Python sandboxing e maxia negra

Eloy Pérez González

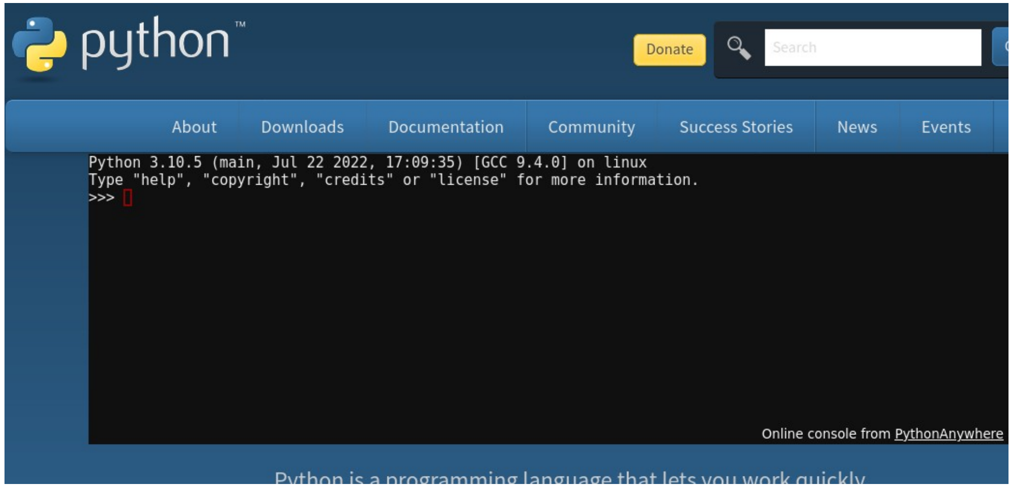
Que é unha sandbox?

- Entorno restrinxido

- Non se permiten certas accións ou comandos

Para que serve unha sandbox?

- Python na web
  - Yepcode
  - Code Academy
- Servicios na nube
  - Lambda functions
- Análise de malware



```
Python 3.10.5 (main, Jul 22 2022, 17:09:35) [GCC 9.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 
```

Online console from PythonAnywhere

Python is a programming language that lets you work quickly

Que tipos de sandboxes hai?

- Sandbox a nivel de linguaxe ✗
  - Sandbox en Python → pysandbox

- Sandbox a nivel de SO ✓
  - Python en Sandbox
    - Pypy Sandbox (sen mantemento)
    - SECCOMP, SELinux, Docker

Sandbox en Python

- Imos ver de construir unha sandbox…
- Que precisamos evitar?
  - Acceso a información confidencial
  - Agotar os recursos do sistema
  - Escapar da sandbox

Sandbox en Python

- De momento o noso obxetivo:
  - Bloquear “open“
  - Aprender maxia oscura de Python

Sandbox en Python

- Partimos da seguinte clase:

```python
class Sandbox():

    def __init__(self, globals=None, locals=None):
        self.globals = globals or {}
        self.locals = locals or {}

    def execute(self, code_string):
        exec(code_string, self.globals, self.locals)
```

Internals

- globals() → variables globais
- locals() → variables locais da función

Sandbox en Python

- Executamos:

```
sb = Sandbox()
sb.execute("""
open('authorized_keys', 'w').write('ssh-ed25519 ...')
""")
```

Sandbox en Python

- Podemos tentar evitar a función “open“

- Que tal unha blacklist?
  - Simple: filtrado con palabras
  - Complexo: filtrado co AST

Internals

AST (Abstract Syntax Tree)

```
print("hello world")
```

→

```
Module(
  body=[
    Expr(
      value=Call(
        func=Name(id='print', ctx=Load()),
        args=[
          Constant(value='hello world')],
        keywords=[]))],
  type_ignores=[])
```

Sandbox en Python

```
Sandbox().execute("""
open('authorized_keys', 'w').write('ssh-ed25519 ...')
""")   -> Error
```

```
Sandbox().execute("""
__builtins__['op'+'en']('authorized_keys', 'w').write('ssh-ed25519 ...')
""")  -> Ok
```

Internals

__builtins__ → Acceso a obxetos por defecto

Se borramos algo:

```
>>> del __builtins__.open
>>> open
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'open' is not defined
```

