Research Document

Individual Project

Mitov,Lachezar

2022

**Contents**

[**Abstract** 2](#_Toc116064949)

[**Document Approach** 2](#_Toc116064950)

[**Why should you secure your web application?** 3](#_Toc116064951)

[**How does implementing authentication help secure your application?** 3](#_Toc116064952)

[**How does the JWT technology work?** 3](#_Toc116064953)

[**How to implement the JWT technology correctly so that your web application is secure?** 3](#_Toc116064954)

[**Conclusion** 3](#_Toc116064955)

# **Abstract**

Nowadays, the Internet has been widely adopted by everyone. And with the mass adoption there comes questions about the security of the users. In consequence, the interest with cybersecurity has grown significantly. Henceforth, almost all web applications use authentication and for this authentication to work there needs to be a way for the front-end of the application to store user identity data in a secure fashion. One very common way of achieving that is by using JSON Web Tokens (JWT) and this paper intends to explain how to implement JWT correctly.

# **Document Approach**

This paper is written following a concrete structure, which will be explained here. Firstly, the main question, that the document is intended to answer and thus help solve the problem from the Abstract section is:

* How can you secure your web application properly using the JSON Web Token technology?

Secondly, the main question will be split into sub questions, which aim to answer the main question:

1. Why should you secure your web application?
2. How does implementing authentication help secure your application?
3. How does the JWT technology work?
4. How to implement the JWT technology correctly so that your web application is secure?

The document will use the DOT framework methods to answer the sub questions above. Moreover, the answers to the sub question will follow the APA formatting, so that the used sources in this document can be given credit.

Finally, a conclusion about the results of the research will be given and recommendations to show how the research can be applied to (for example) this semester’s group or individual project will be written.

# **Why should you secure your web application?**

Every application on the Internet contains huge amount of data about its customers. For instance, social media apps store so much information about the users that are on the servers that if a hacker manages to get its hands on this data there could be fatal consequences for both the users and the company behind the app. The lack of proactive security strategy can lead to spreading and escalation of malware, attacks on other websites, networks, and other IT infrastructures. Moreover, if hacker attack spread from computer to computer, that would make it very difficult to find the origin of this attack. Henceforth, security should be one of the main priorities when making a web application.

# **How does implementing authentication help secure your application?**

Authentication is part of the web security so the reasons on why you should implement one in your web application interchange with the ones said in the above paragraph. If your website authentication process is lacking, you run the risk of unauthorized users gaining access to sensitive user information. These data breaches can hurt individual users when their personal information is taken, but they can also ruin YOUR company's brand and financial health. Therefore, it is of the upmost importance to implement authentication in your web application.

# **How does the JWT technology work?**

# **How to implement the JWT technology correctly so that your web application is secure?**

# **Conclusion**