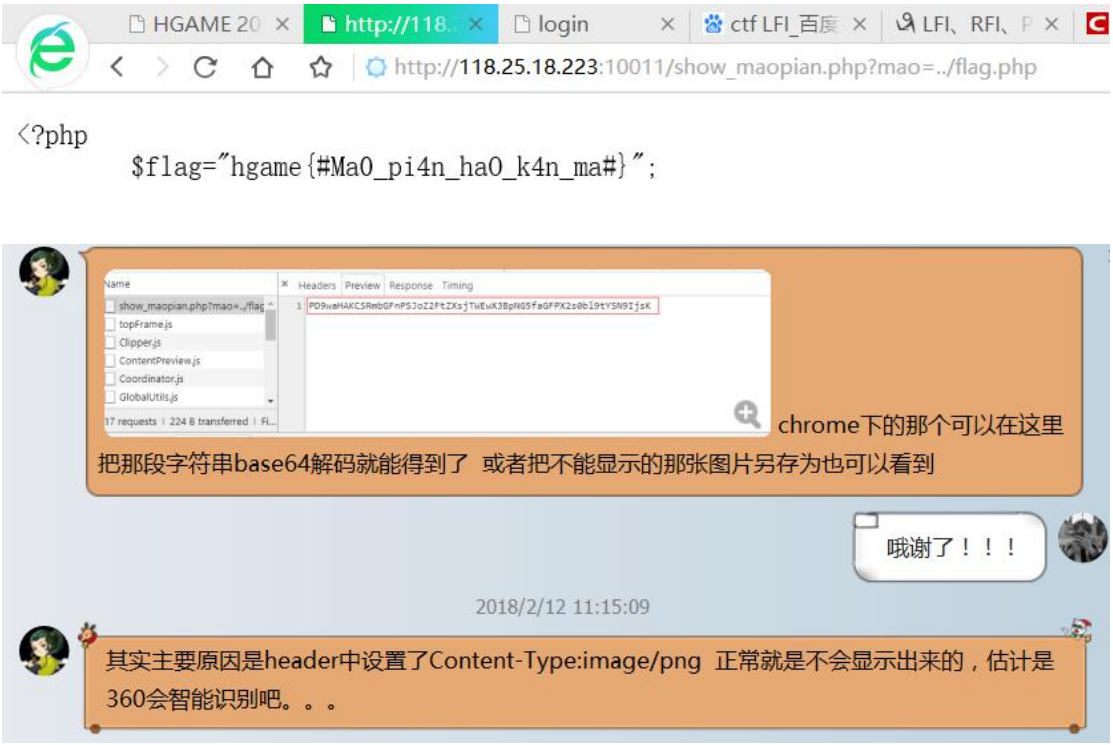
Web

草莓社区-1

hint 给的提示是 LFI 上网查了一下就是本地文件包含漏洞(Local File Include)，猜测一下他的代码应该是 include $_GET['mao'],这样就可以通过 get 请求来获得文件目录下的源代码来了，构造 payload mao=../flag.php，然后我在 Chrome 上一直显示不出来，第二天起床换了 360 直接就出来了感谢 web 客服大佬帮我解决了疑问



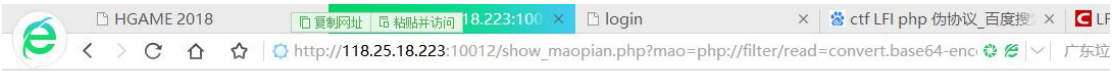
草莓社区-2

这道题 hint 给的也是 LFI 然后我一直按照之前的套路试结果发现不行，浏览器一直会报错告诉我错误这次我觉得可能代码是

require $_GET['mao'] 后来查一下决定用一下那个伪协议来试一试

Payload:

php://filter/read=convert.base64-encode/resource=../flag.php,要说为什么想到这个真的是死马当成活马医了吧=。=然后使用 360 浏览器打开获得 base64 加密



PD9waHAKCSRmbGFnPSJoZ2FtZXshbTRvX3BpNG5fQ2hhT19oYW9fa2FuIX0i0wo=

的一串字母解密后获得源代码，就有 flag 了，毛片超好看=。=

```
<?php
    $flag="hgame{!m4o_pi4n_ChaO_hao_kan!}";
```

Xss-1

首先看源代码 gi 表示全局匹配，大小写都会被替换掉，所以 image 和 script 都不能用，但还是可以用最普通的 img 标签，构造一个 payload <img src=""onerror="alert(1)"> ，发现 Alert(1)的括号被替换了，那么就发现那个只能替换一次所以在前面在加一个左括号就行所以 payload

