sqlmap Cheat Sheet

Installation

```
sudo apt install sqlmap
```

Basic usage

Command	Description
`sqlmap -u <url>`	Run scan against a URL
`sqlmap -r <file>`	Run scan on HTTP request file
`sqlmap --wizard`	Interactive wizard
`sqlmap -h`	Show basic help message
`sqlmap -hh`	Show advanced help message
`sqlmap --version`	Show sqlmap version

Basic options

Option	Description
`-v <verbosity>`	Set verbosity level (0-6)
`--batch`	Don't ask for user input

Target specification

Option	Description
`-u <url>`	Target URL
`-m <file>`	Scan target URLs from a given text file
`-g <query>`	Target Google dork result URLs
`--crawl=<depth>`	Crawl a website starting from the target URL

HTTP request options

Option	Description
`--data 'uid=1&name=test'`	Send a POST request with data
`-H <header>`	Specify a header
`--cookie='PHPSESSID=1234'`	Specify a cookie header
`--user-agent=<ua>`	HTTP user-agent header value

WAF bypass options

Option	Description
`--random-agent`	Use random user-agent
`--csrf-token=<param>`	CSRF token parameter name
`--tamper=<tamper>`	Use tamper script
`--list-tampers`	List available tamper scripts

IP address concealment

Option	Description
`--proxy=<address>`	Use a proxy server
`--tor`	Use Tor anonymity network
`--check-tor`	Ensure that Tor is used properly

Detection options

Option	Description
`--level=LEVEL`	Level of tests to perform (1-5)
`--risk=RISK`	Risk of tests to perform (1-3)
`--technique=<techniques>`	SQL injection techniques to use (default "BEUSTQ", see below)

Injection techniques

Technique	Description
Boolean-based blind (B)	Appends AND/OR to test for true/false responses
Error-based (E)	Forces DBMS to generate an error
UNION query-based (U)	Appends `UNION SELECT`
Stacked queries (S)	Appends `;` to execute multiple queries
Time-based blind (T)	Appends `SLEEP()` to delay response
Inline queries (Q)	Appends inline queries

Session options

Option	Description
`--flush-session`	Flush session files for current target
`--fresh-queries`	Ignore query results stored in session file
`--purge`	Remove all data from session files

Enumeration & exploitation options

Option	Description
`--all`	Retrieve everything
`--banner`	Retrieve DBMS banner
`--fingerprint`	Perform an extensive DBMS version fingerprint
`--current-user`	Retrieve current user
`--current-db`	Retrieve current database
`--dbs`	List databases
`--tables`	List tables
`--columns`	List columns
`--schema`	Enumerate database schema
`--dump`	Dump table entries
`--dump-all`	Dump table entries for all databases
`-D <database>`	Database to enumerate
`-T <table>`	Table(s) to enumerate
`-C <column>`	Table column(s) to enumerate
`--file-read=<file>`	Read a file from the file system
`--os-shell`	Prompt for an interactive shell

Output

Option	Description
`-t <file>`	Save requests and responses to a file