



Cyberscope

Penetration Test Report

GroWealth

January 2025

Audited by © cyberscope

Table of Contents

Table of Contents	1
Risk Classification	3
Review	4
Audit Updates	4
Overview	5
Penetration Assessment Scope	5
Web Technologies	6
Findings Breakdown	7
Diagnostics	8
BPC - Best Practices Compliance	9
Description	9
Recommendation	10
CM - Cross-Domain Misconfiguration	11
Description	11
Recommendation	11
DCV - DNS Configuration Vulnerability	12
Description	12
Recommendation	12
LTC - Latency And Throughput Challenges	13
Description	13
Recommendation	13
MACH - Missing Anti-Clickjacking Header	14
Description	14
Recommendation	14
MCSPH - Missing Content Security Policy (CSP) Header	15
Description	15
Recommendation	15
MSTSH - Missing Strict Transport Security Header	17
Description	17
Recommendation	17
MXH - Missing X-Content-Type-Options Header	19
Description	19
Recommendation	19
SIL - Server Information Leakage	20
Description	20
Recommendation	20
SIUL - Server Instability Under Load	21
Description	21
Recommendation	21

Summary	22
Disclaimer	23
About Cyberscope	24

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://growealth.info
Assessment Scope	Landing Page

Audit Updates

Initial Audit	02 Jan 2025
---------------	-------------

Overview

Cyberscope has conducted a comprehensive penetration test on the web application “GroWealth” hosted at <https://growealth.info/>. 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.

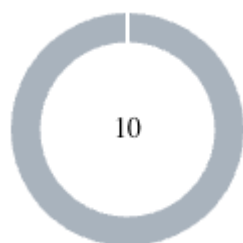
Penetration Assessment Scope

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
Nginx	Web Servers	N/A
React	JavaScript Frameworks	N/A
React Router	JavaScript Frameworks	6.0.0
Ethers	JavaScript Libraries	N/A
core-js	JavaScript Libraries	3.36.1

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	10

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	10	0	0	0

Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	BPC	Best Practices Compliance	Unresolved
●	CM	Cross-Domain Misconfiguration	Unresolved
●	DCV	DNS Configuration Vulnerability	Unresolved
●	LTC	Latency And Throughput Challenges	Unresolved
●	MACH	Missing Anti-Clickjacking Header	Unresolved
●	MCSPH	Missing Content Security Policy (CSP) Header	Unresolved
●	MSTSH	Missing Strict Transport Security Header	Unresolved
●	MXH	Missing X-Content-Type-Options Header	Unresolved
●	SIL	Server Information Leakage	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:

- First Contentful Paint
- Largest Contentful Paint
- Speed Index

Metric	Time
First Contentful Paint	5.4s
Largest Contentful Paint	13.2s
Speed Index	9.1s

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.

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

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.
- **Softfail Without DMARC:** The SPF (Sender Policy Framework) record contains a softfail mechanism without being accompanied by a DMARC record, potentially affecting email deliverability and reputation.

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. Ensure coherence between the SPF record and DMARC policy to maintain consistent email authentication results, thus improving deliverability and security.

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 3919.44 milliseconds. Additionally, fluctuations in data transfer rates indicate potential bottlenecks or inefficiencies in data processing and transmission, impacting system performance.

Stat	Avg	Stdev	Min	Max
Latency	6,768.2 ms	5,558.41 ms	26 ms	30,915 ms
Req/Sec	400.89	207.14	115	843
Bytes/Sec	522 kB	284 kB	153 kB	1.12 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.

MACH - Missing Anti-Clickjacking Header

Criticality	Minor / Informative
Status	Unresolved

Description

The absence of an Anti-Clickjacking header exposes the application to potential Clickjacking attacks. Clickjacking is a malicious technique that tricks users into clicking on unintended elements by disguising them as legitimate UI elements. This can lead to unauthorized actions being performed without the user's knowledge or consent. Without proper protection mechanisms in place, attackers can exploit Clickjacking vulnerabilities to perform actions on behalf of users, such as making purchases, changing account settings, or clicking on malicious links.

The following URLs do not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

1. <https://growealth.info/>
2. <https://growealth.info/robots.txt>
3. <https://growealth.info/sitemap.xml>

Recommendation

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. The team is advised to ensure one of them is set on all web pages returned by the site/app.

