Introduction

The food industry has been revolutionised using applications. However, with the increasing use of these apps, concerns over data security have also been raised. This report focuses on the security of a food-based application.

Objectives

The objectives of this research report are:

- To identify the potential security risks associated with a food-based app.
- To evaluate the existing security measures of the app.
- To provide recommendations for improving the security of the app.

Methodology

To accomplish these objectives, I conducted a comprehensive analysis of the potential security measures of the app. I conducted vulnerability assessments to identify potential vulnerabilities as well as review industry best practices and guidelines for web app security.

Findings

Based on my analysis, I identified the following potential security risks associated with the food-based app and provided potential solutions:

- Weak authentication: The app allows weak passwords which can easily be guessed or hacked. The app will need to enforce strong passwords of minimum length and complexity.
- Insecure data storage: The app stored sensitive information, such as users' names and addresses on the device without proper encryption. The app should use strong encryption to protect sensitive data.
- Inadequate access controls: The app lacks proper access controls, allowing unauthorized users to access sensitive data. The app should implement role-based access control to ensure only authorized users can access sensitive data.
- Insufficient Transport Layer Security: The app did not use HTTPS to encrypt data during transmission, making it vulnerable to eavesdropping attacks.
- Vulnerabilities in Third-Party Libraries: The app uses third-party libraries that had known security vulnerabilities.

Conclusion

The security of a food-based app is crucial to ensure the privacy and safety of its users. This report identified potential security risks.