CTF常用脚本（长期更新）

原创

FunkyPants 于 2018-05-01 15:03:09 发布 6986 收藏 34

分类专栏： Python CTF writeup 文章标签： Python CTF

本文链接：https://blog.csdn.net/FunkyPants/article/details/80156673


Python 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏


CTF writeup

13 篇文章 0 订阅

订阅专栏

CTF常用脚本（长期更新）

1.长串字符串两两分割

```
def long_to_2(str_):
    for i in range(0,len(str_)+1,2):
        print(str_[i:i+2])
```

效果：

```
In[9]: all = '123404B03040A0001080000739C8C4B7B36E4952
In[10]: len(all)
Out[10]: 350
In[11]: for i in range(0,len(all)+1,2):
   ...:     print(all[i:i+2])
   ...:
12
34
04
B0
30
40
A0
00
10
```


字符串分割后，常转换为十六进制输出。

trick：不换行输出

- Python2 print ‘xxx’,
- Python3 print(‘xxx’, end=”)

2.不同进制转换

一般来说，先换算为十进制，再进行后续转换

转为十进制

- 十六进制到十进制 int('0xab', 16)
- 二进制到十进制 int('0b10', 2)

十进制转二进制

- bin(123)

十进制转十六进制

- hex(123)

3.按行读文件的4种方式

3.1使用for循环（最简洁）

```
file = open("sample.txt")

for line in file:
    pass # do something
```

3.2带缓存的文件读取（效率最高）

```
file = open("sample.txt")

while 1:
    lines = file.readlines(100000)
    if not lines:
        break
    for line in lines:
        pass # do something
```

3.3 fileinput模块

```
import fileinput

for line in fileinput.input("sample.txt"):
    pass
```

3.4 常规方法

```
file = open("sample.txt")

while 1:
    line = file.readline()
    if not line:
        break
    pass # do something
```

其中，后两种方法都不推荐。

沙盒绕过

参考文章 https://blog.0kami.cn/2016/09/16/old-python-sandbox-escape/

另外补充：当getattr()方法被禁后，可以使用‘**getattribute**’属性。

遍历目录下所有文件的内容这里写图片描述

```
import os
rootdir = os.getcwd()#可自定义
for parent, dirnames, filenames in os.walk(rootdir):
  for file in filenames:
    with open(parent +'\\' + file, 'r') as f:
      text = f.read() #print(text[0:5])
      if text[0:11111] == '待比较字符串'
        print(text)
```