Sandbox en Python

- Eliminar “open“?

```
del __builtins__.__dict__["open"]
```

Sandbox en Python

```
__builtins__['op'+'en']('builtin-open.txt', 'w').write('pwn!') -> Error
```

```
import os
fd = os.open('import-os.txt', os.O_CREAT|os.O_WRONLY)
os.write(fd, b'pwn!.')  -> Ok
```

Sandbox en Python

- So permitir certos imports

```python
__builtins__.__dict__["__import__"] = our_safe_import
```

Sandbox en Python

`import os` → Error 😌

```
loader = [
    x
    for x in ().__class__.__base__.__subclasses__()
    if x.__name__ == "BuiltinImporter"
][0]

os = loader.load_module("os")    → Ok
```

🤯

Sandbox en Python

- Eliminamos o acceso a __bases__ e __subclasses__

```
» del type.__base__
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
TypeError: cannot set '__base__' attribute of immutable type 'type'
```

Sandbox en Python

- Usamos a maxia de ctypes

```
from ctypes import pythonapi, POINTER, py_object

_get_dict = pythonapi._PyObject_GetDictPtr
_get_dict.restype = POINTER(py_object)
_get_dict.argtypes = [py_object]
del pythonapi, POINTER, py_object

def dictionary_of(ob):
    dptr = _get_dict(ob)
    return dptr.contents.value

type_dict = dictionary_of(type)
del type_dict["__subclasses__"]
```

Sandbox en Python

```
().__class__.__base__.__subclasses__()
```

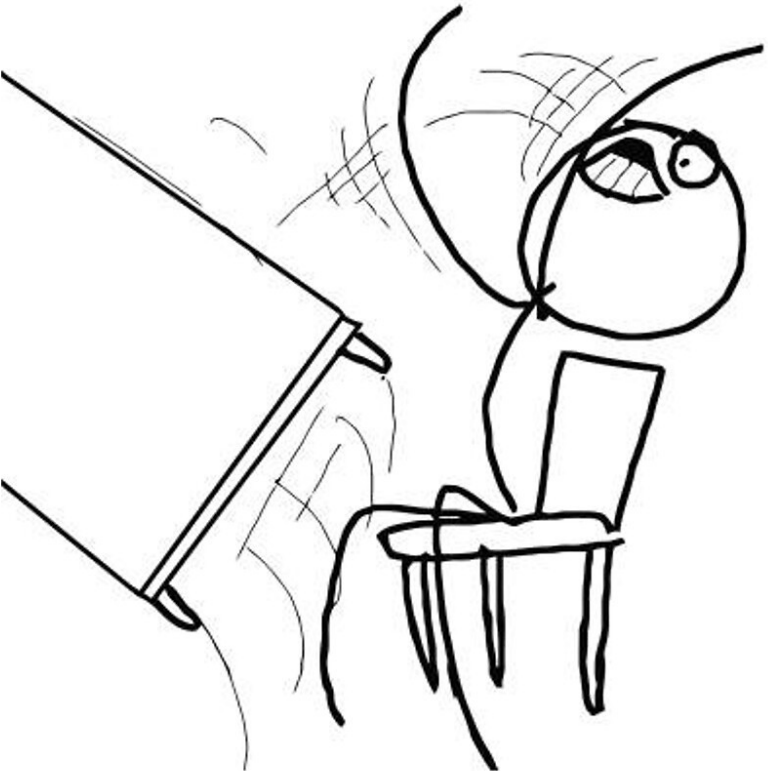
→ Error 😌

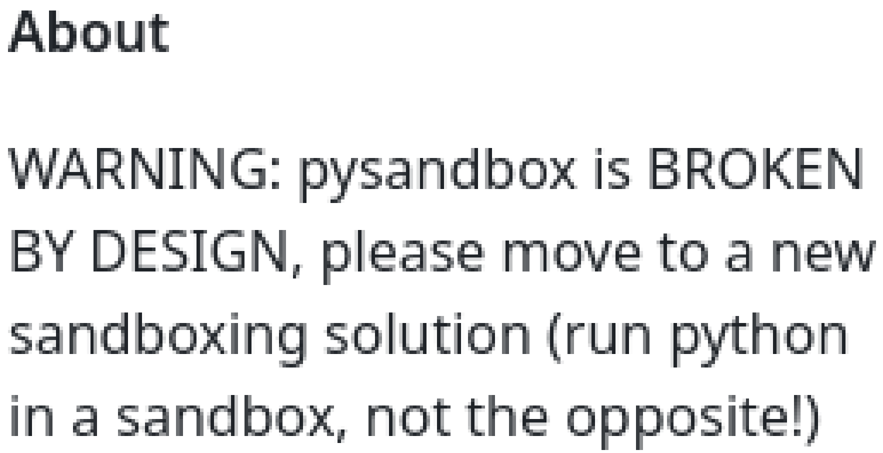
```
try:
  import os
except Exception as e:
  orig_import = e.__traceback__.tb_next.tb_frame.f_locals["orig_import"]

os = orig_import("os")
```

→ Ok 🤯

Sandbox en Python





About

WARNING: pysandbox is BROKEN BY DESIGN, please move to a new sandboxing solution (run python in a sandbox, not the opposite!)

