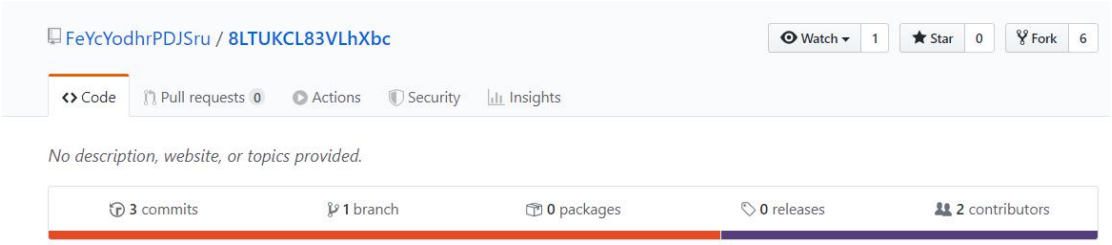
First week CTF_writeup

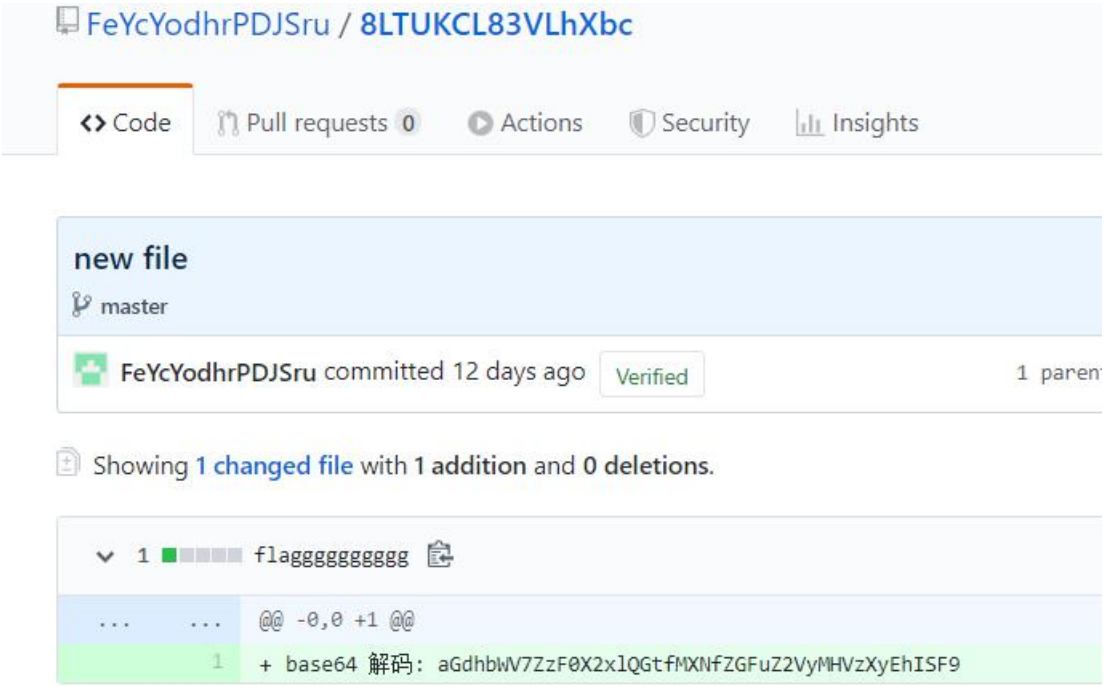
0x1 Web

0x1:Cosmos 的博客

百度了一下 这是个 Git 泄露的问题。 然后下载了 githack 工具，捣鼓了半天。。愣是没有收获，倒是学了一遍 git。。 再看看提示 去 github 找了找
直接搜索大茄子让我把 flag 藏在我的这个博客里，正好找到了唯一的一篇
进去然后看到有三次提交



进去查看



解码获得 flag！

0x2:接 头 霸 王

好名字！看来是跟头有关系了。

You need to come from https://vidar.club/.

