

BUUCTF——MISC(一)

原创

Ki10Moc 于 2021-06-05 13:58:18 发布 121 收藏

分类专栏: [BUUCTF](#) 文章标签: [其他](#) [恰饭](#)

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/m0_52367015/article/details/117201860

版权



[BUUCTF 专栏收录该内容](#)

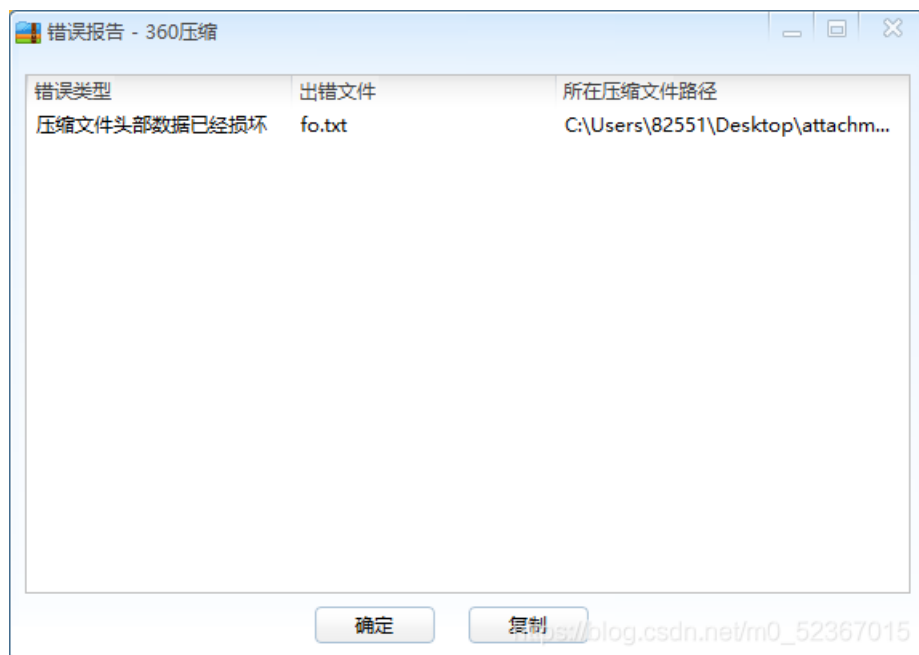
1 篇文章 0 订阅

订阅专栏

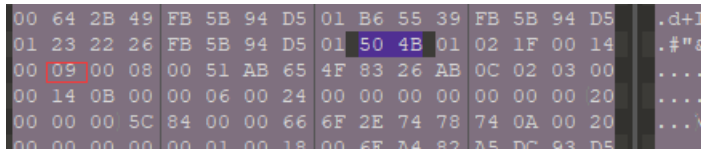
佛系少年

下载附件

提示txt文件头部损坏



拖进010或者winhex



找到txt模块

将这里的09修改为00

打开txt

最下面一行得到佛曰密文

佛曰：遮等諳勝能礙幡藐哆娑梵迦侄羅哆迦梵者梵楞蘇涅侄室實真鉢朋能。奢怛俱道怯都諳怖梵尼怯一罰心鉢謹鉢薩苦奢夢怯帝梵遠朋陀諳陀穆諳所訥知涅侄以薩怯想夷奢醜數羅怯諸

解密：通往新世界



心不动，万物皆不动

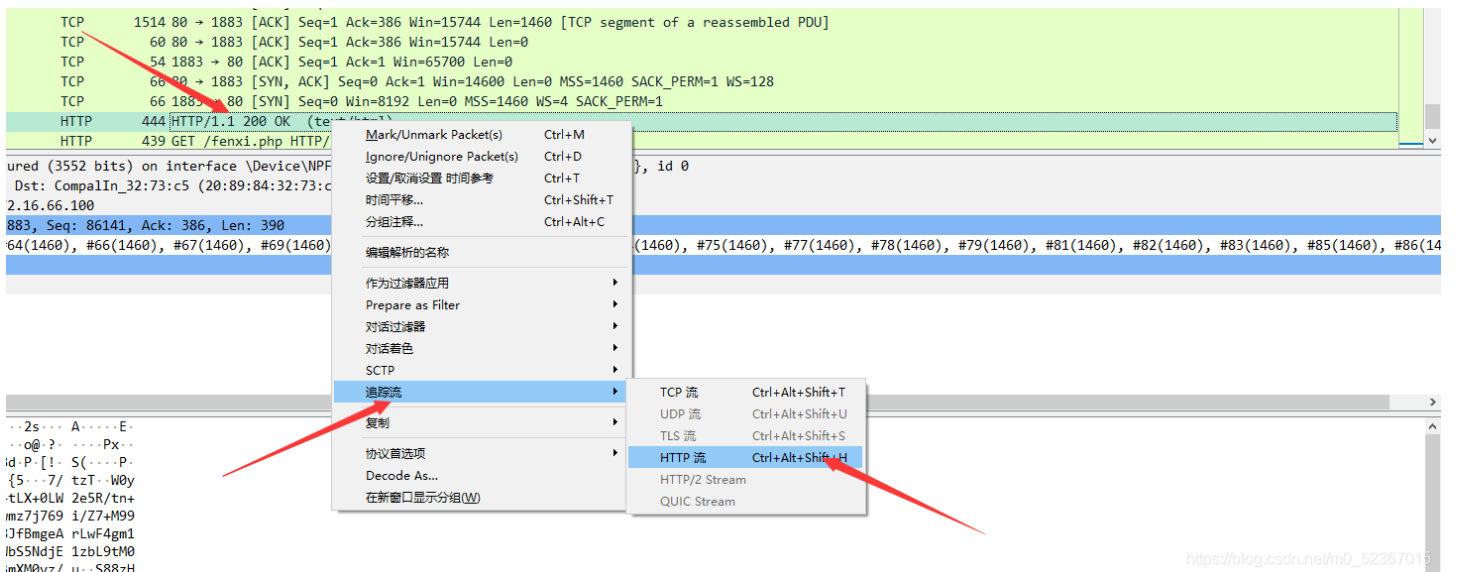
佛曰：遮等諳勝能礙幡藐哆娑梵迦侄羅哆迦梵者梵楞蘇涅侄室實真鉢朋能。奢怛俱道怯都諳怖梵尼怯一罰心鉢謹鉢薩苦奢夢怯帝梵遠朋陀諳陀穆諳所訥知涅侄以薩怯想夷奢醜數羅怯諸

