**DESIGN DOCUMENT**

**Ticketpass**

**Date:** 19th January 2024

**Version:** 6.0

**Made by:** Hristo Ganchev

**Table of Contents**

[1. Introduction 3](#_Toc154007910)

[2. Architecture Constraints and Design Decisions 3](#_Toc154007911)

[3. C4 Model Diagrams 4](#_Toc154007912)

[**Level 1: System Context Diagram** 4](#_Toc154007913)

[**Level 2: Container Diagram** 5](#_Toc154007914)

[**Level 3: Component Diagram (Backend)** 6](#_Toc154007915)

[**Level 3: Component Diagram (Frontend)** 7](#_Toc154007916)

[**Level 3: Component Diagram (Database)** 8](#_Toc154007917)

[**CI Pipeline Diagram** 9](#_Toc154007918)

[**Level 4: Class Diagram** 10](#_Toc154007919)

[4. Explanations and Rationale 12](#_Toc154007920)

[5. Security Report 13](#_Toc154007921)

[**1: Broken access controls** 13](#_Toc154007922)

[**2: Cryptographic failures** 13](#_Toc154007923)

[**3. Injection** 14](#_Toc154007924)

[**4: Insecure design** 14](#_Toc154007925)

[**5: Security Misconfiguration** 14](#_Toc154007926)

[**6: Vulnerable and outdated components** 15](#_Toc154007927)

[**7: Identification and authentication failures** 15](#_Toc154007928)

[**8: Software and data integrity failures** 15](#_Toc154007929)

[**9: Security logging and monitoring failures** 16](#_Toc154007930)

[**10: Server-side request forgery** 16](#_Toc154007931)

[6. Sprints Progress 17](#_Toc154007932)

[**Sprint 1:** 17](#_Toc154007933)

[**Sprint 2:** 17](#_Toc154007934)

[**Sprint 3:** 17](#_Toc154007935)

[**Sprint 4:** 18](#_Toc154007936)

[**Sprint 5:** 18](#_Toc154007937)

[**Sprint 6:** 19](#_Toc154007938)

# **Introduction**

The purpose of this document is to describe the constraints and decisions that the platform is going to be developed under and the flow of the implemented functions by presenting a C4 Model Diagram.

Ticketpass is a platform that provides the user with a wide range of concerts. They can select a concert they would like to attend, purchase tickets for the selected event and gain access to it at the entrance of the venue.

# **Architecture Constraints and Design Decisions**

Based on customer requirements, Spring Boot will be used for the Backend, React for the frontend, and MySQL for Data Management.

