Radolina Petrova

Security report

Table of Contents

[Analyzation of project 2](#_Toc122601873)

[Reasoning 3](#_Toc122601874)

[A1: Broken access control 3](#_Toc122601875)

[A2: Cryptographic failures 3](#_Toc122601876)

[A3: Injection 3](#_Toc122601877)

# Analyzation of project

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Likelihood | Impact | Risk | Action possible | Planned |
| 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 | N/A |
| A4: |  |  |  |  |  |
|  |  |  |  |  |  |
| A6: Vulnerable and outdated components | Unlikely | Moderate | Low | Removal of unused elements and continuous inventory of the components | N/A |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 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