SECURITY REPORT

Individual Track
Bamboo Restaurant

Eindhoven, December 14th, 2021

Table of Contents

Revision History:

Date Changed	Document Version	What was changed
14/12/2021	1	

Introduction

Security has been the fundamental criteria beside the time and money budget when comes to develop and build the software solutions. Recently, lots of news about the security risks has been exploited by the hackers, which cause the damages of more than billions of dollars / euro to the companies, and put the risks of users and companies on the dangers of being threatened. For this report, the application will be checked on the "Top 10 Security risks from OWASP"[1], and taking actions to minimize the security risks for Bamboo project.

What are the risks when securities expoilted

Top 10 Security risks that I take from the *"Top 15 types of cybersecurity risks & how to prevent them"[3],* can potential be problems for Bamboo applications.

- **Malware**
- **Password Theft**
- **Traffic Interception**
- **Phishing Attacks**
- **DDoS**
- **Cross Site Attack**
- **Zero-Day Exploits**
- **SQL Injection**
- **Social Engineering**
- **Ransomware**

Analayze the Top 10 Security Risks

Code	Security risk name	Likelihood	Impact	Risk	Action possible	Planned
A01	**Broken Access Control**	Possible	Severe	High	Check the user roles and the permissions of its	Yes
A02	**Cryptographic Failures**	Likely	Severe	High	Update the hashing libraries and using HTTPS connection	Yes
A03	**Injection**	Very Likely	Severe	High	Sanitize user inputs both front-end and back-end	Yes
A05	**Security Misconfiguration**	Very Likely	Severe	High	Used neccesary libraries for the project, testing the projects before deploying	No, project still in developing, should be in refactoring phase
A07	**Identification and Authentication Failures**	Possible	Severe	High	Put the limitation attempts for login, validate user credentials	Yes
A08	**Software and Data Integrity Failures**	Possible	Severe	High	Review the git commits frequently, more layers of branches	Yes
A04	**Insecure Design**	Possible	Moderate	Moderate	Limit the user interactions to minimize the risks, encrypting the local storage	Yes
A06	**Vulnerable and Outdated Components**	Likely	Moderate	Moderate	Update the Components and Framework every month, testing before deploying.	Yes, it has been in the maintaince phase

A09	**Security Logging and Monitoring Failures**	Possible	Moderate	Moderate	Implementing logging system to keep track the activities and the healthness of applications	No, it will be developed when the main parts of projects finished.
A10	**Server-Side Request Forgery**	Likely	Moderate	Moderate	Improve and update backend framework	Yes, it has been scheduled a month for updates

Conclusions

From the report, the application handles most of the security vulnerables by taking recommended actions. In the future, the projects will be scheduled to maintaince for the performance and increasing the secure level, as this report can point out the top 10 security risks but the unforeseeable ones below top 10, the report has not covered yet and we will find the solutions to handle based on the recommendations from OWSAP.

References

1. *Introduction to OWASP Top 10*. OWASP Top 10 (2021). (n.d.). Retrieved December 14, 2021, from https://owasp.org/Top10/
2. *It Security & Policy Office*. Determining Risk Levels | IT Security & Policy Office. (n.d.). Retrieved December 14, 2021, from https://itsecurity.uiowa.edu/resources/everyone/determining-risk-levels
3. *Top 15 types of cybersecurity risks & how to prevent them*. Executech. (2021, October 13). Retrieved December 14, 2021, from https://www.executech.com/insight/top-15-types-of-cybersecurity-attacks-how-to-prevent-them/