

从CTF比赛真题中学习压缩包伪加密与图片隐写术，最新阿里P7技术体系

原创

开源Python 于 2022-03-21 14:08:28 发布 108 收藏

分类专栏: [程序员](#) 文章标签: [面试](#) [经验分享](#) [开发语言](#)

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_68313184/article/details/123634326

版权



[程序员 专栏收录该内容](#)

6 篇文章 0 订阅

订阅专栏

如遇加密压缩包, 在没有密码提示的情况下, 先判断是不是伪加密

最简单的方法就是看十六进制数据, 第一行如果有 **09** 多半就是了

```
简单的png隐写的附件.zip  www.zip
Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15  Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
00000000 50 4B 03 04 14 00 09 00 08 00 44 90 77 50 E7 C0  PK      Eš\R
00000016 8E 6D EA 2E 02 00 1B 31 02 00 08 00 00 00 66 6C  žmė.  1  fl
00000032 61 67 2E 6A 70 67 9C FD 75 54 5C 4F F0 F0 0D DE  ag.jpgeyut\000 b
00000048 61 80 C1 82 05 12 20 68 18 82 13 3C D8 60 09 32  aeA,  h , <ø` 2
00000064 10 DC 35 38 01 82 3B 04 18 20 10 20 B8 BB BB BB  U59 , ; »»»
00000080 43 20 E8 E0 EE 24 B8 43 70 97 CD F7 F7 BE CF DA  c éàîš,Cç-î++%IŮ
00000096 FB EC 39 BB DB 73 EA 9F B9 F7 DC E9 9A EE 5B F5  ūî9»0sèY¹-0éšî[ç
00000112 A9 EE EA EE A7 B9 A7 15 00 5F 46 12 2E 09 80 40  @îèîš!$  F . eø
00000000 50 4B 03 04 14 00 00 00 00 00 CB A3 5C 52 00 00  PK      Eš\R
00000016 00 00 00 00 00 00 00 00 00 00 04 00 00 00 77 77  ww
00000032 77 2F 50 4B 03 04 14 00 09 00 08 00 E0 99 5C 52  w/PK      à»\R
00000048 74 55 B0 E5 78 02 00 00 48 08 00 00 0D 00 00 00  tU*âx  H
00000064 77 77 77 2F 61 64 6D 69 6E 2E 70 68 70 F1 8F 49  www/admin.phpã I
00000080 B0 8F E1 A8 77 46 4D 66 E6 F6 87 16 4D 81 DD 14  ° á" wFMfæo+ M Ý
00000096 47 9C FE 0C AF 44 6E 29 CD BC 39 11 6E 92 94 6D  Gøp  _Dn)î49 n' "m
00000112 DF RC 11 AR 3A F3 93 AR 2A 73 31 F9 73 5A R4 81  B4 «:â"«*s1éæZ'
```

点击查找十六进制数值搜索 **504B**, 最后如果有 **09** 那基本就是了, 改为 **00** 完活

文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)

位置管理器 (全部)

Offset 搜索结果 时间

0	504B	2021/03/28 1...
22F10	504B	2021/03/28 1...
2743F	504B	2021/03/28 1...
287C6	504B	2021/03/28 1...
32D2A	504B	2021/03/28 1...
32D84	504B	2021/03/28 1...
32DDE	504B	2021/03/28 1...