划重点。不是 vidar 的咱们不让进

0x1:用 burp suite 抓包然后修改了 host 为 vidar.club 不行
百度查到了

3、网页源码注释变为了从百度跳转登陆

referer 字段用于向服务器发送请求时告诉服务器我是从哪个页面链接过来的
加入 referer:www.baidu.com

于是添加了这段 referer: vidar.club

You need to visit it locally.

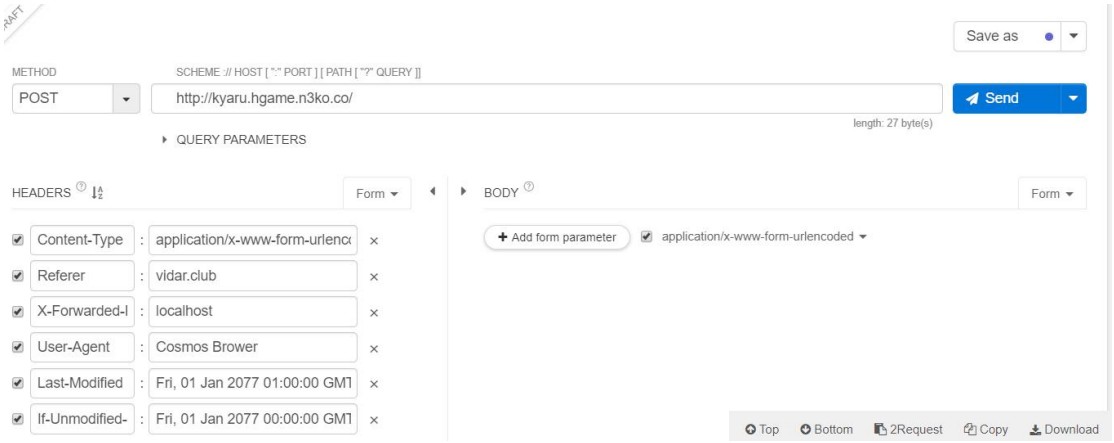
然后提示要本地访问添加 x-forwarded-for: localhost

You need to use Cosmos Brower to visit.

提示要换 Brower
在 user-Agent 加上User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Cosmos Brower
然后说

The flag will be updated after 2077, please wait for it patiently.

Emmm……
网上查了很多说要添加 If-Unmodified-Since 头来过滤信息
但可能我的 burpsuite 有 bug 一直返回不过来，然后饶了很多弯路
最后用 chrome 的一个插件 Talend API Tester 这玩意很好使 然后直接出来




```
<br>
<p class="lead">
                hgame{W0w!Your_heads_@re_s0_many!}
</p>
</div>
```

0x3:Code World

打开 url 403 Forbidden 按 F12

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

What a stupid guy!

用 burpsuite 抓下包

```
<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>
```

出现这个东西 emmm 百度一下 405，说是某个方法不对，更改 POST 试试

```
<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>
```

好的人鸡验证!

