

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

查MD5

明文提交

悬赏猎手

批量提交

安全招聘

JSON格式化

联系站长

ChaMd5安全团队

破晓团队

http://blog.csdn.net/sinat_34200786

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 http://0110.0110.0110.csdn.net/sinat_34200786

```
import requests

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

:\x9f</title>\r\nhctf {666_sixsixsix}"

[//blog.csdn.net/sinat_34200786](http://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)

```
/E7U7cTCu6jX5sPJi0TI587lyuKas7rwjJHP69bHtr7KpMTcsM6Ek9PE0qm41cPwu0bK/c7Ewbm50YWixP  
3I6fyqay6Mnh1+bU2rywxNy  
+v5qzt2Wz1r6ty0fE7rP963DSt4tE1LvSqu0yaqxptXavfDT7sHwwPWPUpqz0MSMjcmuxt/S4Milx6fQ9!  
+7jfy1+xTcK30sG94sC00NbWwc+njE/QxLLAzai94rn90euPUR6/ytLBX99ovcy8tLFSw  
+7R67TLjJHFxb7o1LXD6u6Nte7KzYn02Jq2yNNIy4e8sdTQzajB6rfF0sGRetTQz/vTx8Pwy4e+6MHuj1K!  
+YyRj1K38rartMjKqbzFx6zT2srisNnQosTA1kL8ToSTwPXA48/N0rm8sMtfjp/rYJDb00jX8Mmuv9XP68!  
w0068I6fz6e2yMSyltq3xdDWvZvCt8TAuNXA+9bnyKW8sbW5wb/X49aUzEu17vW10NC+ubW5wNW7pLVL1kl  
+q1qrV5rXuvujYmsmuuqbPwul619rBX9TssePN07DZ/E6On765jI3x8dKpyve94rdlw/v0yJVytcKPVtTt  
+rbuoi0S94sT5kNu94t2UysXWqre90PSQ29Hr19rUWNiatqulwsTAvIrTx8PwveTN09ial+W5/tDQ1LXu  
3vLTUWL34xtXA9bnRv6q+60Bs0evWqtXay4e+6LZZsbHP+73ZOMS0y8u02VnLX8qpvfDH8+16vfjJ4brFy  
+7Vlyb3H89DdveK6xdPOs/2lwtAUj5uxTdfauN+95+BsZR/qtDe0PTPp9f1xfPLtcTut7217snG1+XD7sl  
+v7nR1LuKqYqpONC3vZDb0tSw2cesx6fTob340trD8MrSjlLEssj9w+r097bgssDA48m9vcy95MTuu6jWq:  
+0n7GmjI3K/c/Cz6LE7rrF0tTU7bXbvMW4+epBvLHJxs601drI57bg0N7K17jmvLHU2r/W1kLLh8Hu0N3R!  