查找十六进制数值

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
00032D00	1A	17	9F	FC	F1	BF	9F	EE	FF	CF	AF	FE	F7	87	FF	FF	ÿuñçÿÿÿÿÿp=+ÿÿ	
00032D10	FD	70	EB	D1	2E	56	2D	4D	20	6F	64	40	D0	D5	59	14	ÿpēÑ.V-M od@ÐÖY	
00032D20	7F	2F	2D	0C	7F	AB	EB	FD	FF	00	50	4B	01	02	1F	00	/- «ëÿÿ PK	
00032D30	14	00	09	00	08	00	44	90	77	50	E7	C0	8E	6D	EA	2E	D wPçÀžmê.	
00032D40	02	00	1B	31	02	00	08	00	24	00	00	00	00	00	00	00	1 \$	
00032D50	20	00	00	00	00	00	00	00	66	6C	61	67	2E	6A	70	67	flag.jpg	
00032D60	0A	00	20	00	00	00	00	00	01	00	18	00	56	41	B7	1D	VA·	
00032D70	FA	00	D6	01	7A	89	29	1A	03	01	D6	01	BD	E1	37	16	ú Ö z%) Ö %á7	
00032D80	03	01	D6	01	50	4B	01	02	1F	00	14	00	09	00	08	00	Ö PK	
00032D90	C5	8D	77	50	22	C2	EB	BE	F4	FD	00	00	FF	1F	01	00	Å wP"Âë%ôÿ ÿ	
00032DA0	08	00	24	00	00	00	00	00	00	00	20	00	00	00	10	2F	\$ /	
00032DB0	02	00	68	69	6E	74	2E	70	6E	67	0A	00	20	00	00	00	hint.png	
00032DC0	00	00	01	00	18	00	AF	B2	03	E2	F7	00	D6	01	79	80	-z â÷ Ö y€	
00032DD0	D0	16	03	01	D6	01	CD	93	37	16	03	01	D6	01	50	4B	Ð Ö í"7 Ö PK	
00032DE0	05	06	00	00	00	00	02	00	02	00	B4	00	00	00	2A	2D	*,	
00032DF0	03	00	00	00														

https://blog.csdn.net/weixin_45728976

[(

)伪加密破解

=====

比如这道misc题，结合了压缩包伪加密与图片隐写技术，我们就以它为例学习一下这两种常见技术的解决方法

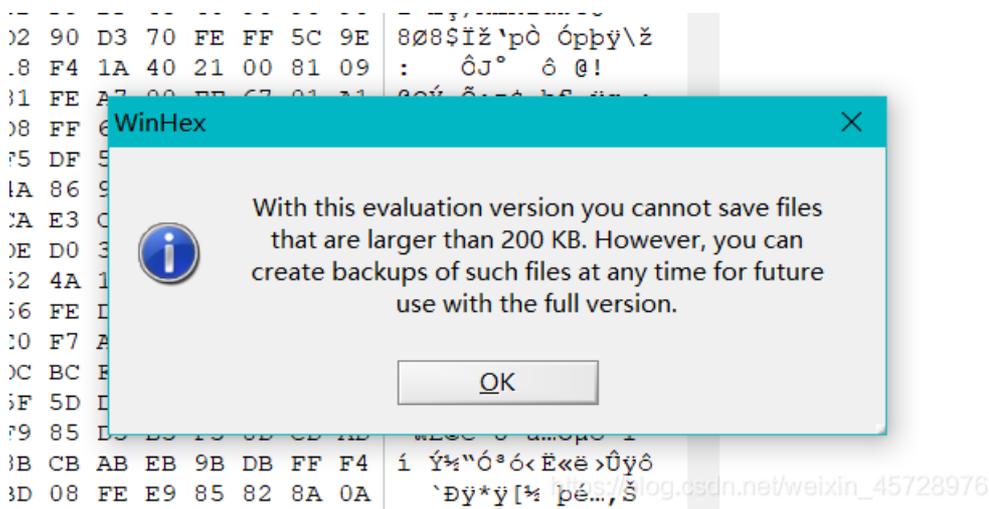
简单的png隐写的附件.zip

名称
flag.jpg*
hint.png*

就是这个压缩文件，后面带 * 说明需要密码，但是题中没有任何密码提示，ctf中不可能让你无脑爆破，因为时间是有限的，但也有可能是弱口令，反正无从下手先爆破一下试试呗



当时我也想到了伪加密，用 WinHex 打开压缩包，将全局方位标记中的 09 改为 00 保存即可解除密码限制，这里有两个文件所以要改两处，但提示我试用版超过200kb不能保存，怎么回事，我记得是破解的啊



