

HGame_Week1WP

Vesperina#000cdc

签到

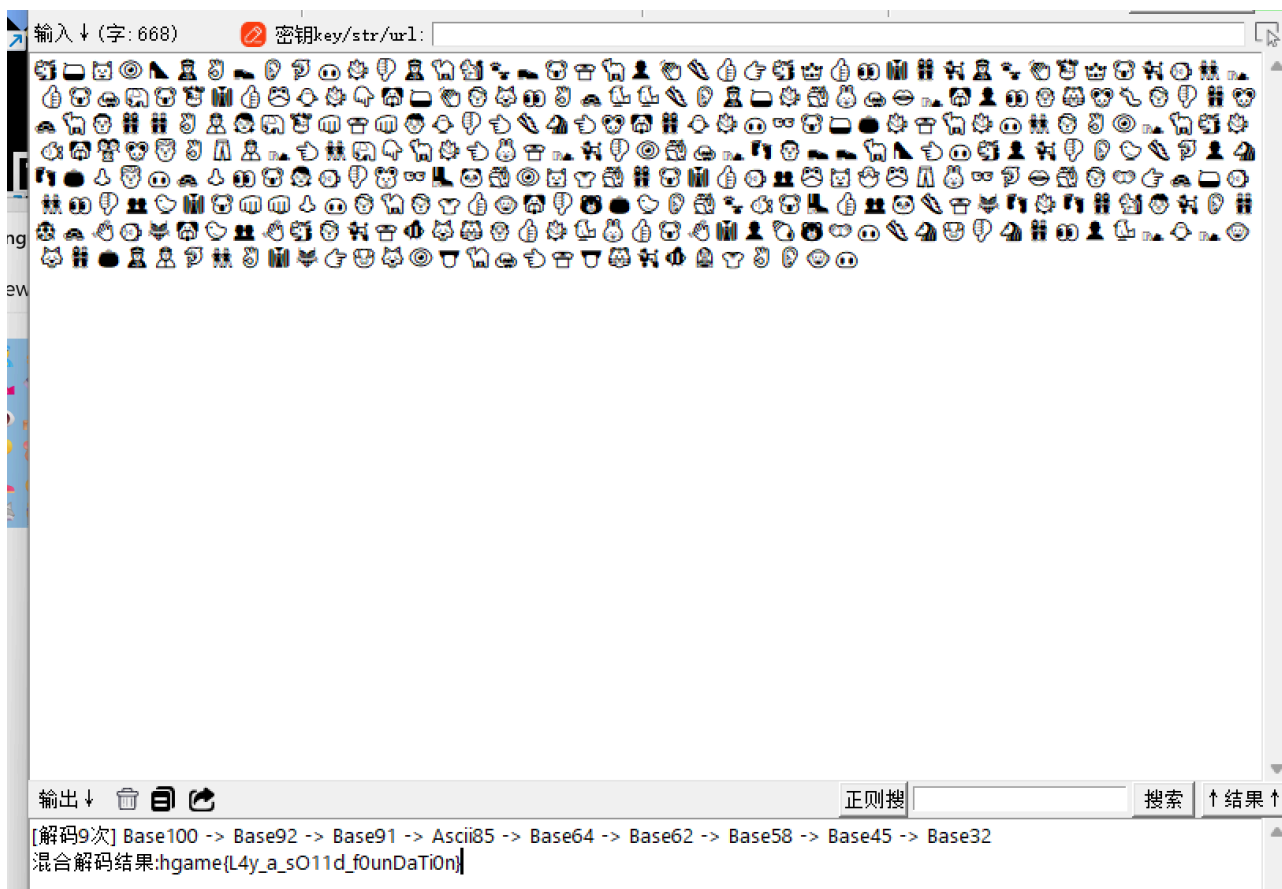
```
xuan@xuan:/mnt/c/Users/xjxua$ nc cloud-big.hgame.vidar.club 31775
ls -la
total 72
drwxr-xr-x    1 root    root    4096 Feb  2 10:14 .
drwxr-xr-x    1 root    root    4096 Feb  2 10:14 ..
drwxr-xr-x    1 root    root    4096 Jan 23  2025 bin
drwxr-xr-x    5 root    root    360 Feb  2 10:14 dev
drwxr-xr-x    1 root    root    4096 Feb  2 10:14 etc
-rw-r--r--    1 root    root     63 Feb  2 10:14 flag
drwxr-xr-x    2 root    root    4096 Jan  8  2025 home
drwxr-xr-x    6 root    root    4096 Jan  8  2025 lib
drwxr-xr-x    5 root    root    4096 Jan  8  2025 media
drwxr-xr-x    2 root    root    4096 Jan  8  2025 mnt
drwxr-xr-x    2 root    root    4096 Jan  8  2025 opt
dr-xr-xr-x 1442 root    root      0 Feb  2 10:14 proc
drwx-----   2 root    root    4096 Jan  8  2025 root
drwxr-xr-x    1 root    root    4096 Feb  2 10:14 run
drwxr-xr-x    2 root    root    4096 Jan  8  2025 sbin
drwxr-xr-x    2 root    root    4096 Jan  8  2025 srv
-rwxr-xr-x    1 root    root     96 Jan 23  2025 start.sh
dr-xr-xr-x   13 root    root      0 Feb  2 10:14 sys
drwxrwxrwt    2 root    root    4096 Jan  8  2025 tmp
drwxr-xr-x    7 root    root    4096 Jan  8  2025 usr
drwxr-xr-x   11 root    root    4096 Jan  8  2025 var
cat flag
hgame{y0ur-cAn_c0nNEct_tO_tH3-RemoTE_3nVlRONm3nt-tO_g3T_flAg0}
```

