HGAME 2020 Week1 wp

由sage填写。虽然只做出四题但还是写一下 wp，按参考价值排序。

Misc

Base全家福

Description
新年即将来临之际，Base家族也团聚了，他们用他们特有的打招呼方式向你问了个好，你知道他们在说什么吗？
R1k0RE1OWldHRTNFSU5SVkc1QkRLTlpXR1VaVENOUlRHTVlETVJCV0dVMlVNTlpVR01ZREtSUlVIQTJET01aVUdSQ0RHTVpWSVlaVEVNWlFHTVpER01KWElRPT09PT09
本次比赛为招新赛，请各位选手不要在当周比赛进行期间至结束后24小时内发布当周比赛题目的writeup
Challenge Address https://www.baidu.com
Base Score 50
Now Score 50
User solved 702

现在看人数，是 真·签到题 了

我没接触过，百度 Base 加密，打开篇描述各种 Base 加密字符的博客， 查到这些

> **Base16的编码表是由16个ASCII可打印字符（数字0-9和字母A-F）构成**
>
> **base32的编码表是由（A-Z、2-7）32个可见字符构成，“=”符号用作后缀填充。**
>
> **base64的编码表是由（A-Z、a-z、0-9、+、/）64个可见字符构成，“=”符号用作后缀填充。**
>
> **base58的编码表相比base64少了数字0，大写字母I，O，小写字母 l (这个是L），以及符号‘+’和‘/’**

或者可以参考

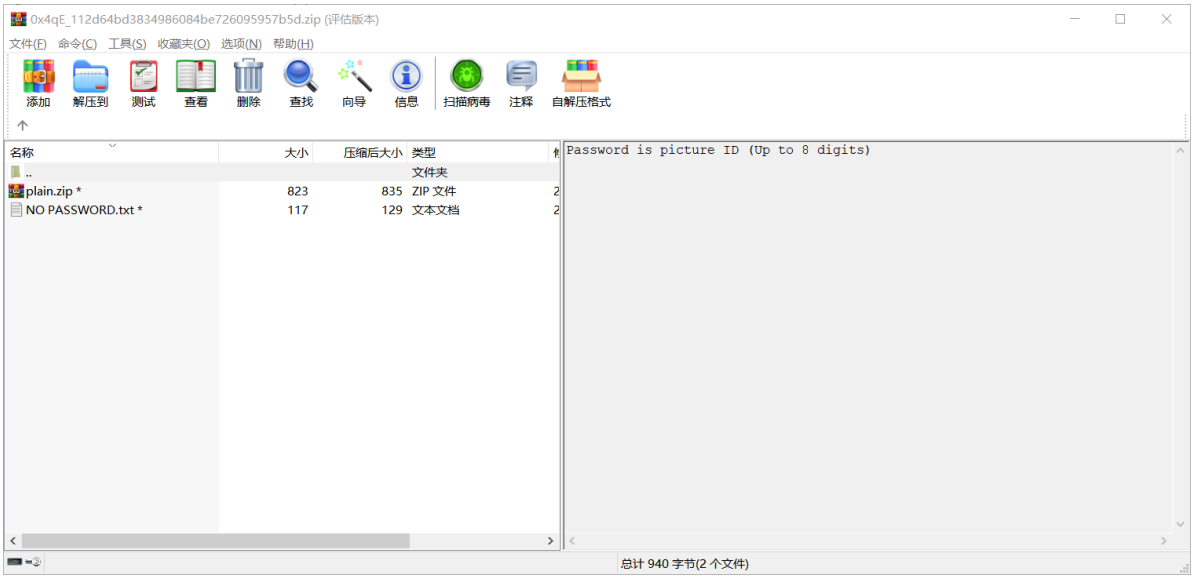
30余种加密编码类型的密文特征分析 https://cloud.tencent.com/developer/article/1748394

仔细比对可能的加密方式后依次用 64 32 16 就解出 flag 了

不起眼压缩包的养成的方法

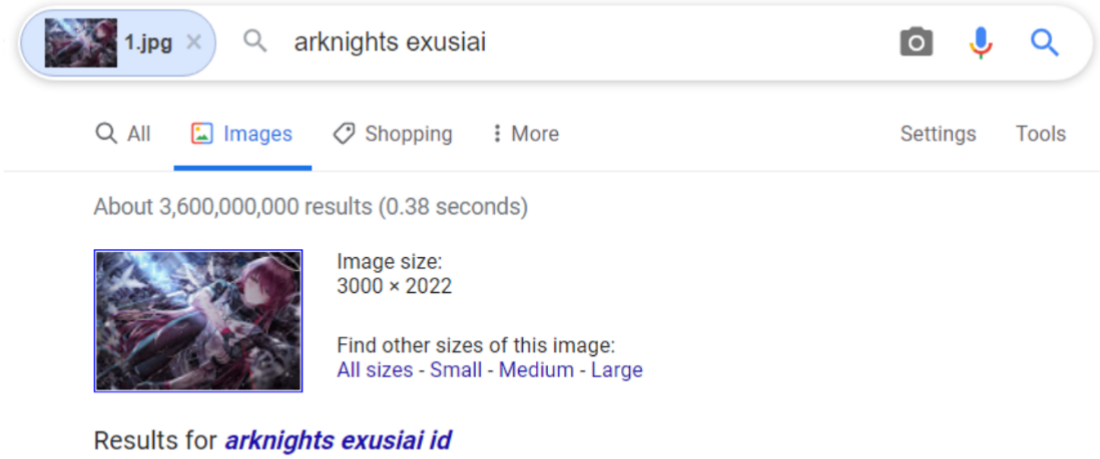
Description
0x4qE给了张图给我，说这图暗藏玄机，你能帮我找出来吗？
Challenge Address https://1.oss.hgame2021.vidar.club/0x4qE_112d64bd3834986084be726095957b5d.jpg
Base Score 100
Now Score 100
User solved 265