https://blog.csdn.net/m0_52367015

数据包中的线索

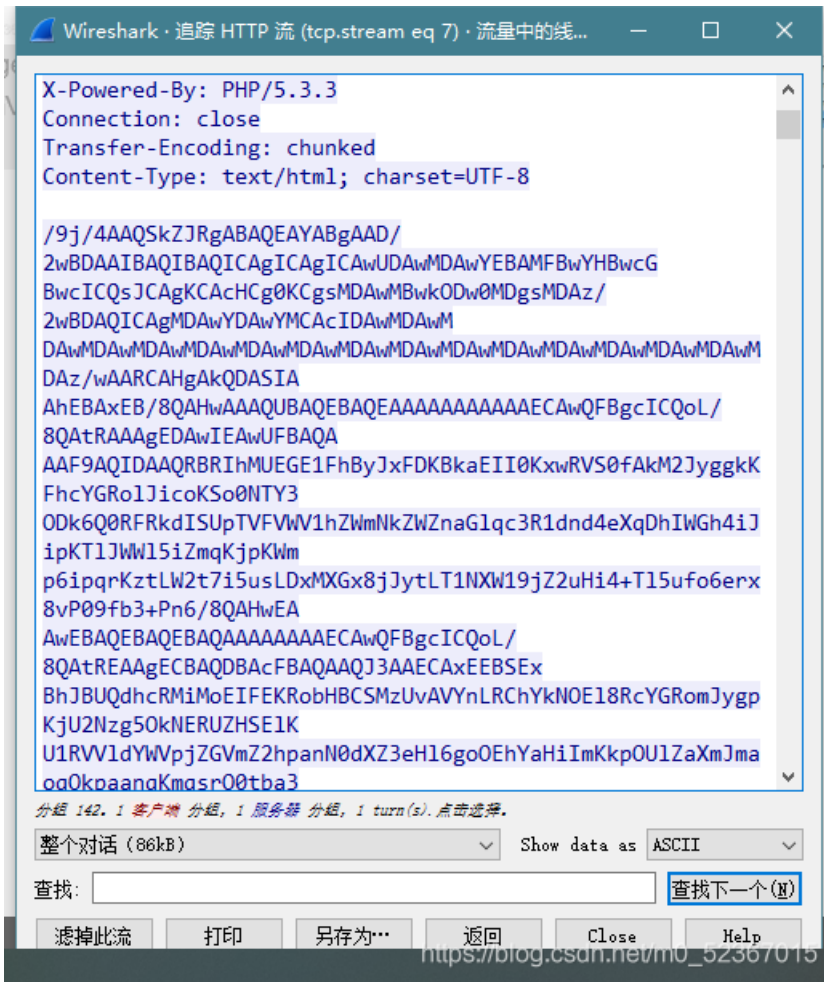
