**3.9 Session 9 reflection**

Pick one or more database technologies to work with and either envision the questions in the context of a web service you have developed during previous reflections or another (imaginary or concrete) web service you are familiar with. Specify in the first response which DBMS you refer to, what is the web service for which you are considering these aspects and be clear when you switch around technologies.

Again, cite all sources and show your code. You do not have to implement the steps, you can merely discuss, but of course you are free to check how much of this can you actually put into practice straight away and document that in your responses.

Each adequate response is worth one point.

MySQL

1. Is there a default username/password that needs to be changed after installation? What are the password requirements? Is adding password protection optional? In which scenarios should it be enabled?

* No, username and password to connection are unique, username can be modified this is attached to an email and its changes. Passwords need to be encrypted.
* To connect to DB password, do not store cleartext password in the DB, use [SHA2()](https://dev.mysql.com/doc/refman/8.0/en/encryption-functions.html#function_sha2) or some other one-way hashing function and store the hash value. To prevent password recovery using rainbow tables, do not use these functions on a plain password; instead, choose some string to be used as a salt, and use hash(hash(password)+salt) values.
* Do not choose passwords that consist of easily cracked or guessed items such as a dictionary word, proper name, sports team name, acronym, or commonly known phrase, particularly if they are relevant to you. The use of upper case letters, number substitutions and additions, and special characters does not help if these are used in predictable ways. Also do not choose any password you have seen used as an example anywhere, or a variation on it, even if it was presented as an example of a strong password.
* The validate\_password plugin component serves to improve security by requiring account passwords and enabling strength testing of potential passwords.
* In any scenario

Source: https://dev.mysql.com/doc/refman/8.0/en/security.html

1. Is there a way to add a layer of encryption (like SSL or similar) to communicate with the database over HTTP or some other internet-facing protocol? How about encrypting the database itself? Would this require certificates or signatures of some sort and how could one generate those free of cost?

* MySQL supports encrypted connections between clients and the server using the TLS (Transport Layer Security) protocol
* MySQL can be compiled for encrypted-connection support using OpenSSL or yaSSL.
* MySQL performs encryption on a per-connection basis, and use of encryption for a given user can be optional or mandatory. This enables you to choose an encrypted or unencrypted connection according to the requirements of individual applications.
* Create the files required for SSL and RSA support in MySQL can be performed using facilities provided by MySQL itself, or by invoking the **openssl** command directly.

NOTE from google: Website owners and developers can source free SSL certificate providers and paid SSL certificates issued by Certificate Authorities (CAs). As the name suggests, **free SSL certificates don't require payment**, and web owners can use them as much as they want.

Source: https://dev.mysql.com/doc/refman/5.7/en/creating-ssl-rsa-files.html

1. Are the any recommendations regarding assigning port numbers and exposing ports?  
   Would your (home) internet provider allow you to expose that port? How would that be configured? Why would it be a bad idea to do so?

* Invest in a firewall.
* MySQL uses port 3306 by default. This port should not be accessible from untrusted hosts.
* It really have a good reason to keep it open

1. What good design techniques and technological options exist for implementing a front-end that never needs to know where the DBMS is located and/or which technology it uses?
2. What kind of security can you achieve using front-end validations alone? Under which circumstances this would feel like a sufficient method to secure the database?

Validate inputs.

Front-end validation production mainly goes through [JavaScript](https://www.codemotion.com/magazine/frontend/javascript/javascript-ultimate-guide/)(in combination with HTML and CSS); whether using a [framework](https://www.codemotion.com/magazine/frontend/javascript/5-javascript-frameworks-to-use-in-2022/)or library.

**The golden rule is that real validation only takes place in the back end, so why discuss front-end validation?**Because front-end validation is immensely useful for increasing the quality of the user experience, which is a determining factor in keeping users on the app by offering them a satisfying experience.

Source: https://www.codemotion.com/magazine/frontend/golden-rules-for-combining-front-end-security-and-ui/

1. What kind of a modular approach to the design of a back-end would allow to easily update and change the DBMS that is being used?

The most popular data model in use today is the relational data model. Well-known DBMSs like Oracle, MS SQL Server, DB2 and MySQL support this model.

1. Are there access log files generated somewhere that you could use to examine any incoming attacks? Where are those files and what do they contain? How would you use them to see if anything is wrong?

