Cyberscope

Penetration Test Report

KonnektVPN

May 2024

Audited by © cyberscope

Table of Contents

Review

Domain	https://konnektvpn.com
Assessment Scope	Landing Page
Initial Report	02 May 2024

Overview

Cyberscope has conducted a comprehensive penetration test on the web application "KonnektVPN" hosted at https://konnektvpn.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. KonnektVPN, as a prime example within the realm of digital currency ecosystems, ensures robust protection of user data and system integrity.

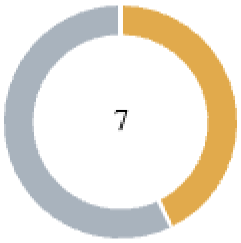
Penetration Assessment Scope

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
Webpack	Miscellaneous	N/A
Open Graph	Miscellaneous	N/A
Lottie Files	Miscellaneous	N/A
HSTS	Security	N/A
Amazon S3	CDN	N/A
React	JavaScript Frameworks	N/A
Emotion	JavaScript Frameworks	N/A
Stripe	Payment Processors	N/A
Amazon Web Services	PaaS	N/A
Next.js	Web Frameworks	14.1.0
Tailwind CSS	UI Frameworks	N/A
Youtube	Video Players	N/A

Findings Breakdown



●	Critical	0
●	Medium	3
●	Minor / Informative	4

	Severity	Unresolved	Acknowledged	Resolved	Other
●	Critical	0	0	0	0
●	Medium	3	0	0	0
●	Minor / Informative	4	0	0	0

Diagnostics

🔴 Critical 🟠 Medium ⚪ Minor / Informative

Severity	Code	Description	Status
🟠	ATA	Anti-CSRF Tokens Absence	Unresolved
🟠	CM	Cross-Domain Misconfiguration	Unresolved
🟠	CHUD	CSP Header Unsafe Directive	Unresolved
⚪	BPC	Best Practices Compliance	Unresolved
⚪	DCV	DNS Configuration Vulnerability	Unresolved
⚪	LTC	Latency And Throughput Challenges	Unresolved
⚪	SIUL	Server Instability Under Load	Unresolved

ATA - Anti-CSRF Tokens Absence

Criticality	Medium
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 demonstrated this vulnerability:

1. https://konnektvpn.com/auth/forgot/
2. https://konnektvpn.com/auth/forgot/?email=zaproxy%40example.com
3. https://konnektvpn.com/auth/login/
4. https://konnektvpn.com/auth/login/?email=zaproxy%40example.com&password=ZAP
5. https://konnektvpn.com/auth/register/
6. https://konnektvpn.com/auth/register/?email=zaproxy%40example.com&first_name=ZAP&is_agree=on&last_name=ZAP&password1=ZAP&password2=ZAP&referrer_code=ZAP
7. https://konnektvpn.com/contact-us/

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

CM - Cross-Domain Misconfiguration

Criticality	Medium
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	Medium
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 directive `style-src 'unsafe-inline'`, allowing inline styles 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 directive to prevent the execution of inline styles, thereby reducing the risk of XSS attacks and enhancing the overall security posture of the web application.

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, Speed Index, and Total Blocking Time indicate subpar performance levels, which could significantly impact user experience and engagement. Moreover, security vulnerabilities were uncovered, particularly concerning the use of deprecated APIs, which expose the application to potential attacks like man-in-the-middle and data interception. Additionally, best practices violations, such as missing meta descriptions and improper meta tag usage, were noted, adversely affecting the application's SEO and overall accessibility. These findings underscore the importance of addressing these issue promptly to ensure the application's usability, security, and compliance with industry standards.

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 demonstrate an important misconfiguration with the Sender Policy Framework (SPF) record, specifically a soft fail without a corresponding DMARC policy. SPF records play a crucial role in email validation, determining authorized sending hosts for a domain. A soft fail means that suspicious emails are not rejected but may be forwarded to spam folders or marked as suspicious, increasing the risk of users falling victim to spoofed or malicious emails. While a DMARC record does exist, its policy is set to “none”.

Recommendation

To mitigate this risk, the team is advised to compile a comprehensive list of authorized email servers for the domain and update the SPF record accordingly. Use the hard fail flag (-all) to ensure unauthorized emails are rejected outright, or set the DMARC policy to quarantine or reject. This provides an additional layer of protection against email spoofing and helps safeguard your organization's email ecosystem from potential threats. Additionally, the team could implement defensive SPF records for all domains within the organization, even those not actively sending emails. This practice, recommended by industry experts such as the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), helps prevent malicious parties from spoofing domains.

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 8972.27 milliseconds. Additionally, fluctuations in data transfer rates indicate potential bottlenecks or inefficiencies in data processing and transmission, impacting system performance.

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.

SIUL - Server Instability Under Load

Criticality	Minor / Informative
Status	Unresolved

Description

The web app highlighted a concerning number of errors (8595), out of which 1112 were timeouts during the assessment period, indicating potential challenges with server stability and resource allocation. Such issues can significantly impact user experience and necessitate a deeper investigation into server health and capacity planning.

Recommendation

To mitigate these challenges, it is advised to conduct a comprehensive analysis of server logs and infrastructure to pinpoint the underlying causes of errors and timeouts. This analysis should inform the optimization of server configurations, potential resource upgrades, and the implementation of robust error handling mechanisms. By addressing these areas, disruptions to user access can be minimized, ensuring a smoother and more reliable service experience.

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