拖进wireshark

过滤http



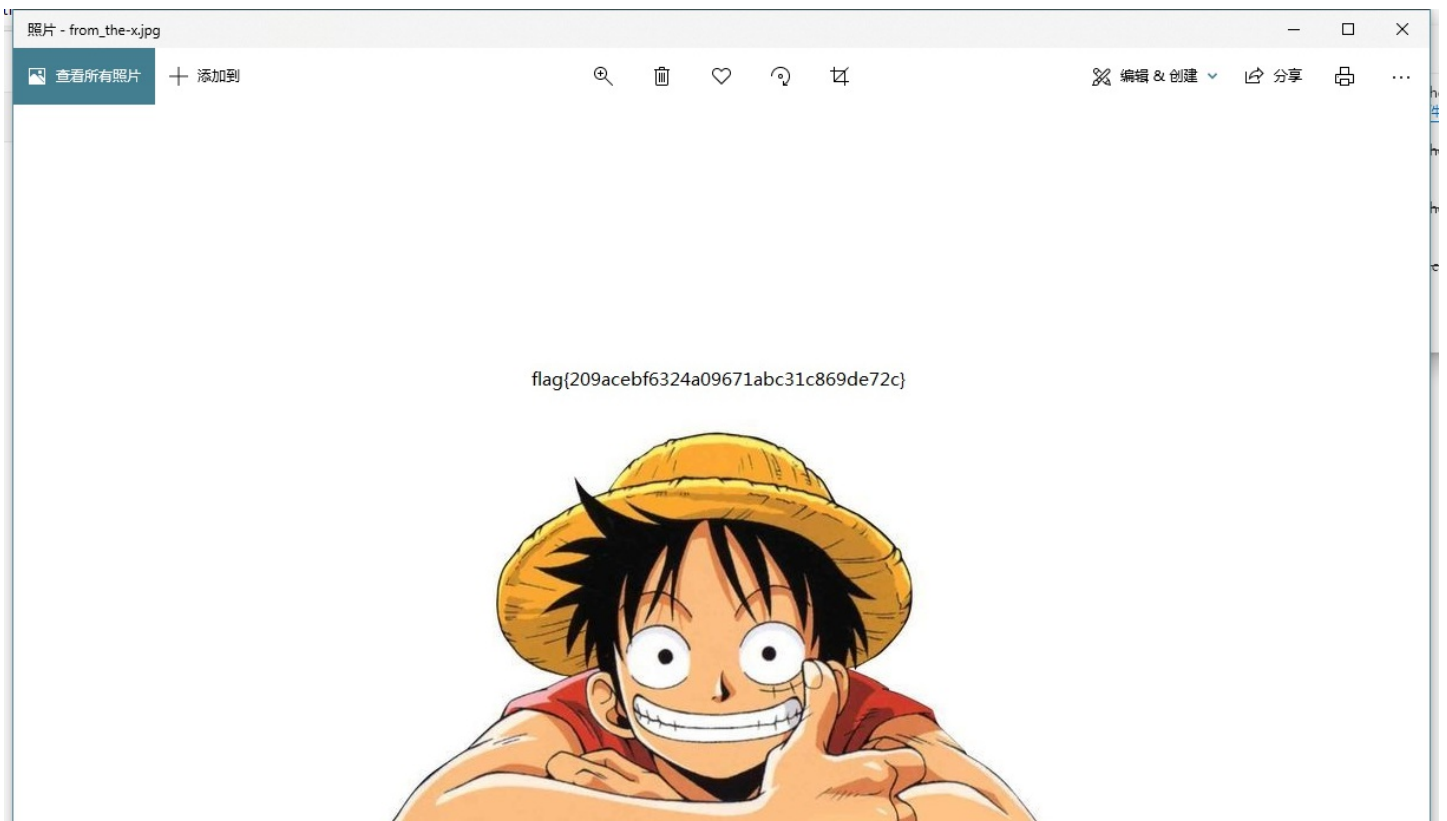
