

DAPP PENETRATION TESTING

V1.0

DATE: 13th MAY 2024

PREPARED FOR: MOONPASS



About BlockApex

Founded in early 2021, is a security-first blockchain consulting firm. We offer services in a wide range of areas including Audits for Smart Contracts, Blockchain Protocols, Tokenomics along with Invariant development (i.e., test-suite) and Decentralized Application Penetration Testing. With a dedicated team of over 40+ experts dispersed globally, BlockApex has contributed to enhancing the security of essential software components utilized by many users worldwide, including vital systems and technologies.

BlockApex has a focus on blockchain security, maintaining an expertise hub to navigate this dynamic field. We actively contribute to security research and openly share our findings with the community. Our work is available for review at our public repository, showcasing audit reports and insights into our innovative practices.

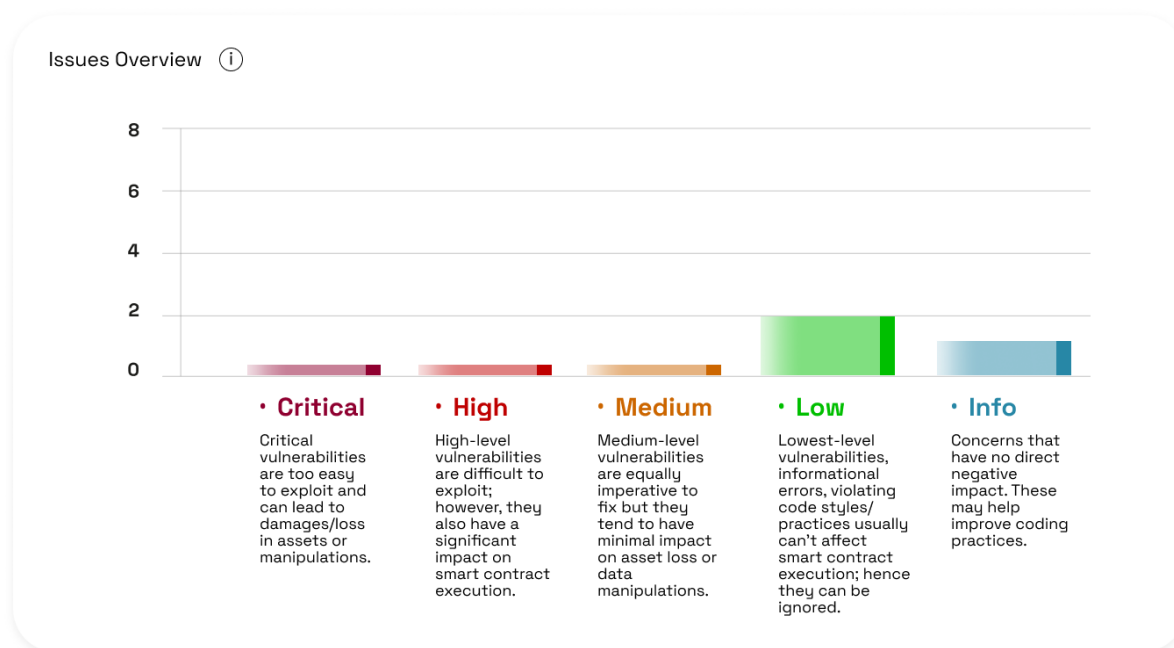
To stay informed about BlockApex's latest developments, breakthroughs, and services, we invite you to follow us on [Twitter](#) and explore our [GitHub](#). For direct inquiries, partnership opportunities, or to learn more about how BlockApex can assist your organization in achieving its security objectives, please visit our [Contact](#) page at our website , or reach out to us via email at hello@blockapex.io.