右键查看详细信息，`Secret hidden IN picture`. 听说图片可能是压缩包，改一下后缀改成 zip，可不过我也不知道 ID 是什么卡住（后来才知道这里其实可以爆破了！）



绕了一大圈子，装上 `foremost` 分开图片和 zip，还是最后翻看去年 0x4qE week1 的 `wp` 才发现竟是 `pivix ID`（后来才发觉这道题出题人不是 0x4qE）。是我知识盲区了 pixiv 都想不到。

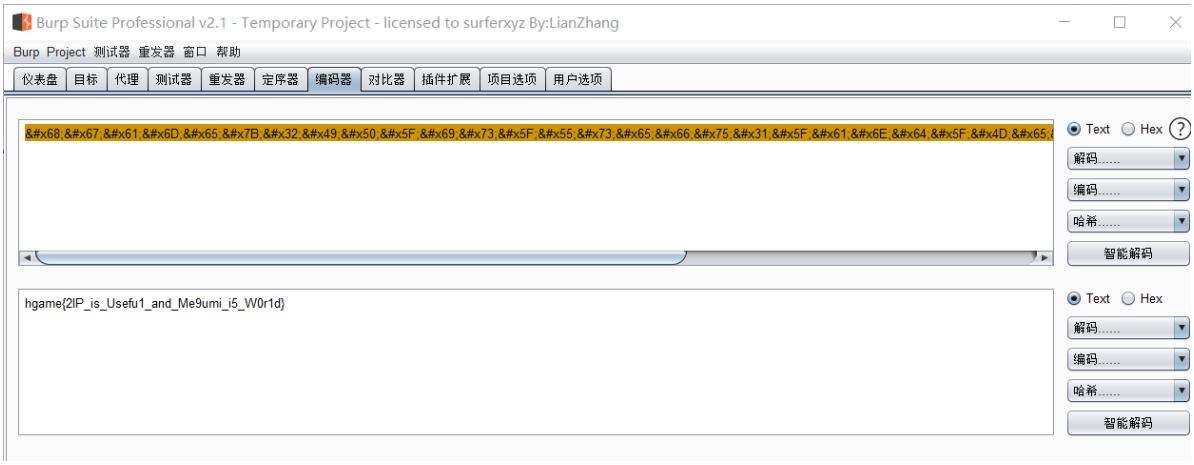
> 压缩包被加密了，密码就是图片的`ID`，，合理猜想应该是`Pixiv ID`，于是把这张图放进`Google`识图里，搜到图片之后找到`ID`，然后把`ID`作为密码解压压缩包。



> 到`pixiv`上去搜这张图片，搜到`ID`为`76953815`，`Google`真好用呀！
>
> 解压后拿到一个`flag.txt`，打开后是一串`Unicode`编码，

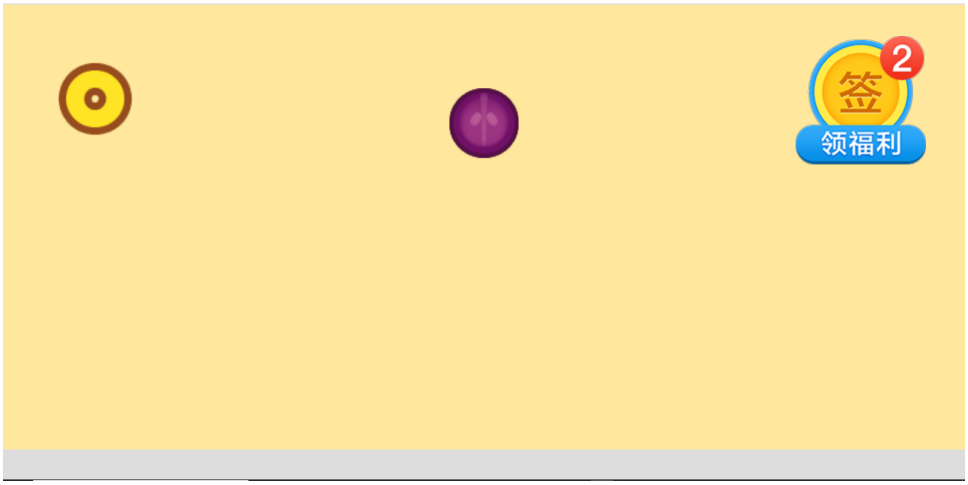
我搜不到 `pivix` 的图哈哈哈哈绝了，换了 `TinEye` 才找到。解压了还有！打开文本，其中有一句 `Because it's too strong or null.` 还以为是说密码跟没似的，用 `AAPR` 爆破了半天，不成，才知道是 `too strong`。后来了解到是**明文攻击**，然而一直报错，以为是压缩软件不对，试了好几个都不行。最后看到文件头想辨别压缩软件的时候误打误撞发现**压缩方式**不是 0800 而是 0000 不对劲，百度了 0000 是按存储方式压缩，终于明白了提示文本文件里 `use storage` 的意思，好，结果又折腾半天甚至换了个 `passware kit` 解密还是报错，最后发现明文攻击过的加密压缩文件里的 txt 不加密了，重新解压了一个全新的，好了。

