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

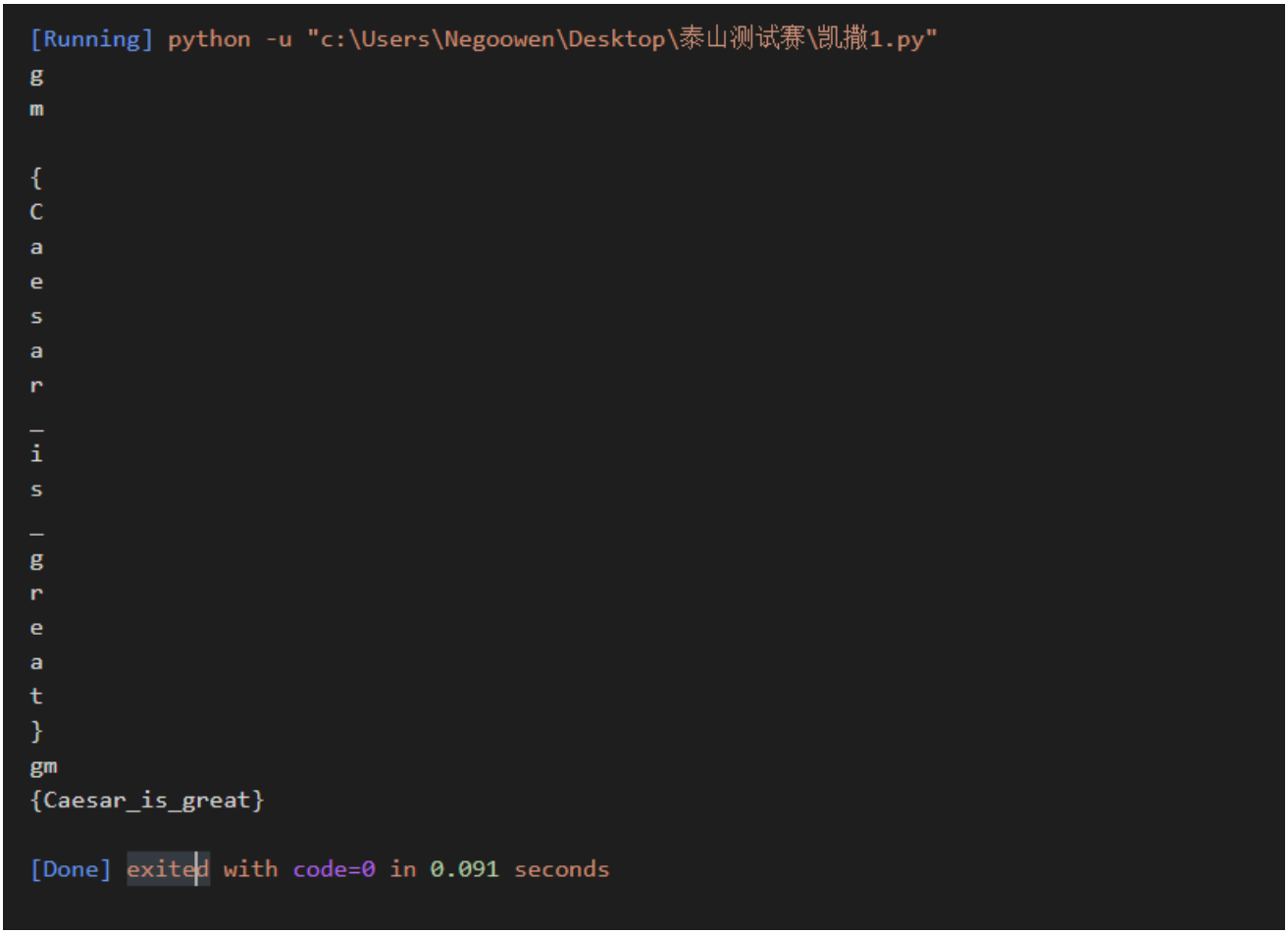
分类专栏： CTF 文章标签： 深度学习 php

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

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)
```



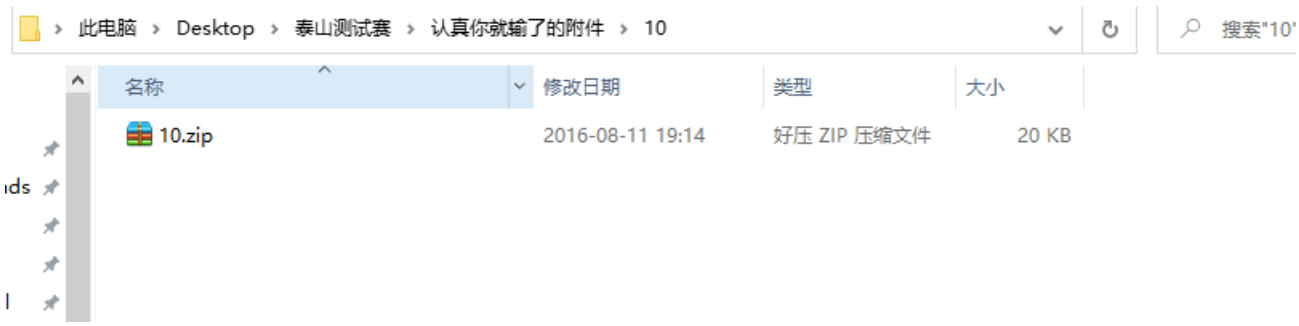
RSA1