POST 和 GET 请求都可以通过 URL 来传递参数并且方法一样

用 postman 这个工具来操作

Emmm 大概是因为 url 编码的原因 用 burpsuite 对+进行 URL 编码是%2b

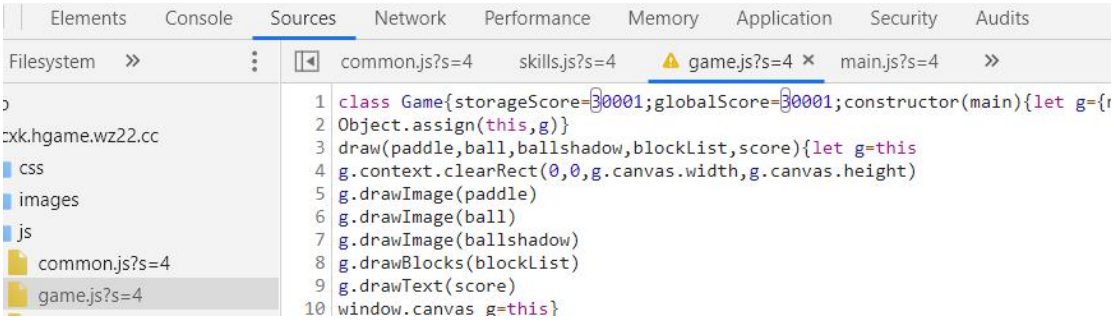
好 der

拿到 flag

0x4:基尼泰美

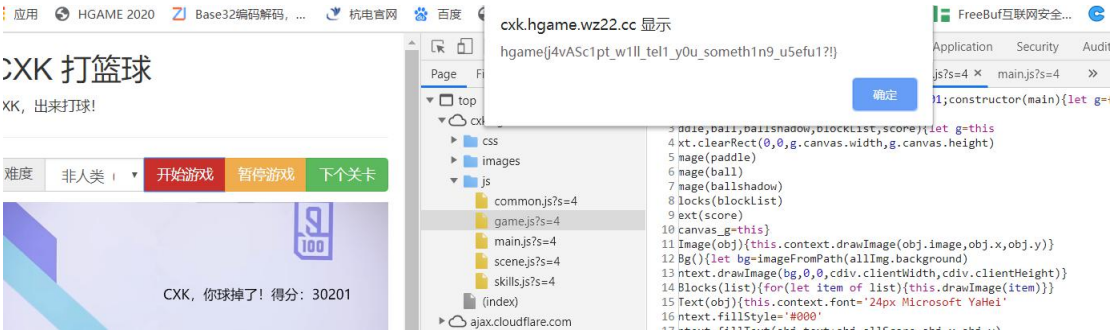
拿到 flag 先抓包了一下发现没什么反应，玩了会游戏 哦哟，cxk 球技不行呀 老掉球 hahahah

后来 alert 提示要大于 30000 分才有 判断可能是个前端审计




```
this.context.fillText('CXK，你球掉了！得分：'+this.globalScore,404,226)
$("#ballspeedset").removeAttr("disabled");let s=this.globalScore;(function(){l
goodGame(){this.globalScore=this.globalScore+this.storageScore;clearInterval(t
this.context.clearRect(0,0,this.canvas.width,this.canvas.height)
```

在这里判断 globalsocore 应该是那个分数判断， 所以修改全局变量 globalscore 大于 30000 分 然后随便抛两个球 拿到 flag！



0x2 Re

0x3 Pwn

第一次做 pwn 题 竟然真的 pwn 出来了 掌握了栈的基本原理

```
int v7; // [sp+A0h] [bp-Ch]@1
int *v8; // [sp+A8h] [bp-4h]@1

v8 = &argc;
v7 = *MK_FP(__GS__, 20);
alarm(8u);
setbuf(_bss_start, 0);
memset(&s, 0, 0xA0u);
puts("Let's 000o\\000!");
gets(&s);
if ( !memcmp("000o", &v6, 7u) )
  backdoor();
result = 0;
v4 = *MK_FP(__GS__, 20) ^ v7;
return result;
}
```

从伪 C 语言分析 需要从令 if 语句为真 会执行一个 backdoor()函数 应该是 pwn 的入口了 所以要令 memcmp()的返回值为 0

```
memcmp("000o", &v6, 7u)
```

memcmp语法

函数原型

int memcmp(const void *str1, const void *str2, size_t n));

参数

- **str1**-- 指向内存块的指针。
- **str2**-- 指向内存块的指针。
- **n**-- 要被比较的字节数。

功能

比较内存区域buf1和buf2的前count个字节。

```
.rodata:080486E0 a0o0o           db '0O0o',0          ; DATA XREF: main+85↑o
.rodata:080486E5 a00             db '00',0
```

“0O0o”字符串地址的 7 位是 “0O0o\0O0”
所以要令 v6==“0O0o\0O0”