Contents

1	Executive Summary	4
1.1	Scope	5
1.1.1	In Scope	5
1.1.2	Out of Scope	5
1.2	Methodology	5
1.3	Project Goals	6
1.4	Status Descriptions	6
1.5	Summary of Findings Identified	7
2	Findings and Risk Analysis	8
2.1	Lack of Comprehensive HTTP Security Headers	8
2.2	Incomplete Functionality leading to error	9
2.3	Insufficient DMARC Policy Implementation	11

1 Executive Summary

This report outlines the results of a black box penetration test on the **paramlabs.moonpass.io**, aimed at identifying exploitable vulnerabilities from an external perspective.



1.1 Scope

1.1.1 In Scope

The penetration testing was aimed at following domain:

1. paramlabs.moonpass.io

Note: The current functionality of the website encompasses only logging via wallet and view the NFT of the wallet owner. This report focuses solely on the features that were accessible and operational at the time of the penetration testing.

1.1.2 Out of Scope

For this penetration test, the focus was confined to the functionalities and content within the domains mentioned in the In Scope section. All external and third-party services, including APIs, as well as any modifications to the server infrastructure, were excluded from the scope. Additionally, the testing did not cover denial of service (DoS) attacks or physical security evaluations.

1.2 Methodology

The methodology employed for the black box penetration testing of the domains outlined in the In Scope section spanned a period of one week. The approach adopted was systematic and consisted of several distinct phases, characteristic of black box testing, where the tester has no prior knowledge of the internal systems.

- **Reconnaissance:** The initial phase involved gathering information about the target domains through public resources. This step is crucial to understanding the environment and identifying potential entry points without internal data.

- **Scanning:** Using automated tools, the domains were scanned for known vulnerabilities and weaknesses. This included port scanning, service identification, and vulnerability scanning to prepare for deeper exploration.

- **Vulnerability Assessment:** The vulnerabilities identified in the scanning phase were then analyzed to determine their exploitability and potential impact on the system. This assessment helped prioritize the vulnerabilities in terms of severity and exploitability.

- **Exploitation:** Critical vulnerabilities identified were exploited to understand the level of unauthorized access or damage that could be achieved in a real-world attack scenario. This phase is conducted with extreme care to avoid any disruption to the live environment.

1.3 Project Goals

The engagement is scoped to conduct an exhaustive security assessment of the targeted web domains. We aim to address the following non-exhaustive list of questions, each targeting fundamental security concerns based on the OWASP Top 10 and other relevant security practices:

1. How robust is the input validation mechanism? Are all inputs, such as those in forms and URLs, properly validated to prevent common vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), and Command Injection?
2. What is the state of authentication and session management? Can attackers compromise passwords, keys, or session tokens, or exploit other implementation flaws to assume the identities of other users?
3. Is sensitive data adequately protected? How is data like personal identifiers protected both in transit and at rest from exposure to unauthorized parties?
4. How effective is the configuration management? Are systems and applications using secure configurations, and are there configurations that unnecessarily expose information (such as stack traces or server version numbers) that could be useful to attackers?
5. Are there any vulnerabilities related to access control flaws? Can attackers access unauthorized features or data by bypassing access control checks, modifying the URL, internal application state, or HTML page, or using custom API attack tools?
6. How are potential Cross-Site Scripting (XSS) attacks handled? Does the application neutralize or safely handle user-supplied data within output to prevent the browser from executing malicious scripts?
7. What is the resilience against automated attacks such as credential stuffing or brute force? Are there measures in place to detect and mitigate automated attacks on application login and API endpoints?
8. How is the application protected against business logic errors? Are there business logic flaws that could be exploited to manipulate application processes or data transactions?

1.4 Status Descriptions

Acknowledged: The issue has been recognized and is under review. It indicates that the relevant team is aware of the problem and is actively considering the next steps or solutions.

Fixed: The issue has been addressed and resolved. Necessary actions or corrections have been implemented to eliminate the vulnerability or problem.

Closed: This status signifies that the issue has been thoroughly evaluated and acknowledged by the development team. While no immediate action is being taken.

