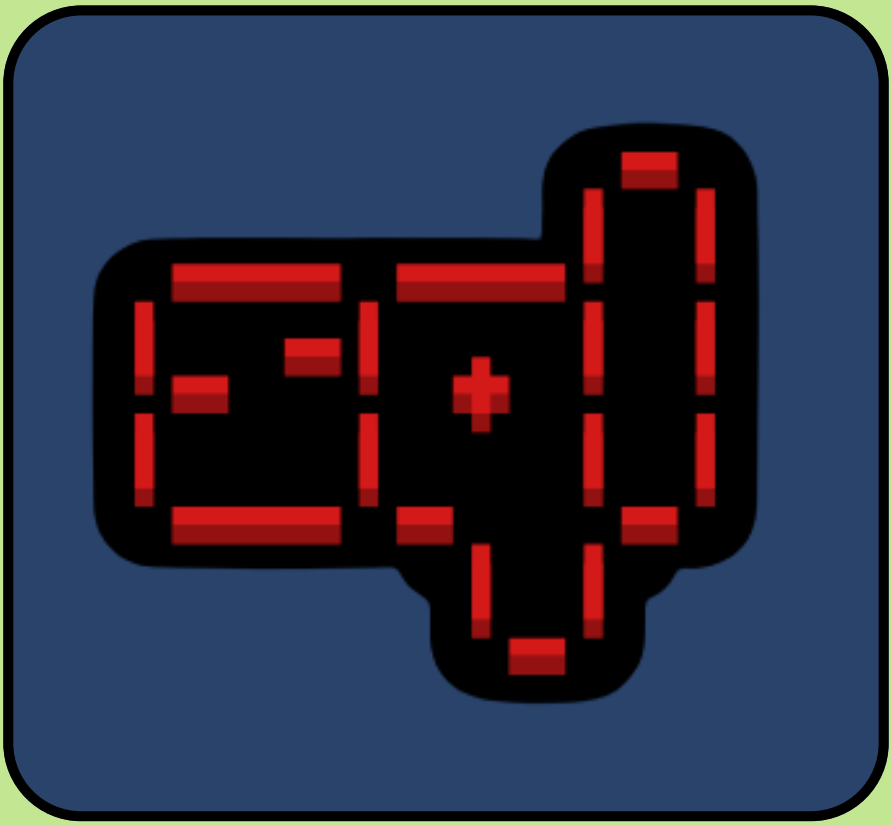
Sqlmap



SQL Injection

Disclaimer/Warning

The Kali Guides provided to you by the Cyber Tech Awareness team are meant for educational purposes ONLY.

The tools covered in the Kali Guides can be used for malicious purposes, but should not be used as such.

The CyberTech Awareness team and the Leahy Center for Digital Forensics and Cybersecurity is NOT responsible any malicious activity conduced with aid from these Kali Guides.

Only use this tool on domains, addresses, files and resources that you have permission to.

Brief Summary

Sqlmap is a tool created to detect potential **SQL injection** vulnerabilities by using automated discovery.

Since the only way to practice this tool is by using live sites, you do need to either practice by using a customized virtual environment, your own websites with SQL injection vulnerabilities, or sites meant to emulate sites with vulnerabilities.

We recommend using WebSecurity Academy to practice using Sqlmap in a safe enviorment.
(https://portswigger.net/web-security)

Helpful Vocabulary

IP Address:

- An Internet Protocol (IP) Address, is similar to a physical home or mailing address. All devices that are connected to the internet have a unique IP address. This allows devices to communicate and send information to specific devices using their IP address.

Domain Names:

- When we want to go a specific website, you need the IP address of the site to access it. Instead of having to remember IP addresses, we can just type in the domain that is associated with a certain IP, and it will be translated to an IP address for you.

URL

- Uniform Resource Locator. These are the full addresses for websites. Domain names make up a portion of a URL, but domain names alone cannot bring a user to a specific place on a site. An example of a URL is https://www.kali.org/docs/.

