Table of Contents

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
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

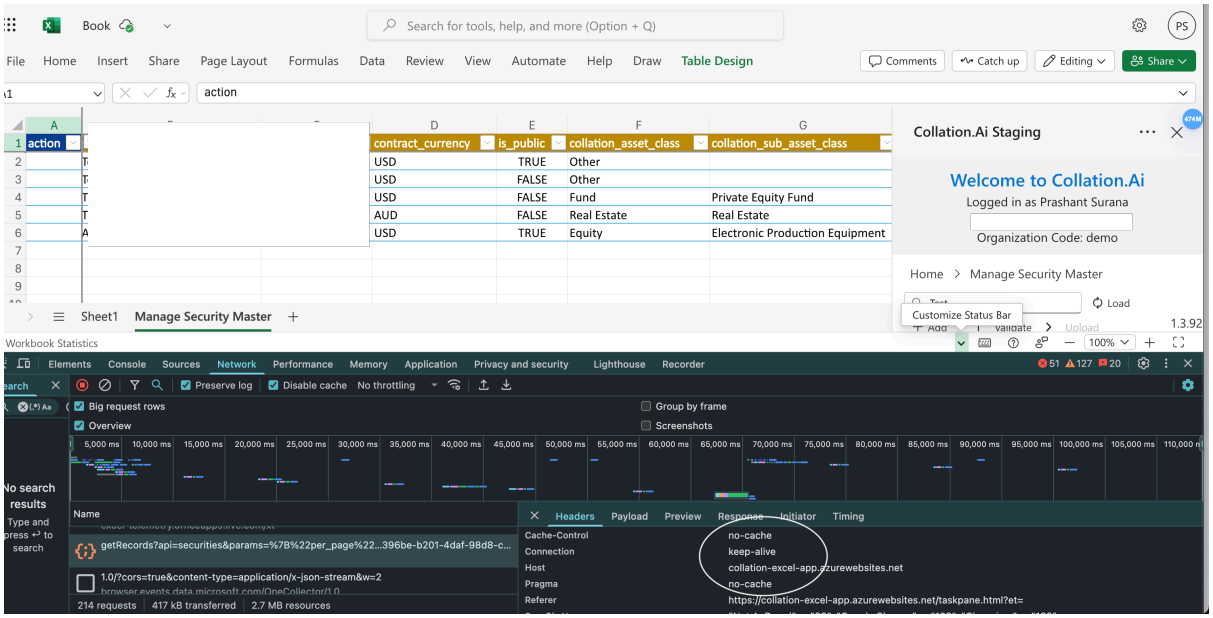
The Burp report was application-level only. Has a broader vulnerability assessment or network/operating system–level scan been conducted? If so, please share the latest reports.

- Attachment: defender-scan-reports.pdf
- Our Azure infrastructure in 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 middlewear which can no-cache header set. This is fixed and deployed



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