

创建时间: 2020/1/28 13:16

更新时间: 2020/1/30 19:57

作者: 羔

hgame_week2_wp

- [hgame_week2_wp](#)
 - [web](#)
 - [Cosmos的博客后台](#)
 - [Cosmos的新语言](#)
 - [Reverse](#)
 - [Classic_CrackMe](#)
 - [babyPy](#)
 - [crypto](#)
 - [Verification_code](#)
 - [Remainder](#)
 - [misc](#)
 - [Cosmos的午餐](#)
 - [所见即为假](#)
 - [地球上最后的夜晚](#)
 - [玩玩条码](#)
 - [后记](#)

~~有点赶时间，就大致写一下了，下周一定做完一题写一个,Ditto在这个时候不好用，求推荐~~

web

Cosmos的博客后台

- 通过伪协议能拿到3个php文件
admin.php
login.php
index.php

  cosmos-admin.hgame.day-day.work/?action=php://filter/read=convert.base64-encode/resource=./index.php

- 重点是这里的可以debug参数，然后通过 `eval("var_dump($$debug);")`; 这个\$\$可以读取到其他变量，要读的就是admin_password和admin_username,

```

<?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);");
    }
}
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();
        }
    }
}

```

- 账号貌似就是 Cosmos!，密码好像是0e开头的MD5码，然后这里涉及php中的一个漏洞？0e会被看做是科学计数法而不是字符串，所以查到一个字符串的MD5是0e开头就可以了，我当时用的是s878926199a
- 然后这里我试了其他的绕过，读取本地的flag都不行，最后是用这个 file://localhost/flag

Welcome Cosmos!



Cosmos的新语言

一个会随机方式生成的随机字符串，要用脚本写，直接贴了

```

import base64
import urllib.request
import re
import time

def rot13(s, OffSet=13):
    def encodeCh(ch):
        def f(x): return chr((ord(ch)-x+Offset) % 26 + x)
        return f(97) if ch.islower() else (f(65) if ch.isupper() else ch)
    return ''.join(encodeCh(c) for c in s)

def decrypt(cc):
    result = ''
    for i in cc:
        result = result+chr(ord(i)-1)
    return result

def strrevv(cc):
    result = ''
    for i in cc:
        result = i+result
    return result

urlmiwen = 'http://1e3bc03039.php.hgame.n3ko.co/index.php'
urljiami = 'http://1e3bc03039.php.hgame.n3ko.co/mycode'

for i in range(1, 20):
    print('第'+str(i)+'次尝试')
    receiv = urllib.request.urlopen(urlmiwen)
    data = receiv.read().decode('utf-8')
    #print(data)
    resu = re.search('^</code>](.*?)<br>$', data, re.M)
    miwen = resu.group(0)[-4]
    print(miwen)

    receiv = urllib.request.urlopen(urljiami)
    data = receiv.read().decode('utf-8')
    #print(data)
    resu = re.search('^echo\.(.*?)$', data, re.M)
    jiamifun = resu.group(0)[5:-1]

```

```
print(jiamifun)
print('-----')
for j in range(1,15):
    print(jiamifun)
    print(miwen)
    jie=jiamifun[0:6]
    if(jie=='base64'):
        try:
            miwen=base64.b64decode(miwen).decode()
            jiamifun=jiamifun[14:]
            continue
        except:
            break
    if(jie=='strrev'):
        try:
            miwen=strrevv(miwen)
            jiamifun=jiamifun[7:]
            continue
        except:
            break
    if(jie=='encryp'):
        try:
            miwen=decrypt(miwen)
            jiamifun=jiamifun[8:]
            continue
        except:
            break
    if(jie=='str_ro'):
        try:
            miwen=rot13(miwen)
            jiamifun=jiamifun[10:]
            continue
        except:
            break
print("答案")
print(miwen)
data={'token':miwen}
request = urllib.request.Request(url=urlmiwen)
formdata = urllib.parse.urlencode(data).encode()
respos = urllib.request.urlopen(request,formdata)
print(respos.read().decode())
time.sleep( 30 )
break
```

