T-Train – Proposed Security

T-Train is a system which aims to make train commuting easy and straight-forward. Since public communication plays a vital role in many people's lives, it is very important to ensure the system is secure and complies with the industry set standards. Before I declare that information is secure within the system I intend to put multiple measures in place, all of which are detailed below.

1. Input filtering

If there exists a form in your application, it will be used to break into your database, or so does the phrase say. To prevent destructive inputs that could lead to SQL injection, each input will be escaped so that it can no longer change the database connection method. An escaped string is treated as simply content which means that it cannot be mistaken with SQL.

To combat cross-site scripting I intend to filter every input by trimming it, which means removing empty spaces on either side of the input, and then sanitise it, which translates to replacing all html characters such as '<' into their respective character codes, such as &copy, that will be later correctly evaluated by the browser instead of being stored in the database as-is.

As for input validation, test plan is already in preparation for each and every input field. These detailed logs should be more than enough to ensure only the expected data gets put to the right place. Even if a customer makes a mistake in the process, they can change the details as they enter the settings.

2. Password protection

Where it is possible we aim to provide the customers with as much freedom as possible, and passwords are one of them. The only requirement is that the password is at least 8 characters long. This ensures a compromise between the user's convenience and the security of the system.

Since these password tend not to be very secure, T-Train makes sure that even if the database access is breached, the passwords will not fall to the wrong hands unencrypted. Each password will be hashed with a special sequence, known as salt, added before. This way even is someone gets access to the data, instead of a valid password, all they will see is a nonsense string of over 200 characters in length.

Obviously many users may want to secure their accounts with stronger passwords, including numbers and special characters, which will be allowed to everyone. This includes access to 2FA which stands for Two-Factor Authentication. Any user that wishes to turn it on, will be able to do so in the settings.

3. Mandatory 2FA for Staff

All staff members of T-Train will be required to use Two Factor Authentication before they can access their accounts. This is especially important in case a staff member had by accident made their password public. This additional security measure should prevent unauthorized access to staff accounts. If the authentication is failed, the staff member will be notified and asked to reset their password.

With staff accounts being able to change most core features of the system, this protection step is very important. They will also be asked to regularly change their password, at least once a quarter. Every unauthorized access issue will be reported to the supervisor for future reference.

4. Activity logging

Every activity performed within the system is logged and associated with the account in question. This includes but is not limited to: login, listing users, booking a ticket. Along with each action is also logged their unique ID and timestamp. This includes staff more than it does users. These logs cannot be deleted by anyone without a direct access to the database, and even if deleted, the database features a similar system to detect who did the deletion. Thus, every activity is logged.

The logs are to be accessed only when requested by a supervisor in order to solve a conflict of any kind. That will also mean a report has to be constructed explaining why they were accessed, what data was checked and what was done with it afterwards.

5. Connection over HTTPS only

While this may not matter as much as the direct security measures, precautions are also great to have in place. Allowing HTTPS only will ensure that all connection is partially encrypted and that no vital information is left in plain text. This may also help against simply unwanted connections to the service.

In order to protect their internet privacy many users may decide to use a VPN and other specialistic tools, therefore if T-Train will notice use of a VPN, proxy or any other kind of possibly risky connection, a captcha mechanism will be shown for the user to complete before letting them in.

6. Possible Anti-DDOS approach

One of many issues which can meet a web application like T-Train are DDOS attacks. To protect against them we may have to resort to third-party companies such as Cloudflare that can put all traffic through their services first in order to differentiate valid requests from the compromised ones used by the attacker. This method is not required as of now since the threat of an attack is relatively low, however, once T-Train starts getting friction, this will definitely be a thing to consider.