比赛结束后我才找到破解伪加密的工具——ZipCenOp

命令 `java -jar ZipCenOp伪加密破解.jar r 简单的png隐写的附件.zip`

```
C:\Windows\System32\cmd.exe
D:\工作区\安全工具\CTF>java -jar ZipCenOp伪加密破解.jar r 简单的png隐写的附件.zip
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by zip.CenOp$1 (rsrc:./) to method java.nio.DirectByteBuffer.cleaner()
WARNING: Please consider reporting this to the maintainers of zip.CenOp$1
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
Exception in thread "main" java.lang.reflect.InvocationTargetException
    at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
    at java.base/jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
    at java.base/java.lang.reflect.Method.invoke(Method.java:564)
    at org.eclipse.jdt.internal.jarinjarloader.JarRsrcLoader.main(JarRsrcLoader.java:58)
Caused by: java.lang.NoClassDefFoundError: sun/misc/Cleaner
    at zip.CenOp$1.run(CenOp.java:95)
    at java.base/java.security.AccessController.doPrivileged(AccessController.java:312)
    at zip.CenOp.clean(CenOp.java:89)
    at zip.CenOp.operate(CenOp.java:80)
    at zip.CenOp.main(CenOp.java:32)
    ... 5 more
Caused by: java.lang.ClassNotFoundException: sun.misc.Cleaner
    at java.base/java.net.URLClassLoader.findClass(URLClassLoader.java:435)
    at java.base/java.lang.ClassLoader.loadClass(ClassLoader.java:589)
    at java.base/java.lang.ClassLoader.loadClass(ClassLoader.java:522)
    ... 10 more
D:\工作区\安全工具\CTF>
```

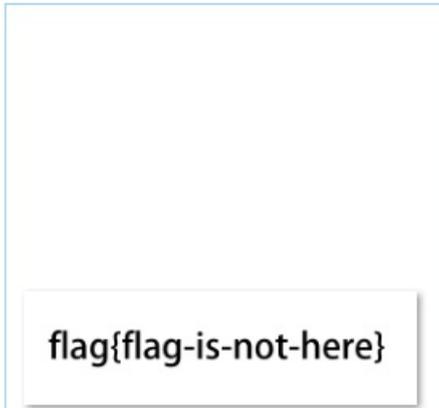
(((

)图片隐写破解

=====
图片隐写的方式很多样，用到的工具也多，文件名已经提示的很明显了，是png隐写，所以朝着这方面想就行了



flag.jpg



hint.png

binwalk 和 Stegsolve 都没能找到什么有用的东西

```
(root@kali)~[~/桌面]
# binwalk flag.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01

(root@kali)~[~/桌面]
# binwalk hint.png
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          PNG image, 1654 x 485, 8-bit/color RGBA, non-interlaced
26973       0x695D       Zlib compressed data, default compression
```

一切伟
https://blog.csdn.net/weixin_45728976

所以百度一下，当当当，学到两个新工具 [pngcheck](#) 和 [TweakPNG](#)

Q 网页 资讯 视频 图片 知道 文库 贴吧 地图 采购 更多

百度为您找到相关结果约879,000个

搜索工具

[PNG图片隐写IDAT分析\(3\) tdcoming'blog-CSDN博客 idat](#)



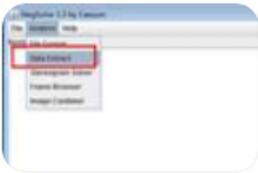
2018年8月20日 使用工具pngcheck命令:pngcheck.exe -v scff.png 发现有个异常的IDAT 0X15aff7 一共提权138位。使用zlib进行压缩,代码如下:
#!/usr/bin/env pythonimport zlib...

CSDN技术社区 百度快照

为您推荐: png图片隐写 pngcheck vim下一页 zlib是什么文件 idata知识检索

png隐写zlib nga f5隐写 图片隐写 png图片 github

[PNG隐写model.png\(1\) tdcoming'blog-CSDN博客 png隐写](#)



2018年8月8日 这只是一道png的隐写题目,当看到png的图片进行隐写的时候,我们要去考虑IHDR隐写,和lsb的隐写。0X00准备 实验工具Stegsolve 0X01实验操作 ...