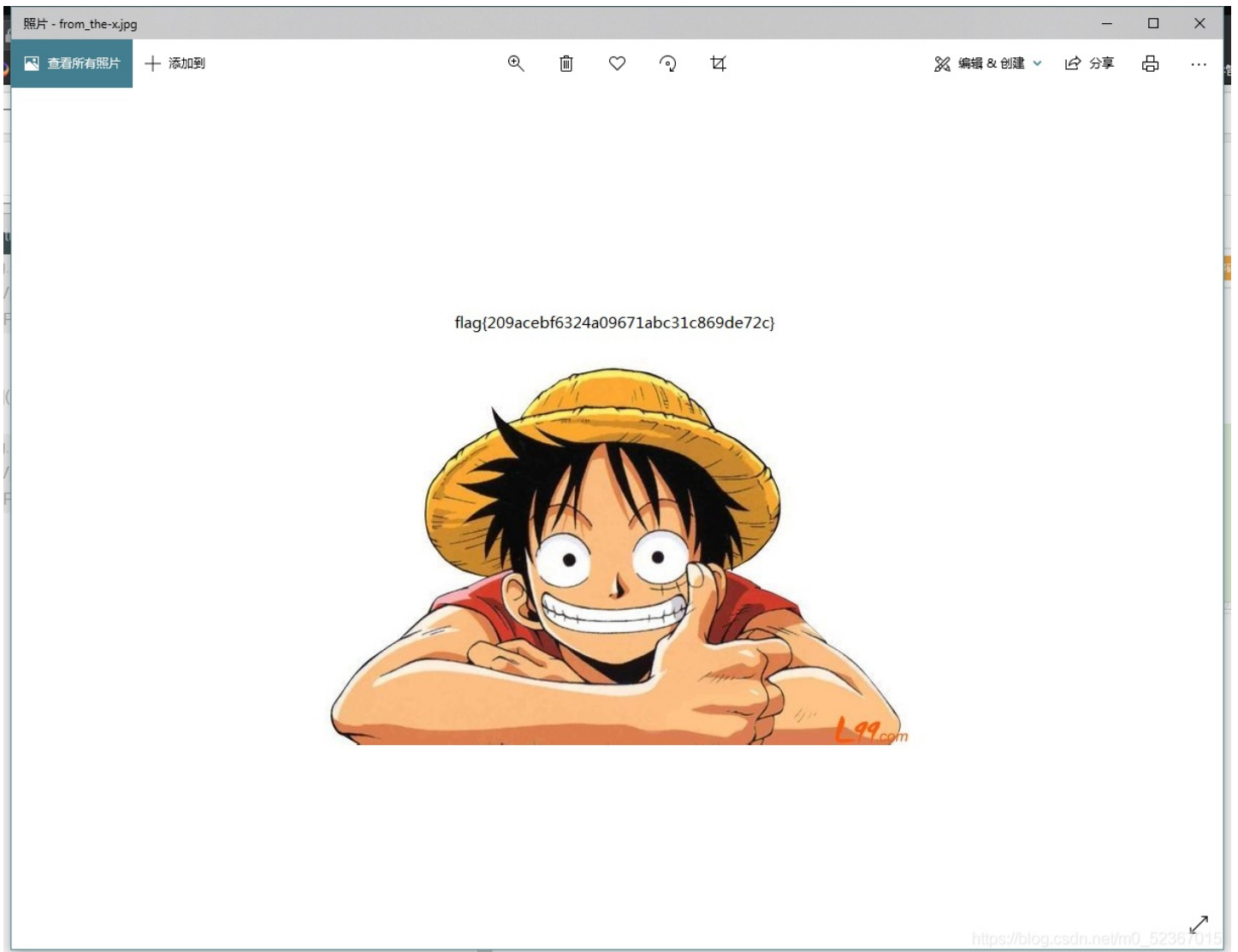
https://blog.csdn.net/m0_52367015