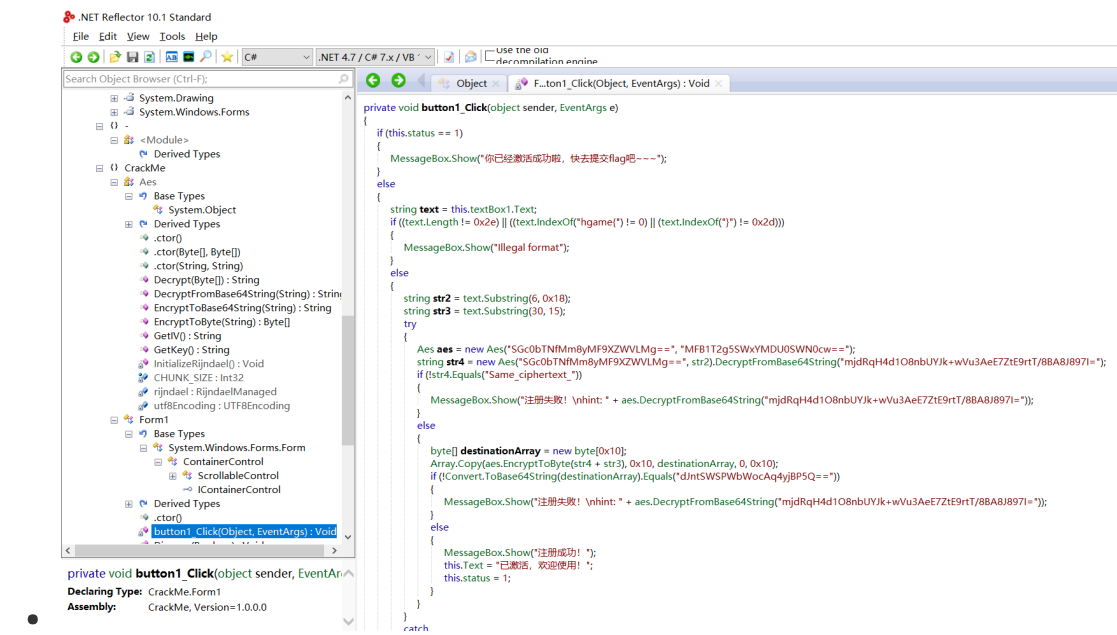
```
print(jiamifun)
print(miwen)
time.sleep( 3 )

1061e93ed0971910ec653ba97601763b
答案
1061e93ed0971910ec653ba97601763b
<html><head></head><body><code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br>highlight file</span><span style="color: #007700"></span><span st
</span><span style="color: #0000BB">$code&nbsp;</span><span style="color: #007700">=&nbsp;</span><span styl
></span><span style="color: #DD0000">'mycode'</span><span style="color: #007700">);<br>eval(</span><span s
r></span>
</span>
</code><br>
VFdwRk0wMXRlVFPuJFwclRWUnZ0RTFXYjNsTlYxcHJUbnBaTUZreVNUwLBSR040VFdwbk0wNUhUVDA9<br>
hgame{$!mple-5CRipt~WlH~pYthoN~or~pHP}
</body>
</html>
```

Reverse

Classic_CrackMe

- 自己跟傻子一样用ida调了半天，感觉不太对，后来发现有专门软件，也搞了半天
- Net Reflector软件



- 学习aes里的cbc，然后学会了就挺好解的了，真心不难
- 自己偷懒用的网站在线解，后来因为编码问题卡了我3个多小时，头疼，python自己写吧

babyPy

- 源代码就不贴了，根据题目提示 `CPython uses a stack-based virtual machine`. 搜索得到

Python 代码先被编译为字节码后，再由Python虚拟机来执行字节码，Python的字节码是一种类似汇编指令的中间语言，一个Python语句会对应若干字节码指令，虚拟机一条一条执行字节码指令，从而完成程序执行。

