Listen Up

Security Report

Mohammad Nazibul Kabir Khan

4263308

Content

Report Table

	Likelihood	Impact	Risk	Actions possible	Planned
A01: Broken Access Control	Unlikely	Severe	High	Protected route	Yes
A02: Cryptographic Failures	Very Unlikely	Severe	Low	No password is stored or shown	Done
A03: Injection	Very Unlikely	Moderate	Moderate	There is no made-up query needed.	Done
A04: Insecure Design	Very Unlikely	Severe	Moderate	Logic is used that return exceptions	Done
A05: Security Misconfiguration	Likely	Moderate	Moderate	CSRF is disabled and error message is precise	Yes
A06: Vulnerable and Outdated Components	Very Unlikely	Minor	Low	No unused or outdated dependencies are to be used	Done
A07: Identification and Authentication Failures	Likely	Moderate	Moderate	Password regex to be used	Yes
A08: Software and Data Integrity Failures	Likely	Moderate	Moderate	Secure CI/CD pipeline is to be implemented	Done
A09: Security Logging and Monitoring Failures	High	High	High	Only be allowed to enter limited amount of wrong credentials	No
A10: Server-Side Request Forgery	High	Moderate	Moderate	Improve framework implementation	No

Description

Broken access control

Firstly, in the front-end of ListenUp software solution protected route is implemented. After a user log in JWT library decodes the access token which was provided as response to successful login. Decoding access token provides the list of roles that particular user has, and the route to each destination is protected by the roles. Therefore, specific route cannot be accessed if user do not have access to it.

Even if the front-end is manipulated and user get into the page somehow, back end will stop the user to do any kind of action, because each action is protected by roles in back end too.

Cryptographic failure

Password user input when making an account is encoded to random string. If admin wants to see the list of user data, they can only see the name and their activity which is not related to the information needed to login.

Injection

Currently application is not using made-up query. All the methods used is already generated by JPA repository so therefore, there is no big security threat.

Insecure Design

There is logic in both backend and front end to restricts third party to do actions that need special authentication. Moreover, a user cannot do invalid action or put invalid input in this software system. Invalid action or input first have to go through front end logic then again if front end is being manipulated backend of the software is going to stop it.

Security Misconfiguration

Cross-site request forgery (CSRF) is disabled. Error messages are precise but not informative. Application does not have unused features or plugins

Vulnerable and outdated components

ListenUp software does not have vulnerable and outdated components.

Identification and authorization failures

Regex for strong password is used in both the front end and backend, therefore it will prevent user to make account with weak password. And software is using refreshed tokens, therefore it will check if the correct user is logged in to perform actions those requires authentication.

Software and data integrity failure

To prevent software and data integrity failure secure CI/CD environment is implemented in the software solution.

Security logging and monitoring failures

Not implemented.

Server-side request forgery

Not implemented