Preface

The main goal of this checklist is to be able to check for basic security vulnerabilities on your project. The list will be gradually expanded to accommodate new items to check during the security checkup. If you have any ideas for new items to add to the list, please let me know (and especially let me know, if I made any mistake).

Required tools/accesses:

- Browser
- Postman (optional, but useful)
- Access to database, e.g. using DBeaver

Resources:

- https://jwt.io/ - for decoding and checking JWT (tokens)

The checklist

Registration

1. Registration confirmation token has an expiration date (depends on the application, but 24h is a good practice)
2. Registration confirmation token expires after reaching the expiration date
3. API registration request is sent using https
4. Registration data is not sent as parameters of the API login request

Login

1. API login request is sent using https
2. Login credentials are not sent as parameters of the API login request

User access

1. All user types are confirmed to have the proper rights, according to the documentation
2. Users cannot access other users' data by manipulating the user ID in the URL
3. Users cannot access parts of application restricted to them using a direct URL e.g access an admin panel

Other

1. All API requests containing sensitive data use https and don't contain sensitive data in URL parameters
2. User session has an expiration date (preferably 30 minutes of inactivity)
3. All generated tokens have an expiration date