

# 签退

问卷

# Happy2023!

不做等白送，放第三提示直接进去，然后用curl发包，写个sh脚本批量发，好像100次就可以了。

# 签到

各自base一把梭

# 躺平问答

就是单纯答题，常识题都是直接搜就行了，第0题在注释里：

```
<div class= question-q >  
    " 0."  
    <!-- 114514*1919810 -->  
    <div style="color: #FAFAFA">其实，这题没出错</div> == $0
```

第三题在平台下面的运行状态里：

## [Scheduled] Platform System Upgrade

The scheduled maintenance has been completed.

Jan 3, 22:30 - 23:31 CST

第四题在 GEEKGAME 的 GitHub仓库里，另外几个用站长工具和类似的几个能查出来，第八题在物联网档案馆。最后一个指GitHub，不过时间要换成 GMT就行。

# 二维的码

反色汉信码，然后PDF417

# 神秘的.....文字?

base64先解，然后用 xxencode 解，但是奇怪的是，直接贴进去好像解不出来，于是我删了前面一部分就能解了。然后解出来下一个是morse电码，直接解就是了。

## HTTP百解

没存 payload.....抱着随便试试的心态做出来就没管了，现在又要再写又懒得弄了，主要是看群友说用curl能做，然后去查了参数，发现里面 -F 参数能传表单解决了最后那个500的问题。

## 躺平问答 · Beta版

答题之后 url 有点怪异，于是 base64 解了之后带上数量访问过去就行。

## 我抄，盒！

百度直接找照片信息解析，然后照着填就行了。

另外一个flag在详细信息里直接看程序名称就找到了。

## 口算大整数

☰ 目录收起

- (1)低加密指数分解攻击
  - 01. e=2把密文c开平方求解
  - 02. e=2 Rabin加密中的N可...
  - 03. e=3 小明文攻击
- (2)Roll按行加密
- (3)模不互素
- (4)共模攻击
- (5)低解密指数攻击
- (6)根据公钥计算得到私钥
- (7)分解n得到相同的几个p
- (8)已知n,e,d求p,q
- (9)私钥文件修复
- (10)低加密指数广播攻击
- (11)已知dp,dq求解m
- (12)CopperSmith定理攻击
  - 01. Stereotyped messages ...
  - 02. Partial Key Exposure Att...
  - 03. Factoring with high bits...

### 03. e=3 小明文攻击

适用情况：e较小，一般为3。

**公钥e很小**，明文m也不大的话，于是 $m^e = k*n + m$  中的k值很小甚至为0，爆破k或直接开三次方即可。

攻击原理：假设用户使用的密钥 e=3。考虑到加密关系满足：

$$C \equiv m^3 \pmod N$$

那么：

$$m^3 = C + k * N$$
$$m = \sqrt[3]{C + k * N}$$

攻击者可以从小到大枚举 k，依次开三次根，直到开出整数为止。

题目: 03-Jarvis OJ -Crypto-Extremely RSA

Extremely hard RSA196 SOLVERS

没想到RSA4096都被你给破了，一定是我的问题，给了你太多信息，这次我只给你一个flag的加密值和公钥，仍然是RSA4096，我就不信你还能解出来。

## V我≈50

不知道正确解法是怎么来的。

我试着先在本本地跑代码，然后远程过去，再跑一次，发现时间差不是很大，所以一个个试过去，因为能答三次，所以能试出来种子。

## 躺平flag提取器

IDA 打开一把梭，然后我是动调过去的，因为程序似乎是解密flag而不是加密flag

## 躺平flag提取器·极速版

IDA和GDA一把梭，GDA开 apk，然后解压apk后在lib里ida打开。两个都搜字符串就行了。