SQL

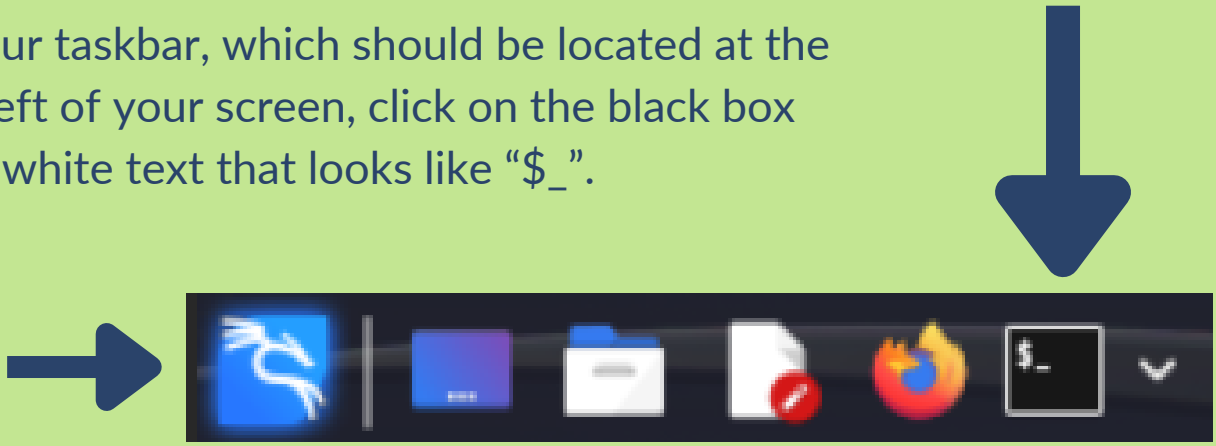
- Structured Query Language. This is a programming language created for storing and processing data in databases. This is one of the most important languages for data management.

SQL Injection

- process of asking the SQL server to do something it shouldn't do. When a webpage isn't secured correctly, those who connect to a website can write SQL code to request information from servers. Information which usually shouldn't be displayed, like passwords and usernames, could be shown to someone who writes SQL injections.

How to Access Sqlmap Through the Terminal

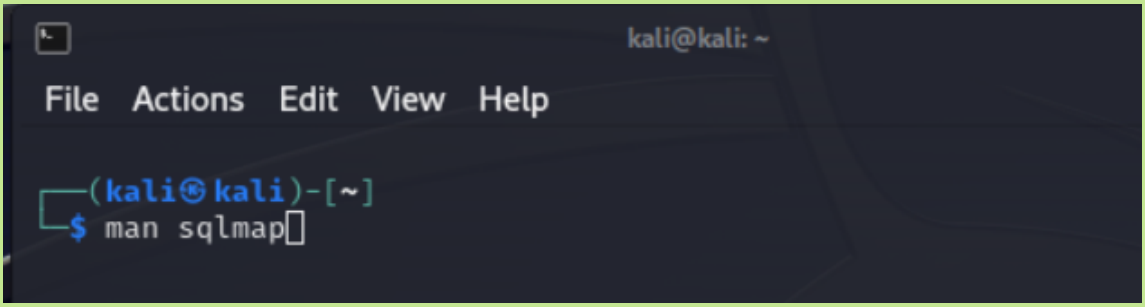
In your taskbar, which should be located at the top left of your screen, click on the black box with white text that looks like “$_”.



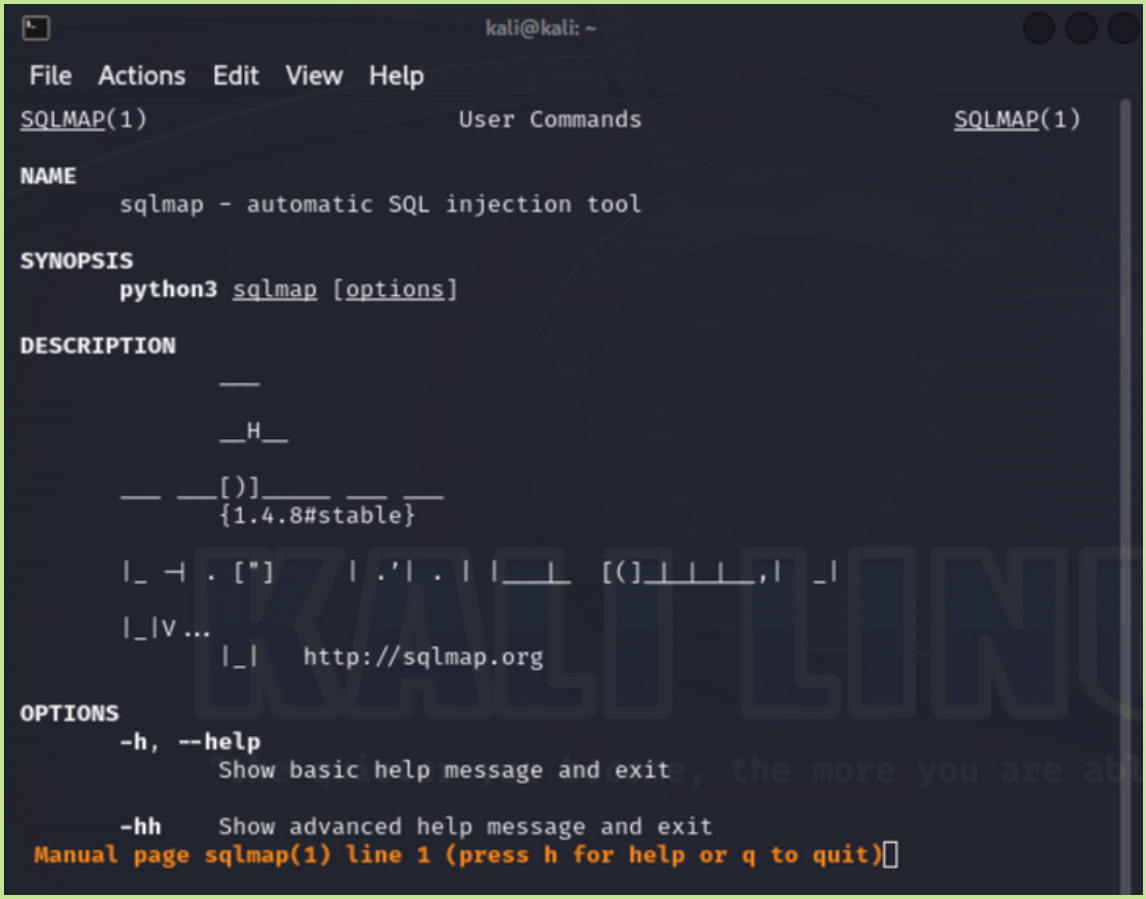
*If the black box isn't there, click on the blue dragon symbol and type “**Terminal Emulator**” into the search bar.*