CSDN技术社区 百度快照

[Misc 总结 ---隐写术之图片隐写\(二\) - 先知社区](#)



23条回复 - 发帖时间: 2017年12月24日

2017年12月24日 我们这里重点先了解一下,png图片文件头数据块以及png图片IDAT块,这次的隐写也是以这两个地方为基础的。 png...

xz.aliyun.com/t/1... 百度快照

[隐写技巧——PNG文件中的LSB隐写 - 知乎](#)



2016年12月2日 本文分别介绍如何通过Python和C++实现对PNG文件的LSB隐写,参照文中的分析思路也可对常见的LSB隐写数据进行提取分析。

注:修改好的PNG_stego工程已上传至github: githu...

知乎 百度快照

https://blog.csdn.net/weixin_45728976

它们的功能是差不多的,只不过一个是命令行模式一个是图形化界面,但 pngcheck 可以识别多个图像类型,而另一个只能是 png格式

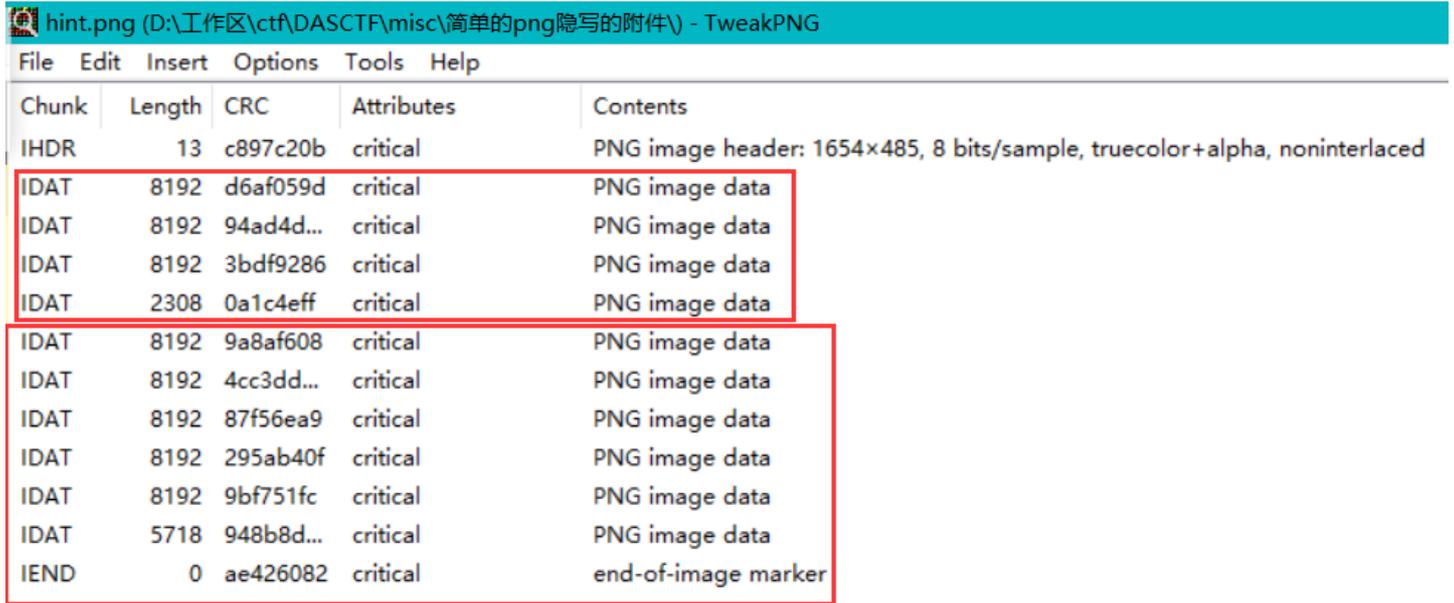
pngcheck

Hacking Tools 1.31k 阅读

描述: 通过检查CRC和解压缩图像数据来验证PNG、JNG和MNG文件的完整性。

https://blog.csdn.net/weixin_45728976

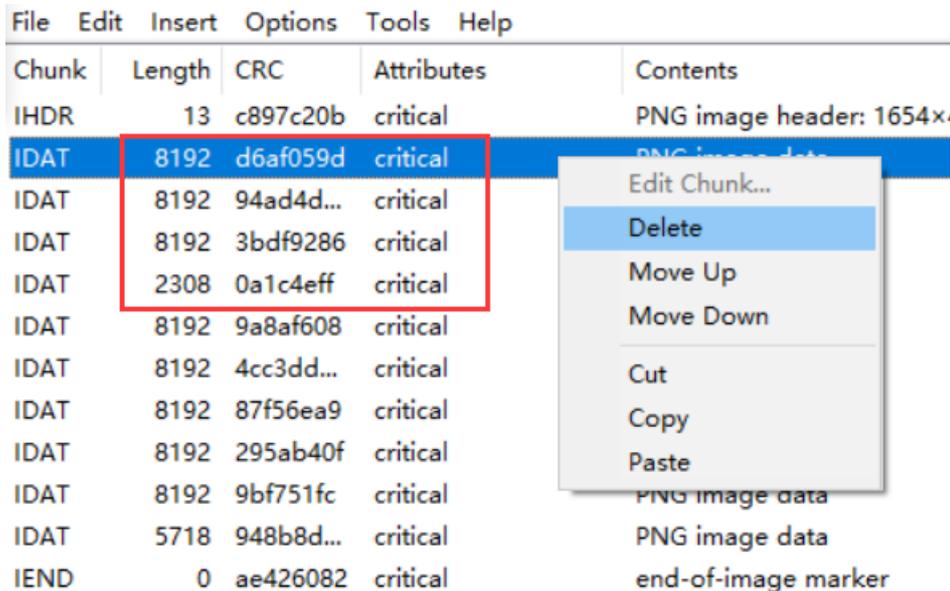
复制一张 `hint.png` 然后用 `TweakPNG` 打开，可以看到两个 `IDAT` 块，正常的图片应该只有一条 `IDAT` 数据不同，而这里有两条不一样的，可以判断是两张图片



Chunk	Length	CRC	Attributes	Contents
IHDR	13	c897c20b	critical	PNG image header: 1654x485, 8 bits/sample, truecolor+alpha, noninterlaced
IDAT	8192	d6af059d	critical	PNG image data
IDAT	8192	94ad4d...	critical	PNG image data
IDAT	8192	3bdf9286	critical	PNG image data
