




超菜鸟级ctf

原创

恋物语战场原  于 2019-04-27 15:44:23 发布  2713  收藏 22

分类专栏: [CTF](#) 文章标签: [ctf 简单](#)

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_26406447/article/details/89602601

版权



[CTF 专栏收录该内容](#)

16 篇文章 7 订阅

订阅专栏

超菜鸟级ctf

前言

大佬们为我这些菜鸟准备的ctf平台来练习(紧抱大佬的腿), 特意为没打过ctf的我们准备了一些超级基础的题来开启我们的第一次ctf之旅...

一共只有6道题吧, 一个半小时左右, 真的是超简单, 结果做的真的是...

下面凭我个人的感觉由简到难的回忆一遍吧

题目

抽屉没锁

这是一道文件上传题, 也是我点开6道题后最先入手的

我的抽屉没有锁, 什么都可以放进来

请选择一个要上传的图片:

选择文件 未选择任何文件 上传

https://blog.csdn.net/qq_26406447

进到页面一看就很直接的会想文件上传漏洞, 真的是第一次玩ctf, 拿到题后瞬间出现的念头是去找张图片与一句话木马copy一下...首先都没有试下有没有过滤就直接考虑的很后面了, 其次即使是要上传图片没文件包含漏洞怎么执行了???, 最后copy命令忘了... (copy x.jpg/b+y.php/a z.jpg)

哎, 后面反应过来直接上传了一个一句话木马的php, flag就弹出来了...没错都不需要菜刀连接

(这里上传个空php文件都会弹flag, 主要考察有没有认识文件上传漏洞吧, 这里传jpg/png文件返回的反而是路径)

图片

拿到第二道题，我一下就懵逼了...这是要考隐写吗??? 这真是为难我胖虎啊...完全不会啊

小明给了我一张图片，可是我却不知道是什么意思



https://blog.csdn.net/qq_26406447

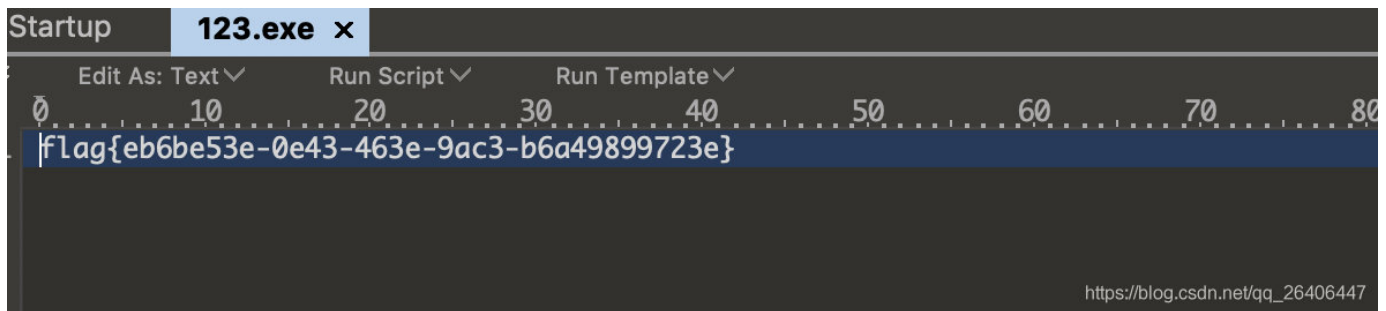
但是将这张图片下载下来，放入文本编辑器后，神奇的事情就发生了

```
▼ Edit As: Hex ▼ Run Script ▼ Run Template ▼
  0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
4:5C80h: E6 AC 16 C0 B8 2C 53 2D 11 F8 45 18 9D 0F 33 5D æ~.À.,S-.øE...3]
4:5C90h: EE 86 C7 13 45 4D 9A B3 86 08 97 71 EA 47 D3 6D î†Ç.EMš³+.-qêGÓm
4:5CA0h: C2 17 A5 96 37 17 83 22 8C 86 99 3A A7 50 26 55 Â.¥-7.f"€†™:SP&U
4:5CB0h: EB 61 34 98 C9 68 8F 67 5F 79 C8 47 36 2A 93 9C ëa4~Éh.g_yÈG6*"œ
4:5CC0h: 94 4A B2 52 F0 8E FA 30 9C CF 67 36 CA 66 49 04 "J²Rðžú0œİg6ÊfI.
4:5CD0h: 28 AE 63 5D 4B E7 01 65 EC 94 E6 AA D8 94 C8 EF (@c]Kç.ei"æªø"Èi
4:5CE0h: BF AA D0 4E 06 6E 1A 6C 99 BE 27 EC 9A B6 E2 A4 ;ªDN.n.l™³'İšŹâµ
4:5CF0h: 8C 98 36 BC 7A 7E 0A E2 EC 23 90 7B DF D3 DF BD €~6¼z~.âi#. {ßÓß½
4:5D00h: 2B 53 1F 2D 3B 4E F3 30 AA B9 0D E6 FE 3F F8 4B +S.-;Nó0ª¹.æp?øK
4:5D10h: 82 D3 98 85 CA A2 00 00 00 00 49 45 4E 44 AE 42 , Ó~...Èç....IEND@B
4:5D20h: 60 82 0A 3C 21 2D 2D 66 6C 61 67 7B 37 36 66 36 ` , .<! --flag{76f6
4:5D30h: 63 36 61 37 2D 61 62 36 65 2D 34 63 30 65 2D 39 c6a7-ab6e-4c0e-9
4:5D40h: 34 32 65 2D 39 34 65 30 34 65 31 31 64 64 36 63 42e-94e04e11dd6c
4:5D50h: 7D 2D 2D 3E }-->
```

