PWN Tools

pwntools is a CTF framework and exploit development library. Written in Python, it is designed for rapid prototyping and development, and intended to make exploit writing as simple as possible.

The primary location for this documentation is at [docs.pwntools.com](https://docs.pwntools.com/), which uses [readthedocs](https://readthedocs.org/). It comes in three primary flavors:

* [Stable](https://docs.pwntools.com/en/stable)
* [Beta](https://docs.pwntools.com/en/beta)
* [Dev](https://docs.pwntools.com/en/dev)

## Getting Started

* [About pwntools](http://docs.pwntools.com/en/latest/about.html)
  + [pwn — Toolbox optimized for CTFs](http://docs.pwntools.com/en/latest/about.html#module-pwn)
  + [pwnlib — Normal python library](http://docs.pwntools.com/en/latest/about.html#module-pwnlib)
* [Installation](http://docs.pwntools.com/en/latest/install.html)
  + [Prerequisites](http://docs.pwntools.com/en/latest/install.html#prerequisites)
    - [Binutils](http://docs.pwntools.com/en/latest/install/binutils.html)
    - [Python Development Headers](http://docs.pwntools.com/en/latest/install/headers.html)
  + [Released Version](http://docs.pwntools.com/en/latest/install.html#released-version)
    - [Python3](http://docs.pwntools.com/en/latest/install.html#python3)
    - [Python2 (Deprecated)](http://docs.pwntools.com/en/latest/install.html#python2-deprecated)
  + [Command-Line Tools](http://docs.pwntools.com/en/latest/install.html#command-line-tools)
  + [Development](http://docs.pwntools.com/en/latest/install.html#development)
* [Getting Started](http://docs.pwntools.com/en/latest/intro.html)
  + [Tutorials](http://docs.pwntools.com/en/latest/intro.html#tutorials)
  + [Making Connections](http://docs.pwntools.com/en/latest/intro.html#making-connections)
  + [Packing Integers](http://docs.pwntools.com/en/latest/intro.html#packing-integers)
  + [Setting the Target Architecture and OS](http://docs.pwntools.com/en/latest/intro.html#setting-the-target-architecture-and-os)
  + [Setting Logging Verbosity](http://docs.pwntools.com/en/latest/intro.html#setting-logging-verbosity)
  + [Assembly and Disassembly](http://docs.pwntools.com/en/latest/intro.html#assembly-and-disassembly)
  + [Misc Tools](http://docs.pwntools.com/en/latest/intro.html#misc-tools)
  + [ELF Manipulation](http://docs.pwntools.com/en/latest/intro.html#elf-manipulation)
* [from pwn import \*](http://docs.pwntools.com/en/latest/globals.html)
* [Command Line Tools](http://docs.pwntools.com/en/latest/commandline.html)
  + [pwn](http://docs.pwntools.com/en/latest/commandline.html#pwn)
    - [pwn asm](http://docs.pwntools.com/en/latest/commandline.html#pwn-asm)
    - [pwn checksec](http://docs.pwntools.com/en/latest/commandline.html#pwn-checksec)
    - [pwn constgrep](http://docs.pwntools.com/en/latest/commandline.html#pwn-constgrep)
    - [pwn cyclic](http://docs.pwntools.com/en/latest/commandline.html#pwn-cyclic)
    - [pwn debug](http://docs.pwntools.com/en/latest/commandline.html#pwn-debug)
    - [pwn disablenx](http://docs.pwntools.com/en/latest/commandline.html#pwn-disablenx)
    - [pwn disasm](http://docs.pwntools.com/en/latest/commandline.html#pwn-disasm)
    - [pwn elfdiff](http://docs.pwntools.com/en/latest/commandline.html#pwn-elfdiff)
    - [pwn elfpatch](http://docs.pwntools.com/en/latest/commandline.html#pwn-elfpatch)
    - [pwn errno](http://docs.pwntools.com/en/latest/commandline.html#pwn-errno)
    - [pwn hex](http://docs.pwntools.com/en/latest/commandline.html#pwn-hex)
    - [pwn phd](http://docs.pwntools.com/en/latest/commandline.html#pwn-phd)
    - [pwn pwnstrip](http://docs.pwntools.com/en/latest/commandline.html#pwn-pwnstrip)
    - [pwn scramble](http://docs.pwntools.com/en/latest/commandline.html#pwn-scramble)
    - [pwn shellcraft](http://docs.pwntools.com/en/latest/commandline.html#pwn-shellcraft)
    - [pwn template](http://docs.pwntools.com/en/latest/commandline.html#pwn-template)
    - [pwn unhex](http://docs.pwntools.com/en/latest/commandline.html#pwn-unhex)
    - [pwn update](http://docs.pwntools.com/en/latest/commandline.html#pwn-update)
    - [pwn version](http://docs.pwntools.com/en/latest/commandline.html#pwn-version)

## Module Index

Each of the pwntools modules is documented here.

