week1 writeup

WEB

1.Cosmos 的博客

点进去就是

> # Cosmos 的博客
>
> 你好。欢迎你来到我的博客。
>
> 大茄子让我把 flag 藏在我的这个博客里。但我前前后后改了很多遍，还是觉得不满意。不过有大茄子告诉我的**版本管理工具**以及 GitHub，我改起来也挺方便的。

提示是git，那么猜想是否能访问.git文件夹，将网址后缀加上/.git/config，发现可以访问，使用GITHACK，将这个项目clone到本地，只有一个html和两个CSS，查看一番后无解，于是重点放在.git文件夹中，浪费了一堆时间在本地搜索后还是没什么发现，于是在config文件中发现了github上的网址，到远程仓库中查看，发现有3次提交记录，逐次查看，发现第一次提交记录是一个base64字符串，解码后得到flag

2.接 头 霸 王

看到臭鼬的那一刻就知道又要开始换头了，一进去需要从vidar.com过来，加个**referer: https://vidar.club/**

然后需要本地访问，加个**x-forwarded-for: 127.0.0.1**，然后需要用Cosmos浏览器（什么鬼），UA中加上Cosmos，然后就是最令人发狂的一步，~~赛博朋克又要延迟发售子~~资源要到2077年发布，一开始直接想到添加data，但是尝试好几次都不成功，鸽了一天再回来看服务器的response：

> HTTP/1.1 200 OK Content-Length: 1245 Content-Type: text/html; charset=UTF-8 Date: Fri, 17 Jan 2020 17:21:45 GMT Last-Modified: Fri, 01 Jan 2077 00:00:00 GMT Server: HGAME 2020 Server: Apache/2.4.29 (Ubuntu) Vary: Accept-Encoding Connection: close

发现了**Last-Modified: Fri, 01 Jan 2077 00:00:00 GMT**这个东西，于是尝试加上**If-Modified-Since**，找一个这个时刻之前的时间，发现flag出来了。

3.Code World

首先浏览器访问是一个403，用BS查看一下发现是个重定向，那估计没法用浏览器做了，换成curl，访问之后发现是个人鸡验证，但是之前一直不知道发送的格式是什么，后面才知道是A+B的形式，尝试a=10+0，发现不行，结果发现是+号的url处理问题，采用urlencode之后，+号变成%2B，拿到flag。

4.ji尼泰玫

这题nb。~~玩到30000分就好了~~

查看一下F12，发现是js逻辑的游戏，在最后球落地结束时，如果分数大于30000分，会向服务器发送一串字符串，由score和一堆七七八八的组成，原本想用python模拟发包，但想了想图省事，直接在最后一步球落地的时候的逻辑判断处打个断点，然后象征性的玩一下，200分，落地了，网页停住，修改score为30000，继续运行，flag出现。

MISC

1.欢迎参加HGame

一串很奇怪的字符串，不过又很有规律，百度一下发现是base64，转出来是一串摩斯码，翻译一下变成flag

2.壁纸

~~天天换老婆有点花心哈~~

拿到图片，扔进UE，Ctrl+F，找到了最后一串50 4b 03 04开头的字节码，初步判断是一个压缩包，可能是系统原因，用UE取出来会发生一些字节码乱序，后面后notepad++也是这样，后来用另一个工具才成功，取出后发现真的是个压缩包，里面有一个flag.txt，现在就是找密码了，备注说PW is ID，很快找到了PIXIV上的原图，ID是8位纯数字，之前由于奇奇怪怪的问题导致压缩包数据不对，密码一直试不开，头很大，过了1天再回来重新对比修复了压缩包的字节码后密码就对上了，成功取到flag。

4.签到题ProPlus

英文不太好，第一句长串用3位一组的栅栏密码然后位移5的凯撒变成一个英语句子，如法炮制用在第二个上，得到H开头的压缩包密码，解开后发现是Ook语言，上网随便找个网站解析后是base32的字符串，解码后得到一长串字符串，初步估计是base64，用base64解码后发现不能解，但是出现png这几个字，怀疑是base64转图片，于是用chrome转base64图片码后得到一个二维码，扫码得到flag。