Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Securing Angular Applications - Authentication and Authorization Techniques

Hareesh Kumar Rapolu

hareeshkumar.rapolu@gmail.com

Abstract

The following research project has underscored that securing angular applications by authentication and authorization has been identified to be of immense vitality as it aids in tackling sensitive user data in a systematic sense. Utilizing techniques like JSON Web Tokens for authentication and Role-Based Access Controls for authorization has been proven to be instrumental in securing angular applications. Furthermore, the challenges have been minimised by the incorporation of secured data management and reinforcing data encryption and HTTPS. This has ultimately contributed to enhancing the possibilities of overall security posture therefore securing angular applications.

Keywords: Authentication, Authorization, JWT, RBAC, Security, XSS, CSRF

I. INTRODUCTION

This research project will explain the significance of securing Angular applications by the utilisation of authentication and authorization. It will render that ignoring security at times will result in data breaches along with unauthorised access and loss of user trust. Angular will serve with built-in features to limit the possibilities of common vulnerabilities such as XSS and CSRF. However, the research project will also shed light on demonstrating techniques for authentication and authorization which will be used to secure angular applications. Furthermore, identifying the challenges and strategies to mitigate those challenges will be portrayed and the best practices will also be cohesively discussed in this research project resulting in positive outcomes.

Figure 1: Depicting JSON Web Tokens

II. STATING A BRIEF OVERVIEW OF AUTHENTICATION AND AUTHORIZATION

The following section states that authentication and authorization both stand to be vital aspects in the context of securing angular applications. This is because both of these aspects tend to mitigate the chances of vulnerabilities and attacks. On one hand, the implicit use of authentication is crucial for securing angular applications. This is because it checks the identity of a user which makes sure that only authorized individuals get complete access to the sensitive data functionalities. This is interlinked within the application which helps to prevent unauthorised access and thereby safeguard user privacy[1]. On the other hand, the application of authorization is an important perspective in terms of securing angular applications. The reason behind this is that it determines the necessary actions allowed by a user to perform within the application thereby safeguarding the sensitive data to get into the hands of cyber criminals. Additionally, it this intriguing to monitor the activities of a logged-in user which seeks to make sure that the integrity of the application and user privacy are maintained.

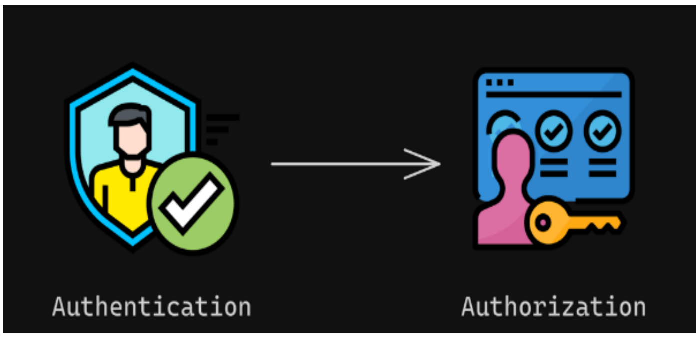

Figure 2: Highlighting the Role of Authentication and Authorization

III. DEMONSTRATING THE TECHNIQUES USED FOR AUTHENTICATION AND AUTHORIZATION TO SECURE ANGULAR APPLICATIONS

This section illustrates the techniques used for authentication and authorization for securing angular applications. These techniques are considered to be of immense relevance as theydetermine role-based access controls to manage permissions efficiently. The technique used for authorization to secure angular applications refers to the utilisation of Role-Based Access Controls also abbreviated as "RBAC"[2]. This technique is regarded as a suitable one as it restricts access to specific resources which are fully based on the roles of the users. Significantly, the route guards in angular are applied holisticallyto robust these permissions. This results in providing access to authorised users to gain control of sensitive data. Similarly, the technique used for authentication to secure angular applications is JSON Web Tokens. This technique is implemented in a synchronised manner to verify the identities of the users. It is observed that when successful login is anticipated then the server generates user information in the JWT which is in turn stored within the client side. This served to be advantageous for securing angular applications by defending against common vulnerabilities such as XSS and CSRF[3]. As a result, this enables the developers to guard their applications from unauthorised access and data breaches.

IV. HIGHLIGHTING THE CHALLENGES WHILE SECURING ANGULAR APPLICATIONS

In the following section, significant challenges were identified while securing angular applications. These challenges need to be controlled to establish positive outcomes. These challenges are mentioned below.

Rendering Data Encryption and Security: Data encryption and security are sometimes considered to be significant challenges while securing angular applications. This is due to the fact that it needs proper security for the stored data along with transmission and validation mechanisms[4]. This results in failing to protect confidential user data from unauthorised access or tampering.

Session Management Concerns: Securing angular applications at times poses significant challenges in managing the sessions. This indicates that it acquires proper handling of the token followed by revocation and expiration. This often leads to security vulnerabilities if not managed accurately.

The complexity of Authentication and Authorization: The complexity of authorization and authentication in securing angular applications poses a vital challenge. This type of challenge occurs during the implementation of JWT and RBAC[5]. However, this results in difficulties for the developers while integrating with third-party services therefore minimising data sensibility.