* [pwnlib.adb — Android Debug Bridge](http://docs.pwntools.com/en/latest/adb.html)
* [pwnlib.args — Magic Command-Line Arguments](http://docs.pwntools.com/en/latest/args.html)
* [pwnlib.asm — Assembler functions](http://docs.pwntools.com/en/latest/asm.html)
* [pwnlib.atexception — Callbacks on unhandled exception](http://docs.pwntools.com/en/latest/atexception.html)
* [pwnlib.atexit — Replacement for atexit](http://docs.pwntools.com/en/latest/atexit.html)
* [pwnlib.constants — Easy access to header file constants](http://docs.pwntools.com/en/latest/constants.html)
* [pwnlib.config — Pwntools Configuration File](http://docs.pwntools.com/en/latest/config.html)
* [pwnlib.context — Setting runtime variables](http://docs.pwntools.com/en/latest/context.html)
* [pwnlib.dynelf — Resolving remote functions using leaks](http://docs.pwntools.com/en/latest/dynelf.html)
* [pwnlib.encoders — Encoding Shellcode](http://docs.pwntools.com/en/latest/encoders.html)
* [pwnlib.elf.config — Kernel Config Parsing](http://docs.pwntools.com/en/latest/elf/config.html)
* [pwnlib.elf.corefile — Core Files](http://docs.pwntools.com/en/latest/elf/corefile.html)
* [pwnlib.elf.elf — ELF Files](http://docs.pwntools.com/en/latest/elf/elf.html)
* [pwnlib.exception — Pwnlib exceptions](http://docs.pwntools.com/en/latest/exception.html)
* [pwnlib.filepointer — FILE\* structure exploitation](http://docs.pwntools.com/en/latest/filepointer.html)
* [pwnlib.filesystem — Manipulating Files Locally and Over SSH](http://docs.pwntools.com/en/latest/filesystem.html)
* [pwnlib.flag — CTF Flag Management](http://docs.pwntools.com/en/latest/flag.html)
* [pwnlib.fmtstr — Format string bug exploitation tools](http://docs.pwntools.com/en/latest/fmtstr.html)
* [pwnlib.gdb — Working with GDB](http://docs.pwntools.com/en/latest/gdb.html)
* [pwnlib.libcdb — Libc Database](http://docs.pwntools.com/en/latest/libcdb.html)
* [pwnlib.log — Logging stuff](http://docs.pwntools.com/en/latest/log.html)
* [pwnlib.memleak — Helper class for leaking memory](http://docs.pwntools.com/en/latest/memleak.html)
* [pwnlib.qemu — QEMU Utilities](http://docs.pwntools.com/en/latest/qemu.html)
* [pwnlib.replacements — Replacements for various functions](http://docs.pwntools.com/en/latest/replacements.html)
* [pwnlib.rop.ret2dlresolve — Return to dl\_resolve](http://docs.pwntools.com/en/latest/rop/ret2dlresolve.html)
* [pwnlib.rop.rop — Return Oriented Programming](http://docs.pwntools.com/en/latest/rop/rop.html)
* [pwnlib.rop.srop — Sigreturn Oriented Programming](http://docs.pwntools.com/en/latest/rop/srop.html)
* [pwnlib.runner — Running Shellcode](http://docs.pwntools.com/en/latest/runner.html)
* [pwnlib.shellcraft — Shellcode generation](http://docs.pwntools.com/en/latest/shellcraft.html)
* [pwnlib.shellcraft.aarch64 — Shellcode for AArch64](http://docs.pwntools.com/en/latest/shellcraft/aarch64.html)
* [pwnlib.shellcraft.amd64 — Shellcode for AMD64](http://docs.pwntools.com/en/latest/shellcraft/amd64.html)
* [pwnlib.shellcraft.arm — Shellcode for ARM](http://docs.pwntools.com/en/latest/shellcraft/arm.html)
* [pwnlib.shellcraft.common — Shellcode common to all architecture](http://docs.pwntools.com/en/latest/shellcraft/common.html)
* [pwnlib.shellcraft.i386 — Shellcode for Intel 80386](http://docs.pwntools.com/en/latest/shellcraft/i386.html)