1.5 Summary of Findings Identified

S.No	Severity	Findings	Status
#1	LOW	Lack of Comprehensive HTTP Security Headers	OPEN
#2	LOW	Insufficient DMARC Policy Implementation	OPEN
#2	INFO	Incomplete Functionality leading to error	OPEN

2 Findings and Risk Analysis

2.1 Lack of Comprehensive HTTP Security Headers

Severity: Low

Status: Open

Location

<https://paramlabs.moonpass.io/>

Description paramlabs.moonpass.io lack several security headers in their HTTP responses. These headers are essential for safeguarding against various web security vulnerabilities, including XSS, clickjacking, and MIME type sniffing. The absence of these headers leaves the websites exposed to potential exploits that could compromise user data and undermine website integrity.

The absence of these headers can lead to several security risks:

- **Content-Security-Policy(CSP):** Without CSP, sites are vulnerable to Cross-Site Scripting(XSS) attacks as there are no restrictions on dynamic resources.
- **X-Content-Type-Options:** No implementation of this header allows browsers to MIME-sniff the content type, leading to incorrect execution of non-executable MIME types as executable.
- **X-Frame-Options:** Without this header, external entities can frame site content, increasing susceptibility to clickjacking attacks.
- **Referrer-Policy:** Lack of this header can result in the full URL being leaked to third-party websites through the referrer header when links are clicked.
- **Permissions-Policy:** Not using this header allows all third-party websites to access various browser features and APIs, which should be restricted.

Recommendation To mitigate the risks associated with the absence of these security headers, it is recommended to implement the above headers across both domains.

References

[Content Security Policy\(CSP\)-MDN Web Docs](#)

[X-Content-Type-Options-MDN Web Docs](#)

[X-Frame-Options-MDN Web Docs](#)

[Referrer Policy-MDN Web Docs](#)

[HTTP Strict Transport Security\(HSTS\)-MDN Web Docs](#)

