

Exploit Development: Fuzzing

Objectives:

- Discover vulnerable input using Wireshark.
- Create python script to remotely interface with vulnerable software on target machine.
- "Fuzz" input to test for vulnerability and get familiar with vulnerable software CPU registers (EIP, ESP, EAX, etc) for code execution control mapping purposes.

Outline:

Code Snippets:

+

Resources:

- <https://docs.python.org/3/library/ftplib.html>