General:

Estas opciones se relacionan con asuntos generales.

-v VERBOSE Nivel de verbosidad (0-4, Predeterminado: 0).

--version Muestra el número de versión y sale.

--output-dir=OUT.. Establece la ruta del directorio de salida personalizado.

-s SESSION\_FILE Carga la sesión desde un archivo almacenado (.sqlite).

--flush-session Limpia los archivos de sesión del destino actual.

--ignore-session Ignora los resultados almacenados en el archivo de sesión.

-t TRAFFIC\_FILE Registra todo el tráfico HTTP en un archivo de texto.

--batch Nunca solicita la entrada del usuario, utiliza el comportamiento predeterminado.

--skip-heuristics Omite la detección heurística para la inyección de código.

--codec=CODEC Fuerza el códec para la codificación de caracteres (p. ej., 'ascii').

--charset=CHARSET Conjunto de caracteres de inyección relacionado con el tiempo (p. ej.,

"0123456789abcdef")

--check-internet Verifica la conexión a Internet antes de evaluar el destino.

--answers=RESPUESTAS Establece respuestas predefinidas (p. ej., "quit=N,follow=N")

Destino:

Esta opción debe proporcionarse para definir la URL de destino.

-u URL, --url=URL URL de destino.

--url-reload Recarga la URL de destino después de la ejecución del comando.

-l LOGFILE Analiza el destino desde el archivo de registro del proxy HTTP.

-m BULKFILE Analiza múltiples destinos proporcionados en un archivo de texto.

-r REQUESTFILE Carga la solicitud HTTP desde un archivo.

--crawl=CRAWLDEPTH Rastrea el sitio web comenzando desde la URL de destino

(Predeterminado: 1).

--crawl-exclude=.. Regexp para excluir páginas del rastreo (p. ej., "logout").

-x SITEMAP\_URL Analiza el destino(s) desde el archivo sitemap(.xml) remoto.

--method=METHOD Fuerza el uso del método HTTP dado (p. ej., PUT)

Solicitud:

Estas opciones se pueden usar para especificar cómo conectarse a la URL de destino.

-d DATA, --data=.. Cadena de datos que se enviará a través de POST.

--host=HOST Encabezado de host HTTP.

--referer=REFERER Encabezado de referencia HTTP.

--user-agent=AGENT Encabezado de agente de usuario HTTP.

--random-agent Utiliza un encabezado de agente de usuario HTTP seleccionado aleatoriamente.

--param-del=PDEL Establece el carácter para dividir los valores de los parámetros.

--cookie=COOKIE Encabezado de cookie HTTP.

--cookie-del=CDEL Establece el carácter para dividir los valores de las cookies.

-H HEADER, --hea.. Encabezado adicional (p. ej., 'X-Forwarded-For: 127.0.0.1').

--headers=HEADERS Encabezados adicionales (p. ej., 'Accept-Language: fr\nETag: 123').

--proxy=PROXY Utiliza un proxy para conectarse a la URL de destino.

--tor Utiliza la red Tor.

--tor-port=TOR\_P.. Establece el puerto del proxy Tor (predeterminado: 8118).

--tor-check Comprueba si Tor se utiliza correctamente.

--auth-url=AUTH\_.. URL del panel de inicio de sesión.

--auth-data=AUTH.. Parámetros y datos de inicio de sesión.

--auth-type=AUTH.. Tipo de autenticación HTTP (básica, resumen, portadora).

--auth-cred=AUTH.. Credenciales de autenticación HTTP (p. ej., 'admin:admin').

--ignore-code=IG.. Ignora el código de error HTTP (problemático) (p. ej., 401).

--force-ssl Fuerza el uso de SSL/HTTPS.

--ignore-proxy Ignora la configuración predeterminada del proxy del sistema.

--ignore-redirects Ignora los intentos de redirección.

--timeout=TIMEOUT Segundos de espera antes de que se agote el tiempo de espera de la conexión (predeterminado:

30).

--retries=RETRIES Reintenta cuando se agota el tiempo de espera de la conexión (predeterminado: 3).