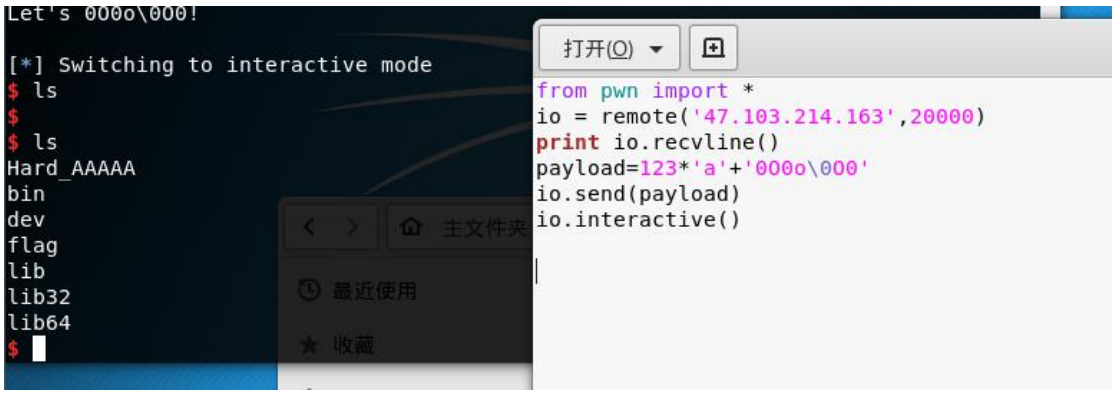
```
-000000AC s              db ?
```

s 的地址

```
-00000031                db ? ; undefined
```

v6 的地址

而 AC-31=7B=123
然而刚开始这里我也是第一次不知具体咋 pwn 出来的 一直在尝试 payload 后来给我试出来 Pwn 出来后了解了原理



0x4 Crypto

0x1:InfantRSA

签到题目 只要求一个 e 的逆元即可，通过 python 的 gmpy 库求解

贴上代码：

```
import gmpy2
import libnum
p = 681782737450022065655472455411;
q = 675274897132088253519831953441;
e = 13;
c = 27569846508236107014517368841149631154217290260855985901984l
n = p*q;
fai = (p-1)*(q-1);
d = gmpy2.invert(e,fai);
m = pow(c,d,n);
print libnum.n2s(m);
```

```
Python 2.7.16+ (default, Jul  8 2019, 09:45:29)
[GCC 8.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import libnum
>>> s=39062110472669388914389428064087335236334831991333245
>>> print(libnum.n2s(s))
hgame{t3Xt600k_R5A!!!}
>>>
```

0x2:Affine

从题目知道，flag 形式为 hgame{};

```
TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM'
MOD = len(TABLE)
cipher='A8I5z{xr1A_J7ha_vG_TpH410}';
flag='hgame{}';
i=TABLE.find('h')
I=TABLE.find('g')
for x in range(100):
    for y in range(100):
        ii = (x*i + y) % MOD
        II = (x*I + y) % MOD
        if(TABLE[ii]=='A' and TABLE[II]=='8'):
            print(x)
            print(y)
            print
```

```
PS G:\CTF> python -u "g:\CTF\S2_01.py"
13
14

13
76

75
14

75
76
```

通过暴力列举解出 A,B 的通解 A=13, B=14;
然后再解密
贴上代码：

```
# A = 13, B = 14;
TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM'
MOD = len(TABLE)
cipher='A8I5z{xr1A_J7ha_vG_TpH410}';
flag='';
for x in cipher:
    if(TABLE.find(x)==-1):
        flag += x;
    for i in range(len(TABLE)):
        if(TABLE[(i*13+14)%MOD]==x):
            flag += TABLE[i]
print(flag)
```

```
PS G:\CTF> python -u "g:\CTF\S2.py"
hgame{M4th_u5Ed_iN_cRYpt0}
```

0x4:Reorder

0x5 Misc

0x1 欢迎参加 HGame!