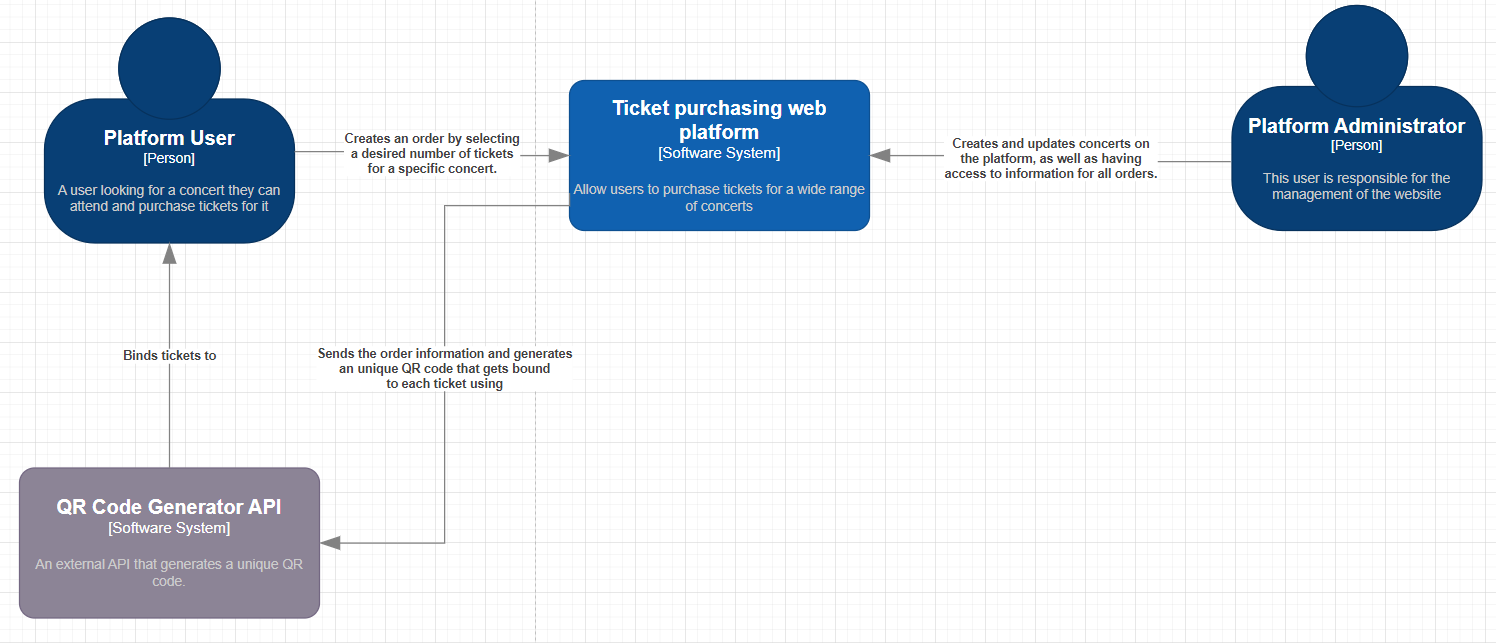
Spring Boot is a framework that provides the developer with a quick compilation of their product and thus the development of the application is conducted more efficiently. What is more, Spring Boot has a large and active community, as well as a wide ecosystem, which will significantly reduce development time. By using this framework, the Dependency Inversion Principle will be followed, promoting loose coupling and avoids the need of continuously and repetitively re-declaring services/repositories throughout the application. The Single-Responsibility Principle and the YAGNI (You Aren’t Gonna Need It) Principle will also be followed.

React uses a virtual DOM and updates only the necessary elements to the UI (User Interface). This clearly follows the KISS (Keep It Simple, Stupid) Principle, making the website application easier to compile and maintain, and promotes a better user experience. Moreover, the framework is perfect for the DRY (Don’t Repeat Yourself) principle, since a component is declared only once and then can be reused in the entire application, without the need of copy-pasting code. The Single-Responsibility Principle will also be followed.

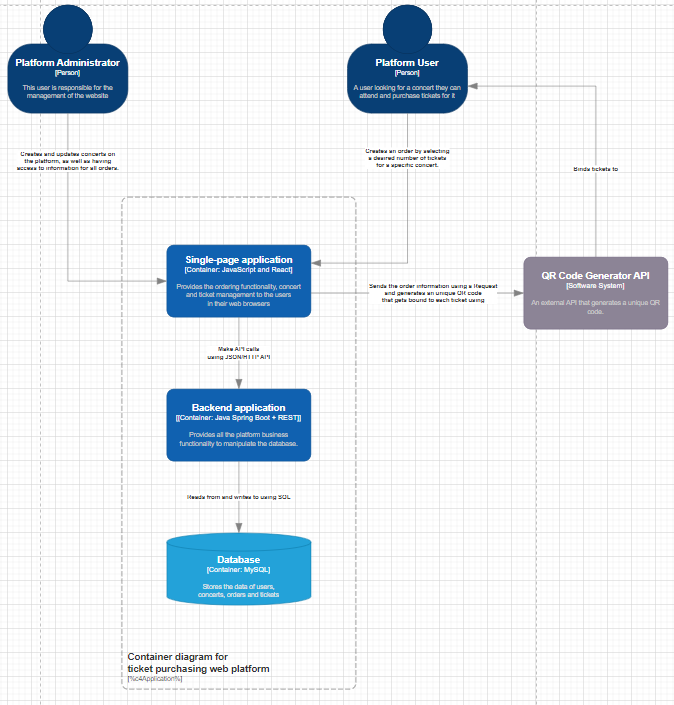
MySQL will be used due to the wide ecosystem of tools and libraries. This will make the database much more adaptable to the development environment. MySQL also has a track record for reliability and performance.