Python `dis` 模块支持对Python代码进行反汇编，生成字节码指令。

所以这个可以看做python的“汇编”（字节码），因为代码量不长，所以直接手动还原了，还原途中可以用 `dis.dis(your function)` 在python中调试看看还原是否正确

- 贴两个自己用的网站

[死磕python字节码-手工还原python源码](#)

上面的主要用于入门，大概理解操作

[Disassembler for Python bytecode \(官方\)](#)

这个主要用来查询

- Binary operations remove the top of the stack (TOS) and the second top-most stack item (TOS1) from the stack. They perform the operation, and put the result back on the stack.
- 自己还原出来这个样子，魔鬼00o，所以自己用的时候替换一下

```
4
    000=000[::-1] #倒着存储下来
5
    00o=list(000)
6
    for 00 in range(1,len(00o))
7
        0o=00o[00-1] ^ 00o[00]
8
        00o[00]=0o
9
    0=bytes(00o)
10
    return 0.hex() #在类里定义的hex方法，应该不是这样写，但是凑合吧
```

- 加解密过程实际比较简单，反着写出来就行了

```
import dis

def encrypt(000): # bytes
    000 = 000[::-1] # 倒着存储下来
    flag = list(000)
```

```

for i in range(1, len(flag)):
    t = flag[i-1] ^ flag[i]
    flag[i] = t
O = bytes(flag)
return O.hex() # 在类里定义的hex方法

def decrypt(000): # hex
    bb = bytes.fromhex(000)
    flag = list(bb)
    for i in range(len(flag)-1, 0, -1):
        t = flag[i-1] ^ flag[i]
        flag[i] = t
    O = bytes(flag)
    return O

#print(dis.dis(encrypt))
ff = '7d037d045717722d62114e6a5b044f2c184c3f44214c2d4a22'
print(decrypt(ff)[: -1])

```

- 运行就能出flag了

crypto

Verification_code

- 连接，然后得到 `sha256(XXXX+WajmGd603L41r4tJ) == 3bac9e613c4980046ba2466eb52d3f912447d578ad8394e53a1d3eedf78bfbb1` 这样的字符串
- 需要让你提交XXXX的内容
- 写python就行了，可以用pwntools的东西，60秒内出来就行，很快的
- 输入xxxx后还要输入令人羞耻的东西

```

[+] Opening connection to 47.98.192.231 on port 25678: Done
sha256(XXXX+X8cac03dTDTXyG5g) == f83eedf2dfc93eab52b16a9d276a478df93b16f47cf89082347821fb2bf4f4b0

('ef8lX8cac03dTDTXyG5g', 'f83eedf2dfc93eab52b16a9d276a478df93b16f47cf89082347821fb2bf4f4b0')
[*] Switching to interactive mode
Give me XXXX: The secret code?
> $ I like playing Hgame
Ok, you find me.
Here is the flag: hgame{It3Rt00|S+I5_u$3fu1~Fo2_6rUtE-f0Rc3}
Bye~
[*] Got EOF while reading in interactive
$

```

-

Remainder

- “烤个孙子” 形象生动，考一个孙子定理
- 会用一下公式，然后求出 m^e
- 一开始自己直接开65537的根，解了半天，怀疑人生，后来记起来这个有点像rsa，3个素数的那种

```
中国剩余定理.py X
p = gmpy2.mpz(945982963057133766525404116319494343)
q = gmpy2.mpz(150088216417404963893679242888992998)
r = gmpy2.mpz(145897736096689096151704740327665176)
c1 = gmpy2.mpz(784307860116505212245619248148436142)
c2 = gmpy2.mpz(495763564234742221882051873068841676)
c3 = gmpy2.mpz(481310779626494978331892926378614427)

ji = p*q*r
he = gmpy2.invert(p*q*r)*p*q*c3 + gmpy2.invert(p*r*q)*r*c2 + gmpy2.invert(p*q*r)*p*q*c3
c = gmpy2.powmod(he, 1, ji)
print('-----')
phi = (p-1)*(q-1)*(r-1)
d = gmpy2.invert(gmpy2.mpz(65537), phi)
mm = gmpy2.powmod(c, d, ji)
print((number.long_to_bytes(mm)).decode())
```