<img src=""(onerror="alert(1)">就行

Xss-2

按照上题思路(>只能被替换一次就直接先输入了然后闭合这个 input 标签，然后就可以随便找个标签产生错误用 onerror 来 alert（1）就行，构造 payload：

(>"> <link rel="stylesheet" type="text/css" href="null" onerror="alert(1)" >

```
function charge(input) {
    input = input.replace(/script/gi, '_');
    input = input.replace(/img/gi, '_');
    input = input.replace(/image/gi, '_');
    input = input.replace(/\(/, '_');
    input = input.replace(/\>/,'_');
    return '<input value="' + input + '" type="text">';
    }
```

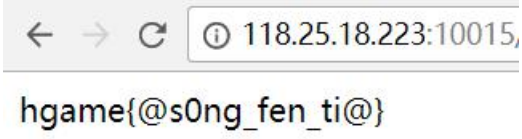
```
(>">
<link rel="stylesheet" type="text/css" href="null" onerror="alert(1)" >
```

请带着payload找fantasyqt(QQ 744399467)

最简单的 sql 题

我看了一下他最后和最前面会加上一个单引号那就使得 sql 语句为'suibian' or '1'='1' 就行所以构造 payload

Sadf' or 'a'='a 用户名随便就可以登录了得到 flag



Misc

Easypassword

题目给了 hint 说暴力破解，想了想觉得破解的时候还可以做题就暴力破解了，因为是 zip 压缩格式就用了 ziperello 软件大概跑了一小时吧跑出来了答案解压缩里面一个就是 txt 就是 flag