解压出一个 `flag.zip`，有密码但是没其他信息了，`winhex`，呀有东西，复制，不知道 `&#x` 是什么加密，百度，搜到的全是 &#x，索性放到 `Burpsuite` 解码器，拿到 flag。~~后来才知道好像是 Unicode转中文~~



Web

watermelon



打开就是熟悉的大西瓜界面，咦，页面怎么有点扭曲，F12调一下，调到长宽比最大，要打2000分，~~正好圆一下我一星期都没合出来两个大西瓜的梦，~~一发入魂五个大西瓜（图片自行脑补），竟然真给 flag

然后就跑路做 Misc 了

智商检测鸡

检测一下智商，做完这些简单的定积分题目然后获取Flag吧！(积分式全部为ax+b的形式)

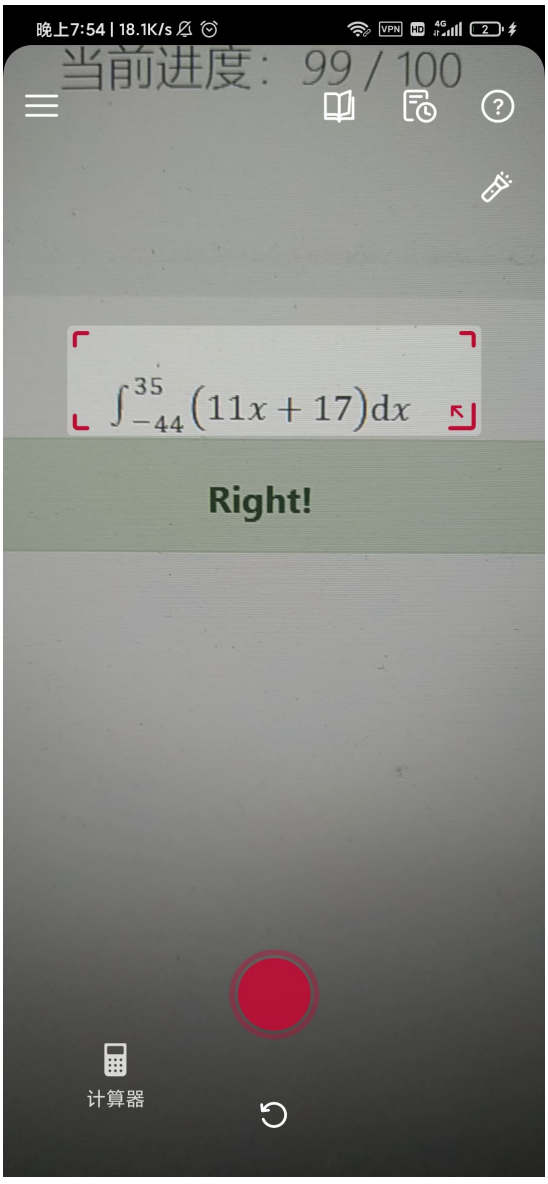
当前进度：0 / 100

$$\int_{-92}^{31}(12x+17)\mathrm{d}x$$

保留两位小数 检测智商

试了好多办法，没思路，数据在服务器我篡改不了，但问题就是要篡改，找了好些教程也没搞懂到底要在哪里注入，是在什么 Console 还是在哪里（或许是在这个输入框里？），又要写怎样的代码来注入？php 漏洞？js？sql注入？ 果然**不能浮沙筑高楼**啊。

这周快结束的时候，想想怎么还是再整一题吧，~~也沦落到手冲100题的地步~~。测试的时候也用过在线定积分计算网站，不过想想还是太慢，竟有人真能真那么做。python 似乎能算定积分，奈何我不知道怎么绑定参数的位置。最后还是想到**图像识别**，一查真有图像识别做定积分的工具，下载 `photomath`



若是开多端协同再加个复制粘贴自动提交的脚本应该就全自动了，奈何剩不到半个钟来不及折腾了，只能靠手不到20分钟搞定。

检测一下智商，做完这些简单的定积分题目然后获取Flag吧！(积分式全部为ax+b的形式)

当前进度：*100* / 100

all have done!
hgame{3very0ne_H4tes_Math}

Right!

-2567.5 检测智商