没错，你没看错flag就在最后面...这就跟我们将图片和一句话木马用copy合并一样...这里相当于将图片和flag合并了...
来，给你一个神器

来,给你一个神器

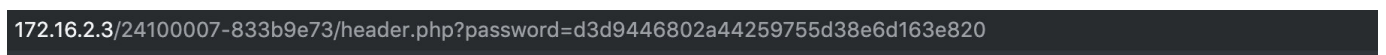
点击神奇之后会下载一个123.exe，这时候我的心又一凉，这是要逆向??? 头大
但说来你不信，将这个exe放入文本编辑器后，神奇的事情又发生了



好直接的flag...

小明的生日

下面来说下这道我觉得坑的不能再坑的题



小明国庆节放完假以后再给三个月就满16了，他父母会给他生日一个惊喜!

这里首先我们要注意他的URL，有password，很自然的想能不能sql注入，首先这里不存在sql注入，其次这里没有回显，那我觉得就没有必要再尝试注入了（主要是注不出来）...但我们发现后面有个md5值...这也是很神奇，在我们打开页面后就有的不是我们输入的，直接扔到md5的网站一查是10...OK，又迷失方向了，然后瞎尝试了一堆数，都没有成功。

其实从上面的一顿瞎操作让我们直接忽视了网络安全中最重要的一点，信息收集。没错我们看页面的文字提示，这时候我们来进行整理信息，国庆节10月，小明生日1月，小明16岁，惊喜...OK我们可以把惊喜理解为flag，前面的md5的10对应10月份，没错我们要输入的是小明生日，也就是1的md5值，是的这样flag就出来了...（这一顿解释我自己都...）

AliBaba

这是一道真逆向题了

敢来挑战吗?



还记得阿里巴巴和四十大盗的故事吗? 聪明的女仆用自己的智慧化险为夷, 救了阿里巴巴一家。你会像这一女仆一样聪明吗? 现在阿里巴巴设计了一个小小的比赛, 你敢来挑战证明一下你自己吗?

提示:
取得比赛题目后, 解答题目即可得到一条线索, 这是你证明自己的凭据, 有礼物哟!

[获取题目](#)

如果你获得了证明自己的凭据, 你就可以拆礼物了!