If the team expects the page to be framed only by pages on their server (e.g. it's part of a FRAMESET) then they'll want to use SAMEORIGIN, otherwise if the team never expects the page to be framed, they should use DENY. Alternatively, the team could consider implementing Content Security Policy's "frame-ancestors" directive.

Reference: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

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 are missing a Content Security Policy (CSP) header.

1. <https://growealth.info/>
2. <https://growealth.info/robots.txt>
3. <https://growealth.info/sitemap.xml>

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](#)

MSTSH - Missing Strict Transport Security Header

Criticality	Minor / Informative
Status	Unresolved

Description

The absence of the HTTP Strict Transport Security (HSTS) header poses a security risk to the application. HSTS is a crucial web security mechanism that instructs compliant web browsers to interact with the server using only secure HTTPS connections, thereby enhancing the overall security of communication between the client and the server. By enforcing HTTPS usage, HSTS helps mitigate various security threats, including man-in-the-middle attacks, network eavesdropping, and protocol downgrade attacks.

The following URLs are a sample of all the occurrences where an HTTP Strict Transport Security (HSTS) header was not set.

1. <https://growealth.info/>
2. <https://growealth.info/@react-refresh>
3. <https://growealth.info/@vite/client>
4. <https://growealth.info/api/v1/cms/activePresale>
5. <https://growealth.info/api/v1/cms/get-upcoming-investment?offset=0&limit=5>
6. <https://growealth.info/api/v1/cms/get-upcoming-investment?offset=0&limit=6>
7. <https://growealth.info/api/v1/cms/getAllPhase>
8. <https://growealth.info/api/v1/users/count>

Recommendation

To enhance the security of the application and enforce secure communication over HTTPS, it is essential to ensure that the web server, application server, load balancer, or any other relevant components are configured to enforce Strict Transport Security (HSTS). By configuring the application to enforce Strict Transport Security (HSTS) and following best practices for HSTS implementation, the application can significantly reduce the risk of network-based attacks, protect sensitive data in transit, and enhance overall security posture.

References:

1. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Headers_Sheet.html
2. <https://owasp.org/www-community/Security-Headers>
3. http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

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://growealth.info/>
2. <https://growealth.info/@react-refresh>
3. <https://growealth.info/@vite/client>
4. <https://growealth.info/api/v1/cms/activePresale>
5. <https://growealth.info/api/v1/cms/getAllPhase>

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://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 information through one or more “X-Powered-By” HTTP response headers. This header discloses the underlying technology stack, which can aid attackers in identifying the frameworks and components the web application relies on, potentially exposing known vulnerabilities associated with these components.

The following URLs expose the “X-Powered-By” header in their response.

1. <https://growealth.info/api/v1/cms/activePresale>
2. <https://growealth.info/api/v1/cms/get-upcoming-investment?offset=0&limit=5>
3. <https://growealth.info/api/v1/cms/get-upcoming-investment?offset=0&limit=6>
4. <https://growealth.info/api/v1/cms/getAllPhase>
5. <https://growealth.info/api/v1/users/count>

Recommendation

To mitigate the risk associated with information leakage via the “X-Powered-By” HTTP response header, the team is advised to configure the web server, application server, and any intermediaries (e.g., load balancers) to remove or suppress the "X-Powered-By" header from HTTP responses. This prevents the disclosure of information about the underlying technology stack. By implementing this configuration change, the team can reduce the risk of attackers exploiting known vulnerabilities in the application's technology stack.

References:

1. [OWASP Web Security Testing Guide: Fingerprint Web Application Framework](#)
2. [Troy Hunt: Shhh, don't let your response headers talk too much](#)

SIUL - Server Instability Under Load

Criticality	Minor / Informative
Status	Unresolved

Description

The web app highlighted a concerning number of errors (26,909), out of which 3,056 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.

In summary:

- The conducted test used 3000 concurrent connections in 30 seconds timespan.
- The number of requests that were sent was 56,614 requests in 33.34 seconds.
- The number of connection errors (including timeouts) that occurred were 26,909.
- The number of connection timeouts that occurred were 3,056.

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

cyberscope.io