2.2 Incomplete Functionality leading to error

Severity: Info

Status: Open

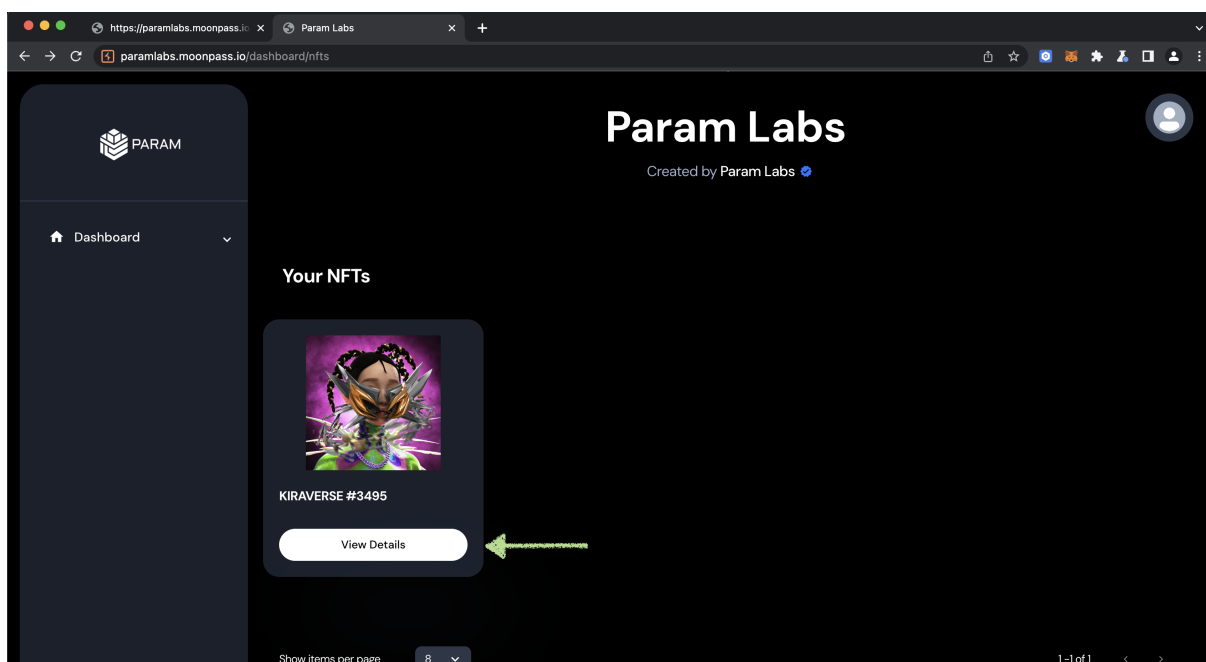
Location

<https://paramlabs.moonpass.io/dashboard/nfts/0/ADDRESS/ID>

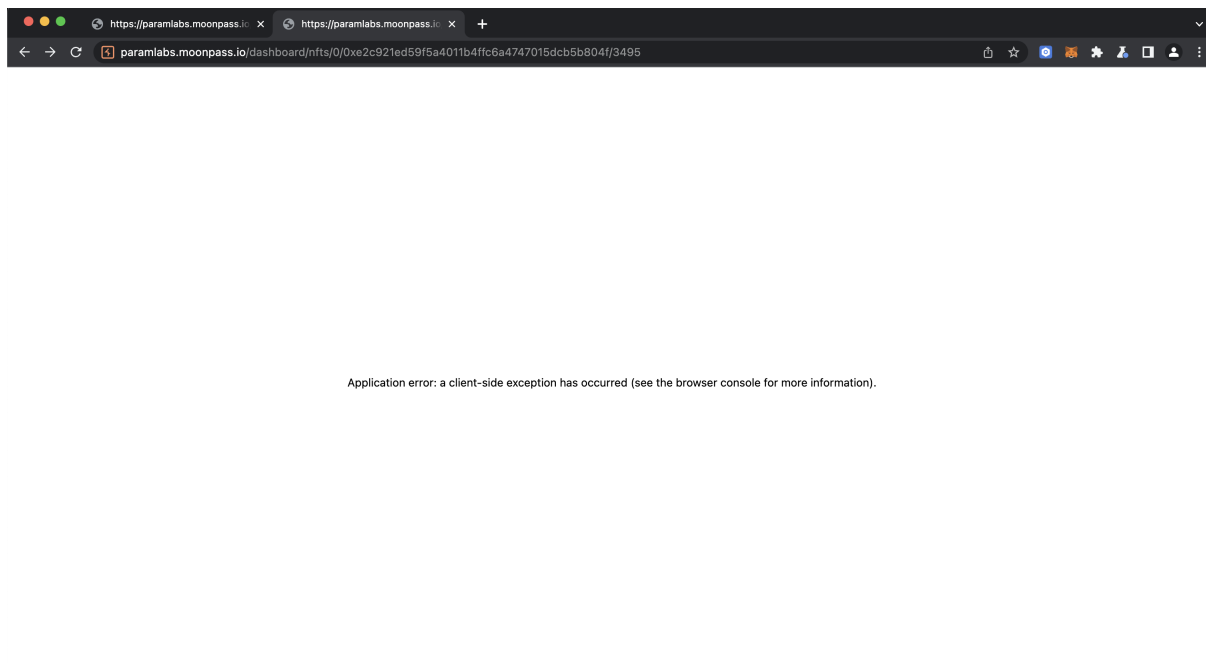
Description In the dashboard user have provision to see its NFTs. For detailed information regarding the nft and "View Detail" is given. During the engagement it was observed that the functionality is buggy and upon clicking a Client-Side exception error is thrown.

Proof of Concept

1. Click on the View Detail under the NFT in the dashboard.



2. Client-side error is thrown.



Recommendation It is recommended to fix the issue to enhance the user-experience.

