




202109泰山杯测试赛writeup题解

原创

偷一个月亮  于 2021-09-29 15:19:40 发布  620  收藏 1

分类专栏: [CTF](#) 文章标签: [深度学习](#) [php](#)

本文为博主原创文章, 未经博主允许不得转载, 否则追究法律责任。

本文链接: <https://blog.csdn.net/yiqiushi4748/article/details/120549390>

版权



[CTF 专栏收录该内容](#)

43 篇文章 5 订阅

订阅专栏

2021泰山杯测试赛writeup题解

Caesar

```
s="ch\at;X[hUeQZcNU_QL^f"  
index = 4  
a = ""  
for i in s:  
    print(chr(ord(i)+index))  
    a += chr(ord(i)+index)  
    index += 1  
print(a)
```

```
[Running] python -u "c:\Users\Negoowen\Desktop\泰山测试赛\凯撒1.py"
```

```
g  
m
```

```
{  
C  
a  
e  
s  
a  
r  
-  
i  
s  
-  
g  
r  
e  
a  
t  
}
```

```
gm  
{Caesar_is_great}
```

```
[Done] exited with code=0 in 0.091 seconds
```

RSA1

rsa 的RSA Padding Attack攻击

```

# -*- coding: utf-8 -*-#
#-----#
# Name:      RSA6padAttack
# Date:      2021-09-29
# Author    = 'Negoo_wen'

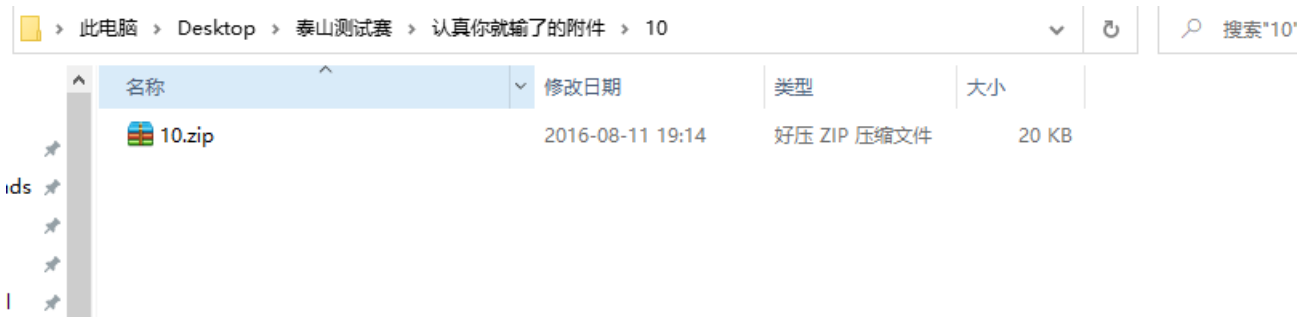
import gmpy
import libnum
def getM2(a,b,c1,c2,n,e):
    a3 = pow(a,e,n)
    b3 = pow(b,e,n)
    first = c1-a3*c2+2*b3
    first = first % n
    second = e*b*(a3*c2-b3)
    second = second % n
    third = second*gmpy.invert(first,n)
    third = third % n
    fourth = (third+b)*gmpy.invert(a,n)
    return fourth % n

e=0x3
a=1
b=-1
c1=0x7ba5502ecbc3b15ad8c2db8f30a593eb062dde4d7dfacadf0a28291d1a576389a18dfba0607c0243f843f637449089dd2090d47ee9845d4147f02afd4d891f19L
c2=0x891ac4f663df41c1f6433ee3513d749c3ba02fe0aacd7f51d791b9bac4f7e5194bd484d78d972c344faf600f7d3aa580485774768efc47ab8ddb67eeeb330fa1L
padding2=1
n=0xb28ae8f29f8b90e8b8c5667b2b71e49929446b41f7f7a3e9e45bc52a1e8c45d59c1788be48a9c365d51feee0b2cd3295001cdad1ba5ccf808686b5ce5a269ae5L
m = getM2(a,b,c1,c2,n,e)-padding2
print hex(m)
print libnum.n2s(m)

```

英 简

10.ex1



10.zip\xl\charts

名称	大小	压缩后大小	类型
..(上层目录)			
chart1.xml	3.31 KB	1.03 KB	XML 文档
chart2.xml	2.93 KB	1 KB	XML 文档
flag.txt	1 KB	1 KB	文本文档

flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag {M9eVfi2Pcs#}

extractall

hint.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
喜欢解压是吧，喏，密码就是压缩包名字，自己玩去吧