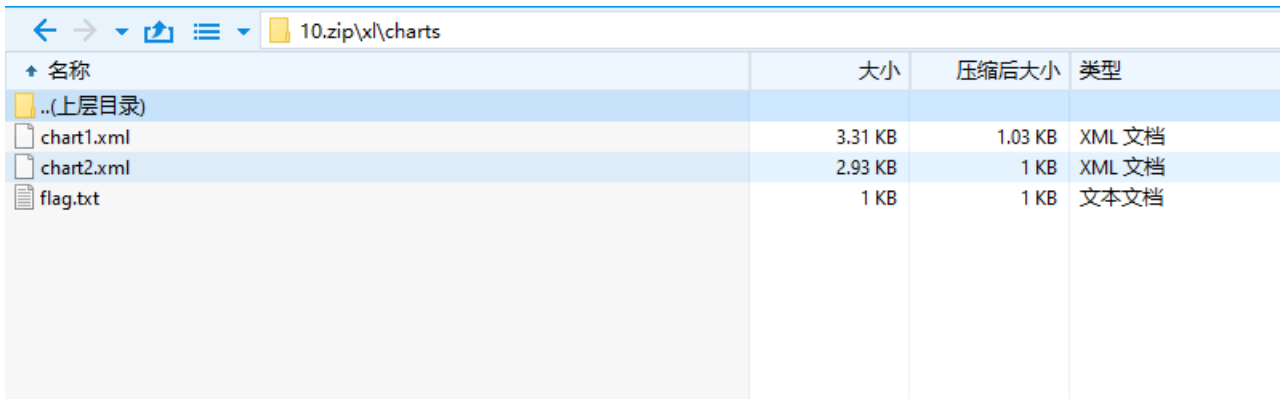
rsa 的RSA Padding Attack攻击

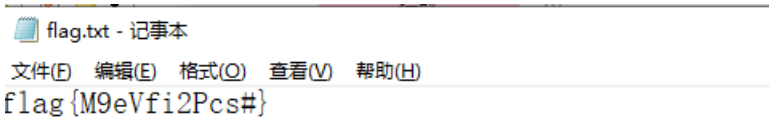
```python
# -*- coding: utf-8 -*-#
#-------------------------------------------------------------------------------
# Name:      RSA6padAttack
# Date:      2021-09-29
__Author__ = 'Negoo_wen'