2.3 Insufficient DMARC Policy Implementation

Severity: Low

Status: Open

Location

1. moonpass.io
2. paramlabs.moonpass.io

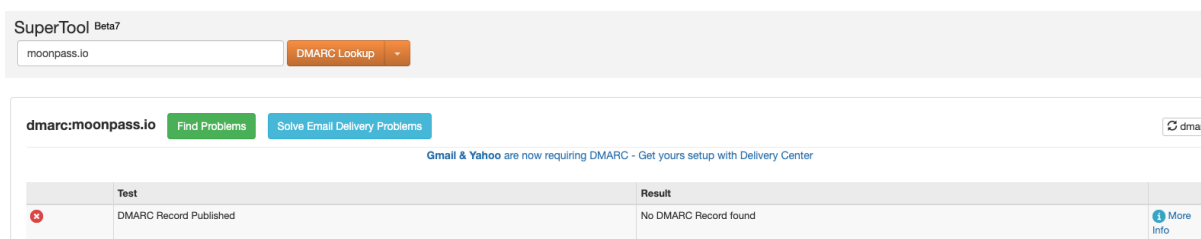
Description An analysis of the DMARC records for the domains moonpass.io and paramlabs.moonpass.io reveals inadequate configurations that compromise email security and integrity. Specifically, moonpass.io lacks a DMARC record entirely, and moonpass.io has a DMARC policy set to "none," which does not instruct receiving servers to take any action against emails failing DMARC checks. Successful spoofing attempts have been demonstrated using a fake mailer, confirming the vulnerability.

Impact The absence of effective DMARC and SPF records allows attackers to send emails that appear to originate from these domains, potentially leading to phishing attacks, loss of client trust, and damage to the reputation of the business.

Proof of Concept

Testing involved the following steps:

1. Examination of DNS records revealed no DMARC record for moonpass.io and an ineffectual DMARC policy for paramlabs.moonpass.io.

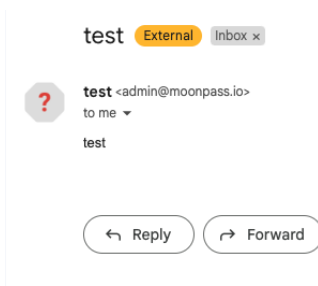


The screenshot shows the SuperTool DMARC Lookup interface. At the top, the domain 'moonpass.io' is entered in the search bar, and the 'DMARC Lookup' button is highlighted. Below the search bar, the results for 'dmarc:moonpass.io' are displayed. A table shows the test results:

Test	Result
DMARC Record Published	No DMARC Record found

A red 'x' icon is next to the test name, indicating a failure. A 'More Info' link is available for the result.

2. Attempts to spoof emails from both domains were successful, indicating that the current configurations do not prevent email impersonation.



The screenshot shows an email interface with a message from 'test' (External) in the 'Inbox'. The email header shows 'test <admin@moonpass.io>' and 'to me'. The body of the email is empty. At the bottom, there are 'Reply' and 'Forward' buttons.

Recommendation To mitigate the risks associated with email spoofing and enhance overall email security, it is advised to implement robust DMARC and SPF records across all domains.

References

[DMAR Email Security](#)

Disclaimer:

The application provided for security assessment has been reviewed using methodologies to date, and there are cybersecurity vulnerabilities and flaws in the application , which are documented in this report, the Source Code compilation, deployment, and functionality (performing the intended functions).

The assessment makes no claims or guarantees about the code's/website security. Furthermore, it cannot be deemed a sufficient evaluation of the code's/website efficiency and safety, bug-free status, or any other safety claims. While we did our best to conduct the analysis and produce this report, it is essential to mention that you should not solely rely on it — To ensure security, we recommend conducting many independent audits and launching a public bug bounty programme.

Any web application is developed, deployed and maintained on a particular platform. The platform, server, its programming language and any other software or application related to it can have vulnerabilities that can lead to attacks or hacks. Thus, our audit can not guarantee the explicit security of the audited product.