HBCTF——WriteUp&&涨姿势（5）

原创

浅零半泣 于 2017-06-18 21:40:31 发布 818 收藏

分类专栏： CTF

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/sinat_34200786/article/details/73440999

版权

CTF 专栏收录该内容

19 篇文章 0 订阅

订阅专栏

WriteUp

1. 葡萄牙-签到

涨姿势

1. 西班牙-666
2. 波兰-父亲的信
3. 法国-四六级查询

葡萄牙-签到

原题

解题思路

```
最深不过套路？
```

WriteUp

```
签到题不用费太多心思，如果做不出肯定是懂的套路不够多
```

```
习惯性右键—源代码，并没有可疑的东西，页面上也没有，那F12看看？
```

GET	base.css	pcat.cc
GET	jquery-1.8.3.min.js	pcat.cc
GET	jquery.marquee.min.css	pcat.cc
GET	index.css	pcat.cc
GET	bg.png	pcat.cc
GET	Museo500-Regular-webfont.woff	pcat.cc
GET	hbctf{console_taolu}.ttf	pcat.cc

http://blog.csdn.net/sinat_34200786

西班牙-666

原题

```
<meta  http-equiv='Content-Type'  content='text/html;charset=utf-8'/>
<title>你会喊666吗？</title>
<?php
error_reporting(0);
require_once('flag.php');
if(!isset($_GET['sss'])){
        show_source('index.php');
        die();
}
$sss=$_GET['sss'];
if(strlen($sss)==666){
        if(!preg_match("/[^0-6]/",$sss)){
                eval('$sss='.$sss.';');
                if($sss!=='0x666'){
                        if($sss=='0x666'){
                                echo  $flag;
                        }
                }
        }
}
?>
```

http://blog.csdn.net/sinat_34200786

解题思路

```
代码审计，绕过就行
```

WriteUp

```
由条件：
1. $sss !== '0x666'
2. $sss == '0x666'
   可知 $sss 的值需要等于数值 0x666，而又不能等于字符串 '0x666'，其中涉及PHP的弱类型比较
3. if(!preg_match("/[^0-6]/",$sss))     $sss 只能包含 0--6 的数字
4. if(strlen($sss)==666)     $sss 的长度等于 666
```

```
通过分析可知我们需要创建一个长度为 666 ，只包含0 -- 6的数字，数值上等于 0x666且不等于字符串 '0x666'的参数，所以我们
```

```
HEX   666
DEC   1,638
OCT   3 146
BIN   0110 0110 0110
```

https://blog.csdn.net/sinat_34200786

```
import requests

url = 'http://pcat.cc/sss/?sss='+'0'*662+'3146'
html = requests.get(url)
print(html.content)
```

```
c\x9f</title>\r\nhbctf{666_sixsixsix}"
```

//blog.csdn.net/sinat_34200786

涨姿势点

```
刚开始看到 if(strlen($sss)==666)时就在想有这么长的url的么？当时直接否定了填充到666个长度的想法。
然后第一个条件想不到办法绕过，然后没有然后了。。
```

波兰-父亲的信

原题

letter.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
/E7U7cTCu6jX5sPJi0TI5871yuKas7rwjJHP69bHtr7KpMTcsM6Ek9PE0qm41cPwu0bK/c7Ewbm50YWixPr
3I6fyqay6Mnh1+bU2rywxNy
+v5qzt2Wz1r6ty0fE7rP963DSt4tE1LvSqcu0yaqxptXavfDT7sHwwPWPUpqz0MSMjcmuxt/S4Mi1x6fQ9
+7jfy1+xTcK30sG94sC00NbWwc+njE/QxLLAzai94rn90euPUr6/ytLBX99ovcy8tLFSw
+7R67TLjJHFxb7olLXD6u6Nte7KzYn02Jq2yNNIy4e8sdTQzajB6rfF0sGRetTQz/vTx8Pwy4e+6MHuj1K
+YyRj1K38rartMjKqbzFx6zT2srisNnQosTA1kL8ToSTwPXA48/N0rm8sMtfjp/rYJDb00jX8Mmuv9XP68
w0068I6fz6e2yMSy1tq3xdDWvZvCt8TAuNXA+9bnyKW8sbW5wb/X49aUzEu17vW10NC+ubW5wNW7pLVL1k
+qlqrV5rXuvujYmsmuuqbPwu1619rBX9TssePN07DZ/E6On765jI3x8dKpyve94rdlw/v0yJVytcKPVtTt
+rbuoi0S94sT5kNu94t2UysXWqre90PSQ29Hr19rUWNiatqu1wsTAvIrTx8PwveTN09ia1+W5/tDQ1LXuj
3vLTUWL34xtXA9bnRv6q+6OBs0evWqtXay4e+6LZZsbHP+73Z0MS0y8u02VnLX8qpvfDH8+16vfjJ4brFy
+7VLyb3H89DdveK6xdPOs/21wtaUj5uxTdfauN+95+BszrS/qtDe0PTPp9f1xfPLtcTut7217snG1+XD7s
+v7nR1LuKqYqp0NC3vZDb0tSw2cesx6fTob340trD8MrSj1LEssj9w+r097bgssDA48m9vcy95MTuu6jWq
+On7GmjI3K/c/Cz6LE7rrF0tTU7bXbvMW4+epBvLHJxs601drI57bg0N7K17jmvLHU2r/W1kLLh8Hu0N3R
G/wPX1tdDE5cjYmstf6o7ZWbTLzNi+rb60ucqaorFN1dq5ysqk0qmy6NLU1LXSwcrSxMLHp9K3saaOn8u1
```

解题思路

