2019 DDCTF 部分writeup

转载

weixin_30794499 于 2019-05-11 20:28:00 发布 25 收藏
原文链接：http://www.cnblogs.com/cnnnnnn/p/10849910.html

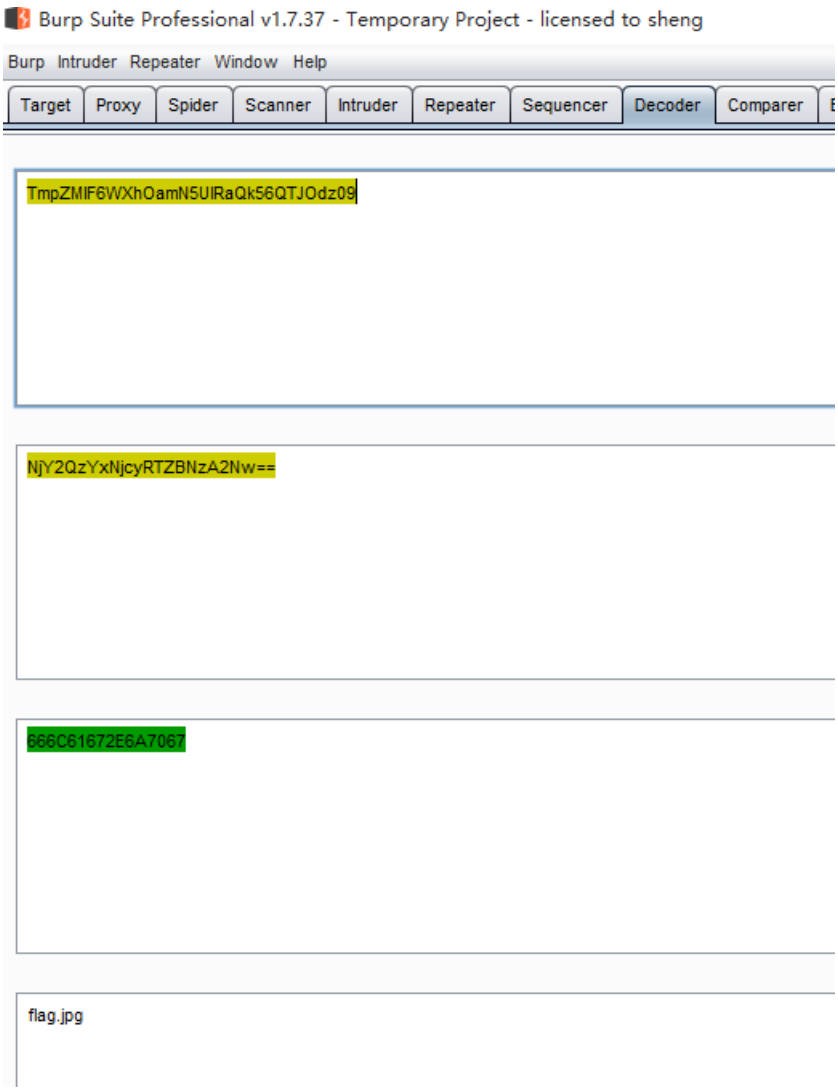
网上的wp已经很多了，但wp普遍很简略。我尽量写的详细一点。

一、WEB

滴~

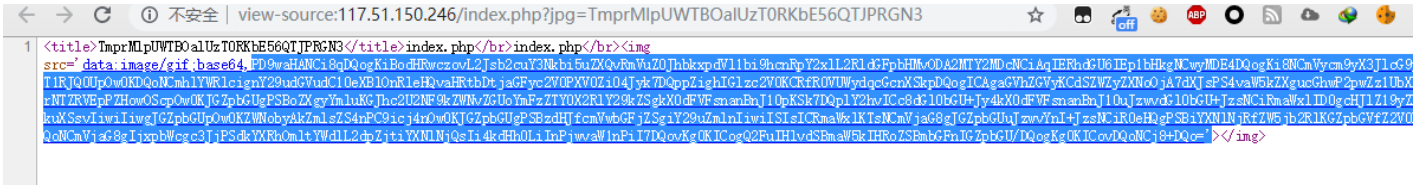
拿到题目后首先右键查看源代码，发现图片是以base64传送的

而且看url发现里面应该是包含了文件名，并且用了某个编码。测试过后是转16进制ascii码后两层bases64



（解码工具是burpsuite）

用同样的规则编码index.php，为TmprMlpUWTBOalUzT0RKbE56QTJPRGN3，访问并查看源代码，内容就是index的源码了，再用base64解码。