hgame{y0ur-cAn_c0nNEct_tO_tH3-RemoTE_3nVlRONm3nt-tO_g3T_flAg0}

Misc

1.打好基础

随波逐流一把梭

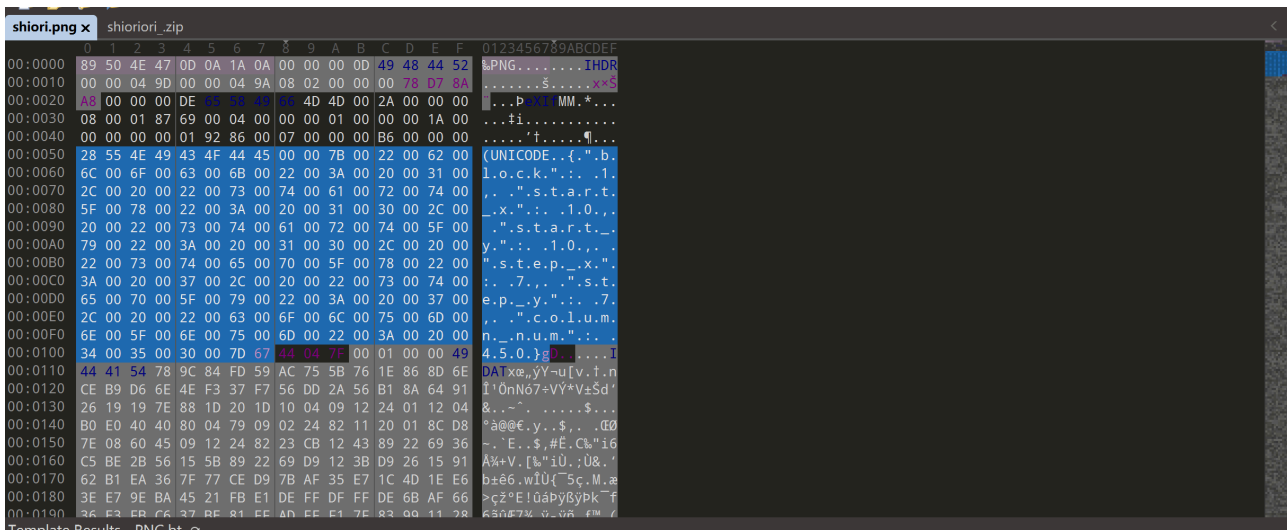


hgame{L4y_a_s011d_f0unDaTi0n}

2.shiori不想找女友

7z发现附件里还有个压缩包，是真加密，爆破不开

cancan图片，010发现文件头有奇妙小数据，疑似是坐标点位



脚本提取成图片

```
from PIL import Image

def solve():
    img = Image.open('shiori.png').convert('RGB')
    pix = img.load()
    w, h = img.size

    # 参数设置
    start_x, start_y = 10, 10
    step_x, step_y = 7, 7
    target_width = 450

    # 1. 线性提取: 把所有采样点存入一个单纯的列表, 不分行
    bits = []
    # 严格按照 y 在外、x 在内的顺序, 模拟最原始的数据流
    for y in range(start_y, h, step_y):
        for x in range(start_x, w, step_x):
            r, g, b = pix[x, y]
            bits.append(r & 1)

    # 2. 重新组装: 按 450 宽度切分
    target_height = len(bits) // target_width
    final_img = Image.new('1', (target_width, target_height))

    for i in range(target_width * target_height):
        x = i % target_width
        y = i // target_width
```

```

        final_img.putpixel((x, y), bits[i])

    final_img.save('STRICT_450_RESULT.png')
    print("请检查 STRICT_450_RESULT.png")

if __name__ == "__main__":
    solve()

```

This_is_a_key_for_u

输入密码解压缩



hgame{bec0use_lilies_are_7he_b1st}

Web

1.魔理沙的魔法目录

F12搜索time

```

o['i'] = [-0x1 * -0x1b91 + -0x15d7 + -0x4e5, 0x1 * 0x7b5 + 0x8e0 + 0x351 * -0x5, 0x199f + 0x399 * 0x1 + -0x1c66, 0x25 * 0x101 + 0x1 * -0x11bd +