Log data records every activity happening on the device, and applications across the network. To assess the security posture of a network, SIEM solutions must collect and analyze different types of log data.

There are six different types of logs monitored by SIEM solutions:

* [Perimeter device logs](https://www.manageengine.com/log-management/siem/collecting-and-analysing-different-log-types.html#l1)
* [Windows event logs](https://www.manageengine.com/log-management/siem/collecting-and-analysing-different-log-types.html#l2)
* [Endpoint logs](https://www.manageengine.com/log-management/siem/collecting-and-analysing-different-log-types.html#l3)
* [Application logs](https://www.manageengine.com/log-management/siem/collecting-and-analysing-different-log-types.html#l4)
* [Proxy logs](https://www.manageengine.com/log-management/siem/collecting-and-analysing-different-log-types.html#l5)
* [IoT logs](https://www.manageengine.com/log-management/siem/collecting-and-analysing-different-log-types.html#l6)

Different log formats

* CSV
* JSON
* Key Value Pair

Within a log file, you’ll find data including:

* The URL of the page or resource being requested
* The HTTP status code of the request
* The IP address of the request server
* A timestamp of the hit (time and date)
* The user agent making the request (e.g., Googlebot)
* The method of the request (GET/POST)

Source: https://www.manageengine.com/log-management/siem/collecting-and-analysing-different-log-types.html

1. How would one set up a backup and/or replication system so that one could reasonably recover from failures or attacks? How much of this can be automated? How often should backups be taken?

Backup Methods

### Making a Hot Backup with MySQL Enterprise Backup

### Making Backups with mysqldump

### Making Backups by Copying Table Files

### Making Delimited-Text File Backups

### Making Incremental Backups by Enabling the Binary Log

### Making Backups Using Replicas

### Recovering Corrupt Tables

### Making Backups Using a File System Snapshot

How do I automatically backup MySQL database?

**Using GUI Solutions**

1. Create a backup job by clicking Jobs > Add Backup Job.
2. Establish a connection with your MySQL Server.
3. Select the databases you want to back up.
4. Specify the location where the backups will be stored. ...
5. Create a backup schedule.
6. Enter your email to receive fail/success notifications.

Source: <https://dev.mysql.com/doc/mysql-backup-excerpt/8.0/en/backup-methods.html>

Google

1. Is any of the information stored in the database considered private information under Quebec law? Are there additional federal laws you should consider? How about international rules and regulations? What would your legal obligations be to protect this information from being leaked or breached? Do you need to allow users to audit or delete their own data?

**8.4. Right to erasure**

Under the Quebec Private Sector Act, an individual may require an organisation to:

* cease disseminating personal information about them;
* de-index any hyperlink that provides access to that information, if the dissemination contravenes the law or a court order; and
* re-index any hyperlink that provides access to that information.

Such a request may be made when the following conditions are met:

* the dissemination of this information causes the person serious injury in relation to the person's right to respect of their reputation or privacy;
* the injury is clearly greater than the public interest in knowing the information or the right to free expression (the balance of convenience criterion); and
* the remedy requested does not exceed what is necessary to prevent the perpetuation of the injury.

In assessing the balance of convenience criterion, the following, in particular, must be taken into account:

* the fact that the person concerned is a public figure;
* the fact that the information concerns the person when they are a minor;
* the fact that the information is up to date and accurate;
* the sensitivity of the information;
* the context in which the information is disseminated;
* the time elapsed between the dissemination of the information and the request made; and
* where the information concerns a criminal or penal procedure, the obtaining of a pardon or the application of a restriction on the accessibility of records of the courts of justice.

What would your legal obligations be to protect this information from being leaked or breached?

<https://www.dataguidance.com/sites/default/files/cai_fi_vol_rens_pers_citoyen_eng.pdf>

Please note that on 21 September 2021, the [National Assembly](http://www.assnat.qc.ca/en/index.html) adopted [Act to modernize legislative provisions as regards the protection of personal information](https://www.dataguidance.com/legal-research/bill-64-act-modernize-legislative-provisions) ('Act 25' formerly known as 'Bill 64'). Act 25 provides for an entry into force over three years, but most of the provisions will enter into force in September 2023. Act 25 resulted in significant changes to various laws in order to modernise the regulatory framework for the protection of personal data in Quebec.

Source: https://www.dataguidance.com/notes/quebec-data-protection-overview