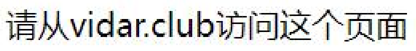
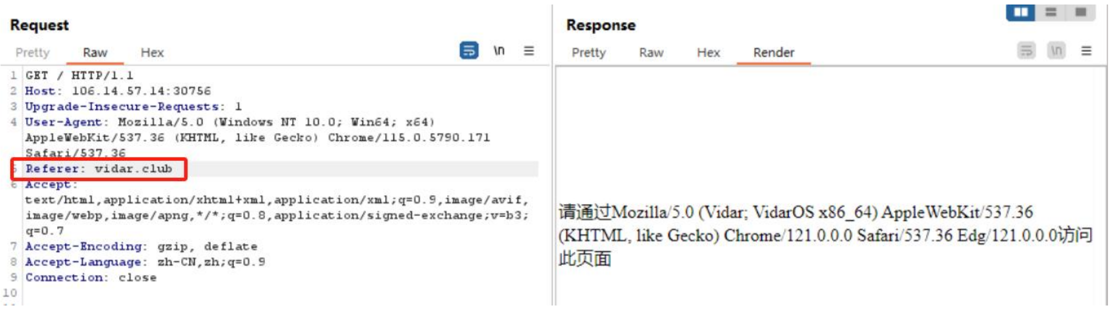
Web:ezHTTP

访问网址



请从vidar.club访问这个页面

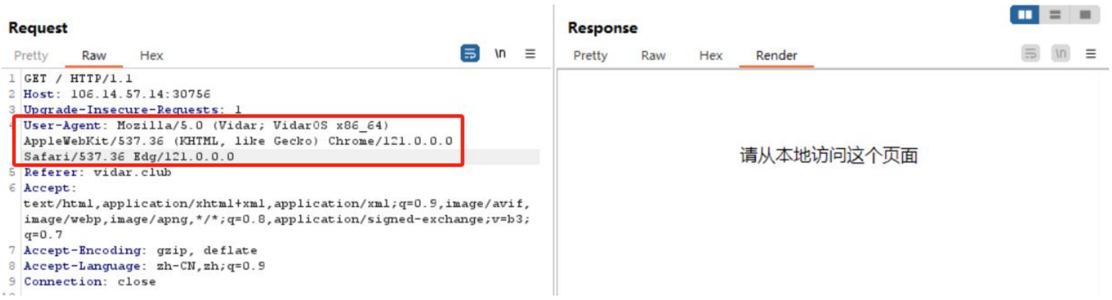
抓包一下，修改 Referer



```
GET / HTTP/1.1
Host: 106.14.57.14:30756
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Safari/537.36
Referer: vidar.club
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

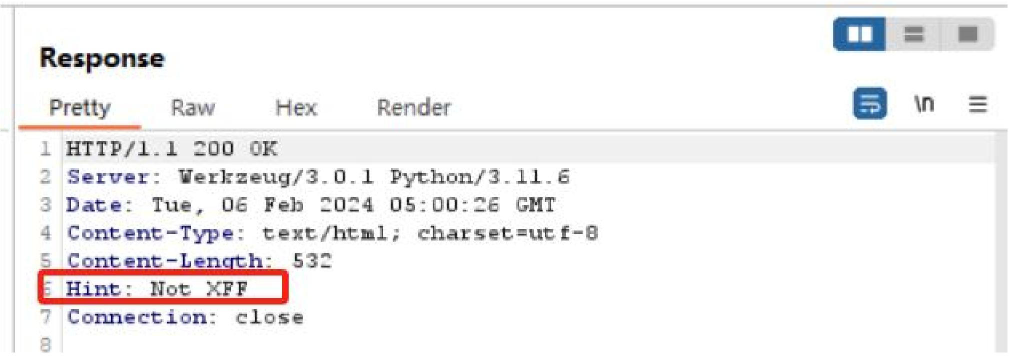
请通过Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0访问此页面

再修改 UA



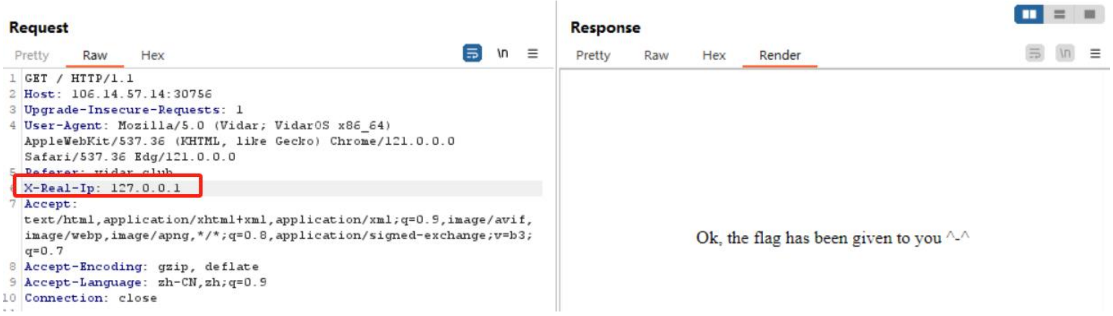
```
GET / HTTP/1.1
Host: 106.14.57.14:30756
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Vidar; VidarOS x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0
Safari/537.36 Edg/121.0.0.0
Referer: vidar.club
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