b['c'] = ['ctf_token', 'localStorage', 'getItem', -0x15d * -0xf + 0x33 * -0x11 + -0xb * 0x18d, '_0x42f4d2', 0x8b7 + -0x8 * 0xb0 + -0x1 * 0x337,
o['p'] = 0x0,
o['l'] = 0x6,

```

查询到这个是心跳包机制

o['c'] = ['ctf_token', 'localStorage', 'getItem', -0x15d * -0xf + 0x33 * -0x11 + -0xb * 0x18d, '0x42f4d2', 0x8b7 + -0x8 * 0xb0 + -0x1 * 0x337, '0x21e468', 'POST', 'method', 'application/json', 'Content-Type', 'headers', 'username', 'JSON', 'stringify', 'body', 'fetch', 0xf6b * -0x1 + -0x1 * -0xb79 + 0x3f4, 'ok', 'json', 'token', 'setItem', '登录成功:', 'console', 'log', '0x4ec099\$\$2', '0x3c5928', 'Authorization', -0x14f3 * 0x1 + -0x10f * 0xd + 0x22c0, 'time', 'status', -0x2214 * 0x1 + 0x1ddd + 0x5c8, -0x1546 + 0x1e69 + -0x790, 'removeItem', '时间记录成功', '0x32363c', '0x5092a9\$\$2', '心跳错误', 'error', '_0x115f39'],

请求路径和参数

你头

载荷

预览

响应

后动器

时间

▼ 常规

请求网址

http://local-2.hgame.vidar.club:30883/record

请求方法

POST

状态代码

●

200 OK

远程地址

127.0.0.1:7890

引荐来源网址政策

strict-origin-when-cross-origin

▼ 响应标头

☐ 原始

Access-Control-Allow-Origin

*

名称	×	标头	载荷	预览	响应	启动器	时间
local-2.hgame.vidar.club	▼ 请求载荷 查看解析结果						
main.484c7ddc.min.css	{ "time": 10 }						
palette.ab4e12ef.min.css							
css?family=Roboto:300,300i,400,400i,700,700i%7CR...							
bundle.79ae519e.min.js							
tracker.js							
KFO7CnqEu92Fr1ME7kSn66aGLdTylUAMa3yUBA.wo...							
search.2c215733.min.js							
search_index.json							
favicon.png							
login							
favicon.png							
record							
check							
record							
check							

