# Custom PoC : Python Buffer Overflow

Author: Harshal Harekar

Date: 28/10/2025

Modify Exploit-DB PoC to trigger overflow and gain control of EIP.

## Summary:

Modified a Python PoC targeting a vulnerable binary with a classic buffer overflow. Adjusted offset using pattern\_create/pattern\_offset, then injected shellcode via . Verified EIP overwrite and redirected execution to a NOP sled. Final payload spawns a reverse shell, confirming successful exploitation and control of program flow.