欢迎大家参加 HGAME 2020!
来来来，签个到吧~
Li0tIC4uLi0tIC4tLi4gLS4tLiAtLS0tLSAtLSAuIC4uLS0uLSAtIC0tLSAuLi0tLi0gLi4tLS0gLS0tLS0gLi4tLS0gLS0tLS0gLi4tLS4
tIC4uLi4gLS0uIC4tIC0tIC4uLi0t

长得都一个样子，百度了一下，哦原来是要 base64 解密
获得了摩斯密码
.-- ...-- .-.. -.-. ----- -- . ..--.- - --- ..--.- ..--- ----- ..--- ----- ..--.- .... --. .- -- ...--

解密

W3LC0ME_TO_2020_HGAM3

获得 flag

0x2 壁纸

下载得到一张图片壁纸 放到 binwalk 里发现有一个 zip 文件里面藏着 flag.txt

用 winhex 打开 zip 发现不是伪加密，文档注释说密码是照片的 ID？？？？

后来百度了一下 怎么查找图片的 ID？？？ 还真有。。。

https://saucenao.com/search.php //通过这个网址最后真的找到了图片 ID

解密成功。。。

\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

得到 ASCII 码 转换一下得到 flag

hgame{Do_y0u_KnOW_uNiC0d3?}

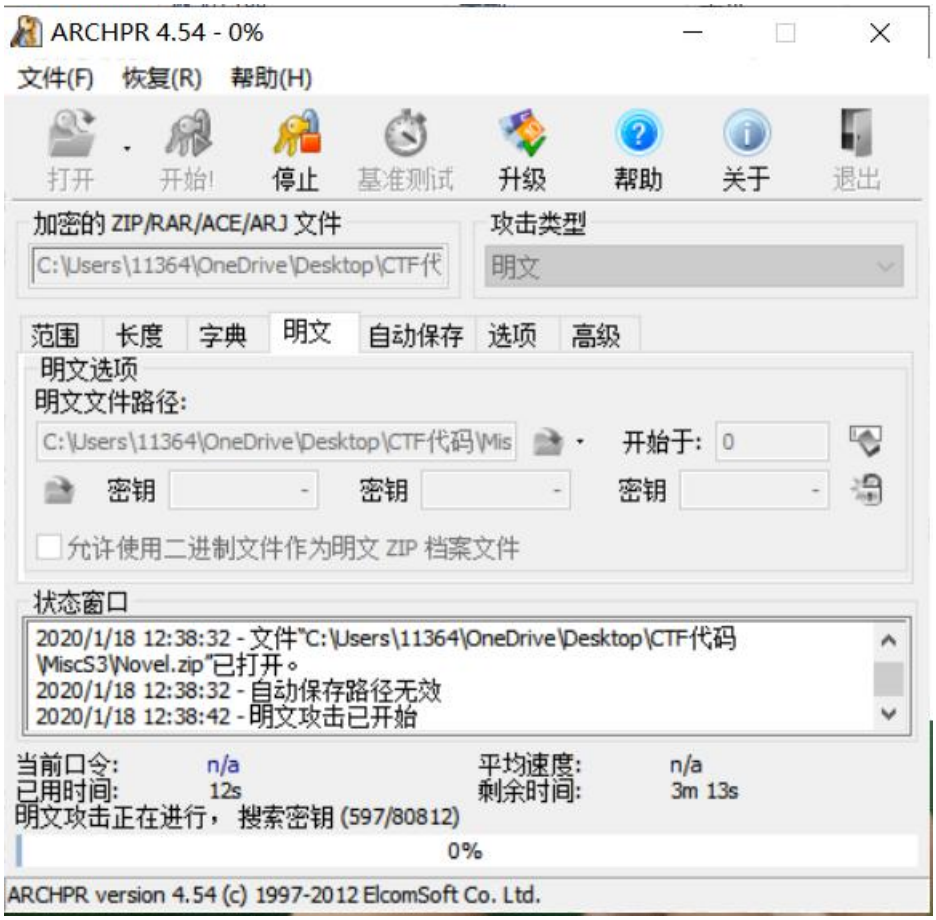
0x3 克苏鲁神话

下载得到 zip 包解压又得到一个 zip 包，

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
Novel.zip	25,825	25,778	WinRAR ZIP 压缩...	2020/1/11 0:37	C5BDF273
Bacon.txt	124	114	文本文档	2020/1/11 0:36	CF79DBAE

