Radolina Petrova

Security report

Table of Contents

[Analyzation of project 2](#_Toc124544725)

[Reasoning 3](#_Toc124544726)

[A1: Broken access control 3](#_Toc124544727)

[A2: Cryptographic failures 3](#_Toc124544728)

[A3: Injection 3](#_Toc124544729)

[A4: Insecure design 4](#_Toc124544730)

[A5: Security Misconfiguration 4](#_Toc124544731)

[A6: Vulnerable and outdated components 4](#_Toc124544732)

[A7: Identification and Authentication failures 4](#_Toc124544733)

[A8: Software and data integrity 4](#_Toc124544734)

[A9: Security Logging and Monitoring Failures 5](#_Toc124544735)

[A10: Server-side request forgery 5](#_Toc124544736)

# Analyzation of project

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Likelihood | Impact | Risk | Action possible |
| A1: Broken access control | Unlikely | Severe | Low | Double-checking the identity of the user before executing actions |
| A2: Cryptographic failures | Unlikely | Severe | Low | Hashing and decoding of sensitive information |
| A3: Injection | Unlikely | Severe | Low | Usage of prepared statements only |
| A4: Insecure design | Likely | Severe | High | Unit and integration tests for all critical flows |
| A5: Security Misconfiguration | Unlikely | Severe | Low | No unnecessary features |
| A6: Vulnerable and outdated components | Unlikely | Moderate | Low | Removal of unused elements and continuous inventory of the components |
| A7: Identification and Authorization failures | Unlikely | Severe | Low | Using secure way of authorization and authentication |
| A8: Software and data integrity failures | Likely | Severe | High | Usage of digital signatures |
| A9: Security logging and monitoring failures | Likely | Moderate | High | Input validation |
| A10: Severe side request forgery | Likely | Severe | High | Implementing defence in depth |

# Reasoning

## A1: Broken access control

The broken access control principle enforces, that the user cannot act outside of their limits. They are authorized to perform certain actions and should not be able to force browse to a page, where they are not authorized for. Bypassing control checks by parameter tampering or metadata manipulation should also be prevented, in order for unauthorized users to act as authorized ones.

The impact on my application would not be that severe, because the data, that I am saving does not have that great of an importance and the most damage that can be done is deleting or modifying certain user’s musical content. The chance of this affecting my application is very unlikely, because before executing certain actions, the identity of the user is verified by the JWT secret, which cannot be tempered. Furthermore, force browsing is prevented by checking the identity of the user from the token, before displaying the information.

## A2: Cryptographic failures

The cryptographic failures principle enforces, that sensitive data should not be transferred in plain text. Not only the transmitting of data, but also its storage requires extra protection.

The impact on my application would again be not that severe, because the data does not have that great of an importance. The likeliness of it affecting my application is also not that big, because all sensitive data is decoded, when being transferred or hashed, when being saved.

## A3: Injection

The injections principle enforces, that data an application is vulnerable to these attacks, when user-supplied data is not validated, dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter and hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures.

The impact on my application could be severe because whole sets of data can be deleted. The likeliness of this affecting my application is small, because I am using JPA Repository methods and for the more complex queries, which depend on the user input, I use named queries.

## A4: Insecure design

The insecure design principle enforces that secure design is methodology that constantly evaluates threats and ensures that code is designed and tested to prevent know attacks. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. Secure design can be ensured by using libraries with secure design patterns, integrating security language into the stories, segregation of layers depending on the exposure and protection needs.

## A5: Security Misconfiguration

The security misconfiguration principle enforces that installed and enabled unnecessary features, not setting security setting to secure values, enabling of default account and their passwords, not right configuration of latest security features can lead to a very vulnerable application. This can be prevented by an automated process for verification of the effectiveness of the configuration and settings in the environments, as well as a minimal platform without any unnecessary features, components, and documentation.

## A6: Vulnerable and outdated components

The vulnerable and outdated components principle enforces that the usage of older versions of components, where there are deprecated methods, not scanning for vulnerabilities regularly, not testing the compatibility of updated, upgraded, or patched libraries can lead to big security risks. This can be prevented by continuously inventory of the versions of the components, obtaining components from official secure sources and removing unused components, dependencies etc.

## A7: Identification and Authentication failures

The identification and authentication failures principle enforce that the usage of plain text for saving sensitive data can lead to this kind of failure, missing or ineffective multi-factor authentication or exposing session identifier in the URL as well as exposure or reusage of session identifiers can lead to critical authentication-related attacks. This can be prevented by implementing multi-factor authentication, alignment of password lengths or by limitation or delaying of failed login attempts.

## A8: Software and data integrity

The Software and data integrity principle enforces those failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks. An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. This can be prevented by usage of digital signature, consumption of trusted repositories by libraries and dependencies etc.

## A9: Security Logging and Monitoring Failures

Security logging and monitoring failures enforces that without logging and monitoring, breaches cannot be detected. Insufficient logging, detection, monitoring, and active response occurs any time. This can be prevented by correct encoding of the data for prevention of injections or attacks, logging of validation failures with sufficient context.

## A10: Server-side request forgery

SSRF principle enforces that flaw occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall. As modern web applications provide end-users with convenient features, fetching a URL becomes a common scenario. As a result, the incidence of SSRF is increasing. Also, the severity of SSRF is becoming higher due to cloud services and the complexity of architectures.