# 

# 

# Sqlmap

Een automatische SQL-injectie en database-overname tool

Sqlmap is een open source penetratietesttool die het proces automatiseert van het detecteren en misbruiken van SQL-injectiefouten en het overnemen van databaseservers. Het wordt geleverd met een krachtig detectiemechanisme, vele niche-functies voor de ultieme penetratietester en een breed scala aan switches, gaande van databasevingerafdruk, over gegevens die uit de database worden opgehaald, tot toegang tot het onderliggende bestandssysteem en opdrachten op het besturingssysteem via uitbesteding, of-band verbindingen

## Benodigde software

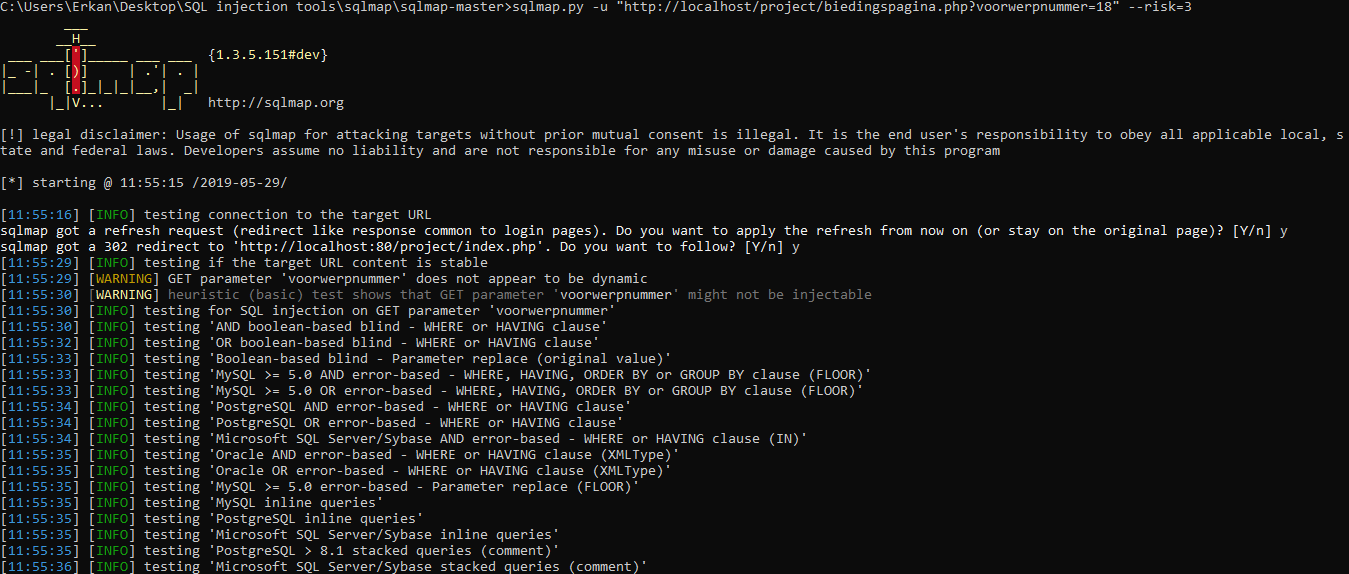
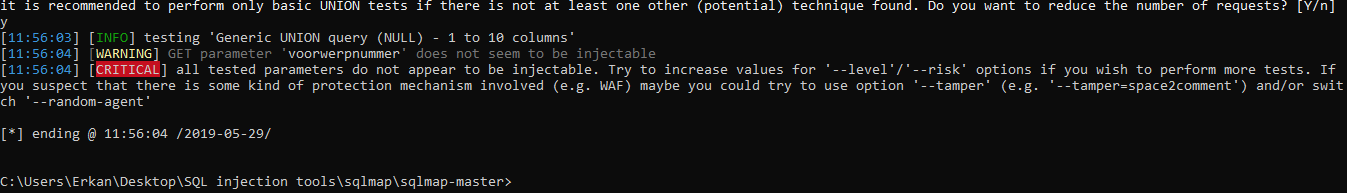
* Python versie 2.6, 2.7 en 3.x (uitgevoerd op versie 2.6.0).
* GitHub: <https://github.com/sqlmapproject/sqlmap>
* Handleiding: https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/

## Uitgevoerde taken (commando’s)

1. sqlmap.py -u “<http://localhost/project/biedingspagina.php?voorwerpnummer=18>” --level=5
   1. Hiermee geef ik aan een target URL op met daarin een securitylevel van 5 (hoogste).
2. sqlmap.py -u “<http://localhost/project/biedingspagina.php?voorwerpnummer=18>” –risk=3
   1. Hiermee geef ik een target URL op met daarin een risklevel van 3 (hoogste).

## Uitkomsten

Na de test met een securitylevel van 5 is er gebleken dat alle parameters niet injecteerbaar zijn door deze tool.



Na de test met een risklevel van 3 is er gebleken dat alle parameters niet injecteerbaar zijn door deze tool.

## Conclusie

Hieruit blijkt dat er geen SQL injectie kan worden gedaan met deze tool vanwege onze mysql prepared statement.