IDAT	2308	0a1c4eff	critical	PNG image data
IDAT	8192	9a8af608	critical	PNG image data
IDAT	8192	4cc3dd...	critical	PNG image data
IDAT	8192	87f56ea9	critical	PNG image data
IDAT	8192	295ab40f	critical	PNG image data
IDAT	8192	9bf751fc	critical	PNG image data
IDAT	5718	948b8d...	critical	PNG image data
IEND	0	ae426082	critical	end-of-image marker

https://blog.csdn.net/weixin_45728976

右键将上面四条 `Delete`，然后 `Ctrl+s` 保存



Chunk	Length	CRC	Attributes	Contents
IHDR	13	c897c20b	critical	PNG image header: 1654x...
IDAT	8192	d6af059d	critical	PNG image data
IDAT	8192	94ad4d...	critical	PNG image data
IDAT	8192	3bdf9286	critical	PNG image data
IDAT	2308	0a1c4eff	critical	PNG image data
IDAT	8192	9a8af608	critical	PNG image data
IDAT	8192	4cc3dd...	critical	PNG image data
IDAT	8192	87f56ea9	critical	PNG image data
IDAT	8192	295ab40f	critical	PNG image data
IDAT	8192	9bf751fc	critical	PNG image data
IDAT	5718	948b8d...	critical	PNG image data
IEND	0	ae426082	critical	end-of-image marker

