Security penetration test
for Insights API

Service provided for Hyfe Inc.

December 2, 2024
Prepared by: Olha Lesiuk
Presented to Paul Rieger

The information contained within this report is considered proprietary and confidential to Hyfe. Inappropriate and unauthorized disclosure of this report or portions of it could result in significant damage or loss to the Hyfe. This report should be distributed to individuals on a need-to-know basis only. Paper copies should be locked up when not in use. Electronic copies should be stored offline and protected appropriately.

DISCLAIMER

The information presented in this document is provided as-is and without warranty. Vulnerability assessments are a “point in time” analysis. As such, it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, new vulnerabilities may likely have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks, and applications.

1. Scope

Testing and verification were performed from November 19, 2024, to December 2, 2024. This project's scope was limited to the API and the network infrastructure mentioned below. Tests were conducted using a production environment of the Hyfe Insights API. All other applications and servers were out of scope. The following hosts were considered to be in scope for testing.

Network					
IP address	**Hostnames**	**Port**	**Protocol**	**Service**	**Service Information**
108.138.51.72	v2.api.hyfe.ai	443	TCP	SSL/HTTP	Amazon CloudFront httpd
108.138.51.72	v2.api.hyfe.ai	80	TCP	HTTP	Amazon CloudFront httpd

Supported Methods: **GET HEAD POST OPTIONS**
SSL-cert: Subject commonName=v2.api.hyfe.ai
Subject Alternative Name: DNS: v2.api.hyfe.ai
Issuer: commonName=Amazon RSA 2048 M02/orgranizaitonName=Amazon/countryName=US
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2024-01-23T00:00:00
Not valid after: 2025-02-20T23:59:59
MD5: 69f1:4b75:28ba:27df:3e4d:08ee:1d16:c331
SHA-1: 9415:b924:8126:d0a7:7161:4bc4:635f:5b2c:6b9f:6e7c
Other addresses for v2.api.hyfe.ai (not scanned): 108.138.51.20, 108.51.94, 108.138.51.26

TLS Certificate has not been revoked

OCSP Staple:	Not Enabled
OCSP Origin:	Good
CRL Status:	Good

Protocol Support

TLSv1.2
TLSv1.3

2. Summary of findings

Security testing was performed according to the OWASP API Testing, OWASP REST Security Cheat Sheet, and OWASP API Security tools which demonstrates the following results.

Name	Risk level	Number of alerts
Cross-Domain misconfiguration	Medium	1
Strict-Transport-Security Header not set	Low	1
X-Content-Type-Options Header missing	Low	1
Re-examine Cache-control directives	Informational	1

Severity scoring:

- Critical – Immediate threat to key business processes.
- High – Direct threat to key business processes.
- Medium – Indirect threat to key business processes or partial threat to business processes.
- Low – No direct threat exists. The vulnerability may be exploited using other vulnerabilities.
- Informational – This finding does not indicate vulnerability but states a comment that notifies about design flaws and improper implementation that might cause a problem in the long run.

3. Alert details

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross-Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/derived-events/aggregated?limit=1000&offset=0&device_id=b5a0cf86-1485-4593-b7d7-fac7e66db228&aggregation=weekly&start_date=2024-10-01T13:42:14.941Z&end_date=2024-11-11T13:42:14.941Z&direction=desc&omit_empty_buckets=false&fields=avg_duration&metrics=cough_oasis
METHOD	**GET**
Evidence	access-control-allow-origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third-party domains, using unauthenticated APIs on this domain. However, web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs. This reduces the risk. An attacker could use this misconfiguration to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Solution	Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/weakness
CWE id	264
WASC id	14
Plugin id	10098

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/notes/9102c778-a366-4b27-8cb5-1325181f116c
METHOD	**DELETE**
URL	https://v2.api.hyfe.ai/
METHOD	**GET**
URL	https://v2.api.hyfe.ai/favicon.ico
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc%7D/stats
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/derived-events/aggregated?limit=1000&offset=0&device_id=b5a0cf86-1485-4593-b7d7-fac7e66db228&aggregation=weekly&start_date=2024-10-01T13:42:14.941Z&end_date=2024-11-11T13:42:14.941Z&direction=desc&omit_empty_buckets=false&fields=avg_duration&metrics=cough_oasis
METHOD	**GET**

URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/derived-events?limit=1000&offset=0&device_id=b5a0cf86-1485-4593-b7d7-fac7e66db228&metric=cough_burst&from=2024-10-01T13:42:14.941Z&to=2024-11-11T13:42:14.941Z&direction=desc&fields=start_time,uid,device_id,metric,duration_s,burst_size&order_by=duration_s
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/devices
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/devices/b5a0cf86-1485-4593-b7d7-fac7e66db228
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/events/aggregated?limit=1000&offset=0&device_id=b5a0cf86-1485-4593-b7d7-fac7e66db228&aggregation=daily&start_date=2024-11-01T10:40:32.899402Z&end_date=2024-11-13T10:40:32.899402Z&direction=asc&omit_empty_buckets=false&fields=count&metrics=cough_burst
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/events?limit=1000&offset=0&device_id=b5a0cf86-1485-4593-b7d7-fac7e66db228&metric=cough&start_date=2024-11-01T10:40:32.899402Z&end_date=2024-11-01T10:40:32.899402Z&direction=desc&fields=time,uid,device_id,metric,value1,value2&order_by=time
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/insights/clock?from=2024-11-10T10:40:32.899402Z&to=2024-11-13T10:40:32.899402Z&device_id=b5a0cf86-1485-4593-b7d7-fac7e66db228&metric=cough
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/insights/streak?start=2024-11-13T10:40:32.899402Z&device_id=b5a0cf86-1485-4593-b7d7-fac7e66db228&tracking_threshold_minutes=60

METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/insights/trend?date=2024-11-13T10:40:32.899402Z&device_id=b5a0cf86-1485-4593-b7d7-fac7e66db228&granularity=month&metric=cough
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/notes
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/notes/7b5dbca9-1bfb-4208-b04d-7d7b376eecca
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/notes?limit=100&offset=0&start_date=2024-11-01T13:42:14.941Z&end_date=2024-12-11T13:42:14.941Z&triggers_id&direction=desc
METHOD	**GET**
URL	https://v2.api.hyfe.ai/robots.txt
METHOD	**GET**
URL	https://v2.api.hyfe.ai/sitemap.xml
METHOD	**GET**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc
METHOD	**PATCH**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/devices
METHOD	**POST**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/events
METHOD	**POST**

URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/notes
METHOD	**POST**
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/notes/7b5dbca9-1bfb-4208-b04d-7d7b376eecca
METHOD	**PUT**
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	HTTP Strict Transport Security - OWASP Cheat Sheet Series https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE id	319
WASC id	15
Plugin id	10035

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/derived-events/aggregated?limit=1000&offset=0&device_id=b5a0cf86-1485-4593-b7d7-fac7e66db228&aggregation=weekly&start_date=2024-10-01T13:42:14.941Z&end_date=2024-11-11T13:42:14.941Z&direction=desc&omit_empty_buckets=false&fields=avg_duration&metrics=cough_oasis

METHOD	**GET**
Other info	This issue still applies to error-type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still a concern for browsers sniffing pages away from their actual content type. At the "High" threshold this scan rule will not alert client or server error responses.
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. Ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)
CWE id	693
WASC id	15
Plugin id	10021

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like CSS, JS, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://www.google.com/url?q=https://v2.api.hyfe.ai/jwt/coughpro/users/9c980c1f-13e8-4ec7-9b4d-122f49b425dc/derived-events/aggregated?limit%3D1000%26offset%3D0%26device_id%3Db5a0cf86-1485-4593-b7d7-fac7e66db228%26aggregation%3Dweekly%26start_date%3D2024-10-01T13:42:14.941Z%26end_date%3D2024-11-11T13:42:14.941Z%26direction%3Ddesc%26omit_empty_buckets%3Dfalse%26fields%3Davg_duration%26metrics%3Dcough_oasis&sa=D&source=apps-viewer-frontend&ust=1732714144879177&usg=AOvVaw2oHhsVyjN3bSHY_hqaEiPJ&hl=en-GB
METHOD	**GET**

Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
CWE id	525
WASC id	13
Plugin id	10015

3. HTTPS methods, input validation, and error handling were tested based on the Hyfe Insights API documentation which is based on the OpenAPI 3.0 specification.
API supports both API Key and Bearer token authentication(JWT).

References
CoughPro Postman API tests
CoughMonitor Postman API tests