* [pwnlib.shellcraft.mips — Shellcode for MIPS](http://docs.pwntools.com/en/latest/shellcraft/mips.html)
* [pwnlib.shellcraft.thumb — Shellcode for Thumb Mode](http://docs.pwntools.com/en/latest/shellcraft/thumb.html)
* [pwnlib.term — Terminal handling](http://docs.pwntools.com/en/latest/term.html)
* [pwnlib.timeout — Timeout handling](http://docs.pwntools.com/en/latest/timeout.html)
* [pwnlib.tubes — Talking to the World!](http://docs.pwntools.com/en/latest/tubes.html)
* [pwnlib.tubes.buffer — buffer implementation for tubes](http://docs.pwntools.com/en/latest/tubes/buffer.html)
* [pwnlib.tubes.process — Processes](http://docs.pwntools.com/en/latest/tubes/processes.html)
* [pwnlib.tubes.serialtube — Serial Ports](http://docs.pwntools.com/en/latest/tubes/serial.html)
* [pwnlib.tubes.sock — Sockets](http://docs.pwntools.com/en/latest/tubes/sockets.html)
* [pwnlib.tubes.ssh — SSH](http://docs.pwntools.com/en/latest/tubes/ssh.html)
* [pwnlib.ui — Functions for user interaction](http://docs.pwntools.com/en/latest/ui.html)
* [pwnlib.update — Updating Pwntools](http://docs.pwntools.com/en/latest/update.html)
* [pwnlib.useragents — A database of useragent strings](http://docs.pwntools.com/en/latest/useragents.html)
* [pwnlib.util.crc — Calculating CRC-sums](http://docs.pwntools.com/en/latest/util/crc.html)
* [pwnlib.util.cyclic — Generation of unique sequences](http://docs.pwntools.com/en/latest/util/cyclic.html)
* [pwnlib.util.fiddling — Utilities bit fiddling](http://docs.pwntools.com/en/latest/util/fiddling.html)
* [pwnlib.util.getdents — Linux binary directory listing](http://docs.pwntools.com/en/latest/util/getdents.html)
* [pwnlib.util.hashes — Hashing functions](http://docs.pwntools.com/en/latest/util/hashes.html)
* [pwnlib.util.iters — Extension of standard module itertools](http://docs.pwntools.com/en/latest/util/iters.html)
* [pwnlib.util.lists — Operations on lists](http://docs.pwntools.com/en/latest/util/lists.html)
* [pwnlib.util.misc — We could not fit it any other place](http://docs.pwntools.com/en/latest/util/misc.html)
* [pwnlib.util.net — Networking interfaces](http://docs.pwntools.com/en/latest/util/net.html)
* [pwnlib.util.packing — Packing and unpacking of strings](http://docs.pwntools.com/en/latest/util/packing.html)
* [pwnlib.util.proc — Working with /proc/](http://docs.pwntools.com/en/latest/util/proc.html)
* [pwnlib.util.safeeval — Safe evaluation of python code](http://docs.pwntools.com/en/latest/util/safeeval.html)
* [pwnlib.util.sh\_string — Shell Expansion is Hard](http://docs.pwntools.com/en/latest/util/sh_string.html)
* [pwnlib.util.web — Utilities for working with the WWW](http://docs.pwntools.com/en/latest/util/web.html)

## Bytes

The bytes vs text distinction is so important that it even made it to this main page. See the [pwntools-tutorial](https://github.com/Gallopsled/pwntools-tutorial/blob/master/bytes.md) repo for the latest tutorial finally explaining the difference once and for all (hopefully).

# Indices and tables

* [Index](http://docs.pwntools.com/en/latest/genindex.html)
* [Module Index](http://docs.pwntools.com/en/latest/py-modindex.html)
* [Search Page](http://docs.pwntools.com/en/latest/search.html)

[Next](http://docs.pwntools.com/en/latest/about.html)