请从本地访问这个页面



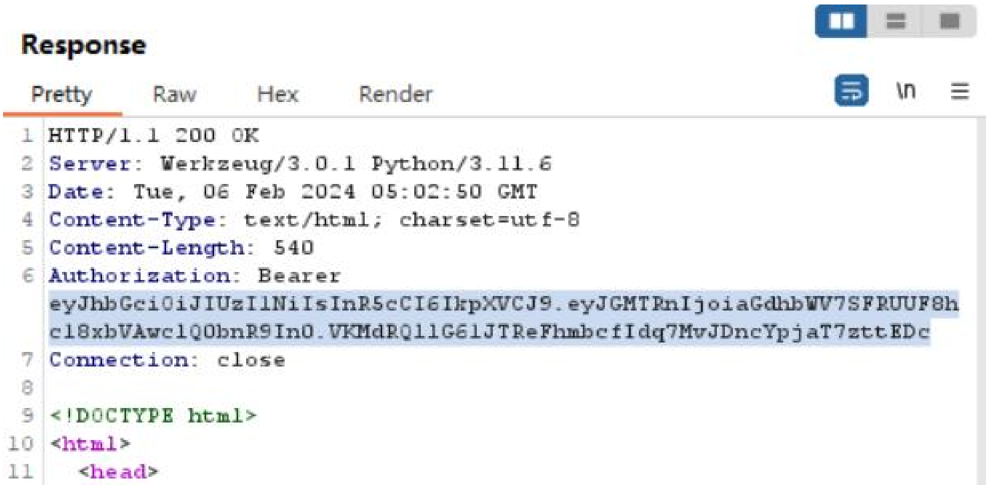
```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.1 Python/3.11.6
Date: Tue, 06 Feb 2024 05:00:26 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 532
Hint: Not XFF
Connection: close
```

提示非 XFF，几番尝试之后发现 X-Real-Ip 可以



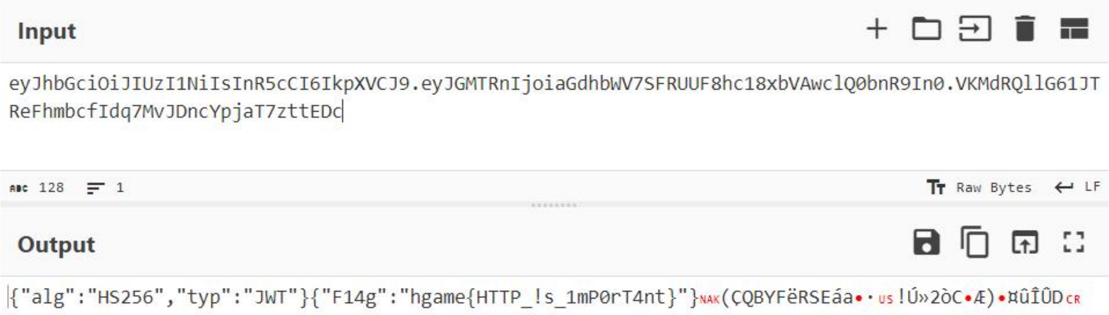
```
GET / HTTP/1.1
Host: 106.14.57.14:30756
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Vidar; VidarOS x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0
Safari/537.36 Edg/121.0.0.0
Referer: vidar.club
X-Real-Ip: 127.0.0.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Ok, the flag has been given to you ^-^



