Cyberscope

Penetration Test Report

Gaia Animal Welfare

July 2024

Audited by © cyberscope

Table of Contents

Review

Domain	https://www.gaia-blockchain.com
Registrar	Infomaniak Network SA
Creation Date	06 May 2024
Assessment Scope	Landing Page
Initial Report	24 July 2024

Overview

Cyberscope has conducted a comprehensive penetration test on the web application “Gaia Animal Welfare” hosted at https://www.gaia-blockchain.com. This report focuses on evaluating the security and performance aspects of the web application. The assessment encompasses various facets of the application, including but not limited to authentication and authorization mechanisms, data handling and storage practices, network security measures, and response to high traffic volumes.

The expansion of blockchain technology has introduced a myriad of innovative applications, each with its own unique security challenges. Gaia Animal Welfare, as a prime example within the realm of digital currency ecosystems, ensures robust protection of user data and system integrity.

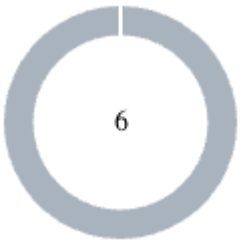
Penetration Assessment Scope

The scope of this assessment extends to identifying vulnerabilities and weaknesses in the application's architecture and functionality, with the aim of providing actionable recommendations to enhance its security posture. The evaluation focused specifically on the landing page of the web app. The assessment included only the landing page of the web app. The report aims to offer a comprehensive understanding of the application's strengths and areas for improvement, facilitating informed decision-making to mitigate risks, fortify against potential cyber threats, and bolster overall security resilience.

Web Technologies

Technology	Category	Version
Chart.js	JavaScript Graphics	N/A
Google Font API	Font Scripts	N/A
RSS	Miscellaneous	N/A
Open Graph	Miscellaneous	N/A
Webpack	Miscellaneous	N/A
Module Federation	Miscellaneous	N/A
HSTS	Security	N/A
Google Analytics	Analytics	GA4
Elementor	Page Builders	3.23.2
WordPress	CMS	6.6.1
jQuery	JavaScript Libraries	3.7.1
core-js	JavaScript Libraries	3.32.0
Apache HTTP Server	Web Servers	N/A
RankMath SEO	SEO	N/A
WPML	Translation	4.6.11

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	6

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	6	0	0	0

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	ATA	Anti-CSRF Tokens Absence	Unresolved
	BPC	Best Practices Compliance	Unresolved
	DCV	DNS Configuration Vulnerability	Unresolved
	MCSPH	Missing Content Security Policy (CSP) Header	Unresolved
	MXH	Missing X-Content-Type-Options Header	Unresolved
	SIL	Server Information Leakage	Unresolved

ATA - Anti-CSRF Tokens Absence

Criticality	Minor / Informative
Status	Unresolved

Description

The absence of Anti-CSRF (Cross-Site Request Forgery) tokens poses a significant security risk to the application. CSRF attacks involve an attacker tricking a user into performing actions on a web application without their knowledge or consent. This vulnerability arises due to the lack of protection mechanisms, such as Anti-CSRF tokens, which prevent unauthorized requests from being executed.

It was observed that no Anti-CSRF tokens were present in the HTML submission forms across various endpoints of the application. Without Anti-CSRF tokens, attackers can forge requests and manipulate user sessions to perform malicious actions, potentially leading to unauthorized data modification, account takeover, or other security breaches.

The following URLs is a sample of all the occurances that demonstrated this vulnerability:

1. https://www.gaia-blockchain.com
2. https://www.gaia-blockchain.com/
3. https://www.gaia-blockchain.com/announcing-the-upcoming-gaia-telegram-bot-mine-earn-and-invite-friends-for-rewards/
4. https://www.gaia-blockchain.com/ar/
5. https://www.gaia-blockchain.com/author
6. https://www.gaia-blockchain.com/author/gaia/

Recommendation

To mitigate the absence of Anti-CSRF tokens and prevent CSRF attacks, the following recommendations are provided:

- Choose a reputable library or framework that includes built-in protections against CSRF attacks or provides features to easily implement Anti-CSRF mechanisms.
- Integrate Anti-CSRF packages such as OWASP CSRFGuard, which offer robust defense mechanisms against CSRF vulnerabilities.
- Ensure that the application is free from XSS vulnerabilities, as CSRF defenses can be bypassed using XSS attacks. Implement proper input validation and output encoding to mitigate XSS risks.
- Generate unique, unpredictable nonces for each form submission and embed them within the forms. Upon form submission, validate the nonce to verify the authenticity of the request. Be cautious of predictable nonces, as they can be exploited by attackers.
- For sensitive or high-risk operations, implement confirmation mechanisms to require users to confirm their actions. This adds an extra layer of security to prevent unauthorized requests.
- Incorporate ESAPI (OWASP Enterprise Security API) Session Management control, which includes components specifically designed to mitigate CSRF attacks.
- Refrain from using the GET method for requests that trigger state changes or sensitive operations, as GET requests can be easily manipulated and abused by attackers.
- Consider checking the HTTP Referer header to verify if requests originated from expected pages. However, be aware that this approach may not be foolproof and can be circumvented by certain user agents or proxies.

By implementing these recommendations, the application can significantly reduce the risk of CSRF attacks and enhance its overall security posture. For additional information and resources on CSRF vulnerabilities and mitigation strategies, refer to the following references.

1. http://projects.webappsec.org/Cross-Site-Request-Forgery
2. https://cwe.mitre.org/data/definitions/352.html

BPC - Best Practices Compliance

Criticality	Minor / Informative
Status	Unresolved

Description

Several issues spanning performance, security, and best practices were identified as part of the assessment. Performance metrics including Speed Index indicate subpar performance levels, which could significantly impact user experience and engagement. These findings underscore the importance of addressing these issues promptly to ensure the application's usability, security, and compliance with industry standards.

