RED4SEC

Security Audit Report

18/06/2024

Inheriti 2.0

Public Report

RED4SEC

Summary

This report has been prepared for **SafeTech** and presents a summary of the results of the security audit completed on the **Inheriti 2.0** project. It is based on the technical report which contains all the details and technical descriptions of the security assessment carried out by Red4Sec Cybersecurity.

The analysis showed that the project did contain critical and high risk vulnerabilities deficiencies that have been corrected.

Scope

Red4Sec Cybersecurity has made a thorough audit of the **Inheriti 2.0** security level against attacks, identifying possible errors in the design, configuration or programming; therefore, guaranteeing the availability, integrity and confidentiality of the project and the possible assets treated and stored.

The scope of this evaluation includes the following items provided by **SafeTech**:

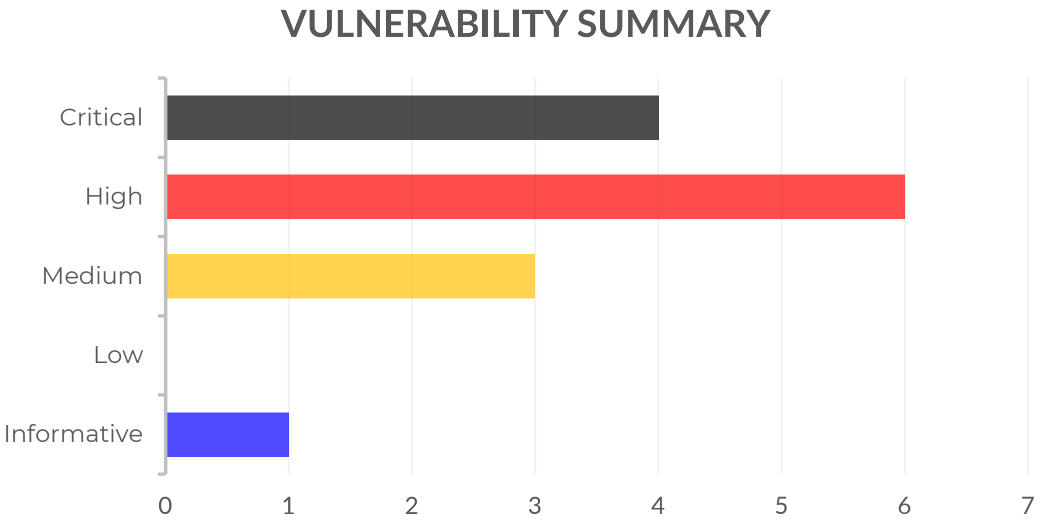
- **Audit:** https://app-preprod.inheriti.com
- **Fixes Review:** https://app-stg.inheriti.com

Executive Summary

The security audit against **Inheriti 2.0** has been conducted between the following dates: **01/04/2024** and **08/04/2024**.

Once the analysis of the technical aspects has been completed, the examination shows that the audited project contained critical vulnerabilities that have been mitigated by the development team.

During the security assessment, a total of **14 vulnerabilities** were detected and classified by their risk level.



Conclusions

The security analysis of the **Inheriti** application uncovered a series of severe vulnerabilities that initially exposed the project to significant risk, potentially leading to unauthorized access and data breaches, compromising the application's overall integrity. However, all identified vulnerabilities and deficiencies have been corrected, ensuring that the application is secure.

The Authentication Bypass vulnerability, which posed a significant risk by allowing unauthorized users to bypass the authentication process, has been resolved, securing access to sensitive data. Similarly, the Arbitrary Secret Message Overwrite vulnerability, which, if exploited, could have allowed an attacker to overwrite or modify secret messages, has been effectively mitigated.

Previously, the application suffered from an Unauthenticated API Access vulnerability and abuse of query manipulation vulnerability, both marked as critical risks, allowing unauthorized access to the system and manipulation of data. These, along with the API's vulnerability to insecure direct object references and the incorrect JWT expiration verification, have been corrected to prevent unauthorized data access and manipulation.

The Lack of Rate Limit on SMS Validation, which could potentially have enabled an attacker to overload the system or validate fraudulent requests, along with the exposure of "private notes" and Premature Passphrase Exposure, have all been secured against unauthorized access to sensitive information.

Issues such as the process abort functionality not working properly, incorrect HTTP header handling, and stored cross-site scripting (XSS) previously represented medium-risk vulnerabilities. These have now been resolved to ensure robust system functionality and enhanced data security.

The design of the management of all the parties involved in the encryption and decryption of the secrets needs improvement to minimize unnecessary backend involvement. The current design allows secrets to unnecessarily pass through the backend, which poses additional risks. Therefore, it is recommended to conduct a white-box code audit of all parts of the system, allowing for a more thorough understanding of the internal workings of the system and potentially uncovering further vulnerabilities.

In conclusion, following a thorough review and significant improvements in several areas, including data validation, access controls, authentication procedures, and overall design, the web application now adheres to security best practices, thereby enhancing the overall security posture.

Disclaimer

This document only represents the summarized results of the security assessment conducted by Red4Sec Cybersecurity and should not be used in any way to make investment decisions or as investment advice on a project.

Likewise, the report should not be considered neither "endorsement" nor "disapproval" of the guarantee of the correct business model of the analyzed project, nor as guarantee on the operation or viability of the implemented financial product.

Red4Sec makes full effort and applies every resource available for each audit, however it does not warrant the function, nor the safety of the project and it cannot be deemed a sufficient assessment of the project's utility and safety, bug-free status, or any other declarations of the project. Additionally, Red4Sec makes no security assessments or judgments about the underlying business strategy, or the individuals involved in the project.

RED4SEC

Invest in Security, invest in your future