```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.1 Python/3.11.6
Date: Tue, 06 Feb 2024 05:02:50 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 540
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SFRUUF8h
c18xbVAwclQ0bnR9In0.VKMdRQ1lG61JTReFhmbcfIdq7MvJDncYpjaT7zttEDc
Connection: close

<!DOCTYPE html>
<html>
  <head>
```

有加密，尝试解一下



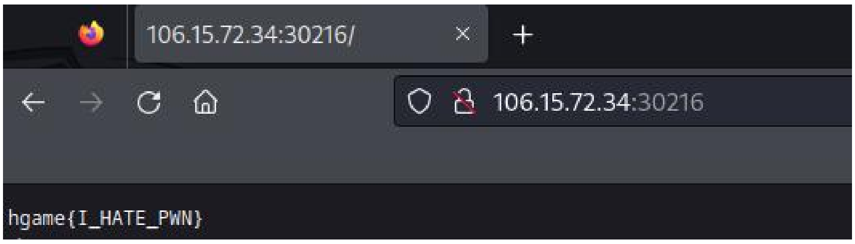
```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SFRUUF8hc18xbVAwclQ0bnR9In0.VKMdRQ1lG61JT
ReFhmbcfIdq7MvJDncYpjaT7zttEDc
```

```
{"alg":"HS256","typ":"JWT"}{"F14g":"hgame{HTTP_!s_1mP0rT4nt}"}NAK(ÇQBYFëRSEáa•·US!Ú»2òC•Æ)•¤ûÎÛDCR
```

拿到 flag:hgame{HTTP_!s_1mP0rT4nt}

PWN:EzSignIn

linux 虚拟机访问给定网址



```
hgame{I_HATE_PWN}
```

拿到 flag:hgame{I_HATE_PWN}

CRYPTO: ezMath

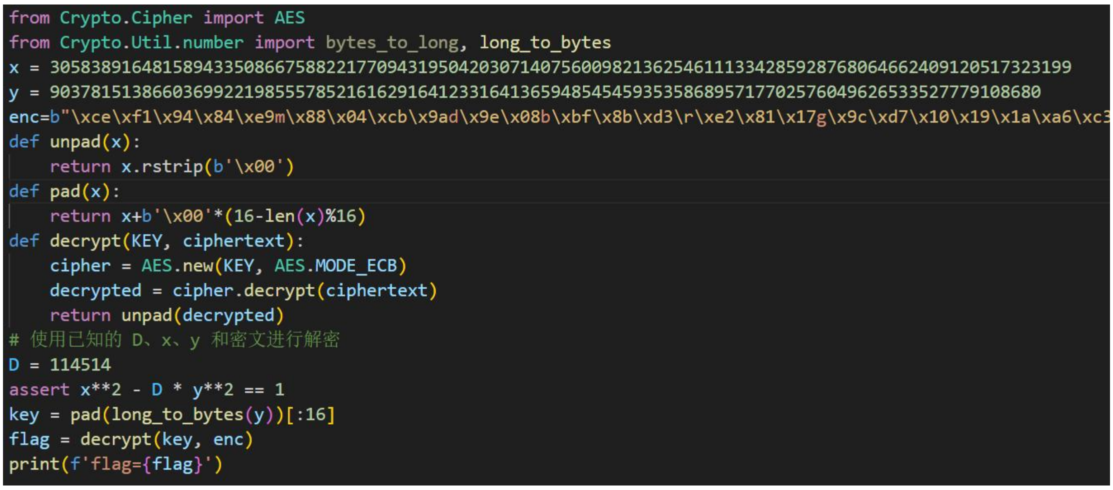
用连分数法解佩尔方程(x**2 - D * y**2 == 1)特解

