

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



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 ``，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 `` 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

← → ↻ ⓘ 118.25.18.223:10015
hgame{@s0ng_fen_ti@}

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

$$\text{密文} = \text{明文}^E \bmod N$$

$$\text{明文} = \text{密文}^D \bmod N$$

根据这两个和两个软件我觉得很好用



BigInt.exe



RSATool2v17.exe

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

RSA-Tool 2 by tE!

Keysize (Bits): 256 **Number Base**: 10

Random data generation: Start 00000000 0%

Public Exponent (E) [HEX]: 10001

1st Prime (P):
67224075749364794428732058474003045721608833621575253476846710465526366557782871672
64844797530347881153376471545728177228869882730086666365807

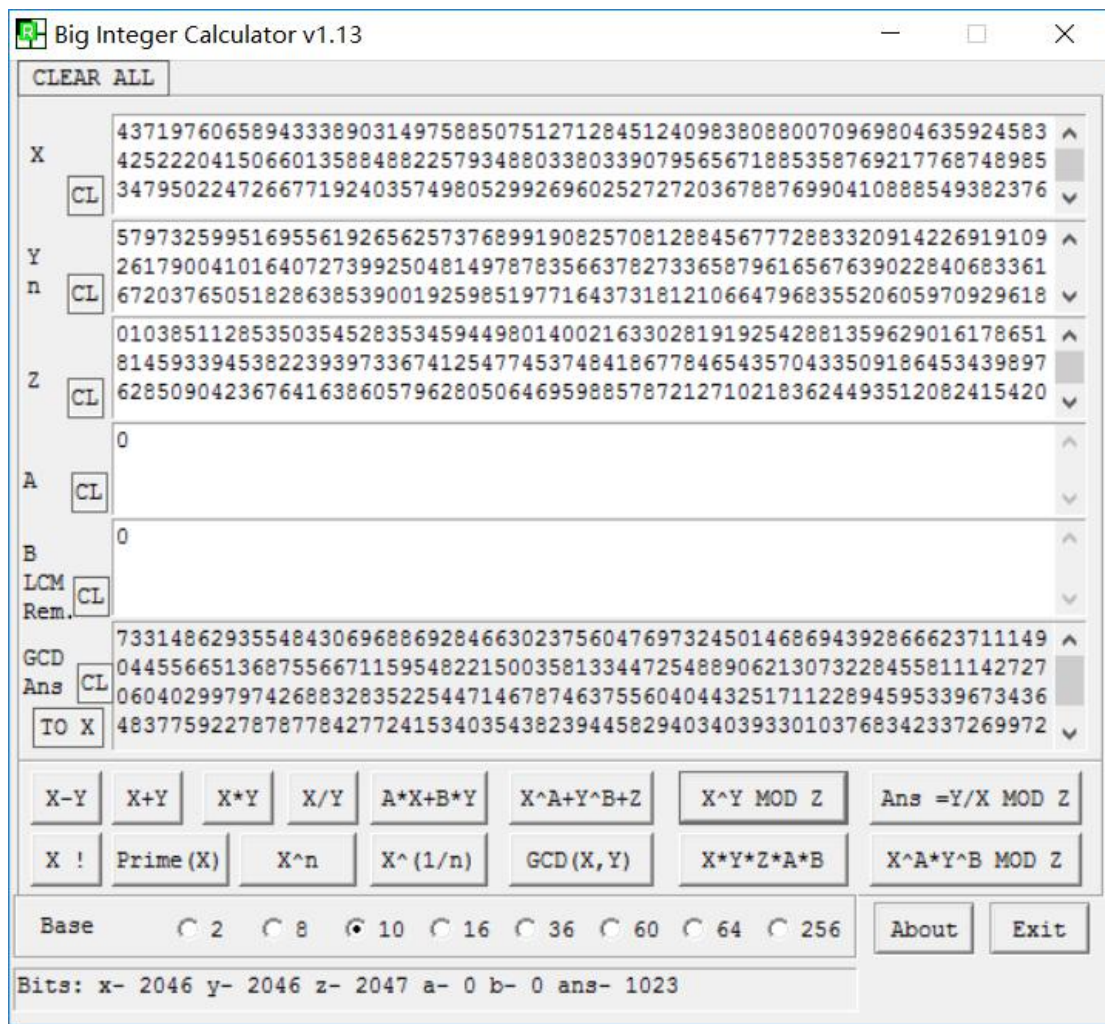
2nd Prime (Q):
43379127657118330152316223686977562429606765674161593995316431725070847817817971515
410474392037818149046718091344525818647452862614261258250943