只修改时间，显示缺少认证



请求头里面找认证

▼请求标头 ☐ 原始	
Accept	*/*
Accept-Encoding	gzip, deflate
Accept-Language	zh-CN,zh;q=0.9,en;q=0.8
Authorization	334c3e06-b740-413d-b8eb-e21b9586ac2c
Content-Length	11
Content-Type	application/json
Host	local-2.hgame.vidar.club:30883
Origin	http://local-2.hgame.vidar.club:30883
Proxy-Connection	keep-alive
Referer	http://local-2.hgame.vidar.club:30883/
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36

修改认证





hgame{You_4R3-A1So-a_MAh0U-t5uKAI-nOW!ee0db}

Crypto

1.Classic

RSA解密

```
n =
1035816088247368826817025484943065574584282177165358535166376031985
8899404725492026530020771366656483989669414034733558114794339286897
2670366375164657970346843271269181099927135708348654216625303445930
8228210386745908170177737884127119910327014311276740687509860336161
38121464799190131518444610260228947206957
leak =
6614588561261434084424582030267010885893931492438594708489233399180
372535747474192128
c =
3816494795431604480251464087128556270786979335490716562233684043248
8893861610651450862702262363481097538127040490478908756416851240578
6771954599962527555665107864867073401070579712175572952170728676734
8536935837028950654993211987979147427967756308037745659213903550116
3534305008864900509896586230830001710243
```

```

e = 65537

p_high = leak << 230
PR.<x> = PolynomialRing(Zmod(n))
f = p_high + x

roots = f.small_roots(X=2^230, beta=0.4, epsilon=0.03)

if roots:
    delta_p = int(roots[0])
    p = p_high + delta_p
    q = n // p
    phi = (p - 1) * (q - 1)
    d = inverse_mod(e, phi)
    m = pow(c, d, n)

    m_hex = hex(m)[2:]
    if len(m_hex) % 2 != 0: m_hex = '0' + m_hex
    rsa_result = bytes.fromhex(m_hex).decode(errors='ignore')

    print("\n" + "="*50)
    print("RSA Decrypted Text:")
    print(rsa_result)
    print("="*50)
else:
    print("Failed to find the root. Try adjusting epsilon to
0.02.")

```

```

=====
RSA Decrypted Text:
Vigenere,key=hgame
=====

```

将flag.txt的换行都去掉，然后解密

Ane Hmnknèdi joptiy cae rvz izzlittqh ie Vukltèrq; ma cae jpxsf tyupawlj iz 1553 ff zhq Maglueu Miazht Bmxaosfe Iklxezu, yqx pz wmw ugmqh hltqv Cogqrèyk dgi au huw 1586 pspdscmqray, lqecons Flrlmwv crarnry ovljifik lod xoxeq glttgvpks.Ux byep e rky fs jecxi anraynn 26 Cmisgr mpwnaniay luol g dqgr uf oeyjs, qeytizk pz tti aotxi vl "tti btbdihqanpl iibllx."Iz xok 19tt glttgvf, Hanfhme qbwusqh pzs biyoopmj cemoukse, hlrihiyons e mgtmp iroi xogt qrkkd uxz zwa-glttgvf-rozk tett.euewmc,P nobi fuu isbrd xmrk cxezyioes irktaugdewny. Flpy ie cvar rphm:VUHHX{Tti Julxmzooz sm zhq Rlc azh ane Apk}

密钥

The Vigenère cipher was not invented by Vigenère; it was first proposed in 1553 by the Italian Giovan Battista Bellaso, yet it was named after Vigenère due to his 1586 improvements, leaving Bellaso wrongly credited for three centuries.It used a key to cycle through 26 Caesar alphabets like a deck of cards, earning it the title of "the unbreakable cipher."In the 19th century, Babbage exposed its periodic weakness, delivering a fatal blow that ended its two-century-long myth.anyway,I hope you would like classical cryptography. This is your flag:VIDAR{The Collision of the New and the Old}

最终结果是VIDAR{The Collision of the New and the Old}

但评测错误，把空格改成英文空格就正确了

VIDAR{The Collision of the New and the Old}