```
from math import isqrt, floor
#连分数法解佩尔方程(x**2 - D * y**2 == 1)特解
def pell_minimum_solution(n):
    m = isqrt(n)
    if m * m == n:
        return None
    a = [m]
    b, c = m, 1
    while True:
        c = (n - b * b) // c
        tmp = (b + isqrt(n)) // c
        a.append(floor(tmp))
        b = a[-1] * c - b
        if a[-1] == 2 * a[0]:
            break
    p, q = 1, 0
    for j in range(len(a) - 2, -1, -1):
        t = p
        p, q = q + p * a[j], t
    if (len(a) - 1) % 2 == 0:
        x0, y0 = p, q
    else:
        x0, y0 = 2 * p * p + 1, 2 * p * q
    return x0, y0
if __name__ == "__main__":
    while True:
        try:
            n = 114514
            result = pell_minimum_solution(n)
            if result:
                x, y = result
                print(f"{x}^2 - {n} * {y}^2 = 1")
                break
            else:
                print(f"No solution for n = {n}.")
        except ValueError:
            print("Invalid input. Please enter an integer.")
        except KeyboardInterrupt:
            print("\nExiting...")
            Break
```

3058389164815894335086675882217709431950420307140756009821362546111334285928768064662409120517323199^2-114514*9037815138660369922198555785216162916412331641365948545459353586895717702576049626533527779108680^2 = 1 求得方程的解

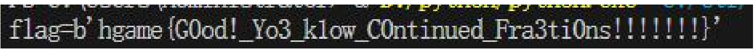
X=3058389164815894335086675882217709431950420307140756009821362546111334285928768064662409120517323199

Y=9037815138660369922198555785216162916412331641365948545459353586895717702576049626533527779108680



```
from Crypto.Cipher import AES
from Crypto.Util.number import bytes_to_long, long_to_bytes
x = 3058389164815894335086675882217709431950420307140756009821362546111334285928768064662409120517323199
y = 9037815138660369922198555785216162916412331641365948545459353586895717702576049626533527779108680
enc=b"\xce\xf1\x94\x84\xe9m\x88\x04\xcb\x9ad\x9e\x08b\xbf\x8b\xd3\r\xe2\x81\x17g\x9c\xd7\x10\x19\x1a\xa6\xc3
def unpad(x):
    return x.rstrip(b'\x00')
def pad(x):
    return x+b'\x00'*(16-len(x)%16)
def decrypt(KEY, ciphertext):
    cipher = AES.new(KEY, AES.MODE_ECB)
    decrypted = cipher.decrypt(ciphertext)
    return unpad(decrypted)
# 使用已知的 D、x、y 和密文进行解密
D = 114514
assert x**2 - D * y**2 == 1
key = pad(long_to_bytes(y))[:16]
flag = decrypt(key, enc)
print(f'flag={flag}')
```

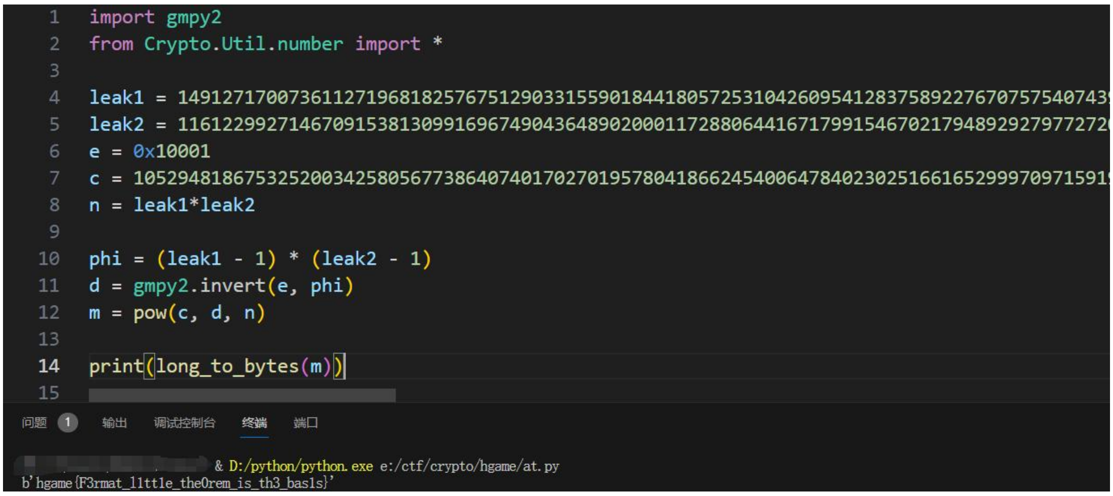
通过已知条件求得 flag