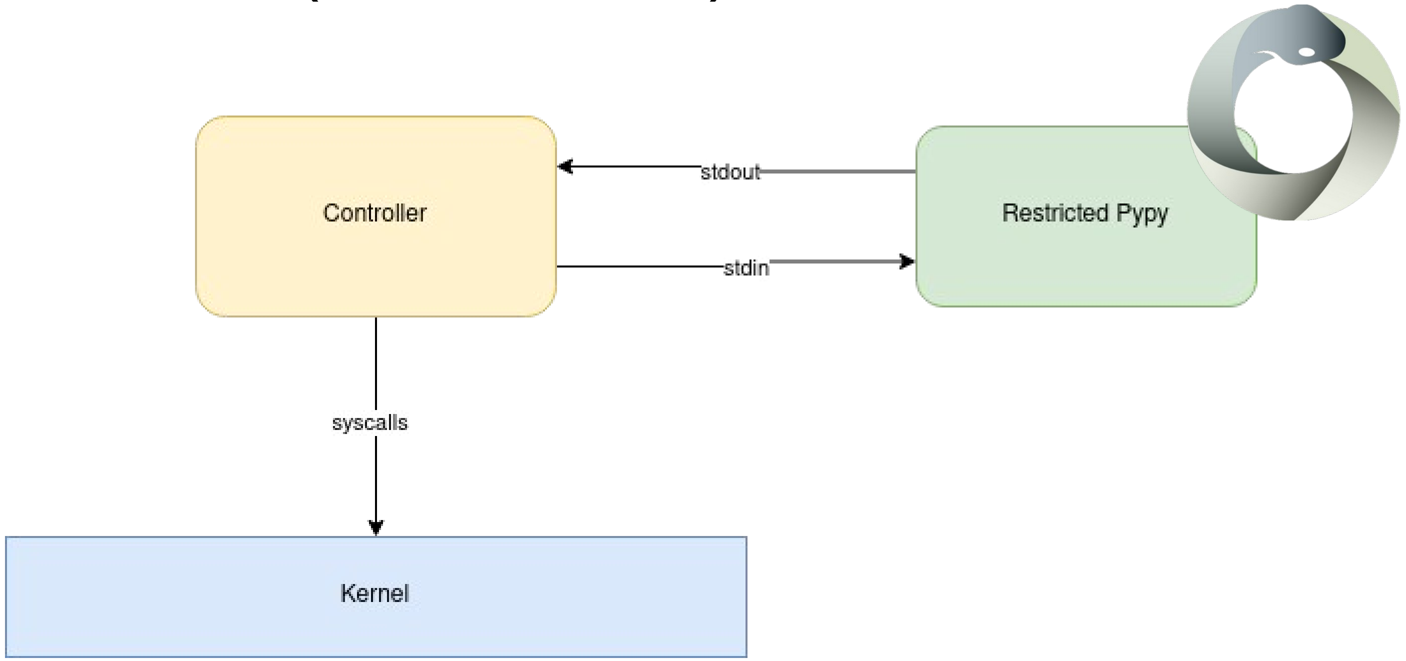
Sandbox en Python

"Os resultados negativos tamén son resultados,
e precisan ser publicados."

- Guido van Rossum

Python en Sandbox

- Pypy sandbox (non mantido)



Python en Sandbox

- SECCOMP
  - Strict mode: read, write, exit e sigreturn
  - BPF mode: Restrinxe syscalls con filtros eBPF
- SELinux sandbox
- Docker
- Máquinas virtuais

Referencias

- Victor Stinner: pysandbox
- The failure of pysandbox
- Jessica McKellar: Building and breaking a Python sandbox - PyCon 2014
- Escaping a Python sandbox
- Pypy Sandbox
- SECCOMP

Isto é todo... de momento

Graciñas!