python沙箱逃逸总结

让用户提交 Python 代码并在服务器上执行，是一些 OJ、量化网站重要的服务。为了不让恶意用户执行任意的 Python 代码，就需要确保 Python 运行在沙箱中。沙箱经常会禁用一些敏感的函数，例如 os，研究怎么逃逸、防护这类沙箱还是蛮有意思的。

执行系统命令

基础知识（有哪些模块可以执行shell命令...

os

commands：仅限2.x

subprocess

timeit：timeit.sys、timeit.timeit("\_\_import\_\_('os').system('whoami')", number=1)

platform：platform.os、platform.sys、platform.popen('whoami', mode='r', bufsize=-1).read()

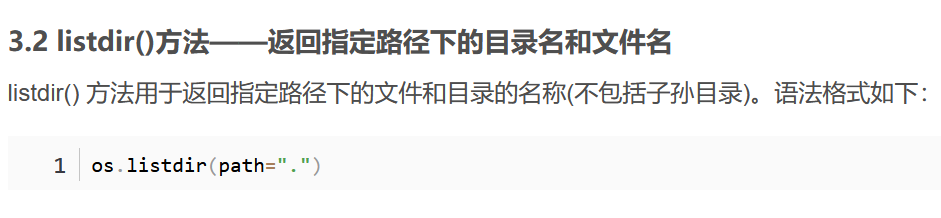
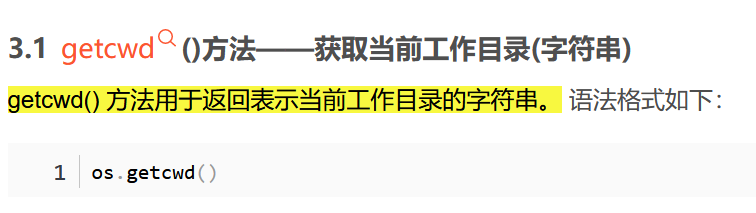
pty：pty.spawn('ls')、pty.os

bdb：bdb.os、cgi.sys

cgi：cgi.os、cgi.sys

…

1. os模块



##os.system(cmd)

##os.popen(cmd)

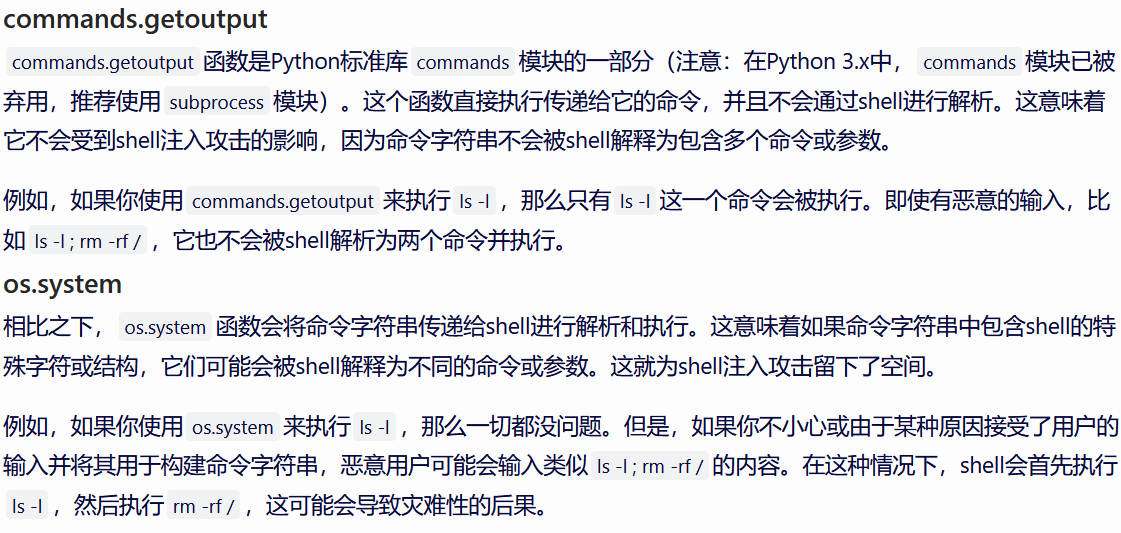
1. command模块：

注意：commands从2.6版开始不推荐使用：该模块已在Python 3中删除。推荐使用subprocess模块在3.x版本中，getstatus()方法被移除，getoutput()和getstatusoutput()被放到了subprocess模块中。

###command.getstatus(file)相当对指定的文件执行ls -ld

###command.getoutput(cmd)执行cmd命令，并返回输出的内容，返回结果为str。

###command.getstatusoutput(cmd)与getoutput相似



1. subprocess模块

subprocess.getoutput(cmd)接收字符串格式的命令，执行命令并返回执行结果

subprocess.getstatusoutput(cmd)执行cmd命令，返回一个元组

subprocess.call()执行指定的命令，返回命令执行状态，其功能类似于os.system(cmd)。

subprocess.check\_call()执行指定的命令，如果执行成功则返回状态码，否则抛出异常。

...