格式: python commix.py [选项]

选项:

-h, --help 显示帮助

General:

These options relate to general matters.

-v VERBOSE Verbosity level: 0-1 (默认 0)

--version 显示版本号和退出。

--output-dir=OUT.. 设置自定义输出目录路径。

-s SESSION\_FILE 从存储加载会话（sqlite）文件。

--flush-session 当前目标的刷新会话文件。

--ignore-session 忽略存储在会话文件中的结果。

目标:

必须提供此选项，以定义目标网址。

-u URL, --url=URL 目标URL

--url-reload 命令执行后重新加载目标网址。

-l LOGFILE Parse target and data from HTTP proxy log file.

要求:

这些选项可以用来指定如何连接到目标网址。

--data=DATA 将要发送的数据字符串。

--host=HOST HTTP主机头。

--referer=REFERER HTTP Referer报头。

--user-agent=AGENT HTTP用户代理标头。

--random-agent 使用一个随机选择的HTTP用户代理标头。

--param-del=PDEL 用于分割参数值的设置字符。

--cookie=COOKIE HTTP Cookie标头。

--cookie-del=CDEL 用于分割饼干值的设置字符。

--headers=HEADERS 额外的标头 (e.g. 'Header1:Value1\nHeader2:Value2').

--proxy=PROXY 使用HTTP代理 (e.g. '127.0.0.1:8080').

--tor 使用Tor网络。

--tor-port=TOR\_P.. 设置Tor代理服务器端口(Default: 8118).

--auth-url=AUTH\_.. 网址登录面板。

--auth-data=AUTH.. 登录参数和数据。

--auth-type=AUTH.. HTTP身份验证类型(e.g. 'Basic' or 'Digest').

--auth-cred=AUTH.. HTTP认证证书 (e.g. 'admin:admin').

--ignore-401 忽略HTTP错误401(Unauthorized).

--force-ssl 使用SSL / HTTPS力。

枚举:

这些选项可以用来枚举目标主机。

--all 挽回一切。

--current-user 检索当前用户名。

--hostname 检索当前主机名。

--is-root 检查当前用户是否有根权限。

--is-admin 检查当前用户是否有管理权限。

--sys-info 检索系统信息。

--users 检索系统用户。

--passwords 检索系统用户密码的哈希值。

--privileges 检索系统用户权限。

--ps-version 检索PowerShell的版本号。

文件访问:

这些选项可用于访问目标主机上的文件。

--file-read=FILE.. 从目标主机读取一个文件。

--file-write=FIL.. 写入目标主机上的文件。

--file-upload=FI.. 在目标主机上上传一个文件。

--file-dest=FILE.. 主机的绝对路径写和/或上传。

模块：:

这些选项可以使用增加的检测和/或注射/使用

--icmp-exfil=IP\_.. “ICMP渗出的注射模。

(e.g. 'ip\_src=192.168.178.1,ip\_dst=192.168.178.3').

--dns-server=DNS.. “DNS渗出的注射模。

(Domain name used for DNS exfiltration attack).

--shellshock “Shellshock”注入模块。

注射:

这些选项可以用来指定要注入的参数和提供自定义注入有效载荷。

-p TEST\_PARAMETER 可检验参数（s）

--suffix=SUFFIX 注入有效载荷后缀字符串。

--prefix=PREFIX 注入有效载荷前缀字符串。

--technique=TECH 指定使用的注入技术。

--maxlen=MAXLEN 设置与时间相关的输出的最大长度

injection techniques (Default: 10000 chars).

--delay=DELAY 设置时间相关的注入技术的自定义时间延迟(Default: 1 sec).

--tmp-path=TMP\_P.. 设置Web服务器的临时目录的绝对路径。

--root-dir=SRV\_R.. 设置Web服务器的根目录的绝对路径。

--alter-shell=AL.. 使用另一种操作系统外壳（例如“任务”）。

--os-cmd=OS\_CMD 执行一个单一的操作系统命令。

--os=OS 强制后端操作系统到这个值。

--tamper=TAMPER 用于篡改注入数据的给定脚本（s）。

检测:

这些选项可用于自定义检测阶段。

--level=LEVEL 执行测试水平 (1-3, 默认: 1).

--skip-calc 跳过检测阶段的数学计算。

其他:

--dependencies 检查第三方（非核心）的依赖关系。

--skip-waf 跳过WAF／IPS / IDS保护启发式检测。