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)
```

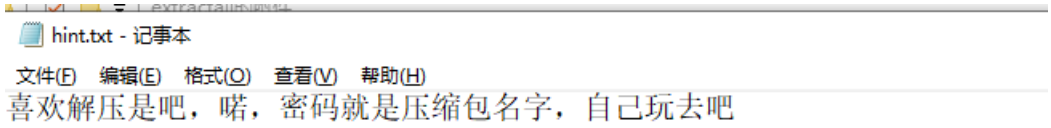
10.exl





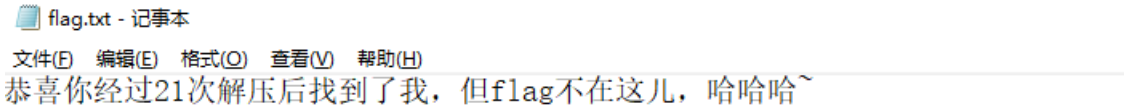


extractall



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  -P "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.
```



who am i

```
λ tree /f
卷 Windows 的文件夹 PATH 列表
卷序列号为 C0000100 2EA2:27F2
C:.
    1RGe0V.zip
    extractall.png
    extractall.png.png
    flag.txt
    hint.txt
    [REFTQ.zip
    提取zip.py
    根据crc32恢复高度.py

└─1
    │  4dHJhY.zip
    │
    └─1
        │  eht8on.zip
        │
        └─2
            │  3RhbGx.zip
            │
            └─3
                │  8smjtq.zip
                │
                └─4
                    │  zmckit.zip
                    │
                    └─5
                        │  fSXNfU.zip
                        │
                        └─6
                            │  9rskp5.zip
                            │
                            └─7
                                │  a93su6.zip
                                │
                                └─8
                                    │  al0o68.zip
                                    │
                                    └─9
                                        │  p0l2vq.zip
                                        │
                                        └─10
                                            │  29fRnV.zip
                                            │
                                            └─11
                                                │  fco9e2.zip
                                                │
                                                └─12
                                                    │  7ztjka.zip
                                                    │
                                                    └─13
                                                        │  bvn8ta.zip
                                                        │
                                                        └─14
                                                            │  a27s40.zip
                                                            │
                                                            └─15
                                                                │  dxzk1l.zip
```

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

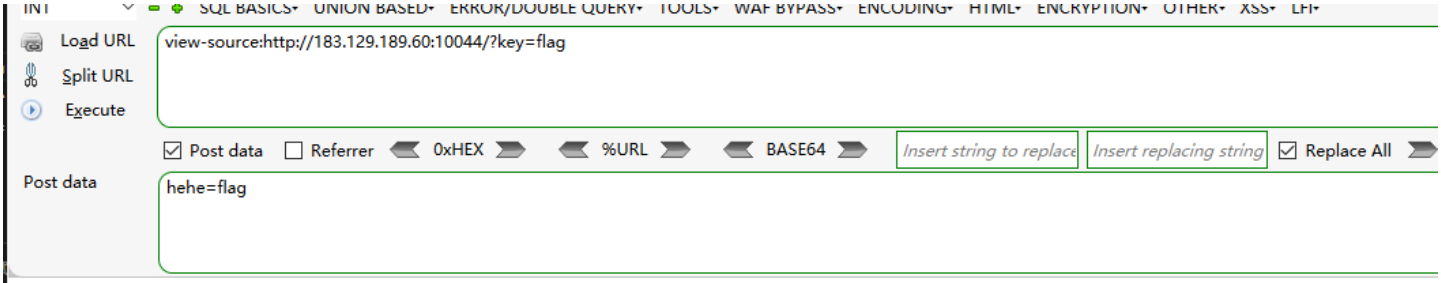
REFTQ1RGe0V4dHJhY3RhbGxfSXNfU29fRnVufQ==

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>";
}
```




```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Welcome</title>
</head>
<body >
</div>
<h1 style="text-align: center">Where is flag?</h1>
<!--
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>";
}
//flag+flaag=DASCTF{XXXXXXX}
-->
</body>
<center>
</html>
<center>DASCTF{27b62da69</center>
```

web1

过滤太多了，时间不够用了