Hacker Tools: NoSQLMap – No SQL, Yes exploitation

BY ANNA HAMMOND · AUGUST 4, 2021 · LAST UPDATED ON MARCH 6, 2025

Ever since big data and real-time applications have become the norm, we've increasingly needed different database solutions. MongoDB, CouchDB, Redis, Cassandra, and so many more NoSQL databases have sprouted, but what about their security? How do we go about finding misconfigurations and vulnerabilities related to NoSQL databases? Time to find out!

This week, we're going to cover NoSQLMap, the antithesis of SQLMap. Let's see how secure our NoSQL databases are!

What is NoSQL?

NoSQL is the opposite of SQL, it's non-relational, it stands for either 'No SQL' or 'Not only SQL' depending on who you ask but in general it refers to non-relational database architectures.

But if data is not being stored in structured tables, then how is it being stored? Well, there are different ways such as graph-based or key-value-based. This allows different use-cases to have different ways of querying their data. Other advantages include more scalability, facilitated by the possibility of data distribution and performance increases.

There are plenty more advantages and a ton of database management systems out there. For now, let's just focus on assessing their security.

NoSQL Database solutions

NoSQL security? Is it even important?

We're going to let the following links speak for themselves

- Hacker ransoms 23k MongoDB databases and threatens to contact GDPR authorities
- MongoDB server leaks 11 million user records from e-marketing service
- Unsecured MongoDB database exposes real-time locations of families
- A Benevolent Hacker Is Warning Owners of Unsecured Cassandra Databases

What is NoSQLMap?

NoSQLMap is an open-source Python tool designed to audit for, as well as automate injection attacks and exploit default configuration weaknesses in NoSQL databases and web applications using NoSQL in order to disclose or clone data from the database.

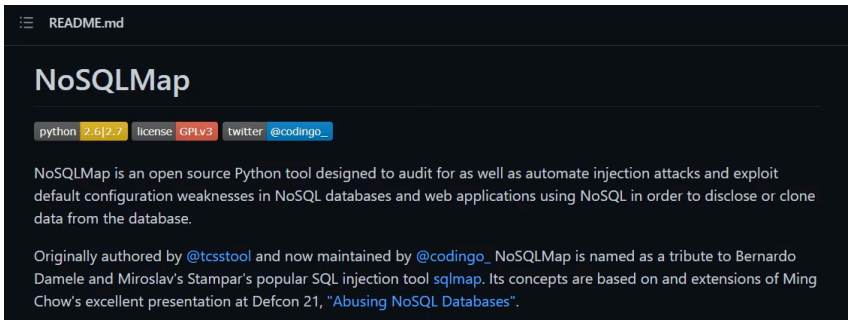
The easiest way to view NoSQLMap is as the NoSQL variant of SQLMap.

NoSQLMap graphic

How to install?

Installing is as easy as cloning the repository and running the **setup.py** script.

```
git clone https://github.com/codingo/NoSQLMap.git
cd NoSQLMap
python setup.py install
```



NoSQLMap README.md

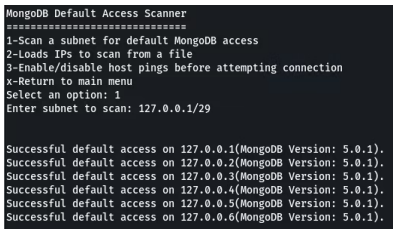
Using the tool

By running **python nosqlmap.py** you can start the interactive CLI for running your checks. In this view, you can see the different things NoSQLMap can do.

Change platform

Use these options to switch between platforms. Currently, NoSQLMap supports MongoDB and CouchDB with additional support being planned in the future.

Scan for Anonymous MongoDB Access



This capability allows you to scan subnets or IP lists for open MongoDB or CouchDB servers.

Let's try this out ourselves. In the screenshot on the left, you can see that we chose to run a scan against a subnet. This will scan every IP address in the supplied subnetwork. We defined `127.0.0.1` as the network address and `29` as the subnet mask. As you can see from the output, it found open MongoDB servers on every IP it scanned in this subnetwork. From there, you can continue exploitation.

Active web exploitation

Check out the youtube video accompanying this article for an example.

What else?

Of course, that's not all NoSQLMap can do. Let's quickly list some other things!

- Bruteforcing logins
- Injecting NoSQL
- Timing based attacks
- Database cloning
- Database enumeration
- So much more...

Conclusion

NoSQLMap is an extremely powerful toolset that will greatly increase your efficiency while searching for vulnerabilities in NoSQL databases.

If you would like to recommend a tool for us to cover next week, then be sure to let us know down below. Also be sure to check out all the previous Hacker Tools articles, such as the last one on JWT_Tool.

Did you know that there is a video accompanying this article? Check out the playlist!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com