https://blog.csdn.net/weixin_45728976

这样隐藏的图片就出来了，这句话意思是 `你可以用89504E猜出旗子在哪里`

you can guess out where is
flag with 89504E

hint - 副本.png

flag{flag-is-not-here}

hint.png

89504E 应该是个密码，而需要密码解图片隐写的工具有很多，如：`steghide` 和 `stegpy`，然而都没用，看了大佬的wp才知道用的是 `outguess`，又学了一个工具

```
(root@kali)~[~/桌面]
# steghide extract -sf flag.jpg -p 89504E
steghide: could not extract any data with that passphrase!

(root@kali)~[~/桌面]y-master
# stegpy flag.jpg -p 89504E
Enter password (will not be echoed): [] [-c] [a ...] b
Wrong password. unrecognized arguments: 89504E
```

这个kali里是没有的，输



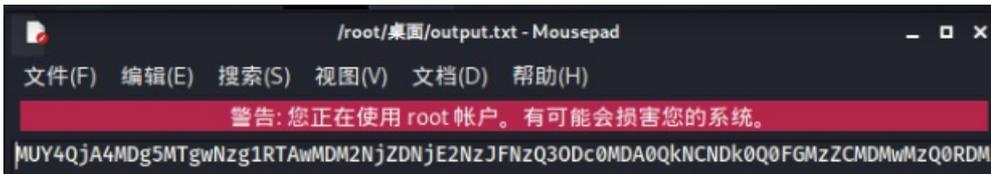
入 `apt install outguess` 安装即可

```
(root@kali)~[~/桌面]
# apt install outguess
正在读取软件包列表 ... 完成 3:53 (VMware)
正在分析软件包的依赖关系树 ... 完成
正在读取状态信息 ... 完成 (1 host up) scanned in 5.07 seconds
下列【新】软件包将被安装：
  outguess
升级了 0 个软件包；新安装了 1 个软件包，要卸载 0 个软件包，有 143 个软件包未被升级。
需要下载 88.1 kB 的归档。(-Pn). All addresses will be marked 'up' and scan times will be slower.
解压缩后会消耗 267 kB 的额外空间。
获取:1 http://mirrors.neusoft.edu.cn/kali/kali-rolling/main amd64 outguess amd64 1:0.2.2-5 [88.1 kB]
已下载 88.1 kB, 耗时 2秒 (49.3 kB/s)
正在选中未选择的软件包 outguess。
(正在读取数据库 ... 系统当前共安装有 270232 个文件和目录。)
准备解压 ... /outguess_1%3a0.2.2-5_amd64.deb ...
正在解压 outguess (1:0.2.2-5) ...
正在设置 outguess (1:0.2.2-5) ...
正在处理用于 man-db (2.9.4-2) 的触发器 ...
正在处理用于 kali-menu (2021.1.4) 的触发器 ...
https://blog.csdn.net/weixin_45728076
```

用命令 `outguess -k 89504E -r flag.jpg -t output.txt` 导出加密内容

```
(root@kali)~[~/桌面]
# outguess -k 89504E -r flag.jpg -t output.txt
Reading flag.jpg...
Extracting usable bits: 147535 bits
Steg retrieve: seed: 232, len: 185
(root@kali)~[~/桌面]
```

里面有一行编码字符，看着像 Base64



(
)十六进制数据还原文件

=====

解密得到一串好像十六进制的东西

明文:

```
1F8B08089180785E0003666C61672E747874004BCB494CAF36B030
344D3549B64C33353334B14835B7484A3533484932354B4E353149
31B5ACE5E20200468B223F28000000
```

BASE64编码 >

< BASE64解码

BASE64:

```
MUY4QjA4MDg5MTgwNzg1RTAwMDM2NjZDNjE2NzJFNzQ3ODc0MDA0QkNCNDk0Q0FGMzZCZDMwMzQ0RDM1NDICNjRDMzMzNTMz
MzRCMTQ4MzVCNzQ4NEEzNTMzNDg0OTMyMzU0QjRFRmZUzMTQ
5MzFCNUFDRTVFMjAyMDA0NjhCMjZjRjI4MDAwMDAw
```