# **C4 Model Diagrams**

## **Level 1: System Context Diagram**

****

## **Level 2: Container Diagram**



## **Level 3: Component Diagram (Backend)**

## **Картина, която съдържа текст, екранна снимка, диаграма, Паралелен Описанието е генерирано автоматичноLevel 3: Component Diagram (Frontend)**

## **Картина, която съдържа текст, екранна снимка, диаграма, линия Описанието е генерирано автоматичноLevel 3: Component Diagram (Database)**



**Картина, която съдържа текст, екранна снимка, номер, Паралелен

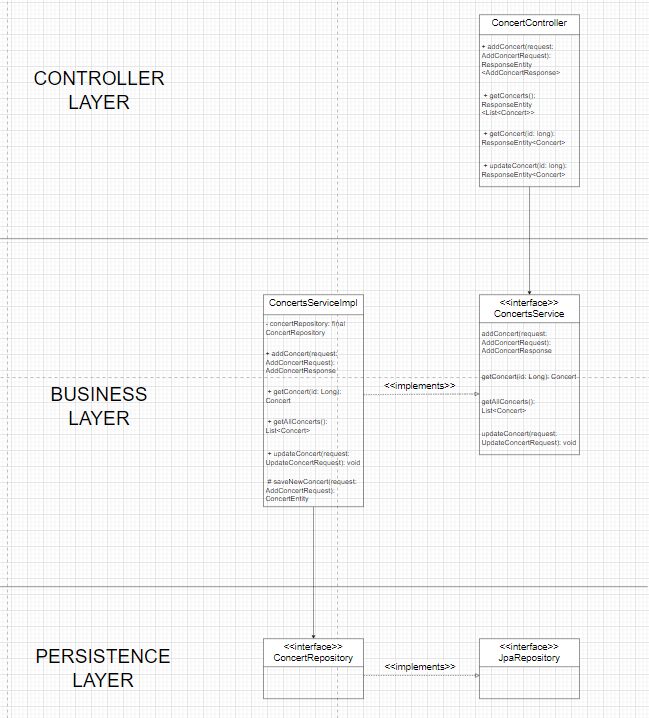
Описанието е генерирано автоматично**

## **Картина, която съдържа текст, екранна снимка, диаграма, номер Описанието е генерирано автоматичноCI Pipeline Diagram**

## **Level 4: Class Diagram**

**Картина, която съдържа текст, диаграма, номер, Шрифт

Описанието е генерирано автоматично**

****

# **Explanations and Rationale**

The manager is responsible for managing the platform. They can add and update concerts from the MySQL Database, can review orders, and overall manage the flow of the platform. They can also ban and unban users, as well as create and delete administrator accounts. They cannot purchase concert tickets through their accounts.

The administrator has the same permissions as a manager, except for the creation and deletion of other administrators. They also cannot purchase concert tickets through their accounts.

The user is a ticketholder. They select a concert, purchase the desired number of tickets, which get bound to their account.

The project is divided into three parts: a single-page application, a backend application, and a database.

The single-page application is updated accordingly, and only necessary UI elements are displayed. This makes the platform much easier to compile and provides the user with a fast and easy experience.

The backend application is implemented using Java Spring Boot. It is responsible for all the logic behind the application. It is separated into 4 different categories (User, Ticket, Order, Concert). Each category consists of a REST Controller that is responsible for managing the HTTP requests, a Service layer where all of the logic is managed, and a Repository that assists with the retrieval and updating of information to/from the database.

The database is where all of the information is stored. Measures will be taken in order to keep sensitive information (e.g. passwords) hidden in case of data leaks.

The repository where the backend application is stored is connected to three CI Pipelines: build, test, and sonarqube-check. If the pipeline prior to the current one fails, all of the other pipelines are skipped in order to not run faulty code.

The first pipeline is responsible for the building of the application. If this pipeline fails, all the others will not be executed.

The second pipeline is responsible for running the tests in the application. First, it compiles the application, and then runs all of the tests in the program. If at least one tests fails, the pipeline fails, too.

The last pipeline in the flow is sonarqube-check. It will not run unless the application successfully compiles. It is responsible for giving more insight into the application. By “scanning” through the code, it recommends pieces of code being changed, which code blocks are duplicate, and what percentage of the application do the tests cover. It is only applied in branches, such as main and master.

