využiju spring security framework - Security - Spring security dependency

<https://stackoverflow.com/questions/37285016/what-is-username-and-password-when-starting-spring-boot-with-tomcat>

<https://www.marcobehler.com/guides/spring-security>

REST Exceptions handling - <https://www.toptal.com/java/spring-boot-rest-api-error-handling>

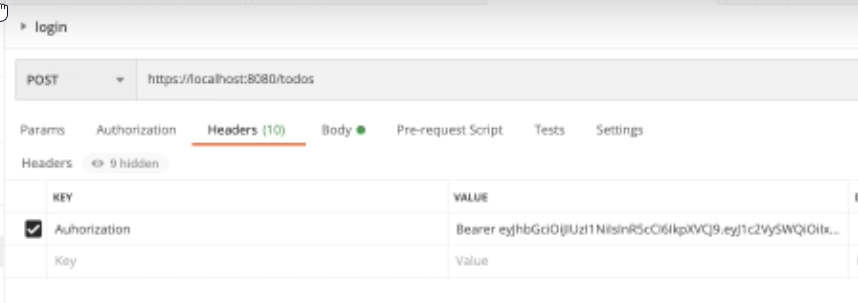
Authentication:

1.registration endpoint - /register - vytvořím novou entitu s registrací

psw zde můžu jako plain text ale ideálně to zakódovat

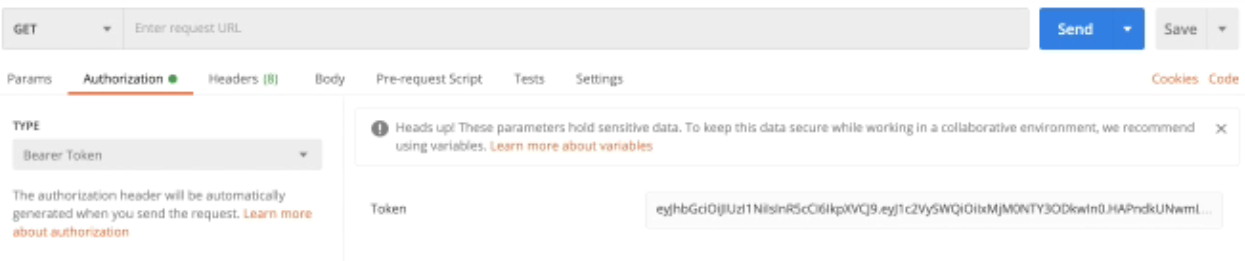
2.login endpoint: username+ psw, jako response bude jwt token (jwt.io) - ten má platnost třeba hodinu.

todle musí uživatel vždy zaslat s get dotazem (token je v Headers):



my to musíme validovat a pak až vrátíme todos

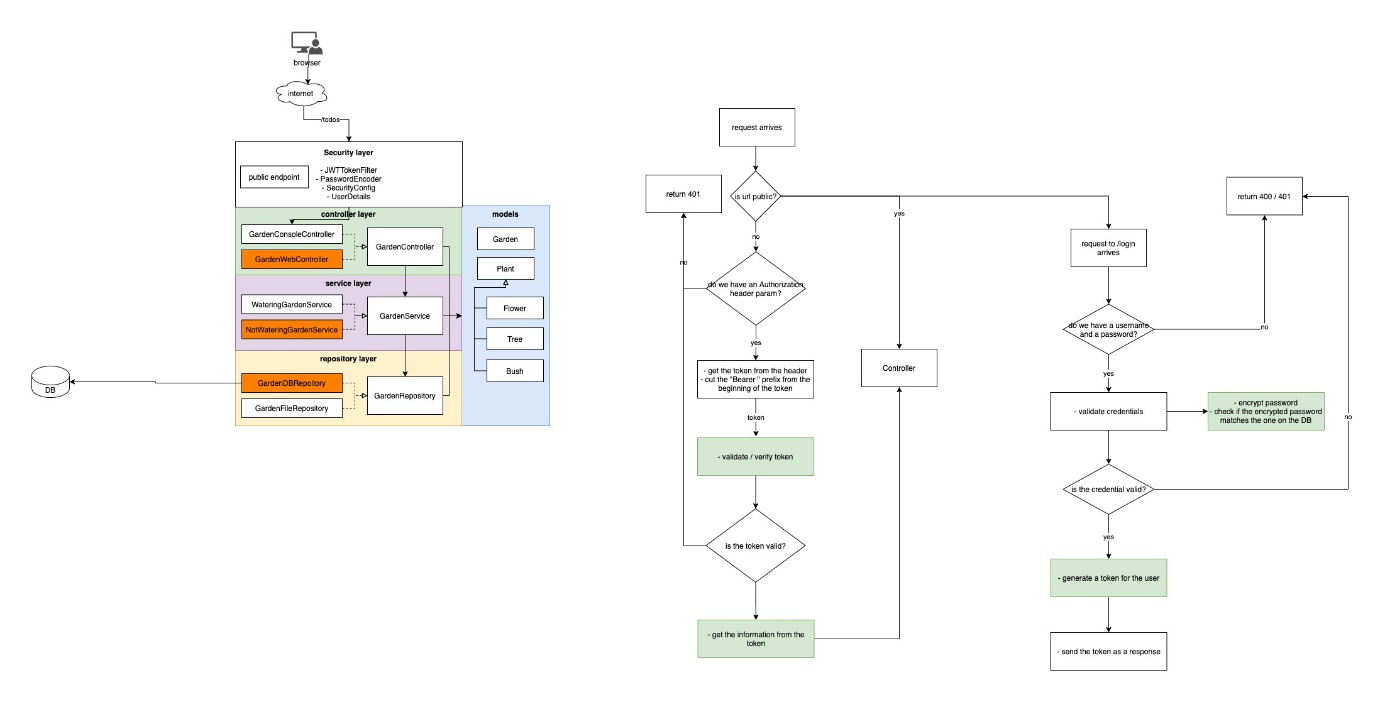
V postmanovi mohu využít část Authorization:

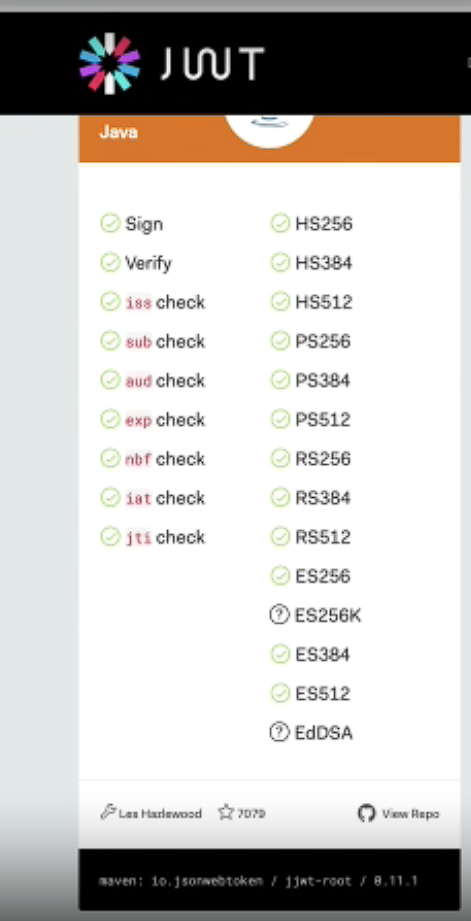


Takže všechny ostatní endpointy kromě login a register musí být dostupné pouze s validním tokenem.

Test Environment:

-inmemory database - použiju H2 database



 Bcrypt pro šifrování hesel