写一个解压脚本循环解压

```
C:\Users\Negoowen\Desktop\泰山测试赛\extractall的附件\extractall.png
C:/Users/Negoowen/Desktop/泰山测试赛/extractall的附件/1/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19
["C:/Users/Negoowen/Desktop/泰山测试赛/extractall的附件/1/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19", 'extractall.png', 'C:/Users/Negoowen/Desktop/泰山测试赛/extractall的附件/1/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19\extractall.png']
unzip -o "extractall" C:/Users/Negoowen/Desktop/泰山测试赛/extractall的附件/1/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/extractall.png -d C:/Users/Negoowen/Desktop/泰山测试赛/extractall的附件/1/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20
Archive:  C:/Users/Negoowen/Desktop/泰山测试赛/extractall的附件/1/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/extractall.png
End-of-central-directory signature not found. Either this file is not
a zipfile, or it constitutes one disk of a multi-part archive.  In the
latter case the central directory and zipfile comment will be found on
the last disk(s) of this archive.
unzip: cannot find zipfile directory in one of C:/Users/Negoowen/Desktop/泰山测试赛/extractall的附件/1/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/extractall.png or
C:/Users/Negoowen/Desktop/泰山测试赛/extractall的附件/1/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/extractall.png.zip, and cannot find C:/Users/Negoowen/Desktop/泰山测试赛/extractall的附件/1/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/extractall.png.ZIP, perIOD.
```

flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
恭喜你经过21次解压后找到了我，但flag不在这儿，哈哈哈~



who am i

```
A tree /f
卷 Windows 的文件夹 PATH 列表
根序列号为 C0000100 2EA2:27F2
C:.
  1RGe0V.zip
  extractall.png
  extractall.png.png
  flag.txt
  hint.txt
  [REFTO.zip
  提取zip.py
  根据crc32恢复高度.py
-1
├── 4dH3NV.zip
│   └── 1
│       ├── eht8on.zip
│       │   └── 2
│       │       ├── 3rhbGx.zip
│       │       │   └── 3
│       │       │       ├── 8smjtq.zip
│       │       │       │   └── 4
│       │       │       │       ├── zmckit.zip
│       │       │       │       │   └── 5
│       │       │       │       │       ├── fsXNFU.zip
│       │       │       │       │       │   └── 6
│       │       │       │       │       │       ├── 9rskp5.zip
│       │       │       │       │       │       │   └── 7
│       │       │       │       │       │       │       ├── a93su6.zip
│       │       │       │       │       │       │       │   └── 8
│       │       │       │       │       │       │       │       ├── a10o68.zip
│       │       │       │       │       │       │       │       │   └── 9
│       │       │       │       │       │       │       │       │       ├── p012vq.zip
│       │       │       │       │       │       │       │       │       │   └── 10
│       │       │       │       │       │       │       │       │       │       ├── 29fRnV.zip
│       │       │       │       │       │       │       │       │       │       │   └── 11
│       │       │       │       │       │       │       │       │       │       │       ├── fco9e2.zip
│       │       │       │       │       │       │       │       │       │       │       │   └── 12
│       │       │       │       │       │       │       │       │       │       │       │       ├── 7ztjka.zip
│       │       │       │       │       │       │       │       │       │       │       │       │   └── 13
│       │       │       │       │       │       │       │       │       │       │       │       │       ├── bvn8ta.zip
│       │       │       │       │       │       │       │       │       │       │       │       │       │   └── 14
│       │       │       │       │       │       │       │       │       │       │       │       │       │       ├── a27s40.zip
│       │       │       │       │       │       │       │       │       │       │       │       │       │       │   └── 15
│       │       │       │       │       │       │       │       │       │       │       │       │       │       │       ├── dxzk11.zip
```

↑ 0.9 KB/s
↓ 7.5 KB/s

英 简

0、
1、
1、 REFTQ
2、 1RGe0V
3、 4dHJhY
5、 3RhbGx
8、 fSXNfU
13、 29fRnV
21 ufQ==

REFTQ1RGe0V4dHJhY3RhbGxfSXNfU29fRnVufQ==

REFTQ1RGe0V4dHJhY3RhbGxfSXNfU29fRnVufQ==

DASCTF{Extractall_Is_So_Fun}

web2

```
<!--  
foreach ($_POST as $item => $value){  
    $$item=$$value;  
    $secret = $$item;  
}  
foreach ($_GET as $key => $value){  
    if ($key=='flag'){  
        $str=$value;  
        $$str=$secret;  
    }  
}  
if (isset($hehe)){  
    echo "<center>".$hehe."</center>";  
}
```

INI

SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL view-source:http://183.129.189.60:10044/?key=flag

Split URL

Execute

Post data

Post data Referrer 0xHEX %URL BASE64 Replace All

hehe=flag

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>Welcome</title>
6 </head>
7 <body >
8 </div>
9 <h1 style="text-align: center">Where is flag?</h1>
10 <!--
11 foreach ($_POST as $item => $value){
12   $$item=$$value;
13   $secret = $$item;
14 }
15 foreach ($_GET as $key => $value){
16   if ($key=='flag'){
17     $str=$value;
18     $$str=$secret;
19   }
20 }
21 if (isset($hehe)){
22   echo "<center>". $hehe. "</center>";
23 }
24 //flag+flaag=DASCTF{XXXXXXX}
25 -->
26 </body>
27 <center>
28 </html>
29 <center>DASCTF {27b62da69</center>
30
31
```

web1

过滤太多了，时间不够用了 ☐