Security and Data protection

research document

for

HeardIT

Author: Mihail Vasilev

Date: 07-06-2024

Contents

[1. Introduction 3](#_Toc169366419)

[2. Main question 3](#_Toc169366420)

[3. Sub-questions 3](#_Toc169366421)

[4. Conclusion 5](#_Toc169366422)

1. Introduction

The purpose of this document is to outline the research that was undertaken to determine the security strategies and methods for protecting the users and their data by the HeardIT application. The research is split into the following sections *– Main research question*, where the main question is defined, *Sub-questions*, where the sub-question derived from the main questions are defined and answered and *Conclusion*, where the answers to the sub-questions are combined in order to answer the main question. The final section is the *References* section where the sources of the information used during the research are presented.

1. Main question

In this section the main question will be established. In order to complete the research, the main question needs to have a concrete answer. For this reason, it is important to define the main question well. This will also allow us to create the sub-questions that will help us answer the main question.

The main research question is:

*How can I ensure that HeardIT provides its users with sufficient data security mechanisms and follows the modern standards and regulations for data protection?*

Answering this question will allow us to determine the most relevant security measures and protection mechanisms that need to be implemented in the HeardIT application. In the next section I will establish the sub-questions that were derived from the main question and I will formulate an answer to each of them.

1. Sub-questions
2. What are the main general application security risks that HeardIT needs to be protected against?

A great starting point into researching the security of the HeardIT application is to outline what are the most common and most likely to encounter issues that web-applications, such as HeardIT, face in the modern world of the internet. Establishing the main requirements for a robust application security can be quite challenging since there are many different dependencies and specifics that each application can have. Thankfully, cyber security experts have outlined the most common prevention measures, risks and security standards that modern applications need to comply with in order to be considered safe. In this case, the best place to begin examining the security of HeardIT is to compare it against the *OWASP Top 10* security standards.

The *OWASP Top 10* is a standard awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications. These include broken access control, cryptographic failures, database injection flaws, insecure design, security misconfigurations, vulnerable and outdated components, identification and authentication failures, software and data integrity failures, security logging and monitoring of failures and server-side request forgery. These ten security standards are crucial for all modern web-applications since they represent a major part in ensuring the applications are secure and well maintained. (OWASP Top Ten | OWASP Foundation, n.d.)

I decided that examining each of them and comparing them to my application requires its own document. There I go in-depth into each security standard, explain their essence and evaluate my application to what degree it complies with each standard. I also outline the measures that are taken or are to be taken during the development process so that HeardIT is a secure and well-maintained web-application.

Please refer to: OWASP Security report - HeardIT.docx

Methods used:

* Literature study – this method was used to determine what general vulnerabilities I need to be aware when developing HeardIT
* Best good and bad practices – this method was used to determine what methods I can use to prevent the researched vulnerabilities

1. What measures need to be taken to comply with the GDPR?

The General Data Protection Regulation (GDPR) sets stringent requirements for organizations handling personal data of EU citizens to ensure data privacy and security. These requirements ensure that EU citizens have control over their data and information that is being shared in the internet and also provides them with a proper outlook of how their data is being used. These requirements are incredibly strict and improper compliance with them can lead to serious lawsuits and government actions. In my case, HeardIT is a web-application that is going to be used by millions of users across the world, including Europe, and as such it is of paramount importance that its user data protections mechanisms and measures comply with the European GDPR. Compliance with these regulations is mandatory for any organization or entity, processing the personal data of EU residents, regardless of location. (General Data Protection Regulation (GDPR) – Legal Text, 2024)

The key requirements include obtaining explicit consent from users before collecting their data, ensuring data is processed lawfully, fairly, and transparently to the user. Collecting only data that is necessary for specified purposes (data minimization) ensures that nothing more than the minimum required data is being stored and handled by the application. Organizations must implement robust security measures to protect personal data and allow users to access, update and delete their data. Any data breaches must be reported to authorities within 72 hours. Organizations must conduct Data Protection Impact Assessments (DPIAs) to identify and mitigate privacy risks. (General Data Protection Regulation (GDPR) – Legal Text, 2024)