Crypto

Easy rsa

这道题是关于 Rsa 算法，然后我就上网学习了一下 rsa 算法我觉得最有用的网站是

http://blog.csdn.net/dbs1215/article/details/48953589

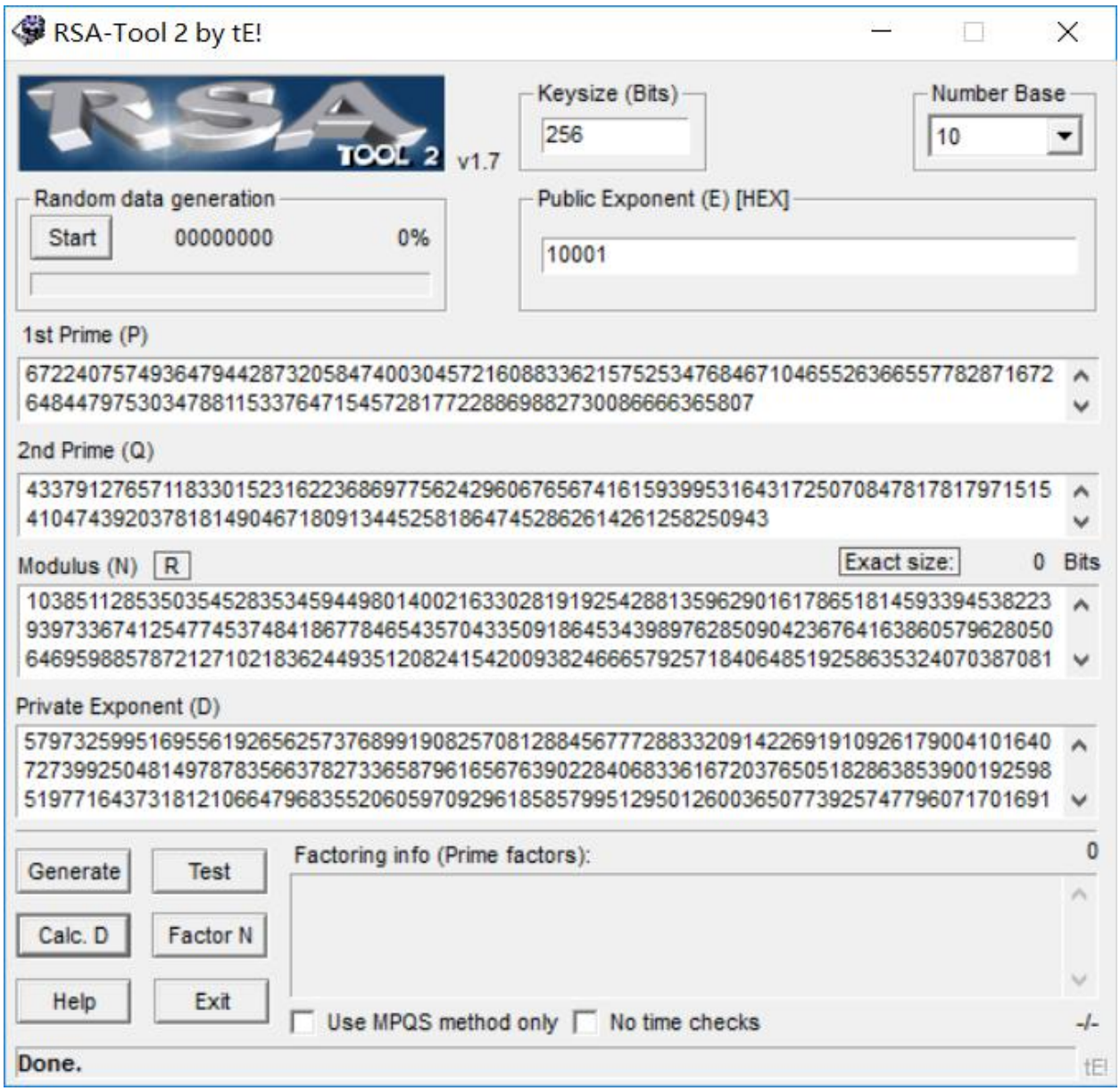
这个网址十分详细的介绍了 rsa 算法

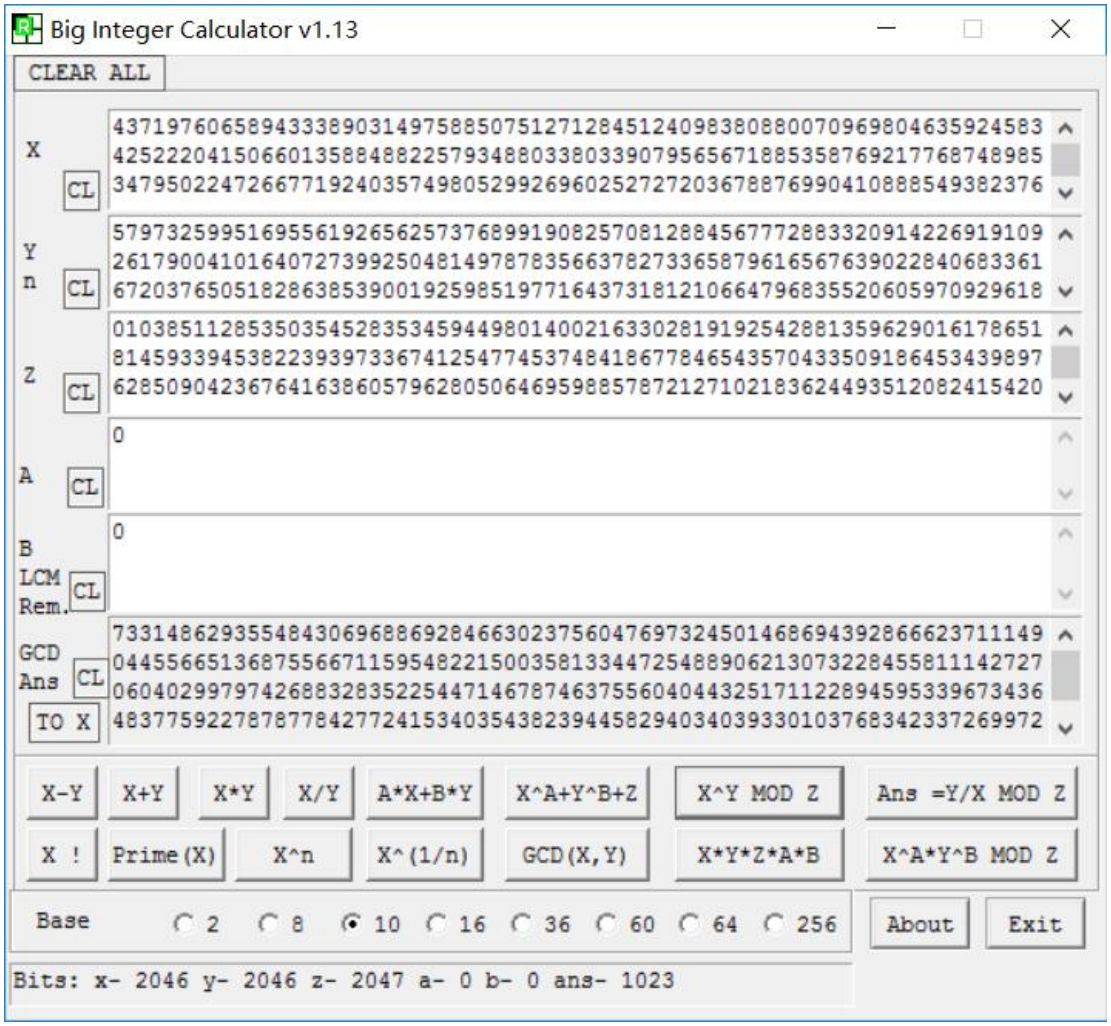
$$密文 = 明文^{E} \bmod N$$

$$明文 = 密文^{D} \bmod N$$

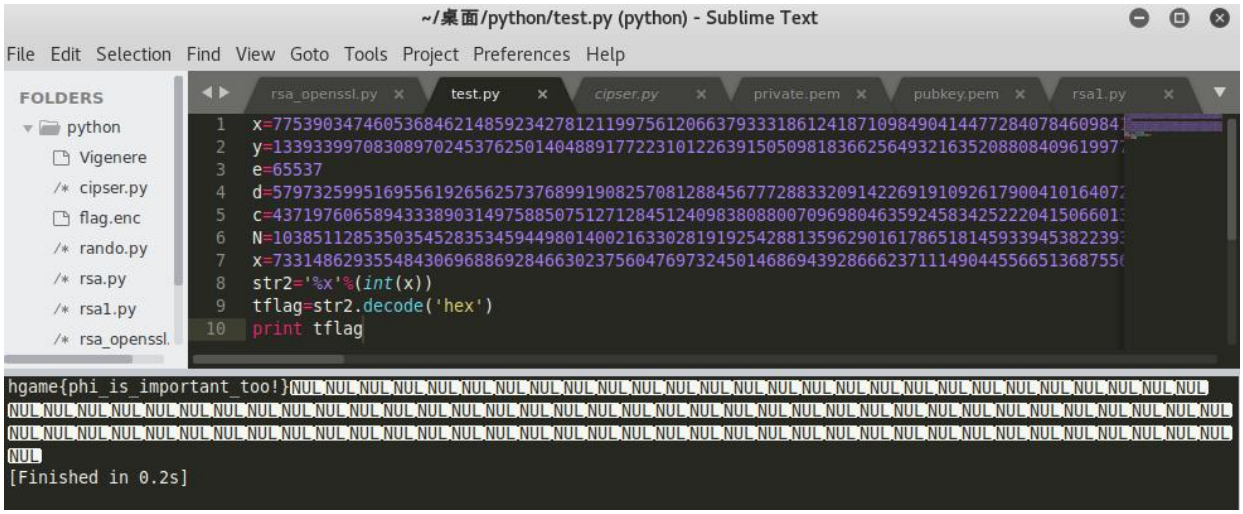
根据这两个和两个软件我觉得很好用

一个用来计算 D 一个用来计算明文的值，先使用 yafu 来分解 N 得到 p q，再把 p q 输入 rsatool 自动得到 D