Modulus (N) ☒ R **Exact size:** 0 Bits
10385112853503545283534594498014002163302819192542881359629016178651814593394538223
93973367412547745374841867784654357043350918645343989762850904236764163860579628050
64695988578721271021836244935120824154200938246665792571840648519258635324070387081

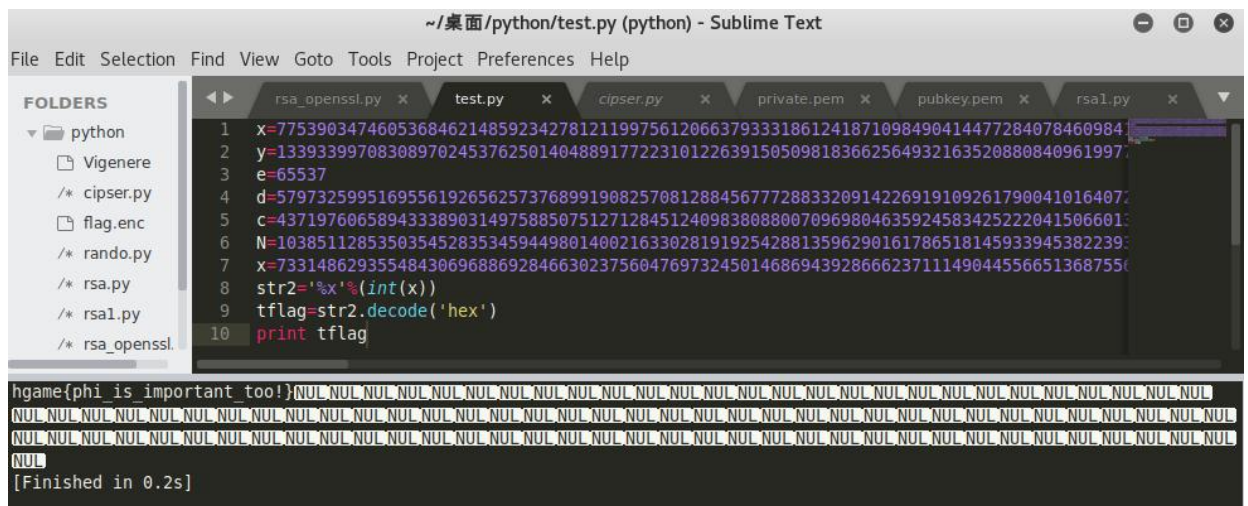
Private Exponent (D):
57973259951695561926562573768991908257081288456777288332091422691910926179004101640
72739925048149787835663782733658796165676390228406833616720376505182863853900192598
51977164373181210664796835520605970929618585799512950126003650773925747796071701691

Generate **Test** **Factoring info (Prime factors):** 0
Calc. D **Factor N**
Help **Exit**
☐ Use MPQS method only ☐ No time checks

Done. tE!



