

## **Table of Contents**

<b>ARCHITECTURE &amp; ASSET COVERAGE .....</b>	<b>2</b>
<b>SCAN &amp; ASSESSMENT SCOPE.....</b>	<b>2</b>
<b>UNREMIEDIATED FINDINGS.....</b>	<b>3</b>
<b>ADDITIONAL DOCUMENTATION .....</b>	<b>3</b>

# Architecture & Asset Coverage

The Burp Scanner report only included a single hostname, though the architecture diagram suggests multiple publicly facing components.

Can you confirm whether additional hosts/IPs exist, and if so, provide either a complete list or a recent vulnerability assessment that covers them?

1. We have already provided [burp scanner agents.collation.ai](https://bots.collation.ai)
2. <https://bots.collation.ai> which platform for building, scheduling, and monitoring complex workflows and data pipelines

## Attachment :

**Burp Scanner Report - bots-collation-ai.html**  
**defender-scan-reports.pdf**

With respect to <https://bots.collation.ai>, we ran an additional test and noted 5 findings **Session token in URL** marked as **medium**. All of these are false positives.

One reported issue flagged the Microsoft/Azure OAuth login flow as vulnerable. To clarify:

- The URL captured by Burp is the **standard Azure AD authorization endpoint**.
- It does **not** contain sensitive tokens.
- It only carries an authorization code (short-lived, single-use, exchanged server-side for tokens).
- The parameters include:
  - `client_id` → public by design.
  - `state` and `nonce` → random values for replay/XSRF protection, not secrets.
- Sensitive credentials (access tokens, refresh tokens, ID tokens) **are never exposed in this redirect**.  
Therefore, this does not represent an exploitable vulnerability.

# Scan & Assessment Scope

The Burp report was application-level only. Has a broader vulnerability assessment or network/operating system-level scan been conducted? If so, please share the latest reports.

- Attachment: [defender-scan-reports.pdf](#)
- Our Azure infrastructure is secured with Microsoft defender. Please find attached report screenshots.
- All Virtual machines are monitored on security patched and auto applied  
We have crowdstrike falcon pro end point protections for secure all desktops and servers.

# Unremediated Findings

The API penetration test identified one medium-severity and two informational findings that were not remediated within expected timeframes. Can you provide an explanation for why these issues remain unresolved, along with any plans or timelines for remediation?

There one medium severity reported by test was no-cache header not set with nodeJS middleware which can no-cache header set. This is fixed and deployed

```
ps curl -X 'GET' \
https://api-dev.collation.ai/v1/7c87f356-5d6c-43f5-baa7-e69bbf1c9e/organizations/?page=1&per_page=20&sort_column=created_at&sort_direction=desc \
-H 'accept: application/json' \
-H ''
39m55
zTc0M
30mE3
jw8NY
Dr5QZU
HTTP/2 200
content-length: 4456
content-type: application/json
date: Mon, 08 Sep 2025 18:28:16 GMT
server: us-east-1
cache-control: no-store, must-revalidate, no-cache
expires: 0
pragma: no-cache
x-ms-middleware-request-id: cfa8f8f8-1642-4d7a-8343-58df819868c4
x-request-id: 08e67081-5c6f-4d83-992b-642b09a449f
x-response-time: 0.806561229994986286
strict-transport-security: max-age=31536000; includeSubDomains
{"organizations":[{"organization_uid":"
ation_uid":"ae5b808e-af32-4b4c-b403-e27
```

The screenshot shows a browser window with a spreadsheet titled "Manage Security Master" and a network inspector. The spreadsheet has columns for contract\_currency, is\_public, collation\_asset\_class, and collation\_sub\_asset\_class. The network inspector shows a request to "getRecords?api=securities&params=%7B%22per\_page%22%3A396be-b201-4daf-98d8-c..." with a response that includes "Cache-Control: no-cache, keep-alive, collation-excel-app.azurewebsites.net, no-cache".

# Additional Documentation

Please provide an up-to-date architecture document, penetration test report, and vulnerability assessment report on all publicly accessible assets.

Please find attached azure-collation-architecture-enhanced.pdf