Safeguarding against Cross-Site Scripting (XSS): At times securing angular applications stands to be vulnerable to cross-site scripting attacks. It could be exploited by the incorporation of malicious code which is injected by user input and third-party libraries. This makes the developers apply for stringent validation and sanitization.

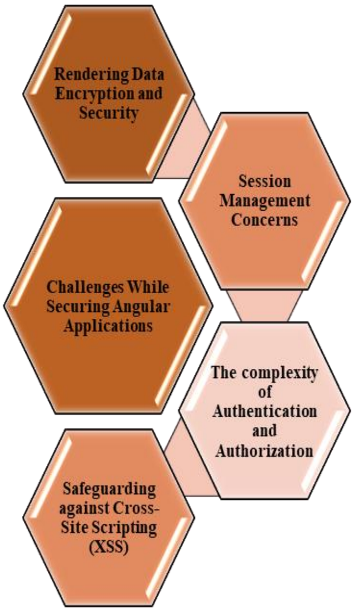
Rendering Data Encryption and Security
Session Management Concerns
Challenges While Securing Angular Applications
The complexity of Authentication and Authorization
Safeguarding against Cross-Site Scripting (XSS)

Figure 3: Understanding Challenges While Securing Angular Applications

V. ILLUSTRATING THE STRATEGIES FOR SECURING ANGULAR APPLICATIONS

This section elucidates effective strategies that are used to secure angular applications. These strategies are mentioned below.

Enforcing HTTPS and Data Encryption: Enforcement of HTTPS and data encryption makes sure that all the transmitted data has the power to shield it from tampering. This requires the structure adoption of encryption mechanisms for local storage and sensitive data handling within the application for protecting user information at rest[6]. As a result, this prevents unauthorized access.

Familiarising with Secured Token Management: Getting familiarised with secured tokens stands to be advantageous for generating storing and refreshing the token in a protected view. It is termed to be appropriate for the expiration times and refresh tokens[7]. This aids in maintaining user sessions and minimising vulnerabilities.

Enforcing HTTPS and Data Encryption
STRATEGIES FOR SECURING ANGULAR APPLICATIONS
Familiarising with Secured Token Management

Figure 4: Strategies for Securing Angular Applications

VI. CONCLUSION

The research project has analysed how to secure an angular application through authentication and authorization. It has been determined to be indispensable in the present digital scenario. The application of JWT for authentication and RBAC for authorization has enhanced user experiences and thus has rendered it with developing application security. These techniques have been identified to be crucial to mitigate common vulnerabilities such as XSS and CSRF. Furthermore, observing the challenges such as session management concerns, data encryption and security, the complexity of authentication and authorization and protection against XSS has been controlled through effective strategies for replication with positive results for delivering the users with a protected experience.

Abbreviations and Acronyms

- JWT- JSON Web Tokens
- RBAC- Role-Based Access Controls
- HTTPS- Hypertext Transfer Protocol Secure
- XSS- Cross-Site Scripting
- CSRF- Cross-Site Request Forgery

Units

- Information is measured in bytes
- Energy is measured in Joules.

Equations

- Data Transmission Rate (R) = [D /T], here, D is the amount of data sent and T is the time taken for transmission
- Energy Consumption for Encryption (E) = [PX t], where, P is the power usage and t is the time running for the encryption process.

REFERENCES

[1] A. Zaid, G. Nieto, H. Alzaid, E. Foo, and J. Gonzalez Nieto, "Secure Data Aggregation in Wireless Sensor Network: a survey," Australian Computer Society, Jan. 2008. Available:https://eprints.qut.edu.au/13090/1/secure_aggregation.pdf

[2] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, "SBVLC: Secure Barcode-Based Visible Light Communication for Smartphones," *IEEE Transactions on Mobile Computing*, vol. 15, no. 2, pp. 432–446, Feb. 2015,doi:https://doi.org/10.1109/tmc.2015.2413791.

[3] M. A. Rahman *et al.*, "Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications," *Ieee.org*, Nov.2018.https://ieeexplore.ieee.org/iel7/6287639/6514899/08534320.pdf

[4] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, "Optical Techniques for Information Security," *Proceedings of the IEEE*, vol. 97, no. 6, pp. 1128–1148,Jun.2009,doi:https://doi.org/10.1109/jproc.2009.2018367.

[5] R. A. Leon, V. Vittal, and G. Manimaran, "Application of Sensor Network for Secure Electric Energy Infrastructure," *IEEE Transactions on Power Delivery*, vol. 22, no. 2, pp. 1021–1028, Apr. 2007, doi: https://doi.org/10.1109/tpwrd.2006.886797.

[6] R. Hasan, R. Sion, and M. Winslett, "Introducing Secure Provenance: Problems and Challenges," Oct. 2007. Available: https://profsandhu.com/cs6393_s13/storagess2007-rhasan.pdf

[7]S.A.Soleymani*etal.*,"https://ieeexplore.ieee.org/iel7/6287639/7859429/07995031.pdf,"*Ieee.org*,Jul.2017.https://ieeexplore.ieee.org/iel7/6287639/7859429/07995031.