QuillAudits

Audit Report
May, 2024

For

ZEUSMIX

Table of Content

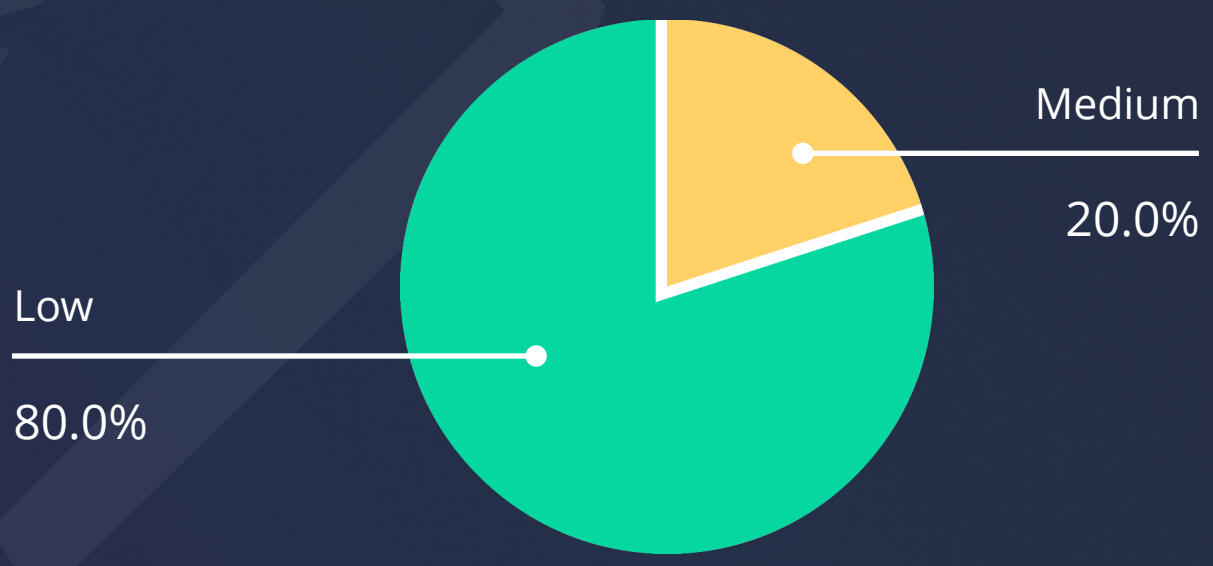
Overview

Overview	Zeusmix is an instant cryptocurrency exchange without registration or KYC. Their key Factors are Speed, Reliability and Anonymity
Scope of Audit	The scope of this pentest was to analyse Zeusmix Web Applications for quality, security, and correctness.
In Scope	https://zeusmix.com/
Timeline	6th May 2024 - 16th May 2024

Number of Issues per Severity

	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	0	1	4	0
Partially Resolved Issues	0	0	0	0
Resolved Issues	0	0	0	0

Security Issues



Checked Vulnerabilities

We scanned the application for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- Improper Authentication
- Improper Resource Usage
- Improper Authorization
- Insecure File Uploads
- Insecure Direct Object References
- Client-Side Validation Issues
- Rate Limit
- Input Validation
- Injection Attacks
- Cross-Site Request Forgery
- Broken Authentication and Session Management
- Insufficient Transport Layer Protection
- Broken Access Controls
- Insecure Cryptographic Storage
- Insufficient Cryptography
- Insufficient Session Expiration
- Information Leakage
- Third-Party Components
- Malware
- Denial of Service (DoS) Attacks
- Cross-Site Scripting (XSS)
- Security Misconfiguration
- Unvalidated Redirects and Forwards

And more...

Techniques and Methods

Throughout the pentest of Zeusmix web applications, care was taken to ensure:

- Information gathering – Using OSINT tools information concerning the web architecture, information leakage, web service integration, and gathering other associated information related to web server & web services.
- Using Automated tools approach for Pentest like Nessus, Acunetix etc.
- Platform testing and configuration
- Error handling and data validation testing
- Encryption-related protection testing
- Client-side and business logic testing

Tools and Platforms used for Pentest:

- Burp Suite
- DNSenum
- Dirbuster
- SQLMap
- Acunetix
- Neucli
- Nabbu
- Turbo Intruder
- Nmap
- Metasploit
- Horusec
- Postman
- Netcat
- Nessus and many more.

Issue Categories

Every issue in this report has been assigned with a severity level. There are four levels of severity, and each of them has been explained below.

High Severity Issues

A high severity issue or vulnerability means that your web app can be exploited. Issues on this level are critical to the web app's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the web app code. Issues on this level could potentially bring problems, and they should still be fixed.

Low Severity Issues

Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational

These are four issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Medium Severity Issues

1. Cross-origin Resource Sharing

Description

Cross-origin resource sharing (CORS) is a browser mechanism which enables controlled access to resources located outside of a given domain. It extends and adds flexibility to the same-origin policy (SOP). However, it also provides potential for cross-domain attacks, if a website's CORS policy is poorly configured and implemented. CORS is not a protection against cross-origin attacks such as cross-site request forgery (CSRF).