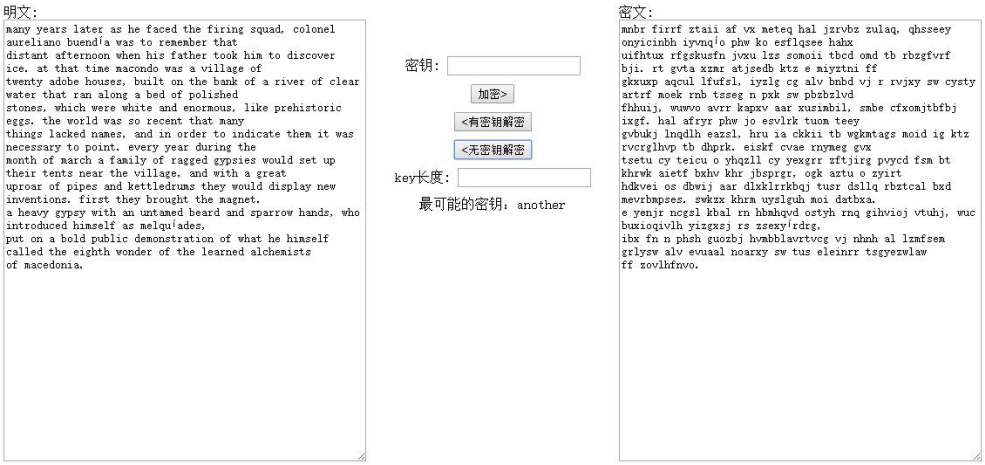


算出明文的十进制之后用 python 跑一下就得到 flag 了



Caesar&&Caesar

这道题是维吉尼亚加密，虽然说校内人员需要一定的解题思路，但是我用了网上的方法只能判断他的秘钥是 7 或者 14 的长度=。=然后就陷入僵局，Google 到一个神奇的网站



然后百度一下第一句话就知道是百年孤独了

One Hundred Years of Solitude 就是 flag

Violence

这道题的给的 hint 是暴力破解我看了一下源码，这个有点像仿射加密，但也有点不同，所以我就强行暴力破解

主要的也是将每种可能性都显示出来然后我那时候是用人眼看的一个一个找因为是有意义的字母，然后我发现有一个

是全英文的我就做 flag 输出成功了