Cyberscope

Penetration Test Report

AITECH Labs

October 2024

Audited by © cyberscope

Table of Contents

Review

Domain	https://www.tenexcasino.com
Assessment Scope	Landing Page

Audit Updates

Initial Audit	09 Oct 2024

Overview

Cyberscope has conducted a comprehensive penetration test on the web application “tenex” hosted at https://www.tenexcasino.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. Tenex as a prime example within the realm of digital currency ecosystems, ensures robust protection of user data and system integrity.

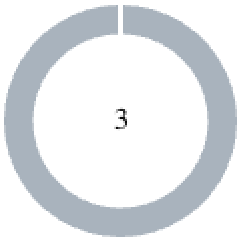
Penetration Assessment Scope

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
Vue.js	JavaScript Frameworks	N/A
Nuxt.js	Web Frameworks	N/A
Sentry	Issue Trackers	N/A
reCAPTCHA	Security	N/A
Cloudflare Browser Insights	Analytics	N/A
Cloudflare	CDN	N/A
Swiper	JavaScript Libraries	N/A
Ethers	JavaScript Libraries	N/A
Core-js	JavaScript Libraries	3.36.1

Findings Breakdown



●	Critical	0
●	Medium	0
●	Minor / Informative	3

Severity		Unresolved	Acknowledged	Resolved	Other
●	Critical	0	0	0	0
●	Medium	0	0	0	0
●	Minor / Informative	3	0	0	0

Diagnostics

🔴 Critical 🟠 Medium ⚪ Minor / Informative

Severity	Code	Description	Status
⚪	BPC	Best Practices Compliance	Unresolved
⚪	DCV	DNS Configuration Vulnerability	Unresolved
⚪	LTC	Latency And Throughput Challenges	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. Moreover, accessibility issues were revealed indicating multiple areas where improvements are needed to enhance user experience, especially for individuals relying on assistive technologies. 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:

- First Contentful Paint
- Largest Contentful Paint
- Speed Index

Metric	Time
First Contentful Paint	1.5s
Largest Contentful Paint	5.9s
Speed Index	2.5s

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.

DCV - DNS Configuration Vulnerability

Criticality	Minor / Informative
Status	Unresolved

Description

The domain's DNS records demonstrate an important misconfiguration. It has been identified that essential records crucial for ensuring security and email deliverability are missing. Specifically, the domain lacks the following crucial records:

- DMARC Record: A Domain-based Message Authentication, Reporting, and Conformance (DMARC) record, leaving the domain vulnerable to email spoofing and phishing attacks.
- DKIM Record: The absence of a DKIM (DomainKeys Identified Mail) record, essential for email authentication, integrity, and authenticity.
- SPF Record: The absence of a Sender Policy Framework (SPF) record means that the domain has no defined policy for identifying authorized mail servers allowed to send emails on behalf of the domain. Without an SPF record, the domain is exposed to email spoofing, and there is a higher risk of emails being marked as spam or rejected by recipient mail servers, leading to potential email deliverability issues.

Recommendation

To mitigate this risk, the team is advised to improve the security and deliverability of email communications by following the recommendations below:

1. Establish and publish a DMARC record to set email authentication policies, specify actions for failed authentication, and receive reports on email authentication results.
2. Configure DKIM records to add cryptographic signatures to outgoing emails, ensuring integrity and authenticity throughout the email delivery process.
3. Configure and publish an SPF record to specify which mail servers are authorized to send emails on behalf of the domain. This will help prevent unauthorized senders from spoofing the domain, improving email authentication and reducing the likelihood of emails being flagged as spam or rejected by recipient servers.

By adhering to these recommendations and rectifying the identified DNS configuration issues, the domain can significantly enhance its email security, mitigate the risk of phishing attacks, and bolster email deliverability and reputation.

LTC - Latency And Throughput Challenges

Criticality	Minor / Informative
Status	Unresolved

Description

As part of the rate-limiting test, the web app highlighted concerns regarding latency and throughput, with varying response times across percentiles and an average latency of 1887.12 milliseconds. Additionally, fluctuations in data transfer rates indicate potential bottlenecks or inefficiencies in data processing and transmission, impacting system performance.

Stat	Avg	Stdev	Max	Min
Latency	1887.12 ms	1709.17 ms	9996 ms	N/A
Req/Sec	1,102.07	271.79	N/A	162
Bytes/Sec	10.7 MB	2.65 MB	N/A	1.58 MB

Recommendation

To enhance system performance, a comprehensive performance analysis is recommended. This analysis should focus on identifying and addressing latency bottlenecks, such as inefficient database queries, resource-intensive operations, or network congestion. Optimization efforts should target the codebase, database queries, and network configurations to improve response times and enhance overall system throughput, resulting in a smoother user experience and improved system efficiency.

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