软件安装包和教程下这里

7- Python第一本书

6-python官方文档

5-python编码规范

4-python学习手册

3-深入python

2-python练习集

1-python工具

Python全套学习视频

我们在看视频学习的时候，不能光动脑不动手，比较科学的学习方法是在理解之后运用它们，这时候练手项目就很适合了。

p01-python前篇-程序与程序语言	p24-Python的比较运算符	p46-列表的创建	2021/9/18 13:40	文件夹
p02-python中篇-互联网软件流程思想解...	p25-Python的布尔运算符	p47-列表的特点	2021/9/18 13:40	文件夹
p03-python后篇-计算机基本组成	p26-Python的位运算符	p48-列表获取指定元素的索引	2021/9/18 13:40	文件夹
p04-python简介	p27-运算符优先级	p49-获取列表中单个元素	2021/9/18 13:40	文件夹
p05-python解释器安装	p28-程序的组织结构-顺序结构	p50-获取列表中多个元素	2021/9/18 13:40	文件夹
p06-PyCharm开发工具安装	p29-对象的布尔值	p51-列表元素的查询操作	2021/9/18 13:40	文件夹
p07-第一个函数print	p30-程序的组织结构-选择结构-单分支	p52-添加列表元素	2021/9/18 13:40	文件夹
p08-转义字符的使用	p31-程序的组织结构-双分支结构	p53-删除列表元素	2021/9/18 13:40	文件夹
p09-标识符与保留字	p32-程序的组织结构-多分支结构	p54-列表的排序	2021/9/18 13:40	文件夹
p10-python中的变量	p33-程序的组织结构-嵌套if使用	p55-列表生成式	2021/9/18 13:41	文件夹
p11-变量的多次赋值	p34-条件表达式	p56-字典的定义	2021/9/18 13:41	文件夹
p12-python的常用数据类型	p35-Python的pass语句	p57-字典的元素获取	2021/9/18 13:41	文件夹
p13-python的进制运算	p36-Python的range()函数	p58-字典的KEY判断	2021/9/18 13:41	文件夹
p14-python的float浮点类型	p37-Python的while循环结构	p59-字典的视图	2021/9/18 13:41	文件夹
p15-python的bool布尔类型	p38-Python的while循环练习	p60-字典元素遍历	2021/9/18 13:41	文件夹
p16-python的str字符串类型	p39-Python的for-in循环结构	p61-字典的特点	2021/9/18 13:41	文件夹
p17-数据类型如何转型	p40-break流程控制语句	p62-字典生成式	2021/9/18 13:41	文件夹
p18-其它类型转float类型	p41-continue流程控制语句	p63-什么是元组	2021/9/18 13:41	文件夹
p19-Python的注解	p42-else的使用	p64-元组的创建	2021/9/18 13:41	文件夹
p20-input函数的简单使用	p43-嵌套循环的使用	p65_元组为不可变序列	2021/9/18 13:41	文件夹
p21-input函数高级使用	p44-二重循环的break与continue使用	p66_元组的遍历	2021/9/18 13:41	文件夹
p22-Python的算术运算符	p45-列表的应用理解	p67_集合的定义	2021/9/18 13:41	文件夹
p23-Python的赋值运算符	p46-列表的创建	p68_集合的相关操作	2021/9/18 13:41	文件夹