--drop-set-cookie Ignora el encabezado Set-Cookie de la respuesta.

Enumeración:

Estas opciones se pueden usar para enumerar el host de destino.

--all Recupera todo.

--current-user Recupera el nombre del usuario actual.

--hostname Recupera el nombre del host actual.

--is-root Comprueba si el usuario actual tiene privilegios de root.

--is-admin Comprueba si el usuario actual tiene privilegios de administrador.

--sys-info Recupera información del sistema.

--users Recupera usuarios del sistema.

--passwords Recupera hashes de contraseñas de usuarios del sistema.

--privileges Recupera privilegios de usuarios del sistema.

--ps-version Recupera el número de versión de PowerShell.

Acceso a archivos:

Estas opciones se pueden usar para acceder a archivos en el host de destino.

--file-read=FILE.. Lee un archivo del host de destino.

--file-write=FIL.. Escribe en un archivo en el host de destino.

--file-upload=FI.. Sube un archivo al host de destino.

--file-dest=FILE.. Ruta absoluta del archivo del host donde se escribirá y/o cargará.

Módulos:

Estas opciones se pueden utilizar para aumentar las capacidades de detección y/o inyección.

--shellshock El módulo de inyección 'shellshock'.

Inyección:

Estas opciones se pueden usar para especificar qué parámetros se deben inyectar y para

proporcionar cargas útiles de inyección personalizadas.

-p TEST\_PARAMETER Parámetros que se pueden probar.

--skip=SKIP\_PARA.. Omitir la prueba de los parámetros dados.

--suffix=SUFFIX Cadena de sufijo de carga útil de inyección.

--prefix=PREFIX Cadena de prefijo de carga útil de inyección.

--technique=TECH Especifique las técnicas de inyección que se utilizarán.

--skip-technique.. Especifique las técnicas de inyección que se omitirán.

--maxlen=MAXLEN Establezca la longitud máxima de salida para las técnicas de inyección relacionadas con el tiempo (predeterminado: 10000 caracteres).

--delay=DELAY Segundos de demora entre cada solicitud HTTP.

--time-sec=TIMESEC Segundos de demora de la respuesta del SO (predeterminado: 1).

--tmp-path=TMP\_P.. Establezca la ruta absoluta del directorio temporal del servidor web.

--web-root=WEB\_R.. Establece el directorio raíz de documentos del servidor web (p. ej., '/var/www').

--alter-shell=AL.. Utiliza un sistema operativo alternativo (p. ej., 'Python').

--os-cmd=OS\_CMD Ejecuta un solo comando del sistema operativo.

--os=OS Fuerza el sistema operativo back-end (p. ej., 'Windows' o

'Unix').

--tamper=TAMPER Utiliza los scripts indicados para manipular los datos de inyección.

--msf-path=MSF\_P.. Establece una ruta local donde se instala metasploit.

Detección:

Estas opciones se pueden utilizar para personalizar la fase de detección.

--level=LEVEL Nivel de pruebas a realizar (1-3, Predeterminado: 1).

--skip-calc Omite el cálculo matemático durante la fase de

detección.

--skip-empty Omite la prueba de los parámetros con valores vacíos.

--failed-tries=F.. Establece una cantidad de intentos de inyección fallidos, en una técnica basada en archivos.

--smart Realiza pruebas exhaustivas solo si las heurísticas son positivas.

Varios:

--ignore-depende.. Ignora todas las dependencias de bibliotecas de terceros requeridas.

--list-tampers Muestra una lista de scripts de manipulación disponibles.

--alert=ALERTA Ejecuta los comandos del sistema operativo host cuando se encuentra el punto de inyección.

--no-logging Deshabilita el registro en un archivo.

--purge Elimina de forma segura todo el contenido del directorio de datos de commix.

--skip-waf Omite la detección heurística de protección WAF/IPS/IDS.

--mobile Imita un teléfono inteligente a través del encabezado User-Agent HTTP.

--offline Trabaja en modo sin conexión.

--wizard Interfaz de asistente simple para usuarios principiantes.

--disable-coloring Deshabilita la coloración de la salida de la consola.