In summary, the assessment identified the following issues:

- Speed Index

Metric	Time
Speed Index	2.6s

Recommendation

The team is advised to address the identified issues and improve the overall quality of the application. Specifically, the team could ensure compliance with web development best practices by addressing the aforementioned issues. By addressing the identified issues, the application can improve its performance, security posture, and compliance with industry standards, ultimately enhancing user satisfaction and engagement.

DCV - DNS Configuration Vulnerability

Criticality	Minor / Informative
Status	Unresolved

Description

The domain's DNS records exhibit a significant misconfiguration, with critical security and email deliverability records missing. Notably, the absence of a DKIM (DomainKeys Identified Mail) record is a major concern. DKIM is essential for email authentication, ensuring that messages are not tampered with and verifying the sender's identity, thereby maintaining email integrity and authenticity. Without DKIM, the domain is vulnerable to email spoofing and phishing attacks, and legitimate emails are more likely to be marked as spam, negatively impacting communication and trustworthiness.

Recommendation

To address this issue and enhance the security and reliability of the domain's email communications, the team is recommended to configure the DKIM records according to their email provider documentation. This will ensure that outgoing emails are properly signed and verified. Implementing DKIM will significantly improve email authentication, reduce the risk of spoofing and phishing attacks, and enhance the deliverability of legitimate emails, thereby maintaining communication integrity and trustworthiness.

MCSPH - Missing Content Security Policy (CSP) Header

Criticality	Minor / Informative
Status	Unresolved

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

The following URLs is a sample of all the occurrences where a Content Security Policy (CSP) header was not set.

1. https://www.gaia-blockchain.com
2. https://www.gaia-blockchain.com/
3. https://www.gaia-blockchain.com/author
4. https://www.gaia-blockchain.com/author/gaia/
5. https://www.gaia-blockchain.com/bergabunglah-dengan-kami-untuk-ama-eksklusif-tentang-crypto-fr-diskusikan-gaia/
6. https://www.gaia-blockchain.com/building-the-shelter/

Recommendation

To address the absence of Content Security Policy (CSP) headers and enhance the security of the application, the following steps are recommended:

- Verify that your web server, application server, load balancer, or any other relevant components are properly configured to set the Content-Security-Policy header in HTTP responses.
- Define a comprehensive CSP policy tailored to the specific requirements and functionalities of your application. Consider including directives such as default-src, script-src, style-src, img-src, font-src, connect-src, frame-src, media-src, object-src, and sandbox, among others, to restrict content loading from unauthorized sources.
- Utilize CSP reporting mechanisms to monitor policy violations and fine-tune your CSP directives over time based on real-world usage and detected issues.

By implementing a robust Content Security Policy (CSP) and adhering to best practices for CSP configuration and management, you can significantly reduce the risk of XSS attacks, data injection vulnerabilities, and other web security threats, thereby enhancing the overall security posture of your application.

References:

1. Mozilla Developer Network: Introducing Content Security Policy
2. OWASP Content Security Policy Cheat Sheet
3. W3C Content Security Policy Specification

MXH - Missing X-Content-Type-Options Header

Criticality	Minor / Informative
Status	Unresolved

Description

The absence of the X-Content-Type-Options header exposes the application to potential MIME-sniffing attacks, particularly affecting older versions of Internet Explorer and Chrome. This vulnerability allows browsers to interpret response bodies as content types other than the declared type, potentially leading to security breaches and data exposure. Even error pages (e.g., 401, 403, 500) remain susceptible to such attacks, necessitating immediate action to safeguard against injection vulnerabilities.

The following URLs is a sample of all the occurrences where a X-Content-Type-Options header was not set.

1. https://www.gaia-blockchain.com/robots.txt
2. https://www.gaia-blockchain.com/wp-content/plugins/3d-flipbook-dflip-lite/assets/css/dflip.min.css?ver=2.2.54
3. https://www.gaia-blockchain.com/wp-content/plugins/3d-flipbook-dflip-lite/assets/js/dflip.min.js?ver=2.2.54
4. https://www.gaia-blockchain.com/wp-content/plugins/complianz-gdpr/assets/css/cookieblocker.min.css?ver=1716998420

Recommendation

To mitigate this risk, the team is advised to ensure that the application or web server configures the Content-Type header accurately and includes the X-Content-Type-Options header set to 'nosniff' for all web pages. Additionally, consider recommending users employ modern, standards-compliant web browsers that either abstain from MIME-sniffing or allow for its suppression via directives from the server or application.

Reference:

https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers

SIL - Server Information Leakage

Criticality	Minor / Informative
Status	Unresolved

Description

The web application server is leaking version information through the "Server" HTTP response header. This disclosure can help attackers identify specific vulnerabilities that the server may be susceptible to, increasing the risk of targeted attacks.

The following version information is being exposed: `lighttpd/1.4.35`

Recommendation

The team is advised to configure the web server, application server, load balancer, etc., to suppress the "Server" header or provide only generic details. This will reduce the risk of exposing specific version information that could be exploited by attackers.

Reference:

1. https://httpd.apache.org/docs/current/mod/core.html#servertokens
2. https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)
3. https://www.troyhunt.com/shhh-dont-let-your-response-headers/

Summary

This report provides a thorough assessment of the web application's security and performance. Through meticulous analysis, the report identifies vulnerabilities and weaknesses in key areas such as data handling and network security. Recommendations are provided to address these issues and enhance the application's resilience against cyber threats.

Overall, the report serves as a valuable resource, offering insights into the application's security posture and actionable recommendations to fortify its defenses. By implementing the suggested measures, the team can strengthen the app’s security foundation and maintain trust among users.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io