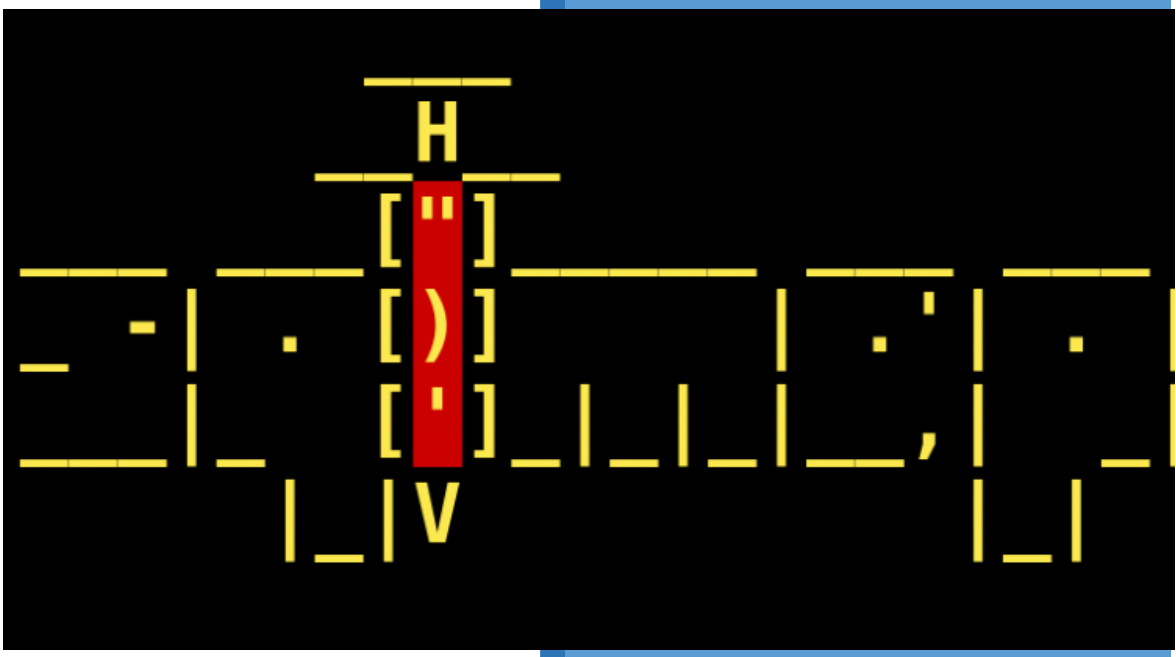
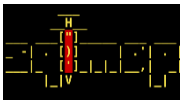
MANUAL DE COMANDOS SQLMAP

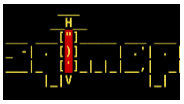


WEB: https://elhackeretico.com/

EL HACKER ETICO



INDICE



AUDITORIA DE SEGURIDAD EN BASES DE DATOS CON SQLMAP

OPCIONES

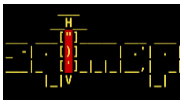
Comando	Funcionalidad
-h / --hh	Ayuda / ayuda avanzada
-v	Verbose. 0 – 6 (por defecto 1)
--version	Muestra la versión del script

OBJETIVO (TARGET)

Comando	Funcionalidad
-u	URL objetivo
-m	Objetivos incluidos en un archivo
-r	Cargar archivo con petición HTTP
-c	Carga opciones desde archivo INI
-d	Conexión directa con la base de datos
-l	Carga archivo de logs
-g	Google Dorks como objetivo

PETICIONES

Comando	Funcionalidad
--data	Cadena de datos a enviar a través de POST
--param-del	Carácter utilizado para dividir valores de parámetros
--cookie	Cabecera de la cookie HTTP
--cookie-urlencode	Codifica las inyecciones de cookies generadas
--load-cookies	Archivo que contiene cookies en formato Netscape
--drop-set-cookie	Ignorar el encabezado Set-Cookie de la respuesta
--user-agent	Encabezado de agente de usuario HTTP
--host	Cabecera de host HTTP
--random-agent	Usa el encabezado de agente de usuario HTTP seleccionado aleatoriamente
--auth-type	Tipo de autenticación HTTP
--auth-cred	Credenciales de autenticación HTTP
--proxy	Utiliza un proxy HTTP para conectarse a la URL de destino
--proxy-file	Cargar lista de proxy desde un archivo
–tor-port=TPORT	Establece un puerto proxy Tor diferente al predeterminado
--check-for	Comprueba si Tor se usa correctamente
--delay	Retraso en segundos entre cada solicitud HTTP
--timeout	Segundos de espera antes de la conexión de tiempo de espera
--retries	Vuelve a intentar cuando se agota el tiempo de espera de la conexión
--randomize	Cambia aleatoriamente el valor de los parámetros dados
--safe-url	SAFEURL para visitar con frecuencia durante la prueba
--safe-freq	Prueba solicitudes entre dos visitas a una URL segura determinada
--skip-urlencode	Salta la codificación de URL de datos de carga útil