In order to comply with GDPR, HeardIT practices data minimization by collecting, storing and handling only the minimum necessary user information for the functioning of the application. This data is regularly reviewed and any unnecessary data is deleted. When accessing the application, explicit consent is obtained from users before collecting and processing their data. Clear information about how the data is going to be used is provided so that the transparency is maintained. Data protection and security assessments are conducted in order to identify and mitigate risks related to data processing activities. Processes for detecting, reporting, investigating and notifying the relevant authorities in case of a data breach are implemented. Agreements and contracts with third-party processors, like Auth0 and Google, are established so that compliance with GDPR is verified for everyone involved.

The General Data Protection Regulations (GDPR) play a very important part in the development of modern web-applications and in general in the processing and handling of user data. The regulations ensure that every user has a transparent overview of how their information is being used and for what purpose.

I want to make clear that this aspect of the development process is the hardest from my personal perspective to evaluate. Proper evaluation and examination of the HeardIT application should be performed by experts both in the cyber security and law departments due to my lack of expertise in the law. This will be done at a later stage of the development process.

Methods used:

* Literature study – this method was used to determine what exactly GDPR means and to what requirements my application needs to be compliant with
* Community research – this method was used to determine what other developers have done to make their platforms GDPR compliant
* Available product analysis – this method was used to determine if there are any services that I can use to protect my user data (Auth0)

1. How to ensure that the application remains secure and well-maintained?

In the modern world where the internet is constantly changing, updating and evolving, application development does not end once a platform is considered “finished”. Once a product is put into production, it is incredibly important for it to be monitored and updated regularly so that it can adapt to the new changes while also remaining safe and secure. Application support is a topic that can encompass many different subjects from delivering new updates to customer support. I have decided that for now I will focus on the aspects that I have experience with which include continuous improvement and updates. (Keep Your Device’s Operating System and Applications up to Date | CISA, n.d.)

Continuous improvements and regular updates for HeardIT are a form of security since it will tackle topics such as keeping different libraries and components up to date, improving existing functionalities and adding new ones. This way, the latest technologies and relevant updates will be added so that HeardIT will be at the forefront of web-applications and it will be able to remain safe against the latest threats. To ensure that these regular maintains and updates are performed, regular security audits from external sources and organizations will be performed. External auditors will be used to review and evaluate the most crucial aspects of the application security measures.

Continuously improving and maintaining HeardIT is one of the main aspects that will allow it to remain relevant and be a safe and secure environment where user data is handled transparently and in compliance with GDPR and other security requirements.

Methods used:

* Community research – this method was used to determine what other developers have done to keep their applications up-to-date
* Best good and bad practices – this method was used to find out what good and bad practices I should be aware of when maintaining HeardIT

1. Conclusion

In conclusion, this research highlighted the measures that are taken in order for HeardIT to ensure data security and compliance with the modern standards by addressing three key areas: general application security risks, GDPR compliance and continuous maintenance. HeardIT was compared to the OWASP Top 10 standards so that the general security risks are avoided and accounted for. Stringent GDPR measures such as explicit user consent and data minimization have been implemented to ensure transparency. Commitment to regular updates, continuous improvement and security audits ensure that HeardIT can maintain robust security and transparency in handling user data. These comprehensive approaches and practices provide a strong foundation for protecting users and their data in the evolving digital landscape.

**References:**

* OWASP Top Ten | OWASP Foundation. (n.d.). <https://owasp.org/www-project-top-ten/>
* General Data Protection Regulation (GDPR) – legal text. (2024, April 22). General Data Protection Regulation (GDPR). <https://gdpr-info.eu/>
* Keep your device’s operating system and applications up to date | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/resources-tools/training/keep-your-devices-operating-system-and-applications-date#:~:text=Routinely%20update%20the%20OS%20and%20apps%20on%20all%20your%20devices.&text=Ensure%20that%20you%20install%20your,these%20may%20be%20phishing%20attempts>.