# **Security Report**

The OWASP Top 10 Security Risks represent the most critical risks to modern web applications. In this security report, it is described how the application deals (or does not deal) with them.

## **1: Broken access controls**

Broken Access Controls involves bypassing access control checks (e.g. executing admin operations while logged in as a user). For this exact reason, the application has two “shields”. One is the @RolesAllowed annotation, which prevents any unauthorized user to run methods eligible for admins only, and another one that checks for the ID of the logged in user, and whether the ID is equal to the one provided in the access token. If it is not, the method is unable to execute.

## **2: Cryptographic failures**

Cryptographic failures may lead to exposing data, including passwords and other personal information. If the passwords in the database are stored without being hashed or encoded, an attacker can easily fetch them and distribute them online, exposing the data of millions of users. For this purpose, all of the passwords in the database are hashed using a B Crypt Password Encoder, and then decoded when logging into the application. By doing this, even if the attacker obtains access to their vulnerable information, it will be complicated for them to encode the passwords.

## **3. Injection**

Injection involves using a form or other text fields for submitting data for executing malicious SQL statements or OS commands. For instance, in a filter statement, instead of writing a keyword, the attacker can write an SQL statement such as “DROP TABLE orders”, which, if not used in a parameterized query, will be read as an SQL statement and executed. To protect the application, instead of using default queries, the database is working only with parameterized queries, meaning that each field that should be filled from the user is read as a parameter. If a user tries to fill in an SQL query instead of a required parameter, the statement will be recognized as a parameter, and the query will not be executed.

## **4: Insecure design**

Insecure design is a risk more focused on flaws in design. If proper security controls are not created in the application, it is vulnerable to attacks. However, the security of the product is taken into consideration, and measures are taken to protect the website. One example is the generation of access tokens. In order to encode a token, a signature key is used. The key is stored in an .env file outside of the repository, meaning that only the website owner has access to it, and no one else. Other measures are the hashing of passwords, parameterized queries, methods accessible only to authorized users, and ID checks.

## **5: Security Misconfiguration**

Security Misconfigurations are very common in software development, and many people are not paying enough attention to them. These breaches can occur if unnecessary frameworks and features are enabled, or latest security features are not configured correctly. This is why imports from unknown origin and/or missing knowledge are avoided and not present. Each import is analyzed before being connected to the project, so that the application stays at a protected level.

## **6: Vulnerable and outdated components**

Vulnerable and outdated components are considered very simple to breach and attack, meaning that the importing and using of a portion of them can expose the application to many threats. They are much easier to exploit, which might cause harm to the application and are not recommended to use. This is why the components that are included in the application are first examined whether they are not vulnerable and still supported. After certainty that a following component is still supported, secure, and up-to-date, it can safely be used in the application. Moreover, both Spring and React have mechanisms for handling unsupported components.

## **7: Identification and authentication failures**

Identification and authentication failures involve the attacker bypassing security measures, gaining access and assuming the identity of a user. This can involve obtaining a user’s orders without being authenticated. As mentioned above, there are already measures that deal with this risk. Both the @RolesAllowed annotations and the ID checks present in the Service Implementations in the Backend prevent unauthorized users from executing endpoints unless they are logged in as the said user.

## **8: Software and data integrity failures**

Software and data integrity failures are mainly caused by plugins, libraries or modules from untrusted sources, which use insecure update mechanisms, or insecure deserialization. An attacker can take advantage of the usage of such components, having the ability to easily manipulate them and take control over the state of the application. This is why only popular libraries are used, since they are considered to be more secure against such circumstances. By doing so, a user with malicious intentions will find it more difficult to exploit these libraries, and therefore gain access to vulnerable parts of the program.

## **9: Security logging and monitoring failures**

Security logging and monitoring failures involves not monitoring suspicious behavior (e.g. failed logins or high-value transactions). Logs can notify an administrator that a user is conducting a suspicious activity or transaction, and from then on they may take action. At the current point in time, logs are only stored locally, however, if any suspicious activity is noticed, there is the possibility to ban the user involved. In case of a false ban, the user ban can also be reverted. In the near future, security logging may be considered.

