安全考量

下列模块具有专门的安全事项:

- `base64`: base64 安全事项，参见 **RFC 4648**
- `hashlib`: 所有构造器都接受一个 "usedforsecurity" 仅限关键字参数以停用已知的不安全和已封禁的算法
- `http.server` 不适合生产用途，只实现了基本的安全检查。 请参阅 安全性考量。
- `logging`: 日志记录配置使用了 eval()
- `multiprocessing`: Connection.recv() 使用了 pickle
- `pickle`: 在 pickle 中限制全局变量
- `random` 不应当被用于安全目的，而应改用 `secrets`
- `shelve`: shelve 是基于 pickle 的因此不适用于处理不受信任的源
- `ssl`: SSL/TLS 安全事项
- `subprocess`: 子进程安全事项
- `tempfile`: mktemp 由于存在竞争条件缺陷已被弃用
- `xml`: XML 安全事项
- `zipfile`: 恶意处理的 .zip 文件可能导致硬盘空间耗尽

`-I` 命令行选项可被用来在隔离模式下运行 Python。 当它无法使用时，可以使用 `-P` 选项或 `PYTHONSAFEPATH` 环境变量以避免在 `sys.path` 中预置一个潜在的不安全路径，如当前目录、脚本的目录或一个空字符串。