- 然后手动拼flag了

misc

Cosmos的午餐

- 隐约记得是流量分析，并且用了ssl，然后要在wireshark里面导入ssl_log.log
- 提出来一个压缩包，里面有个jpg，并且贴心的写了Outguess with key.jpg，搜工具，然后用一下就ok了，密码在备注里

所见即为假

- 压缩包，然后用了伪加密，直接360打开就行
- 压缩包备注有F5 key: NIID7CQon6dBsFLr，看了半天确实也不知道什么东西
- f5是一个隐写工具，同上，clone下来用

地球上最后的夜晚

- 用到了一个pdf的隐写工具wbStego4open
- 得到压缩包密码Zip Password: 0mR#012#b3b%s*IW
居然写着No password.pdf, 欺骗感情
- docx的隐写, 改成zip后缀, 然后解压, 拖到sublime的搜索里面, 搜索hgame就有了

```
D:\Download\LastEveningsOnEarth_pAY0Q13w0k4Bhm6tErSOCfcMeyGrZPHo\Last Evenings on
Earth\00000000\word\secret.xml:
1  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2: <flag>hgame{mkLbn8hP2g!p9ezPHqHuBu66SeDA13u1}</flag>

1 match in 1 file
```

玩玩条码

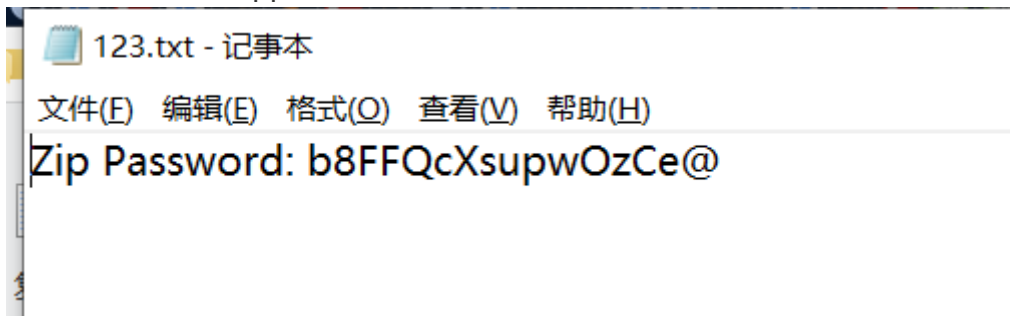
- 有一个JPNPostCode, 肯定要解码的嘛, 狂搜, 没找到什么网站, 手动解码, 一个
一个试



- 既然这个单独给出来了, 我猜测这个就是密码一类的东西
- 给的软件和插件一开始有点看不懂, 查了半天视频隐写稍微我看看可行性还可以的
有.avi后缀的隐写, 于是试了试

license.txt	2004/6/19 20:35	文本文档	3 KB
MSU_stego_video.exe	2006/1/11 11:24	应用程序	130 KB
readme.html	2005/8/10 12:56	Chrome HTML D...	5 KB

用这个软件能得到zippassword



- 里面有个code128

```
Cost 328 ms.  
Found 1 barcode(s) in this file.  
▶ CODE128 hgame{9h7epp1flwIL3fOtsO  
AenDiPDzp7aH!7}  
  
This demo is built with Dynamsoft  
Barcode Reader SDK.  
Get Free Trial >
```

网站解码

后记

自己还是太菜了，时间花的不够多，而且经常进入死胡同，然后挺遗憾web有两道没有做出来，资料都给了，感觉不难了，然后pwn一点没看，re的babypyc环境感觉有点问题，cypto的感觉inv也不难了。但是最后都没有解出来，呜呜呜