拆礼物

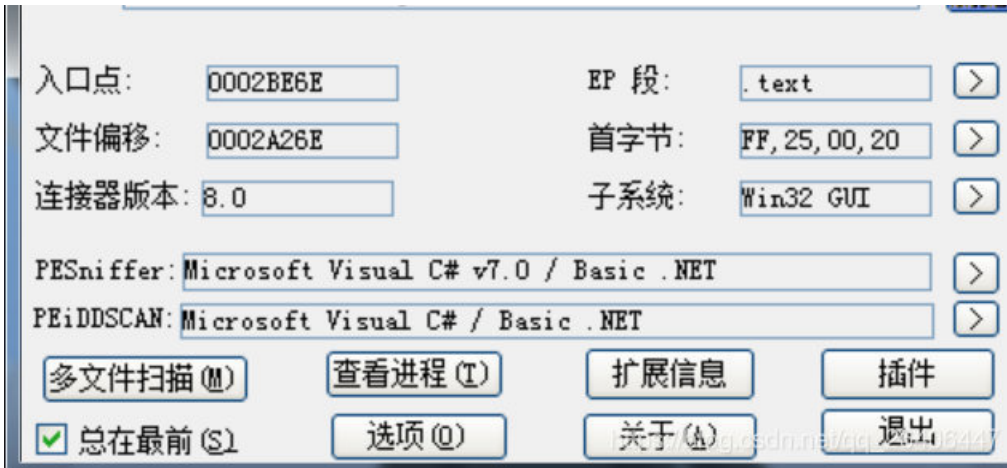
https://blog.csdn.net/qq_26406447

获取题目之后会获得一个ald.zip, 解压后是ald.exe

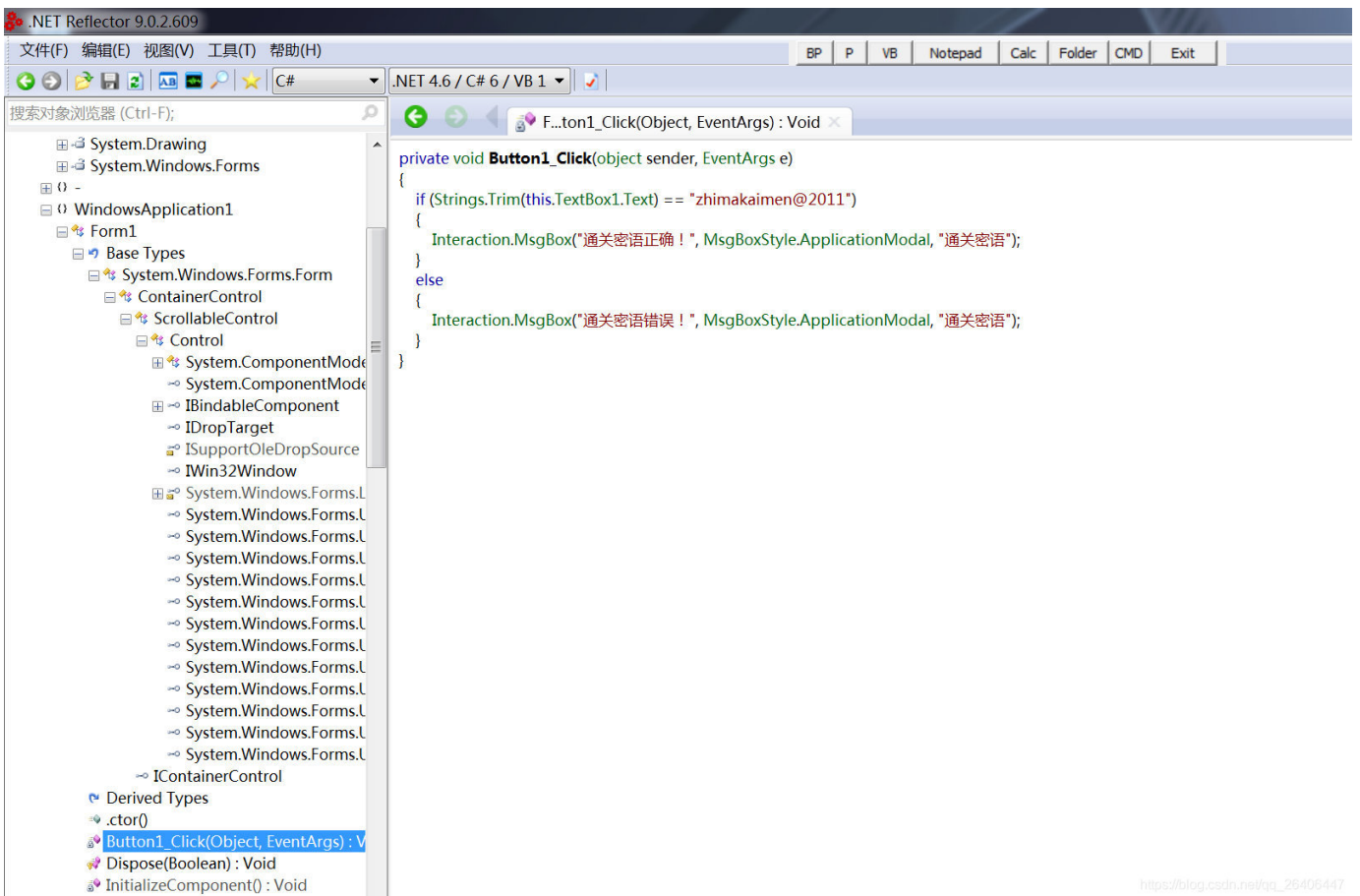


嗯, 我的策略自然是扔进od, 然后找关键字, 但这程序好像不太适合od调, 当然od我也不怎么会用...

经大佬点播, 先用peid查看下程序, 可以发现是个.net程序



大佬告诉我这中.net这种程序直接用NET Reflector来反编译简直爽的不要不要的



可以看到这个逆向工具就很直观了，把程序结构都列出来了，然后我们就很顺利的找到了密码

然后拿这密码去提交就很容易的得到了flag

大草原

这道题是我觉得比较有意思，也是自己有能力做出来，却没有做出来的题（这道题就是一道sql注入题）...

直接打开图片后会进入如下图所示的页面





这里的URL是172.16.2.4/100510015-1f0b4914/

看到下面的输入框，肯定想到了sql注入当然是开始疯狂的注入，手工，sqlmap...结果毫无效果...（事实证明哪里确实也不是注入点），然后审视文字的提示，说到了id，但抓包看了，也没有id字段...

ok，大佬告诉我没有id你自己加一个id去查询啊（没错这里说的用id作为参数去查询...）所以在URL后面加上?id=x，发现页面就跳转到下面的页面了...



这时候已id为注入点会发现非常容易

```
available databases [2]:
[*] information_schema
[*] sql100510015
```

获取数据库名

```
Database: sql100510015
[4 tables]
+-----+
| horse  |
| referers |
