNe
k16TkRNek16TXpNek0wTXpNek56TXpNe1V6TXpNeE16TXpNek16TXpNek16TTBNek16TkRNek16UXpNek01TXpNek5ETT
BNe1V6TXpNME16UXpNVE16TXpVek16TTJNek16TkRNek16Y3pNek0wTXpNek9UTXpNek16TXpNeU16TXpORE16TXpVek1
6TTBNek16T1RNek16UXpORE0xTXpNek5ETXpNek16TXpNME16TXp0ek16TXpRek16TTNNek16T1RNek16RXpNek16TXpN
ek16TXpNe1V6TXpNME16TXpORE16TXprek16TTBNe1F6TkRNek16VXpNek15TXpNek5UTXpNe1V6TXpNME16TXp0ek16T
XpRek5ETTBNek16TXpNek16SXpNek0xTXpNek5ETXpNe1F6TXpNNU16TXpORE0wTXpVek16TTBNek16TWpNek16VXpNek
0wTXpNek5ETXpNemN6TXpNMU16TXpOVE16TXpNek16TXlNek16TkRNek16UXpNek0wTXpNek9UTXpNe1V6TXpNeE16TXp
OVE16TXpJek16TTFNek16TmpNek16UXpNek0zTXpNek5UTXpNe1V6TXpNek16TXpNak16TXpRek16TTFNek16TkRNek16
a3pNek0wTXpRek5UTXpNe1F6TkRNeE16TXpOVE16TXpNek16TTBNek16TnpNek16VXpNek14TXpNek5UTTBNekV6TXpNM
E16TXpORE16TXpRek16TTVNek16TkRNME16VXpNek0wTXpRek1UTXpNe1V6TXpNME16TXpORE16TXpjek16TTFNek16TV
RNek16TXpNek15TXpNek5UTXpNe1F6TXpNME16TXpOVE16TXpRek5ETTFNek16TkRNek16TXpNek0wTXpNek16TXpNe1F
6TXpNM016TXpOVE16TXpVek16TTFNe1F6TVRNek16UXpNek0wTXpNek5ETXpNemt6TXpNME16UXpOVE16TXpVek5ETXhN
ek16T1RNek16VXpNek0wTXpNek9UTXpNe1V6TXpNMU16TXpNek16TXpJek16TTBNek16TkRNek16VXpNek16TXpNek5ET
TBNe1V6TXpNME16UXpNVE16TXpVek16TTNNek16TkRNek16Y3pNek0xTXpNek1UTXpNek16TXpNME16TXpOVE16TXpRek
16TTBNe1F6TWpNek16UXpORE0xTXpNek5ETTBNekV6TXpNMU16TXp0ak16TXpRek16TTNNek16TkRNME16UXpNek16TXp
Nek1qTXpNe1F6TXpNME16TXpORE0wTXpRek16TTBNe1F6T1RNek16UXpNek16TXpNek5ETXpNek16TXpNME16TXp0ek16
TXpVek16TTFNek16TXpNek16TXpNek0wTXpNek5ETXpNe1F6TXpNM016TXpORE0wTXpVek16TTBNe1F6TVRNek16VXpNe
k0xTXpNek5ETXpNemN6TXpNMU16TXpOVE16TXpNek16TXlNek16TkRNek16UXpNek0wTXpNek56TXpNe1F6TkRNMU16TX
pORE16TXpNek16TTBNek16T1RNek16UXpNek0zTXpNek5UTXpNekV6TXpNMU16UXpNVE16TXpVek16TTBNek16TkRNME1
6SXpNek0wTXpRek5ETXpNe1V6TkRNeE16TXpOVE16TXpVek16TTBNek16T0RNek16UXpNek0xTXpNek16TXpNek16TXpN
MU16TXpORE16TXpRek16TTFNek16TkRNME16VXpNek0wTXpRek1UTXpNe1V6TXpNME16TXpORE16TXpjek16TTFNek16T
VRNek16TXpNek15TXpNek5UTXpNe1F6TXpNME16TXpPVE16TXpRek5ETTFNek16TkRNME16RXpNek0xTXpNek5qTXpNe1

原本以为超频满负荷可以直接复制粘贴进去，最后经历了10多分钟风扇的咆哮后放弃了这个想法，改用文件读取。

大致思路比较简单，无非对整个文件疯狂进行base解码即可，最终迭代10次后得到最终文本为：

```
base58 : 2BAja2VqXoHi9Lo5kfQZBPjq1EmZHGEudM5JyDPREPmS3CxrpB8BnC
```

在线找一个base58解码网站即可得到flag。

2.Mix(智商上线系列)

首先明显解码摩斯电码得到

744B735F6D6F7944716B7B6251663430657D

猜测是base系列编码，最终经过base16解码可得到**tKs_moyDqk{bQf40e}**

大致flag的形状已经出来了，猜测可能是凯撒，进一步猜测必定是以h开头，得到凯撒移位后的密码形式：
hYg_acmRey{pEt40s}

发现已经有**hgame**字样，但是中间惨杂着Y_cRy，猜测可能是组合，即**Y_cRypEt40s**的组合，把40看成a和o，结合一下本题密码题的大环境，盲猜是**cRypt0_E4sY**，提交发现不对，改变位置得到E4sY_cRypt0，提交正确(这题应该是有什么套路解法的，反正我是通过逻辑推理~~(莽)~~出来的)。

后记

~~第(maybe最后)~~一次参加比较正式的CTF比赛，还是感受到了技术之路学无止境这个道理。由于对汇编，二进制以及相关方面一窍不通导致在此类题型中遭遇惨败。但通篇来讲Week1的难度还是处于可以接受的层面~~(try除外)~~，玩家体验也较为舒适~~(try除外)~~。虽已可见路的终点，仍将上下求索于此。

本人也会同时将HGAME2019的全解题过程及感想放于个人博客中：http://47.107.239.93/(虽然博客大部分东西都是毫无营养并且无聊透顶的orz).