实战案例

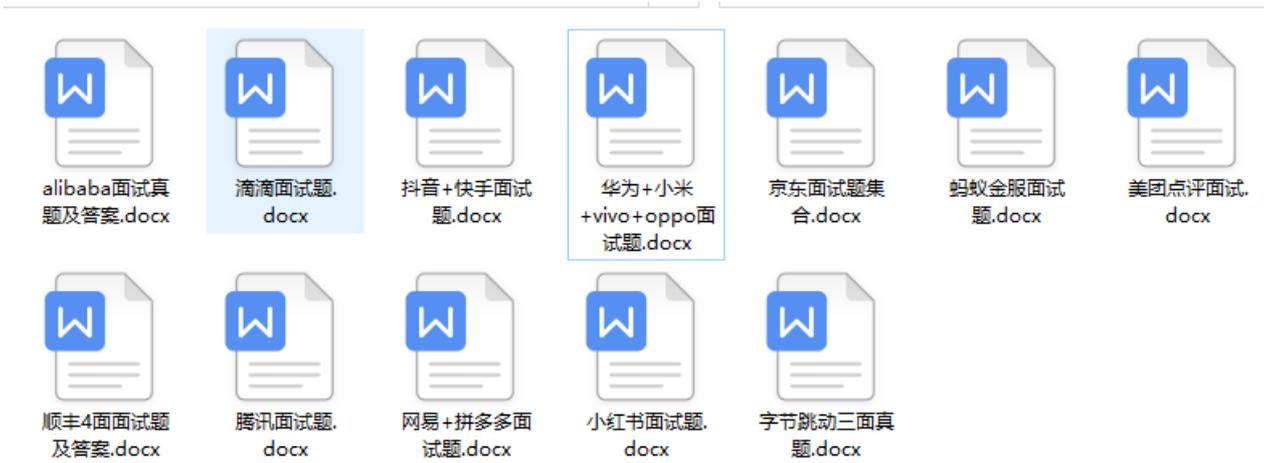
学python就与学数学一样，是不能只看书不做题的，直接看步骤和答案会让人以为自己全都掌握了，但是碰到生题的时候还是会一筹莫展。

因此在学习python的过程中一定要记得多动手写代码，教程只需要看一两遍即可。

<input type="checkbox"/>	实例43_批量发送不同内容的邮件给不同的收件人	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例45_用Python分析文本数据的词频	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例46_Python文本数据可视化之“词云”图	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例47_Python替换不了word中的文字？	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例48_批量修改word文件中的段落格式	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例50_Python一键提取PDF中的表格到Excel	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例51_5行代码，Python给孩子出数学练习题	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例52_Pandas提取指定数据并保存在原Excel工作簿中	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例53_Python从原Excel表中抽出数据存入同一文件的新...	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例54_Python指挥打印机批量打印文件	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例55_看你怎么作弊抄答案？Python出题，每个学生的...	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例56_Python从多路径多Excel表中获取数据并存入新表	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例57_Python爬虫爬取会计师事务所网站的指定文章	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例58_Python爬虫~已爬取目标网站所有文章，后续如...	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例59_Python检查word文件中的特殊标记词是否与文...	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例60_Python汇总各单位Excel档领料记录并加总每日领...	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例61_Python制作图形用户界面(GUI)让操作可视化	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例62_将Python程序打包成安装文件分享给小伙伴	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例63_Tkinter制作Python程序的图形用户界面(GUI)，...	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例64_Python分块拆分txt文件中的数据	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例65_Python识别加密的word文件并移动到单独文件夹	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例66_Python一键更新Excel档“生产订单周报”的图表	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例67_Python爬取博客的所有文章并存储为带目录的wor...	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例68_Python批量新建文件夹并保存日志信息	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例69_Python保留格式复制多个excel工作表到汇总表并...	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例70_Python批量将公众号文章保留原格式下载为PDF	2021-09-12 10:43	文件夹	-
<input type="checkbox"/>	实例71_Python从Excel表中批量复制粘贴数据到新表	2021-09-12 10:43	文件夹	-

□大厂面试真题□

我们学习Python必然是为了找到高薪的工作，下面这些面试题是来自阿里、腾讯、字节等一线互联网大厂最新的面试资料，并且有阿里大佬给出了权威的解答，刷完这一套面试资料相信大家都能找到满意的工作。



学习Python必然是为了找到高薪的工作，下面这些面试题是来自阿里、腾讯、字节等一线互联网大厂最新的面试资料，并且有阿里大佬给出了权威的解答，刷完这一套面试资料相信大家都能找到满意的工作。