```
flag=b'hgame{G0od!_Yo3_k1ow_C0ntinued_Fra3ti0ns!!!!!!!}'
```

CRYPTO: ezRSA

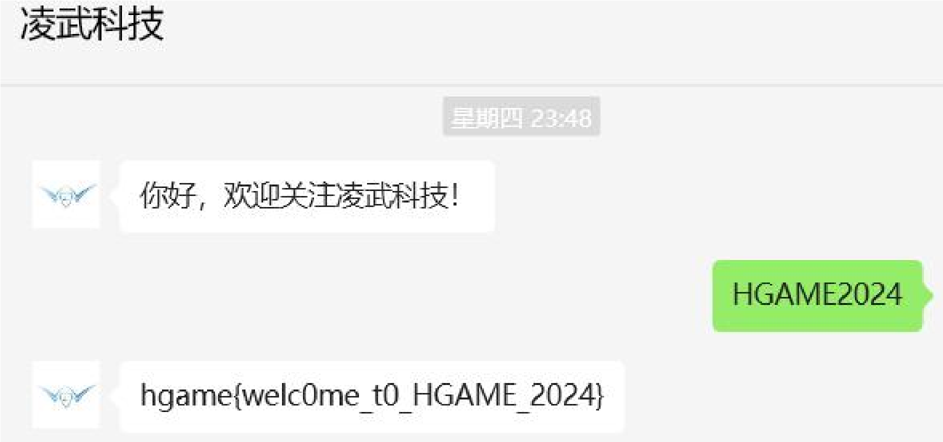
已知 pqec 求 m 的题



```
import gmpy2
from Crypto.Util.number import *

leak1 = 149127170073611271968182576751290331559018441805725310426095412837589227670757540743
leak2 = 116122992714670915381309916967490436489020001172880644167179915467021794892927977272
e = 0x10001
c = 10529481867532520034258056773864074017027019578041866245400647840230251661652999709715915
n = leak1*leak2

phi = (leak1 - 1) * (leak2 - 1)
d = gmpy2.invert(e, phi)
m = pow(c, d, n)

print(long_to_bytes(m))

```

```
[redacted] & D:/python/python.exe e:/ctf/crypto/hgame/at.py
b'hgame{F3rmat_l1ttle_the0rem_is_th3_bas1s}'
```

MISC:签到



凌武科技

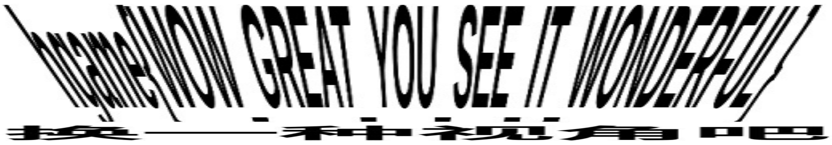
星期四 23:48

你好，欢迎关注凌武科技！

HGAME2024

hgame{welc0me_t0_HGAME_2024}

MISC:SignIn



艰难看出 hgame{WOW_GREAT_YOU_SEE_IT_WONDERFUL}