

Forum:[Hack Forums](#)

Thread: [\[Basic\] SQLMap](#)

Biggy_Asian - October 8, 2024, 1:42 am

Site: <https://sqlmap.org/>

Git: <https://github.com/sqlmapproject/sqlmap>

Kali linux: <https://www.kali.org/>

SQLMap is an SQL Injection tool that will attempt to SQL Inject many types of databases in the hopes of accessing the target database. This tool is old however it is still gold and can still be used. However keep in mind it will not always be viable in some cases. Like all tools they have their limits and drawbacks.

This post is less of a tutorial and more of a start for those whom want to learn. You will use this at some point in the future (I know because I have my self even).

I am not covering a lot of the kinds of arguments you could use when playing with sqlmap however you can always setup your own website that is vulnerable to SQL injections.

Cloning SQLMap:

Code `git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev`Quote:sqlmap works out of the box with Python version 2.6, 2.7 and 3.x on any platform.

Running help:

Code `python sqlmap.py -h`

Running the wizard:

Code `python sqlmap.py -wizzard`

I have SQLMap setup differently via the default installation on Kali so the commands will be slightly different.

Example usage of SQLMap:

Code `sqlmap -u "https://localhost.com" --data="username=123&password=123" --level 3 --risk 3`

Q: So what is happening here?

A: If you understand what is said within the help text and align the commands you can understand pretty easily however I will explain for you still.

Below I will break the script down.

Code `sqlmap # Runs sqlmap`

`-u "https://localhost.com" # defines the target host as "https://localhost.com"`

`--data="username=123&password=123" # The query data sent to the server (url?query=value)`

`--level 3 # tests to perform (1-5)`

`--risk 3 # the risk of the tests (1-5)`

Keep note that the higher the risk/level the longer the process may take. I recommend you start without parsing level/risk and if it fails then you increment by one until you hit 5.

The value within the query will be ignored and replaced with payloads. The only thing you really need is just the query names like "username=" or "password=" but again it doesn't matter about parsing the value as it gets replaced either way (at least in my case anyway).

Bastille - *October 8, 2024, 3:43 am*

That's the kind of content I like to see on HF ? more hacking stuff,

I don't remember using a single time SQLmap, or maybe it's been so long that I don't remember, thanks for the share, I should definitely give it a (re)try

Biggy_Asian - *October 8, 2024, 4:35 am*

(Oct 8, 2024 03:43 AM)Bastille Wrote: [\[CITE\]](#) That's the kind of content I like to see on HF ? more hacking stuff,

I don't remember using a single time SQLmap, or maybe it's been so long that I don't remember, thanks for the share, I should definitely give it a (re)try

It stills works just need to implement some sort of WAF bypass when the time comes which isnt built in sadly one of the things I wish SQLMap had...