| song   |
| uagents |
+-----+
```

恭喜你找到骏马，获得flag{a61ea251-13bc-4f7d-9585-55fe2}

https://blog.csdn.net/qq_26406447

获取表名

```
Database: sql100510015
Table: horse
[3 columns]
+-----+
| Column | Type      |
+-----+
| Where  | varchar(30) |
| id     | int(3)     |
| number | varchar(30) |
+-----+
```

恭喜你找到骏马，获得flag{a61ea251-13bc-4f7d-9585-55fe2}

https://blog.csdn.net/qq_26406447

获取字段名

```
Database: sql100510015
Table: horse
[1 entry]
+-----+
| id | number | Where  |
+-----+
| 1  | five   | lakeside |
+-----+
```

恭喜你找到骏马，获得flag{a61ea251-13bc-4f7d-9585-55fe2}

https://blog.csdn.net/qq_26406447

获取数据

OK可以看到sqlmap十分顺利，这时候将这三个参数带入就能拿到flag了...

总结

这也是自己第一次玩ctf吧感触还是蛮多的

1. 首先是自己能力的不足吧，很多东西都不怎么会，会的东西吧不熟...
2. 其次是思路不清晰，没有一个很好的解题思路，整体十分混乱，至少要做到由易至难的思考吧...
3. 对信息收集的不重视，很多题都没有注意它的提示信息就开始瞎搞，众多大佬都说过，网络攻防（渗透）的核心是信息的收集，自己对信息收集太过轻视