Steps to Reproduce

Change the origin header to https://evil.com

Check the response for

Access-Control-Allow-Origin: https://evil.com

Access-Control-Allow-Credentials: true

Impact

Attacker would treat many victims to visit attacker's website, if victim is logged in, then his personal information is recorded in attacker's server.

Also If the site specifies the header Access-Control-Allow-Credentials: true, third-party sites may be able to carry out privileged actions and retrieve sensitive information.

Recommendation

Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.

Status

Acknowledged

Low Severity Issues

1. Clickjacking

Description

Clickjacking is an attack that fools users into thinking they are clicking on one thing when they are actually clicking on another. Its other name, user interface (UI) redressing, better describes what is going onClickjacking is an attack that fools users into thinking they are clicking on one thing when they are actually clicking on another. Its other name, user interface (UI) redressing, better describes what is going on.

Steps to Reproduce

Visit **https://clickjacker.io/test?url=https://zeusmix.com**

Your website will be rendered in a frame confirmin Clickjacking

Impact

This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online. Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees.

Recommendation

Implement X-Frame-Options header.

Reference - https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Status

Acknowledged

2. WAF Bypass (Origin IP Accessible)

Description

The Web Application Firewall (WAF) in place for the target domain, zeusmix.com, was subjected to security testing to assess its effectiveness in protecting the web application against various threats. During the test, we identified a critical security issue, a WAF bypass, that allows attackers to access the IP address behind the WAF. This security weakness bypasses the protective layer and exposes the vulnerable origin server directly.

Impact

- **DDoS Attacks:** By directly accessing the origin server's IP address, malicious actors can launch Distributed Denial of Service (DDoS) attacks, overwhelming the server with traffic, resulting in service outages and downtime.
- **Brute Force Attacks:** Attackers can perform brute force attacks on the origin server, attempting to crack credentials or exploit vulnerabilities without the protection of the WAF.
- **Server Exploitation:** Vulnerabilities on the origin server can be targeted without hindrance, making it more susceptible to exploitation.

Recommendation

- **Patch and Update:** Ensure that the web application, the WAF, and the underlying server software are up-to-date with the latest security patches and updates.
- **WAF Configuration Review:** Carefully review and adjust the WAF configuration to minimize security weaknesses and ensure that it adequately protects against bypass attempts.
- **Rate Limiting and IP Whitelisting:** Implement rate limiting and IP whitelisting rules on the WAF to reduce the risk of DDoS attacks and unauthorized access.
- **Monitoring and Logging:** Set up comprehensive monitoring and logging mechanisms to detect and respond to suspicious activities effectively.

Proof of Concept

http://31.210.172.92:3000/

Status

Acknowledged

3. Multiple Deprecated Libraries in package-lock.json and yarn.lock

Description

Package-lock and yarn.lock Stores files that can be useful for the dependency of the application. This is used for locking the dependency with the installed version. It will install the exact latest version of that package in your application and save it in package. This arises a problem if the dependency used has an exploit in the version mentioned. It can create a backdoor for an attacker.

Vulnerable Dependencies

axios,pgpass

Recommended Fix

1) Update all the above mentioned Dependencies
2) Remove any Library Not needed.

Impact

Multiple of these libraries have public exploits and CVE-registered issues that have been patched and can help your application stay more secure from any dependency-vulnerable issues.

Status

Acknowledged

4. Order Details accessible without AUTH

Description

The orders after being canceled or completed leaks out the “addressOut” of the user. There is an Auth Header present in such /order/XXXXX requests but even if the header is removed it would still show the same response. The requests without such an Auth Header should not be able to show the txn details.

Steps to Reproduce

Visit **https://api.zeusmix.com/orders/R2A7GLW**

Impact

AddressIN and addressOut details leaked.
The Auth Header does not verify anything in general and can be removed or manipulated.

Recommendation

1. Add a proper access control that only people with valid identification can see such API endpoints.
2. Delete such orders after the order is cancelled or completed to not save history after a period of time.

Status

Acknowledged

Closing Summary

In this report, we have considered the security of the Zeusmix web app. We performed our audit according to the procedure described above.

Some issues of High, medium, low, and Informational severity were found, Some suggestions and best practices are also provided in order to improve the code quality and security posture.

Disclaimer

QuillAudits Dapp security audit provides services to help identify and mitigate potential security risks in Zeusmix. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of Zeusmix. One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your smart contracts for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of the Zeusmix to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks

About QuillAudits

QuillAudits is a leading name in Web3 security, offering top-notch solutions to safeguard projects across DeFi, GameFi, NFT gaming, and all blockchain layers. With six years of expertise, we've secured over 1000 projects globally, averting over $30 billion in losses. Our specialists rigorously audit smart contracts and ensure DApp safety on major platforms like Ethereum, BSC, Arbitrum, Algorand, Tron, Polygon, Polkadot, Fantom, NEAR, Solana, and others, guaranteeing your project's security with cutting-edge practices.

1000+
Audits Completed

$30B
Secured

1M+
Lines of Code Audited

Follow Our Journey

Audit Report
May, 2024

For

ZEUSMIX

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com

audits@quillhash.com