Cyberscope

Penetration Test Report

eventflo

January 2025

Audited by © cyberscope

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Domain	https://eventflo.io
Assessment Scope	Landing Page

Audit Updates

Initial Audit	22 Jan 2024

Overview

Cyberscope has conducted a comprehensive penetration test on the web application “eventflo” hosted at https://eventflo.io. 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. Tenex 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
React	JavaScript Frameworks	N/A
Next.js	Web Frameworks	15.0.3
HSTS	Security	N/A
Google Analytics	Analytics	N/A
Vercel Analytics	Analytics	N/A
Stripe	Payment Processors	N/A
Webpack	Miscellaneous	N/A
PWA	Miscellaneous	N/A
Tailwind CSS	UI Frameworks	N/A
shadcn/ui	UI Frameworks	N/A

Findings Breakdown

Critical	0
Medium	0
Minor / Informative	4

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	4	0	0	0

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	BPC	Best Practices Compliance	Unresolved
	CM	Cross-Domain Misconfiguration	Unresolved
	CHUD	CSP Header Unsafe Directive	Unresolved
	LTC	Latency And Throughput Challenges	Unresolved
	MXH	Missing X-Content-Type-Options Header	Unresolved
	SIUL	Server Instability Under Load	Unresolved

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 First Contentful Paint, Largest Contentful Paint and Speed Index indicate subpar performance levels, which could significantly impact user experience and engagement. Additionally, best practices violations, such as console errors and inspector issues, were identified. 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:

- Largest Contentful Paint
- Speed Index

Metric	Time
Largest Contentful Paint	1.5s
Speed Index	1.6s

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 forementioned 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.

CM - Cross-Domain Misconfiguration

Criticality	Minor / Informative
Status	Unresolved

Description

A Cross-Origin Resource Sharing (CORS) misconfiguration on the web server has been identified, potentially enabling unauthorized data access across domains. While browser implementations restrict access to authenticated APIs, unauthenticated APIs remain vulnerable. This misconfiguration poses a risk of unauthorized data access, particularly if sensitive data is accessible in an unauthenticated manner, relying solely on other security measures like IP address white-listing. Several requests include the “Access-Control-Allow-Origin” HTTP header being set to “*”, allowing cross-domain access from any origin.

Recommendation

To mitigate this risk, the team is advised to ensure sensitive data is not accessible in an unauthenticated manner, implementing additional security measures such as IP address white-listing. Additionally, the team could configure the “Access-Control-Allow-Origin” header to a more restricted set of domains, limiting cross-domain access, or remove CORS headers entirely to enforce the Same Origin Policy (SOP) more strictly. By implementing these measures, the team can strengthen web security and prevent unauthorized data access across domains.

Reference:
https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

CHUD - CSP Header Unsafe Directive

Criticality	Minor / Informative
Status	Unresolved

Description

Content Security Policy (CSP) is a vital security measure that helps detect and prevent various attacks, including Cross-Site Scripting (XSS) and data injection attacks, which can lead to data theft, site defacement, or malware distribution. CSP allows website owners to specify approved sources for content such as JavaScript, CSS, HTML frames, fonts, images, and embeddable objects, enhancing overall web security. While the CSP header exists, it includes the directives `style-src 'unsafe-inline'` and `script-src 'unsafe-inline'`, allowing inline styles and scripts to be executed, which poses a potential security risk.

Recommendation

The team is advised to strengthen the web app's security by ensuring the web server, application server, load balancer, or any other relevant component is correctly configured to set the Content-Security-Policy header. The team is advised to remove the `unsafe-inline` directive from the style-src and script-src directives to prevent the execution of inline styles and scripts, thereby reducing the risk of XSS attacks and enhancing the overall security posture of the web application.

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 are a sample of all the occurrences where an X-Content-Type-Options header was not set.

1. https://eventflo.io/_next/static/chunks/1033-83474ef68ab4172d.js
2. https://eventflo.io/_next/image?url=https%3A%2F%2Feventflo.io%2Fblog%2Ffloco in-in-eventflo%2Fmedia%2Fprod-files-secure.s3.us-west-2.amazonaws.com_flocoi n_banner_2_(3).jpg&w=640&q=75
3. https://eventflo.io/_next/static/css/10a494554a5691eb.css
4. https://eventflo.io/_vercel/insights/script.js

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-develope r/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_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

cyberscope.io