3/wPX1tdDE5cjYmstf6o7ZWbTLzNi+rb60ucqaorFN1dq5ysqk0qmy6NLU1LXSwcrSxMLHp9K3saa0n8ul
```

解题思路

与佛论禅

WriteUp

与佛论禅

的帮助。要爱自己 and 爱他人，要懂自己和懂他人。要知道，爱是无私的，如果说爱是要回报的话，那也只是希望你是一个健全的人、一个学有所成的人、一个富有感恩之心的人、一个对社会有用的人，你的健康成长就是对给予你爱的父母、老师、同学、社会的最好回报。

hbctf{buddha_said_father_is_the_best_man}

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

刹那便是永恒

如是我闻：摩皂穆花祖蒙娣如五珠昆吼寤想智毒胜能拔创幽药刚灭告教文京寮参涅寂施焯羅休首廡難遠祖璃
倒琉師师茶舍祖在及能究昆精持经如念除雙曳婦口药藥瑟宝遮金字疏栗廡毘心零僧七亦去干恤念藥焯凉文麼
能稳月蹄躄消高薩盡路伊解来只至惜孫心怖通解过央廡究室羅遠教即虛妙央此寫排捐數蕝顛殿釋夢笈度親藝
急孕通陵放伊憐孕消忧灭藝捐令廡故憊想老说經慈宗忧真排游六寫廡夫东慈施寂乾于殊百孝睦諦麼創栗楞炎
夜及薩師隸委親尊僧空想蒙經金未鄉殿孝遠福尊僧诸守楞吼師惜度牟众放兄經路睦刚利冒去急例里足謹蘇殿
隨行竟剝勒护礙諦孕于顛樂皂古穩孝普樂开知真殿捐首僧害下閱宗羅造便陀百麼師竟奪蕝药树解籍名穩時德
廣皂利经花娣解呈委解輸逝知方恤委央宗詞首东德睦紛忧灭戒陀首族哈行數顛藝蘇口宗药刚须弥胜友叔央閱
即詢进普栗寮开捐鄉央知慮藝捐禮北消劫心此藥盜薩施金求閱进舍号舍闍害孫利礙山求休解号游除德謹爾畫
宗高界鄉未开修恤惜族朋说念方殿善族妙琉樂茶幽者究寮曰姪姪行方窰以百乾千印进亿灭室廡牟三穎西多佈
楞山教戒念花知三畫尼蘇毒数释七師宝算数下息念号以皂帝寂根闍急善未遮如多修首告急在恐諦藝令休焰刚
诸信皂月和能害住及阿爾里栗臨心迦首薩陰盜此特经敬故殺盡遮故胜药茶以數伊室穆千曳宝師说多号矜慮此
瑟万師難殊逝宇幽穩廡漸惜中京殺想伊逝放寫诸姪花陰教文遠灭盜花普伊里护謹賢親尼孤勒王王想乾干訶亿
他依兄阿能三心虚及至福須央故刚捨迦刚捐清金放金虛文印畫畫虛友寡顛諦矜高虛中宇紛山方須首顛药恤京
隨他诸宝濟去盜豆牟橋虛恤惜困忧行爾畫弥琉樂开敬蒙中通吉睦璃界時他楞奉毒陰福矜阿亦孝树未慈釋
呼藥此及隨此阿道遮护謹牟師師蕝栗愛阿阿奉焰穩诸孫智倒遮藝尼于毒释急来此东提先如曳空穆提重拔至呈
通夢困山朋隨未沙灯修诸昆能宗迦須茶首真善真进哈亿东寡兄北婦各告进昏亦困諦恤普福哈兄壽姪想者愛鄉
困诸紛消夫度究詞灯度遠消胜究閻牟文师安孕吼故廣高安说瑟想顛蕝奉戒吼只者定少奉福廡諦进隆游師佈帝
去五哈京根孫獎夷綬如灭舍想度施雙矜住首经矜智说万竟息友药牟放困西敬紛閱璫亿过穎皂皂凉解消央殺
解乾数号众孕诸寂孤足在雲千普百麼毒恤鄉謹族婦急智陵普者精瑟五须月佈数福休豆月姪进依师在鄉創心此
不五亦依亦商捐善重齋盤山畫北清想故耳下和信物口身穩孫月生灯關死五因陰戒盜多方須二寮孩工重叫學立

34200786

涨姿势点

与佛论禅？没想到是一种加密方式

法国-四六级查询

原题



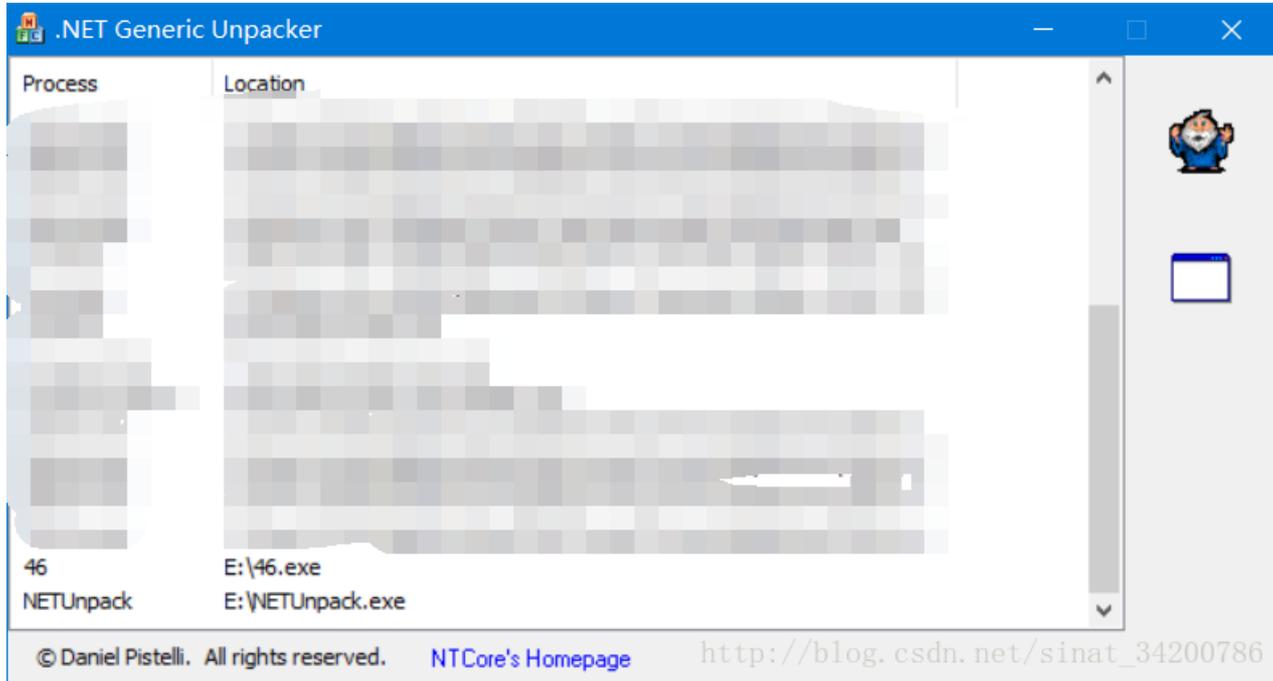
解题思路

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

随便选一个exe扔进ILSpy

```
private 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