```
与佛论禅
```

WriteUp

怎么看都是Base64，先解开这个，但解出来乱码

编码　解码　解码结果以16进制显示

Base64编码或解码结果：

http://blog.csdn.net/sinat_34200786

回想起题目，这应该是中文写的信，那么应该还要GBk编码，然后在用 '与佛论禅' 来解密

```
from base64 import *                #引用自某人（作者没署名）
with open('letter.txt','r') as L:
    a = L.read()
    b = b64decode(a)
    c = b.decode('GBK').encode('utf-8')
    with open('out.txt','wb') as out:
        out.write(c)
```

将解出来的中文解密即可

涨姿势点

法国-四六级查询

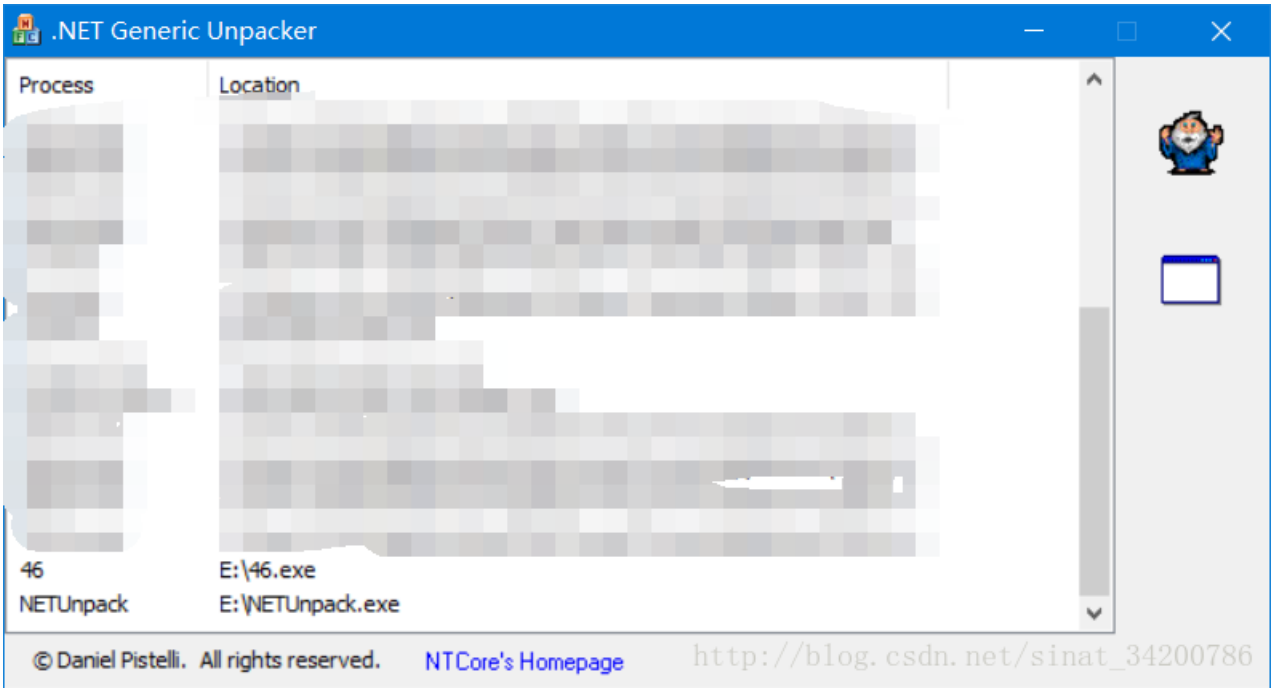
原题

解题思路

```
划一下逆向的水，壳是混淆过的，用PEID等无法直接查出，我怎么知道什么壳的？我看了WP
```

WriteUp

```
其实是 .net 的壳，直接上工具就好了
先打开46.exe，然后打开工具选择46.exe，点一下那个老头就行
```



名称	修改日期	类型	大小
Unpacked_1.exe	2017/6/18 21:28	应用程序	131 KB
Unpacked_2.dll	2017/6/18 21:28	应用程序扩展	6 KB
Unpacked_3.dll	2017/6/18 21:28	应用程序扩展	6 KB
Unpacked_4.dll	2017/6/18 21:28	应用程序扩展	6 KB
Unpacked_5.exe	2017/6/18 21:28	应用程序	24 KB
Unpacked_6.exe	2017/6/18 21:28	应用程序	24 KB
Unpacked_7.exe	2017/6/18 21:28	应用程序	24 KB
Unpacked_8.exe	2017/6/18 21:28	应用程序	131 KB
Unpacked_9.dll	2017/6/18 21:28	应用程序扩展	6 KB
Unpacked_10.exe	2017/6/18 21:28	应用程序	24 KB

http://blog.csdn.net/sinat_34200786

```
随便选一个exe扔进ILSpy
```

```
ivate void button1_Click(object sender, EventArgs e)

  string text = this.textBox1.Text.Trim();
  if (text.Length > 0 && text.Length < 7)
  {
      Random random = new Random();
      int num = random.Next(425, 710);
      MessageBox.Show(string.Format("{0}同学，你的分数为{1}。", text, num));
      if (num == 666)
      {
          MessageBox.Show("flag is aGJjdGZ7Z29vZF9sdWNrX3RvX3V9");
      }
  }
```

http://blog.csdn.net/sinat_34200786

涨姿势点

ILSpy工具的简单使用