-hpp	**Utilizar método de contaminación de parámetros HTTP**
--force-ssl	**Forzar el uso de solicitudes SSL/HTTPS**
--referer	**Cabecera de referencia HTTP**
--eval	**Evalúa el código de Python proporcionado antes de la solicitud**
--csrf-token	**Parámetro utilizado para contener el token anti-CSRF**
--csrf-url	**Dirección URL a visitar para la extracción del token anti-CSRF**

OPTIMIZACIÓN

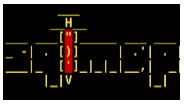
Comando	Funcionalidad
-o	**Activa todos los interruptores de optimización**
--predict-output	**Predice la salida de consultas comunes**
--keep-alive	**Usa conexiones HTTP(s) persistentes**
--null-connection	**Recupera la longitud de la página sin el cuerpo real de la respuesta HTTP**
--threads	**Número máximo de solicitudes HTTP(s) simultáneas (predeterminado 1)**

INYECCIÓN

Comando	Funcionalidad
-p	**Parámetros comprobables**
--skip	**Omite pruebas para parámetros dados**
--skip-static	**Omite parámetros de prueba que no parecen ser dinámico**
--param-exclude	**Regexp para excluir parámetros de las pruebas**
--dbms	**Fuerza back-end DBMS al valor proporcionado**
--dbms-cred	**Credenciales de autenticación de DBMS**
--os	**Fuerza el sistema operativo back-end DBMS al valor proporcionado**
--invalid-bignum	**Usa números grandes para invalidar valores**
--invalid-logical	**Usa operaciones lógicas para invalidar valores**
--invalid-string	**Usa cadenas aleatorias para invalidar valores**
--no-cast	**Desactiva el mecanismo de conversión de carga útil**
--no-escape	**Desactiva el mecanismo de escape de cadena**
--prefix	**Inyecta una carga útil a la cadena de prefijo**
--suffix	**Inyecta una carga útil a la cadena de sufijo**
--tamper	**Usa secuencias de comandos dadas para manipular datos de inyección**

DETECCIÓN

Comando	Funcionalidad
--level	**Nivel de pruebas a realizar (1-5, predeterminado 1)**
--risk	**Riesgo de pruebas a realizar (1-3, predeterminado 1)**
--string	**Cadena para que coincida cuando la consulta se evalúa como True**
--not-string	**Cadena para que coincida cuando la consulta se evalúa como False**



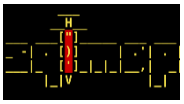
--regexp	**Regexp para que coincida cuando la consulta se evalúa como True**
--code	**Código HTTP que coincide cuando la consulta se evalúa como True**
--text-only	**Compara páginas basadas solo en el contenido textual**
--titles	**Compara páginas basadas solo en sus títulos**

TÉCNICAS

Comando	Funcionalidad
--technique	**Técnicas de inyección de SQL a usar**
--time-sec	**Segundos para retrasar la respuesta DBMS**
--union-cols	**Rango de columnas para probar UNION query SQL inyección**
--union-char	**Carácter a usar para la fuerza bruta número de columnas**
--union-from	**Tabla a usar en la parte FROM de la consulta UNION Inyección SQL**
--dns-domain	**Nombre de dominio usado para el ataque de exfiltración de DNS**
--second-url	**Se busca una respuesta de segundo orden en la URL de la página resultante**
--second-req	**Carga una solicitud HTTP de segundo orden desde el archivo**

ENUMERACIÓN

Comando	Funcionalidad
-a, --all	**Recuperar todo**
-b, --banner	**Recuperar banner DBMS**
--users	**Enumerar usuarios de DBMS**
--password	**Enumera los hashes de contraseña de los usuarios de DBMS**
--roles	**Enumera los roles de los usuarios de DBMS**
--privileges	**Enumera los privilegios de los usuarios de DBMS**
--dbs	**Enumerar bases de datos DBMS**
--tables	**Enumera las tablas de la base de datos DBMS**
--column	**Enumera las columnas de la tabla de la base de datos DBMS**
--schema	**Enumera el esquema DBMS**
--count	**Recupera el número de entradas para la(s) tabla(s)**
--dump-all	**Vuelca todas las entradas de tablas de bases de datos DBMS**
--dump	**Volcar las entradas de la tabla de la base de datos DBMS**
--search	**Buscar columna(s), tabla(s) y/o nombre(s) de base de datos**
-U	**Usuario a enumerar**
-C	**Columna(s) de la tabla de la base de datos DBMS para enumerar**
-T	**Tabla(s) de base de datos para enumerar**



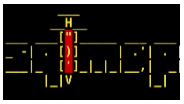
-X	**Excluye identificadores de base de datos DBMS para no enumerar**
--where	**Usa la condición WHERE al volcar la tabla**
--start	**Primera entrada de la tabla de volcado para recuperar**
--stop	**Última entrada de la tabla de volcado para recuperar**
--first	**Primer carácter de palabra de salida de consulta para recuperar**
--last	**Último carácter de palabra de salida de consulta para recuperar**
--sql-file	**Sentencia SQL a ejecutar**
--sql-shell	**Solicitud de un shell de SQL interactivo**
--sql-file	**Ejecuta sentencias SQL desde archivo(s) dado(s)**