This is what the terminal looks like once it’s opened. The default user is “kali@kali” and when you are actually running a sqlmap command it will be followed by other options.

How to Find the Manual for Commands and Tools



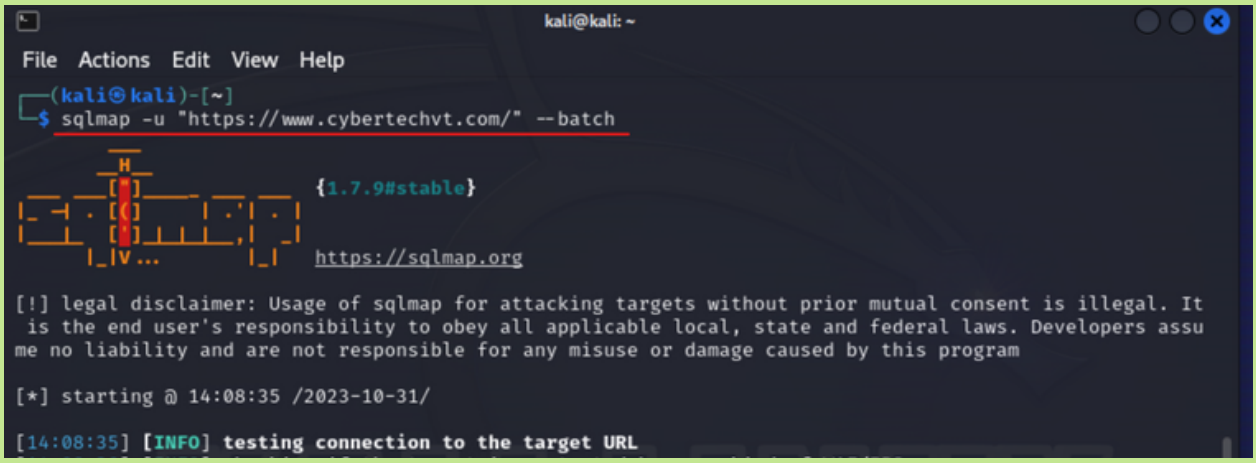
The “man” command displays the manual for the command that can be run in the terminal.



Above is the user manual for the “sqlmap” command

Example : sqlmap -u “URL” --batch

*****ONLY USE THIS COMMAND ON CONNECTIONS YOU’RE AUTHORIZED TO SCAN*****



What is this command doing?

The command will take the provided URL and run a systematic scan to determine any potential SQL vulnerabilities built into the URL or elements of the site. It will display the status of sqlmap and potential information the user may want to know in the terminal.

sqlmap

- Specifies that **sqlmap** is being used

-u

- Uses the next given string as the target URL

”URL”

- The URL of a site which you are allowed to scan for potential SQL injections

--batch

- There are two dashes before “batch”. During the process of a sqlmap scan, sqlmap will ask for permission to do some tasks. --batch tells the program to do the default option instead of asking.

Additional Resources:

Kali Linux SQLmap Official Webpage:
https://www.kali.org/tools/sqlmap/

OWASP Juice Shop:
https://owasp.org/www-project-juice-shop/

Set up the OWASP Juice Shop on Kali with Docker [Quickest Method]:
https://cybr.com/beginner-archives/set-up-the-owasp-juice-shop-on-kali-with-docker-quickest-method/

Bypass admin login with SQL Injections(sqlmap):
https://medium.com/@christophelimpalair/bypass-admin-login-with-sql-injections-sqlmap-bb60d447a1e2