## **10: Server-side request forgery**

SSRF allows attackers to make requests to separate resources. They can send an URL to a destination that is not expected (e.g. a fake banking website that is a perfect copy of a legit one) and therefore scam website users into entering their credentials, from which the attacker can gain access to their accounts in the real platforms. Some of the recommended solutions to this security risk are using HTTPS configuration and scanning URL links for potential threats. At the moment, no firewall preventing such attacks is present in the application, but it will be considered in the upcoming versions of the platform.

**Conclusion**

Overall, the platform is in a secure state, where access tokens are used, passwords and sensitive information is hashed, and requests are safely controlled and difficult to execute unless the user is authorized to do so. Moreover, the program is only using parameterized queries, making SQL Injection more difficult to be executed. However, the application is planning to transfer from HTTP to HTTPS in the near future, as well as taking into account Software and data integrity failures, as well as SSRF (Server-side request forgery), which, at the current moment, the platform is vulnerable to.

(Source: <https://www.zscaler.com/blogs/product-insights/what-owasp-top-10?psafe_param=1&_bt=677493654214&_bk=&_bm=&_bn=g&_bg=154576188893&utm_source=google&utm_medium=cpc&utm_campaign=google-ads-na&gad_source=1&gclid=EAIaIQobChMI-9XkhMiZgwMVjtV3Ch1DkAmoEAAYASAAEgKvD_D_BwE>)

(Source: https://owasp.org/Top10/)

# **Sprints Progress**

## **Sprint 1:**

1. As an administrator, I want to add concerts to the database with the necessary information so that they can be displayed to the users of the platform.

* A database that stores concerts should be created.
* Each concert should have a unique ID, Artist Name, Music Genre, Venue, City, Date, Description, Photo URL, Ticket Price and Tickets Remaining.
* A method that adds concerts to the database should be implemented

## **Sprint 2:**

1. As a user, I want to see all concerts in one place, so that I have a wide selection of different concerts of different genres available in a glance.

* A page where concerts are retrieved from a database should be created
* Each concert should be displayed with their name, photo, and description in the “Concerts” page

## **Sprint 3:**

1. As a user, I want to be able to purchase tickets online so that I can reserve my place in the event I would like to attend fast and easy.

* A “Checkout” page should be implemented.
* A method for making an order should be created.
* All orders made should be stored in the database.

## **Sprint 4:**

1. As an administrator, I want to have all of my users passwords hashed, so that in case of a data leak their personal information will not be available to the public.

* Create a method for hashing a password.
* Create a method that compares the inputted value for password (when logging in) and the hashed password stored in the database.
* Passwords must NOT be stored explicitly in the database.
* Create a method for generating an access token
* Administrators should have authorization for specific methods that regular users cannot access.

1. As a user, I want to be able to see all of my tickets for a specific concert in one place, so that it is easier for me and my friends to show them at the entrance of the venue.

* A “Tickets” page should be created
* All tickets should be stored in the database
* Each ticket that is equal to a specific order ID should be displayed on the page with an unique QR code

1. As an administrator, I want to have access to all orders made, so that I can confirm whether a user that has contacted me has made a valid purchase or not.

* An “All orders” page should be created.
* All orders made by all users should be displayed in the “All orders” page

## **Sprint 5:**

* 1. As an administrator, I want to have the ability to update concerts in case of a schedule change for a specific event so that the users are aware that the event will be held in a different day or venue.
* Make a method that selects the specific concert from the database (by ID)
* Make a method that updates the required fields of the selected concert with newly provided information

1. As a user, I want to be able to search for specific genres, cities or artists, so that I know whether an artist I might like is performing in my area.

* An algorithm that filters concerts based on provided genre, city or artist should be created
* Only the filtered concerts must be displayed in the “Concerts” page

## **Sprint 6:**

1. As a user, I want to see all of my previous and upcoming orders, so that I know which concerts exactly I have been to and which ones I am going to next.

* Both previous and upcoming orders must be stored in the database
* “Upcoming concerts” and “Previous concerts” pages should be implemented
* Concerts should be displayed in each page accordingly

2. As an administrator, I want to notify all ticketholders for a concert that has an updated date or place, so that they keep in mind that the concert has been rescheduled or moved to another venue.

* After a concert is updated, all of the tickets for the concert should also be updated.
* A system for sending real-time notifications should be implemented
* Users should be notified about the update made to their ticket, depending on the updated criteria.