**Discussion/Assignment 7.1 – Database Security**

Patrick Cuauro

Bellevue University

WEB 335-307O Introduction to NoSQL

Professor Krasso

July 4, 2023

## What are the recommended best practices for securing MongoDB database users?

Two of the most recommended best practices when it about secure database users are:

* Create separate security credentials. This means creating a unique MongoDB user for each person or application that accesses the system. This helps to prevent unauthorized access if one of the credentials is compromised.
* Use role-based access control (RBAC). RBAC allows you to define roles that specify the level of access that a user has to the database. This helps to ensure that users only have access to the data they need to access.

## What are the recommended best practices for securing MongoDB database queries?

Some of the most recommended best practices when it about queries:

* Use prepared statements. Prepared statements are a way to pre-compile a query and store it in the database. This can help to prevent SQL injection attacks, as the attacker will not be able to see the actual query that is being executed.
* Validate user input. Before executing a query, you should always validate the user input to make sure that it is safe. This includes checking for malicious characters, such as; or ', that could be used to inject code into the query.

## What are the recommended best practices for securing the data in a MongoDB database?

Some of the best practices in securing the data in MongoDB are:

* Encrypt your data. If a data breach occurs, unauthorized users will gain access to your data. Encrypting your data will make it more difficult for them to read and understand.
* Use the official MongoDB packages. MongoDB provides official packages for all major platforms. These packages are regularly updated with security patches. Using the official packages will help you to stay up-to-date on the latest security fixes.
* Audit your database and logs. MongoDB provides a built-in auditing system that you can use to track who has accessed your database and what they have done. You should also review your logs regularly for any suspicious activity.

## What does the term encryption at rest mean?

Encryption at rest is a security measure that protects data when it is stored on a physical medium, such as a hard drive or a USB drive. The data is encrypted using a cryptographic algorithm, which makes it unreadable to unauthorized users. Only authorized users who have the encryption key can decrypt the data and access it.

## What does the term encryption during transit mean?

Encryption during transit, also known as encryption in transit, is a security measure that protects data while it is being transmitted over a network. The data is encrypted using a cryptographic algorithm, which makes it unreadable to unauthorized users. Only authorized users who have the encryption key can decrypt the data and access it.

Encryption during transit is an important security measure because it can help to protect data from unauthorized access, even if the network is compromised. For example, if an attacker is able to intercept data that is being transmitted over an unencrypted network, they will not be able to read the data because it is encrypted.

## What is MongoDB's recommended password policy?

MongoDB does not have a built-in password policy, but it does recommend that users implement a strong password policy for their MongoDB deployments. The following are some of the recommendations that MongoDB makes:

* Passwords should be at least 12 characters long.
* Passwords should contain a mix of upper and lowercase letters, numbers, and symbols.
* Passwords should not be easily guessed, such as words that can be found in a dictionary or the name of a person, character, product, or organization.
* Passwords should be changed regularly.
* Passwords should not be shared with anyone else.

Sources:

<https://www.mongodb.com/features/security/best-practices>

<https://www.mongodb.com/docs/manual/security/>

<https://cloud.google.com/docs/security/encryption/default-encryption#:~:text=Encryption%20at%20rest%20is%20encryption,state%20drives)%20or%20backup%20media>.

<https://www.mongodb.com/community/forums/t/configure-strong-password-user/13047>