sqlmap Cheat Sheet

Installation

sudo apt install sqlmap

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

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

Target specification	
Option	Description
-u <url></url>	Target URL
-m <file></file>	Scan target URLs from a given text file
-g <query></query>	Target Google dork result URLs
crawl= <depth></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></header>	Specify a header
cookie='PHPSESSID=1234'	Specify a cookie header
user-agent= <ua></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></tamper>	Use tamper script
list-tampers	List available tamper scripts

ir dudress concediment	
Option	Description
proxy= <address></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></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 & expl	oitation 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>	Database to enumerate
-T	Table(s) to enumerate
-C <column></column>	Table column(s) to enumerate
file-read= <file></file>	Read a file from the file system
os-shell	Prompt for an interactive shell

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