HGAME 2020 Week-1 Writeup

{Web}

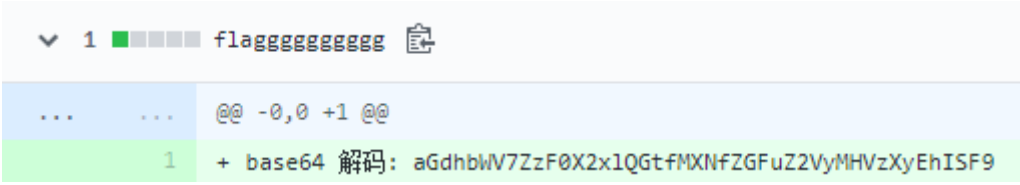
Cosmos 的博客

版本管理工具和**GitHub**多么醒目，那肯定是用git和GitHub了，看了去年的wp，了解了不合理使用git，会产生代码管理的遗留

在url后加/.git提示404

去查找了相关资料用/.git/HEAD发现确实有遗留，用/.git/config去仓库看了看没发现什么（QAQ），然后就开始用Githack，真找下来一个git仓库，但研究了好长时间没半点进度...

最后再看题目，50分签到题应该是想复杂了，重新去GitHub逛了逛...



好趴，被自己蠢哭>>>复制过来base64在线解码

```
hgame{g1t_le@k_1s_danger0us_!!!!}
```

接 头 霸 王

我不是一个好医生，这头我接不上去!

刚开始懵了好一会儿，点链接去vidar.team看了看，试着把协会的url和题目的url拼起来，没啥用处，接着意识到题目中的暗示>>>头不就是请求头吗，用burpsuite抓包，照着lead一步一步下去

前四个头没什么问题

```
POST / HTTP/1.1
Referer:https://vidar.club
X-Forwarded-For:127.0.0.1
User-Agent: Cosmos Brower
```

最后一个卡了好久，最后看到响应头中的Last-Modified，那请求头肯定与之有关

```
If-Unmodified-Since:Fri, 01 Jan 2078 00:00:00 GMT
```

成功拿到flag

hgame{W0w!Your_heads_@re_s0_many!}

Code World!

点开页面发现403，直接F12，发现有提示

```
console.log("This new site is building....But our stupid developer Cosmos did 302 jump to this page..F**k!")
```

有跳转（链接和当前页面的url不一样可以发现），用burpsuite抓包

```
HTTP/1.1 302 Found
Server: nginx/1.14.0 (Ubuntu)
Date: Mon, 20 Jan 2020 03:03:25 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Location: new.php
Content-Length: 211

<html>
<head><title>405 Not Allowed</title></head>
<body bgcolor="white">
<center><h1>405 Not Allowed</h1></center>
<hr><center>nginx/1.14.0 (Ubuntu)</center>
</body>
</html>
```

status_code是302，但主体里是405，肯定是一个提示，405是请求方法不对，那把GET改成POST，Send

```
<center><h1>人鸡验证</h1><br><br>目前它只支持通过url提交参数来计算两个数的相加，参数为a<br><br>现在,需要让结果为10</center>
```

只通过url提交参数，那用？拼呗，拼了好久，唯一的进度是?a=开头时会有

```
<h2>再想想？ </h2>
```

哭了，因为看到要两个数的和想过用?a=b+c&b=5&c=5还有?a=(b=5)+(c=5)等等再通过url编码发送，也试了在主体里传...

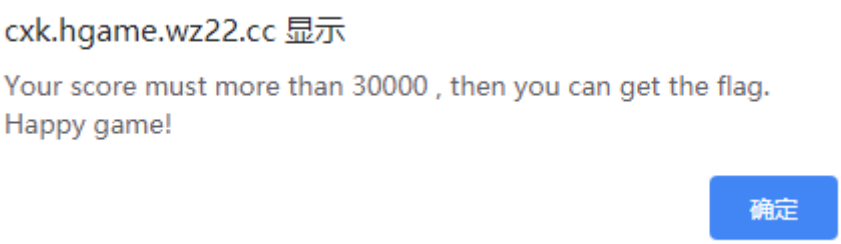
某次，拿了?a=5%2b5 send了一下，就...出了，是我理解错提示了（QAQ）

hgame{C0d3_1s_s0_S@_sO_C0ol!}

ji尼泰玫

刚开始没什么思路，F12也没发现什么，那咋办嘛，试着玩玩...

玩了好久，直到某次掉球



有个弹窗！提示要超过30000分，基本不可能手动玩到，考虑到要比较得分，所以可能会有提交数据，就用burpsuite直接抓包了

```
POST /submit HTTP/1.1
Host: cxk.hgame.wz22.cc
Content-Length: 42
Accept: */*
Origin: http://cxk.hgame.wz22.cc
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://cxk.hgame.wz22.cc/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: __cfduid=df0752c7fc625750ed081d7079d9621351579179952
Connection: close

score=200|9eed93ace91dc055654517b233ea7015
```

POST方法，主体里有东西，那就很明显了，直接改了分数

```
score=99999|9eed93ace91dc055654517b233ea7015
```

拿到flag

```
hgame{j4vASc1pt_w1ll_tel1_y0u_someth1n9_u5efu1?!}
```

{Misc}

欢迎参加HGame!

复制题目，粘贴到百度搜索，结果只有一个，要先base64解码再摩斯密码

base64解码

```
.-- ...-- .-.. -.-. ----- -- . ..--.- - --- ..--.- ..--- ----- ..--- ----- ..--.- .... --. .- -- ...--
```

然后摩斯用在线解密发现flag不对，这里真的自闭了好久，这个flag太顺眼了，没什么不对的，两天之后，老老实实拿着密码表自己手动解密，发现在线解码少了符号的转换（太坑了，符号的对应找了好几久）

按格式来hgame{.+}

hgame{W3LC0ME_TO_2020_HGAM3}

壁纸

下载下来发现一张好看的图片>>>啊，能天使，

图看不出所以然来所以拖进Winhex，发现秘密

```
      flag.txt
           E¨@=ÓÆ
Õ E¨@=ÓÆÕ ç¸œ ÓÆ
Õ PK          Z
  v     Password
 is picture ID.
```

密码是什么ID,会心一笑，就直接去找了

仔细看可以发现

```
50 4B 03 04
```

```
PK
```

这不是zip的文件头吗，看来是两个文件的拼接，那就改后缀名.zip

解压，有一个flag.txt文件，打开的时候果然要密码，输入ID，得到一串编码

```
\u68\u67\u61\u6d\u65\u7b\u44\u6f\u5f\u79\u30\u75\u5f
\u4b\u6e\u4f\u57\u5f\u75\u4e\u69\u43\u30\u64\u33\u3f\u7d
```

\u是Unicode编码呀，但每个\u后要4位，于是手动补0

```
\u0068\u0067\u0061\u006d\u0065\u007b\u0044\u006f\u005f\u0079\u0030\u0075\00u5f
\u004b\u006e\u004f\u0057\u005f\u0075\u004e\u0069\u0043\u0030\u0064\u0033\u003f\u007d
```

在线解码

```
hgame{Do_y0u%0u5fKnOW_uNiC0d3?}
```