QuillAudits

Audit Report
August, 2024

For

BTCFi

Table of Content

Overview

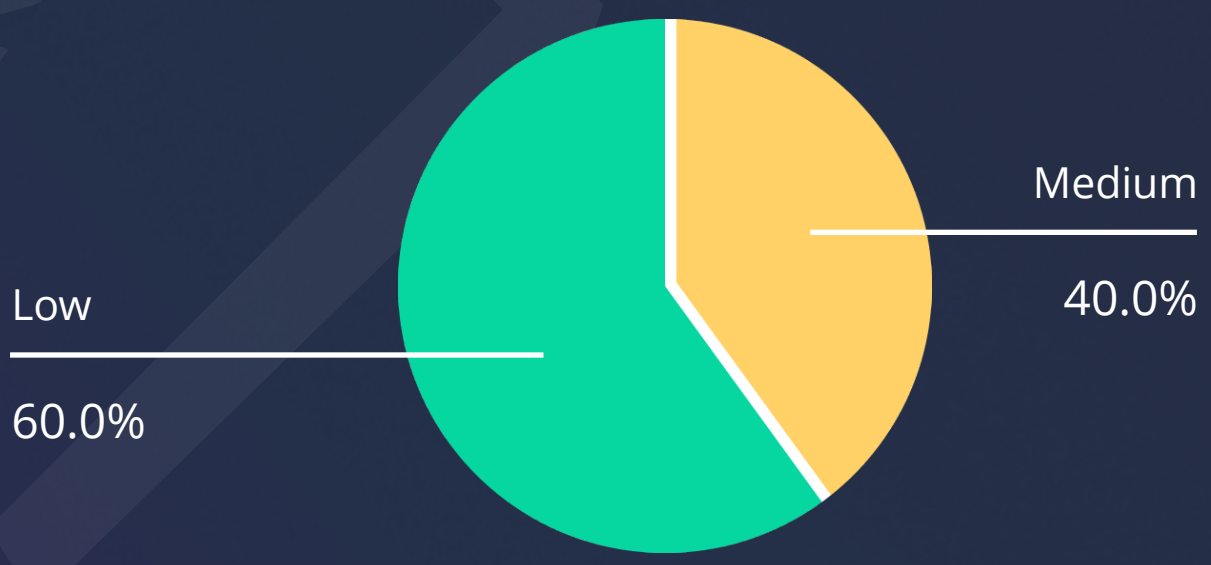
Project Overview	Runesfi are developing a diverse range of products for Runes Protocol which includes Dex, Bridge, Trading Bot, LaunchGround, Explorer, Engraver. We have got a chance to pentest their following in-scope applications for security issues.
Scope of Audit	The scope of this pentest was to analyze Web Applications for quality, security, and correctness.
Timeline	12th June 2024 - 25th June 2024
In Scope	app.btcfi.xyz

Please Note: BTCFi was previously known as “Runes Fi”. The project team rebranded it, and the codebase remains the same. It was audited throughout the timeline given above. Any changes made after June 25th, 2024, will need to be audited.

Number of Issues per Severity

	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	0	2	3	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
- Broken Access Controls
- Insecure Cryptographic Storage
- Insufficient Cryptography
- Insufficient Session Expiration
- Information Leakage
- Third-Party Components
- Rate Limit
- Input Validation
- Injection Attacks
- Cross-Site Request Forgery
- Broken Authentication and Session Management
- Insufficient Transport Layer Protection
- 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 web applications, care was taken to ensure:

- nformation 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. Cpanel and Webmail Exposed

Description

The cPanel and Webmail login interfaces of a server are exposed to the public internet without any access controls or restrictions. This exposure allows anyone to attempt unauthorized access to these interfaces, potentially leading to a full compromise of the server and its associated email accounts.

Vulnerable URL

1. https://app.runesfi.io:2096/
2. https://app.runesfi.io:2083/

Steps to Reproduce

- Open a web browser.
- Navigate to **https://app.runesfi.io:2083/**.
- Navigate to **https://app.runesfi.io:2096/**.
- Observe that the cPanel and Webmail login pages are accessible without any network restrictions.

Impact

Unauthorized access to the cPanel and Webmail can lead to full control over the web server, including the ability to modify web content, access sensitive files, and upload malicious scripts.