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

| | | |
|---|--|--|
| <p>明文:</p> <p>many years later as he faced the firing squad, colonel aureliano buend'a was to remember that distant afternoon when his father took him to discover ice, at that time macondo was a village of twenty adobe houses, built on the bank of a river of clear water that ran along a bed of polished stones, which were white and enormous, like prehistoric eggs, the world was so recent that many things lacked names, and in order to indicate them it was necessary to point, every year during the month of march a family of ragged gypsies would set up their tents near the village, and with a great uproar of pipes and kettledrums they would display new inventions, first they brought the magnet, a heavy gypsy with an untamed beard and sparrow hands, who introduced himself as melquiades, put on a bold public demonstration of what he himself called the eighth wonder of the learned alchemists of macedonia.</p> | <p>密钥: <input type="text"/></p> <p><input type="button" value="加密"/></p> <p><input type="button" value="<有密钥解密"/></p> <p><input type="button" value="<无密钥解密"/></p> <p>key长度: <input type="text"/></p> <p>最可能的密钥: another</p> | <p>密文:</p> <p>mabr firrf ztali af vx meteq hal jzrvbz zulaq, qhsseey onyicinhb iynq'o phw ko esflqsee hahx uifhtux rfgskusfn jvxu las somoii tbod ond tb rbzgfvrif bji. rt gvtz xzaz atjseub ktz e alystni ff gkxup aqcul lfufsl. iyzlg eg alv bmbd vj r rvjxy sw cysty arttrf moek rnb tsseg n psk sw pzbzrlvd fhhuij, wuvvo avrr kapkv aar xuzimbil, smbe cfxomjtbfbj ixtf. hal afryr phw jo esvirk tuona teey gvbuk; lmqdh eszsl, hru sa ckkir tb wkatags moid ig ktz rvcrgilvop tb dhprk, eiskf cvae rymeg gvx tsetu cy teicu o yhgill cy yexgrz zftjirg pvyed fsm bt khrwk aietf bxhv khr jbsprgr, oqk astu o zyirt hdkvei os dbwij aar dlxlrlrkbbj tusr dslq rbztcad bxd mevrtpases. swkx khra uyslguh moi datbxa. e yonj: nqsl kbal rn hbaqcd ostyh rna gihvioj vtuhj, wuc buxioqivlh yizgxsj rs zsexyldrg. ibx fn n phsh guozbj hvmbblavrtvog vj nhnh al lzmfsen grlysw alv evuaal noarky sw tus eleinrr tsgyezvlew ff zovlhfuvvo.</p> |
|---|--|--|

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

```

cip='1917090506070905195f07065f06031505195f035f0a07065f170c5f1407170205101105'
test=[]
for i,x in enumerate(cip):
    if i%2!=0:
        te=[cip[i-1]+cip[i]]
        test.append(te)
#test=[['19'], ['17'], ['09'], ['05'], ['06'], ['07'], ['09'], ['05'], ['19'], ['5f'], ['07'], ['06'], ['5f'], ['06'], ['03'], ['15'], ['05'], ['19'], ['5f']]
xixi=[]
for i in test:
    x=int(i[0],16)
    if x>140:
        xixi.append("_")
    else:
        xixi.append(x)
# xixi=['19', '17', '09', '05', '06', '07', '09', '05', '19', '5f', '07', '06', '5f', '06', '03', '15', '05', '19', '5f']
item={
    "a":1,"b":2,"c":3,"d":4,"e":5,"f":6,"g":7,"h":8,"i":9,"j":10,"k":11,"l":12,"m":13,"n":14,"o":15,"p":16,"q":17,"r":18,"s":19,"t":20,"u":21,"v":22,"w":23
}
for i in item.keys():
    item[i]=ord(i)
#('a': 97, 'c': 99, 'b': 98, 'e': 101, 'd': 100, 'g': 103, 'f': 102, 'i': 105, 'h': 104, 'k': 107, 'j': 106, 'm': 109, 'l': 108, 'o': 111, 'n': 110, 'q': 113)
def res(items1):
    new={v:k for k,v in items1.items()}
    return new
#(97: 'a', 98: 'b', 99: 'c', 100: 'd', 101: 'e', 102: 'f', 103: 'g', 104: 'h', 105: 'i', 106: 'j', 107: 'k', 108: 'l', 109: 'm', 110: 'n', 111: 'o', 112: 'p', 113: 'q')
with open('file.txt','w+') as fp:
    result=""
    for a in range(0,26):
        for b in range(0,26):
            print a,b
            for i in item.keys():
                x=(a*(ord(i)+b-97))%26
                item[i]=x
            # print item
            resv=res(item)
            for j in xixi:
                if j in resv.keys():
                    result+=resv[j]
                else:
                    result+="_"
            result+="\n"
            fp.write(result)

```

```

927 vrphwlphv_lw_wdnhv_d_elw_ri_ylrohqfh
928 uqogvkogu_kv_vcmgu_c_dkv_qh_xkqngpeg
929 tnnfuinfu_iu_uhlft_h_giu_qg_wipmfodf
930 sometimes it takes a bit of violence
931 rnldshldr_hs_szjdr_z_ahs_ne_uhnkdmdb
932 amkcrqkcg_qr_ryica_v_zar_md_tamialc
933 plbatlbp_tg_oxhnp_x_vfg_lc_sflbkzh

```