发现密文



base64解码: <https://the-x.cn/base64>







后门查杀

D盾 Web 查杀 远离木马骚扰
使用代码分析引擎，能追查更为隐藏的后门行为，让你网站运行于安全状态

扫描位置: C:\Users\82551\Desktop\html

文件	级别	说明	大小	修改时间	验证值
C:\Users\82551\Desktop\html\phpinfo.php	1	关键字:phpinfo()	22	2013-09-05 01:32:14	2EABF016
C:\Users\82551\Desktop\html\web.php	3	可疑引用:[\$GET["act"] "php"]	41	2013-09-05 01:31:50	7CA8BF1F
C:\Users\82551\Desktop\html\include\include.php	6	多功能木马	58057	2015-07-09 17:08:21	AA216E4D
C:\Users\82551\Desktop\html\install\index.php	1	写入参数:isfile_config...\$p...	7043	2013-06-30 05:17:44	1936BD3A

```
ob_start();
$mtime = explode(' ', microtime());
$starttime = $mtime[1] + $mtime[0];
define('SA_ROOT', str_replace('\\', '/', dirname(__FILE__)).'/');
define('SELF', $_SERVER['PHP_SELF'] ? $_SERVER['PHP_SELF'] : $_SERVER['SCRIPT_NAME']);
define('IS_WIN', DIRECTORY_SEPARATOR == '\\');
define('IS_GPC', get_magic_quotes_gpc());
$dis_func = get_cfg_var('disable_functions');
define('IS_PHPINFO', (ereg("phpinfo", $dis_func) ? 1 : 0));

if (IS_GPC) {
    $_POST = s_array($_POST);
}
$P = $_POST;
unset($_POST);
/*===== 程序配置 =====*/

//echo encode_pass('angel');exit;
// 如果需要密码验证,请修改登陆密码,留空为不需要验证
$pass = '6ac45fb83b3bc355c024f5034b947dd3'; //angel

//如您对 cookie 作用范围有特殊要求,或登录不正常,请修改下面变量,否则请保持默认
// cookie 前缀
$cookiepre = "";
// cookie 作用域
$cookiename = "";
// cookie 作用域
$cookiename = "";
// cookie 作用域
$cookiename = "";
```

神秘龙卷风

爆破

密码: 5463

Terminal:

```
flag [e4bbef8bdf9743f8bf5b727a9f6332a8] ħ
```

Program code:

Advanced Run again Pause Close terminal

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

https://blog.csdn.net/m0_52367015

[ACTF新生赛2020]outguess

核心价值观编码

社会主义核心价值观：富强、民主、文明、和谐；自

abc

公正民主公正文明公正和谐

https://blog.csdn.net/m0_52367015

```
^C  
flag在哪?  
你Guess一下啊!
```

根据hint
guess一下

```
the default is on.  
root@kalisf:~/桌面# outguess -k 'abc' -r mmm.jpg flag.txt  
Reading mmm.jpg...  
Extracting usable bits: 17550 bits  
Steg retrieve: seed: 93, len: 23  
root@kalisf:~/桌面#
```

得到

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)  
ACTF{gue33_Gu3Ss!2020}  
|
```