GENERAL

Comando	Funcionalidad
-s	**Cargar sesión desde un archivo almacenado**
-t	**Registrar todo el tráfico HTTP en un archivo de texto**
--batch	**Nunca solicite la entrada del usuario, use el comportamiento predeterminado**
--eta	**Mostrar para cada salida la hora estimada de llegada**
--save	**Guardar opciones en un archivo INI de configuración**
--update	**Actualizar sqlmap**
--charset	**Juego de caracteres de inyección SQL ciego**
--crawl	**Rastrear el sitio web a partir de la URL de destino**
--csv-del	**Carácter delimitador utilizado en la salida CSV**
--dump-format	**Formato de datos volcados (CSV (predeterminado), HTML o SQLITE)**
--flush-session	**Vaciar archivos de sesión para el objetivo actual**
--forms	**Analizar y probar formularios en la URL de destino**
--fresh-queries	**Ignorar los resultados de la consulta almacenados en el archivo de sesión**
--hex	**Usar conversión hexadecimal durante la recuperación de datos**
--output-dir	**Ruta personalizada del directorio de salida**
--parse-errors	**Analizar y mostrar mensajes de error de DBMS de las respuestas**
--preprocess	**Usar secuencias de comandos dadas para el preprocesamiento de los datos de respuesta**
--scope	**Regexp para filtrar objetivos del registro de proxy proporcionado**
--test-filter	**Seleccionar pruebas por cargas y/o títulos**

FINGERPRINT

Comando	Funcionalidad
-f, --fingerprint	**Realiza una extensa versión de la huella digital de DBMS**



AUDITORIA DE SEGURIDAD EN BASES DE DATOS CON SQLMAP

BRUTE FORCE

Comando	Funcionalidad
--common-tables	Verifica la existencia de tablas comunes
--common-columns	Comprueba la existencia de columnas comunes

FUNCIÓN INYECCIÓN DEFINIDA POR EL USUARIO

Comando	Funcionalidad
--udf-inject	Inyecta funciones personalizadas definidas por el usuario
--shared-lib	Ruta local de la biblioteca compartida

ACCESO AL SISTEMA DE FICHEROS

Comando	Funcionalidad
--file-read	Lee un archivo del sistema de archivos DBMS de back-end
--file-write	Escribe un archivo local en el sistema de archivos DBMS de back-end
--file-dest	Ruta de archivo absoluta de DBMS back-end para escribir

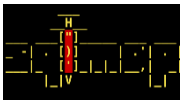
ACCESO AL SISTEMA OEPRATIVO

Comando	Funcionalidad
--os-cmd	Ejecuta un comando del sistema operativo
--os-shell	Solicita un shell de sistema operativo interactivo
--os-pwn	Solicita un shell OOB, Meterpreter o VNC
--os-smbrelay	Solicita un clic para un shell OOB, Meterpreter o VNC
--os-bof	Explotación de desbordamiento de búfer de procedimiento almacenado
--priv-esc	Escalamiento de privilegios de usuario del proceso de la base de datos
--msf-path	Ruta local donde está instalado Metasploit Framework
--tmp-path	Ruta absoluta remota del directorio de archivos temporales

ACCESO AL REGISTRO DE WINDOWS

Comando	Funcionalidad
--reg-read	Lee un valor de clave de registro de Windows
--reg-add	Escribi un valor de clave de registro de Windows data
--reg-del	Elimina un valor de clave de registro de Windows
--reg-key	Genera clave de registro Windows
--reg-value	Valor de clave de registro de Windows
--reg-data	Datos de valor de clave de registro de Windows
--reg-type	Tipo de valor de clave de registro de Windows

COMANDOS DIVERSOS



AUDITORIA DE SEGURIDAD EN BASES DE DATOS CON SQLMAP

Comando	Funcionalidad
-z	Usa mnemotécnicos cortos
--alert	Ejecuta comando(s) del sistema operativo del host cuando se encuentra inyección SQL
--answer	Establece respuestas predefinidas
--check-waf / --identify-waf	Realiza una prueba exhaustiva para una protección WAF/IPS
--cleanup	Limpia el DBMS de tablas y UDF específicos de sqlmap
--dependencies	Verifica si faltan dependencias de sqlmap (opcional)
--gpage	Usa los resultados de Google dork del número de página especificado
--mobile	Imita el teléfono inteligente a través del encabezado HTTP User-Agent
--purge	Elimina de forma segura todo el contenido del directorio de datos de sqlmap
--smart	Realiza pruebas exhaustivas solo si las heurísticas son positivas
--disable-coloring	Deshabilita el coloreado de salida de la consola
--wizard	Interfaz de asistente simple para usuarios principiantes