Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

ILABS

CEH PRACTICAL

@mmar

Aim

Sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features, and a broad range of switches

In this task, we will use sqlmap to perform SQL injection attack against MSSQL to extract databases. you will pretend that you are a registered user on the http://www.moviescope.com website, and you want to crack the passwords of the other users from the website's database.

Other SQL Injection tools

- ✓ Mole (https://sourceforge.net)
- ✓ Blisqy (https://github.com)
- ✓ blind-sql-bitshifting (https://github.com)
- ✓ NoSQLMap (https://github.com)

DEMO

THANKS