明文:

```
<?php
/*
 * https://blog.csdn.net/FengBanLiuYun/article/details/80616607
 * Date: July 4,2018
 */
error_reporting(E_ALL || ~E_NOTICE);


header('content-type:text/html;charset=utf-8');
if(! isset($_GET['jpg']))
    header('Refresh:0;url=./index.php?
jpg=TmpZMlF6WXhOamN5UlRaQk56QTJOdz09');
$file = hex2bin(base64_decode(base64_decode($_GET['jpg'])));
echo '<title>'.$_GET['jpg'].'</title>';
$file = preg_replace("/[^a-zA-Z0-9.]+/","", $file);
echo $file.'</br>';
$file = str_replace("config","!", $file);
echo $file.'</br>';
$txt = base64_encode(file_get_contents($file));

echo "<img src='".$txt."'></img>";
/*
 * Can you find the flag file?
 *
 */

?>
```

BASE64编码 >

< BASE64解码

BASE64:

```
PD9waHANCi8qDQogKiBodHRwczovL2Jsb2cuY3Nkbi5uZXQvRmVuZ
0JhbkxpdVl1bi9hcnRpY2xlL2RldGFpbHMvODA2MTY2MDcNCiAqIER
hdGU6IEp1bHkgNCwyMDE4DQogKi8NCmVycm9yX3JlcG9ydGluZyhF
X0FMTCB8fCB+RV9OT1RJQ0UpOw0KDQoNCmhlYWRlcignY29udG
VudC10eXBlOnRleHQvaHRtbDtjaGFyc2V0PXV0Zi04Jyk7DQppZighIG
lzc2V0KCRfR0VUWydqcGcnXSkpDQogICAgaGVhZGVyKCdSZWZyZ
XNoOjA7dXJsPS4vaW5kZXgucGhwP2pwZz1UbXBaTWxGNldYaE9hb
U41VWxSYVFrNTZRVEpPZHowOScpOw0KJGZpbGUgPSBoZXgyYm
luKGJhc2U2NF9kZWNvZGUoYmFzZTY0X2RlY29kZSgkX0dFVFsnan
BnJ10pKSk7DQplY2hvICc8dGl0bGU+Jy4kX0dFVFsnanBnJ10uJzwvd
Gl0bGU+JzsNCiRmaWxlID0gcHJlZ19yZXBsYWNlKCIvW15hLXpBLVo
wLTkuXSsvIiwiIiwgJGZpbGUpOw0KZWNobyAkZmlsZS4nPC9icj4nO
0KJGZpbGUgPSBzdHJfcmVwbGFjZSgiY29uZmlnIiwiISIsICRmaWxlKT
sNCmVjaG8gJGZpbGUuJzwvYnI+JzsNCiR0eHQgPSBiYXNlNjRfZW5j
b2RlKGZpbGVfZ2V0X2NvbnRlbnRzKCRmaWxlKSk7DQoNCmVjaG8g
IjxpbWcgc3JjPSdkYXRhOmltYWdlL2dpZjtiYXNlNjQsIi4kdHh0LiInPjwv
aW1nPiI7DQovKg0KICogQ2FuIHlvdSBmaW5kIHRoZSBmbGFnIGZpb
GU/DQogKg0KICovDQoNCj8+DQo=
```

在源代码里出现一篇文章，打开后发现是一篇关于echo的，我在这里绕了很长时间，以为要用到echo的漏洞。

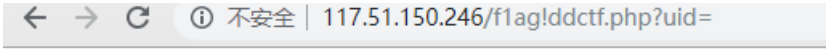
但正解是那个日期，要看那个日期的文章。是关于swp的：

https://blog.csdn.net/FengBanLiuYun/article/details/80913909

所以访问http://117.51.150.246/practice.txt.swp，可看到里面内容：

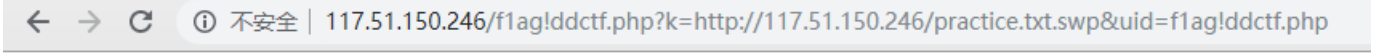
```
f1ag!ddctf.php
通过index代码，可以看到对文件名做了过滤，只能是数字和字母。这个感叹号会被去掉。但还有一句

$file = str_replace("config","!", $file);
这是为了防止读取config，会把config换成！。但这正好满足需求，访问f1ag!ddctf.php
即可。但直接访问是空白的，所以用同样的方法读源代码
```

extract($_GET);这里是一个变量覆盖漏洞，让k和uid为空就可以了。



DDCTF{436f6e67726174756c6174696f6e73}

或者按正常使用，把k指向一个文件，uid和文件内容相同，也能读出flag：



DDCTF{436f6e67726174756c6174696f6e73}

之前的swp文件这里可以现成使用，没必要自己搭个网站让他读。。有些wp就是自己现搭的网站，算是很鬼畜了。。

reverse

【待续】

转载于:https://www.cnblogs.com/cnnnnnn/p/10849910.html