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
Bacon.txt *	124	126	文本文档	2020/1/11 0:36	CF79DBAE
The Call of Cth...	28,672	25,389	DOC 文档	2020/1/11 0:22	472043C8

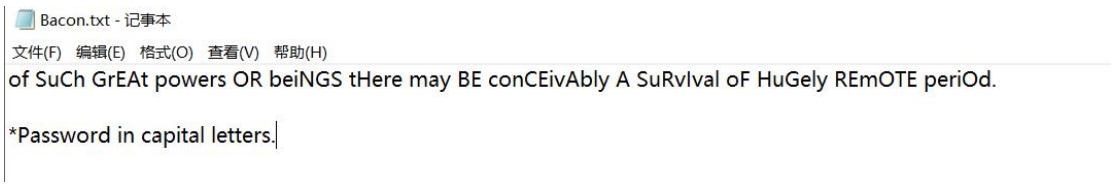
观察发现里面都有 Bacon.txt 文件并且冗余相同，使用明文攻击



破解成功，得到里面的 word 文档，tmd word 文档也是加了密的

提示 Bacon is tasty！

还是要看给的 bacon.txt

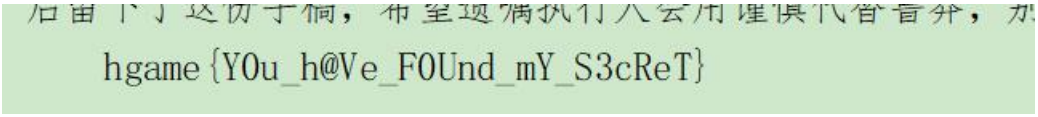


百度 Bacon. 是一种密码并且以 aaaaa aaaab 这种形式。 提示密码在大写字母里。。

捣鼓了很久 想到了 把大写字母和小写字母分别换成 a 和 b 然后成功了

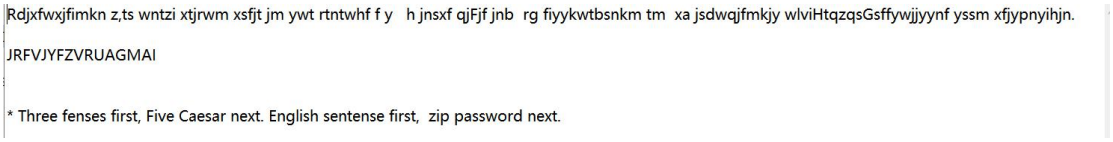
FLAGHIDDENINDOC 得到密码！

打开 word 文档 搜索 hgame 没有搜到 alt+A alt+D 果然隐藏了文字



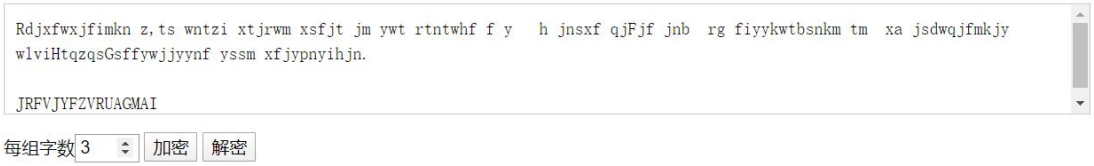
0x4 签到题 ProPlus

下载得到 zip 包解压得到 zip 包和 txt 文件



翻译下*句子，先 3 个栅栏密码再 5 个凯撒，前面是英文句子后面是 zip 密码

栅栏



每组字数 3 加密 解密

凯撒

位移 5 加密 解密

得到了 zip 密码 解密得到里面的 OK.txt 文件

????????????????

F**k 百度一下 原来有 brainf**k Ook！

解密获得了 base32 加密密文

Brainfuck/Ook!在线编码解码

解解密后，这里应该是 base64 加密的图片 去解密一下

*刚开始说格式错误，搞了一会发现原来要有个台头

获得二维码

扫一扫 得到 flag

0x5