Recommendation

Restrict access to cPanel and Webmail interfaces using IP whitelisting to allow only trusted IP addresses.

Consider using a VPN for accessing cPanel and Webmail interfaces to add an additional layer of security.

Regularly monitor server logs for any suspicious access attempts and respond promptly to any potential security incidents.

Status

Acknowledged

2. Outdated Software and Plugins

Description

The website runesfi.io is using outdated WordPress plugins, which may contain known vulnerabilities that can be exploited by attackers. Additionally, the nginx server at dex.runesfi.io is outdated, increasing the risk of exposure to known security flaws.

Vulnerable URL

1. http://runesfi.io
2. http://dexrunesfi.io

Impact

- Outdated WordPress plugins may have vulnerabilities that could be exploited for arbitrary code execution, data leakage, or site defacement.
- An outdated nginx server may have vulnerabilities that can be exploited for remote code execution, information disclosure, or denial of service attacks.

Recommendation

Update WordPress Plugins:

- Update Elementor to version 3.22.1.
- Update Essential Addons for Elementor Lite to version 5.9.24.
- Update Mailchimp for WP to version 4.9.13.
- Update Premium Addons for Elementor to version 4.10.34.
- Update Unlimited Elements for Elementor to version 1.5.111.

This can typically be done through the WordPress admin dashboard under Plugins > Installed Plugins.

Update nginx Server:

- Ensure the nginx server at dex.runesfi.io is updated to the latest stable version.

Status

Acknowledged

Low Severity Issues

3. 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=httpss://test.runesfi.io/swap
https://clickjacker.io/test?url=https://app.runesfi.io/swap

Your website will be rendered in a frame confirming 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

4. Multiple open Ports

Description

The server at IP address 135.181.131.200 (dex.runesfi.io) has open ports, including port 8000, hosting Ordinals. Additionally, the server at IP address 162.214.80.124(app.runesfi.io) has numerous open ports, such as 21, 22, 25, 26, 53, 80, 110, 143, 443, 2222, 3306, and more. Open ports increase the attack surface and may expose the server to various security risks ranging from SSH attacks to MYSQL (3306) attacks due to open port.

Vulnerable URL

1. 135.181.131.200
2. 162.214.80.124

Steps to Reproduce

- Scan the IP addresses 135.181.131.200 and 162.214.80.124 for open ports using a network scanning tool such as Nmap.
- Note down the list of open ports identified during the scan.
  Attempt to access each open port using a web browser or other appropriate tools.

Impact

1. Open ports provide potential entry points for attackers to exploit vulnerabilities, conduct unauthorized access, or launch attacks against the server.
2. Each open port represents a potential service or application running on the server, increasing the risk of unauthorized access, data breaches, and compromise of sensitive information.

Recommendation

Close Unnecessary Ports: Close or block unnecessary ports to reduce the attack surface and mitigate the risk of exploitation.
Implement Firewall Rules: Allow access only to ports that are necessary for the server's intended functionality and services.

Status

Acknowledged

5. Django Login Panel Exposed

Description

The Django login panel located at **https://operations-dash.runesfi.io/admin/login/?next=/** is publicly accessible. While Django's built-in authentication system provides security features, exposing the login panel to the public increases the risk of unauthorized access attempts and potential security breaches.

Vulnerable URL

https://operations-dash.runesfi.io/admin/login/?next=/

Steps to Reproduce

1. Open a web browser.
2. Navigate to the URL **https://operations-dash.runesfi.io/admin/login/?next=/**.
3. Observe that the Django login panel is accessible without any authentication requirements.

Impact

Unauthorized users may attempt to access the Django admin panel, potentially leading to unauthorized access to sensitive information, user accounts, and system settings.

Exposing the login panel increases the risk of brute-force attacks, where malicious actors attempt to guess valid credentials to gain access to the system.

Recommendation

Configure the web server or Django application to restrict access to the login panel based on IP whitelisting or require VPN access for administrators.
Implement rate limiting measures to prevent brute-force attacks on the login panel.

Status

Acknowledged

Closing Summary

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

Some issues of medium and Low 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 BTCFi. 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 BTCFi. 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 BTCFi 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
August, 2024

For

BTCFi

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com

audits@quillhash.com