




巅峰极客第一场CTF部分writeup

原创

郁离歌  于 2018-07-22 20:49:13 发布  5535  收藏 2

分类专栏: [CTF-WRITE-UP](#) 文章标签: [writeup](#) [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/like98k/article/details/81158636>

版权



[CTF-WRITE-UP](#) 专栏收录该内容

23 篇文章 4 订阅

订阅专栏

额, 上午驾校学车, 中午打了会儿安恒的月赛, 就来看巅峰极客的题了。时间关系实力原因没做几个emmmm太菜了wa

MISC-warmup-100pt

拿到一个bmp文件, 套路走一波, 右键查看属性emmm啥都没有。

丢到winhex里面也没有什么明显的提示或者信息。

放大招: stegsolve。放在各个颜色通道里面过一遍。

可以明显的看到每个颜色通道的最低位有异常数据。

将数据提取出来

前两个ook解码, 第三个brainfuck解码之后拼接起来就是flag。

在线解密网址: <https://www.splitbrain.org/services/ook>

flag{db640436-7839-4050-8339-75a972fc553c}

MISC-LOLI-150pt

拿到一张文件后缀是png但是实质是jpg的图片。看起来像是二维码。扫一下发现:

tips:255

255是啥意思呢? 当时就想到最低位, 像素点之类的词汇。放到stegsolve里面跑一下也没发现什么端倪。

最后题目给出提示:0xff

这里有点脑洞了, 将图片转16进制和0xff异或, 也就是将图片的16进制取反。

这里我直接用winhex的异或功能, [《用winhex进行一步异或》](#)

然后可以找到里面有一张小png图片，最后还有一个black and white 的字符串。

图片由黑点和白点组成。但是就想到了二进制，像素点再转为二进制再转ascii码。

flag{e0754197-e3ab-4d0d-b98f-96174c378a34}

WEB-simple cms-300pt

OneThink v1.1的洞。利用点是缓存文件getshell。他会把成功登陆的用户名记录在一个缓存文件中，这里会导致被getshell。

百度做题233333333

[https://www.google.com.hk/search?](https://www.google.com.hk/search?safe=strict&ei=zXIUW__pN8HO0gTcipOoDg&q=onethink+%E4%BA%8C%E6%AC%A1%E5%BC%80%E5%81ab.3...25667.31353.0.31641.21.18.2.0.0.0.419.2617.0j6j5j0j1.12.0...0...1c.1.64.psy-ab..9.1.418...0i30k1.0.YJKBf-VnArQ)

[safe=strict&ei=zXIUW__pN8HO0gTcipOoDg&q=onethink+%E4%BA%8C%E6%AC%A1%E5%BC%80%E5%81ab.3...25667.31353.0.31641.21.18.2.0.0.0.419.2617.0j6j5j0j1.12.0...0...1c.1.64.psy-ab..9.1.418...0i30k1.0.YJKBf-VnArQ](https://www.google.com.hk/search?safe=strict&ei=zXIUW__pN8HO0gTcipOoDg&q=onethink+%E4%BA%8C%E6%AC%A1%E5%BC%80%E5%81ab.3...25667.31353.0.31641.21.18.2.0.0.0.419.2617.0j6j5j0j1.12.0...0...1c.1.64.psy-ab..9.1.418...0i30k1.0.YJKBf-VnArQ)

这里有几个关键点。

- a: 缓存文件路径。
- b: 用户注册成功并成功登陆。
- c: 注册登陆须每次抓包url解码后再发包回去

参考链

接:<http://www.admintony.com/AWD%E8%A5%BF%E7%9F%B3%E6%B2%B9%E7%BA%BF%E4%B8%8B%E>

第一点：扫目录得到www.zip下载源码，本地搭起来环境之后得到目录：/Runtime/Temp/onethink_6d11f0be3af9c28d4120c8fd5fe65a40.php

第二点：注册两个用户 %0d%0a\$x=\$_GET[X];//和%0d%0aeval(\$x);//

第三点：每次注册和登陆在发包的时候URL-encode 必须勾选上再提交，否则会把换行符的url-encode当成字符串来处理。登陆的时候也需要抓包，在用户名前面加上换行符的URL-encode，且勾选上URL-encode

getshell拿flag。

payload: /Runtime/Temp/onethink_6d11f0be3af9c28d4120c8fd5fe65a40.php?X=system('cat /tmp/flag');