The First Decree

The First Decree Website Audit - Q1 2026

Conducted by NCryptsion (Founder)

March 21, 2026

Table of Contents

1 Executing Summary

1.1 Purpose

The purpose of the audit was to evaluate the effectiveness of existing controls, identify potential risks, and ensure compliance with organizational policies and relevant regulatory requirements.

1.2 Scope

- Security headers
- Any data-logging functions

1.3 Time Period

The audit was conducted in a single day, March 21, 2026. The review focuses on the website security and privacy.

2 Findings

Issue	Risk	Area	Impact
Missing Content-Security-Policy Header	CSP is a critical security mechanism that helps protect against cross-site scripting (XSS) and other code injection attacks.	Security headers	Without CSP, attackers could inject malicious scripts, potentially stealing user data, hijacking sessions, or defacing the website.
Missing Permissions-Policy Header	This header controls which browser features and APIs can be accessed by the application and any embedded content (e.g., iframes).	Security headers	Without this policy, malicious scripts or third-party content could access sensitive features like camera, microphone, or geolocation, exposing users to privacy breaches.

3 Analysis

A risk assessment of the website functionalities reveals minimal to no security concerns. However, a privacy risk is identified, as third parties may be able to log visitor requests, because of the CSP and how the resources are loaded.

In accordance with the principles established by the First Decree, it is strongly advised to undertake the implementation of patches and mitigation measures to address the identified concerns.

4 Recommendations

Issue	Recommendation	Priority
Missing Content-Security-Policy Header	Strictly Implement Content-Security-Policy or Locally load the resources	Low
Missing Permissions-Policy Header	Strictly Implement Permissions-Policy by blocking all access	Low

5 Conclusion

Overall, the audit determined that the website demonstrates a generally acceptable level of security, with no critical vulnerabilities identified during the review period. The existing controls appear sufficient to mitigate major security threats, and the overall risk to system integrity remains low.

However, the absence of security headers specifically the Content-Security-Policy and Permissions-Policy introduces notable privacy and client-side security concerns. While these issues are currently assessed as low risk, they could potentially expose users to threats such as unauthorized data access, script injection or misuse of browser features if left unaddressed.

In conclusion, prompt but non-urgent remediation of the identified issues is advised to ensure continued compliance, reinforce user trust and maintain a proactive security posture.