WOOLLEMIA INFOSEC

WOOLLEMIA INFOSEC

Case Study

Comprehensive API Security Assessment for a Healthtech Digital Services Platform

Industry	Healthtech & Digital Services
API Landscape	REST & GraphQL APIs supporting Web, Mobile, and Third-Party Partner Integrations
Assessment Type	Comprehensive API Security Assessment
Technology Landscape	API Gateway, Microservices Architecture, OAuth 2.0 / OpenID Connect, JWT-Based Authentication, Partner Integration APIs
Core Services Delivered	API Discovery & Inventory, Authentication & Authorization Testing, Business Logic & Object-Level Authorization Testing, Rate Limiting & Abuse Case Testing, Data Exposure Review, API Gateway Configuration Review

Executive Summary

Modern applications are increasingly powered by APIs that connect web front-ends, mobile applications, and third-party partners to core business logic and sensitive data. As API surfaces grow in number and complexity, they have become one of the most commonly exploited attack vectors, particularly where authorization logic fails to properly restrict access to individual records or actions.

A healthtech digital services provider engaged Woollemia Infosec to conduct a comprehensive API Security Assessment of its REST and GraphQL API ecosystem, ahead of expanding its partner integration program and launching new patient-facing digital services. The organization wanted independent assurance that its APIs properly enforced authentication, authorization, and data protection controls across every consumer of the platform.

Woollemia Infosec performed a structured assessment covering API discovery, authentication and session handling, object and function-level authorization, business logic abuse cases, rate limiting, and API gateway configuration, aligned with the OWASP API Security Top 10.

The assessment enabled the client to close critical authorization gaps, strengthen protections around sensitive patient data, and establish a sustainable process for securing future API development.

Client Overview

The client operates a suite of patient-facing and partner-facing digital health services delivered through REST and GraphQL APIs consumed by web applications, native mobile applications, and integrated third-party healthcare partners. The API layer supports patient record access, appointment scheduling, secure messaging, billing information, and integration with external laboratory and pharmacy partners.

As the organization expanded its partner ecosystem and introduced new API consumers, it recognized the need for an independent, structured assessment focused specifically on the unique risks APIs present, distinct from a traditional web application assessment.

Business Challenge

The client's API surface had grown rapidly to support new patient features and partner integrations, resulting in a large number of endpoints with varying levels of documentation, authentication requirements, and authorization logic maturity.

The organization required assurance that object-level authorization was correctly enforced across all endpoints, preventing one patient or partner from accessing another's records simply by manipulating identifiers in API requests.

Because the platform handled protected health information, any authorization weakness in the API layer could result in unauthorized disclosure of sensitive patient data, regulatory exposure, and loss of partner trust.

The client also wanted to confirm that APIs exposed to third-party partners enforced appropriate rate limiting and abuse protections, given the sensitivity of the data being exchanged.

Our Understanding

Woollemia Infosec recognized that API security requires a distinct testing approach from traditional web application assessments, with particular emphasis on business logic, object-level authorization, and the trust relationships between different types of API consumers.

Our team understood that in a healthtech context, the most damaging vulnerabilities are rarely exotic technical exploits, but rather broken object-level authorization that allows one user to access another's protected health information through predictable identifiers or insufficiently validated requests.

Our Solution

API Discovery and Inventory

The engagement began with comprehensive API discovery, cataloguing all REST and GraphQL endpoints across patient-facing, partner-facing, and internal service-to-service communication, including undocumented or shadow API endpoints identified during testing.

Authentication and Session Security Testing

Our consultants evaluated the OAuth 2.0 and OpenID Connect implementation, JWT token handling, token expiration and revocation, and session management practices across all API consumer types.

Object-Level and Function-Level Authorization Testing

The core of the engagement focused on systematically testing whether users and partner integrations could access records, actions, or administrative functions beyond their intended privileges, targeting broken object-level authorization and broken function-level authorization.

Business Logic and Abuse Case Testing

Our team tested critical business workflows exposed through the API layer, including appointment scheduling, billing operations, and messaging features, for logic flaws that could be exploited to bypass intended process controls.

Data Exposure and Response Handling Review

The assessment reviewed API responses for excessive data exposure, confirming that endpoints returned only the data fields necessary for the requesting client rather than over-exposing internal record structures.

Rate Limiting and Resource Consumption Testing

Our consultants tested rate limiting and throttling controls across sensitive and high-volume endpoints, evaluating resilience against abuse, scraping, and resource exhaustion attempts, particularly for partner-facing integration APIs.

API Gateway and Configuration Review

The engagement reviewed API gateway configuration, including request validation, logging, security headers, and centralized authentication enforcement, to confirm consistent security controls across all published APIs.

Manual Validation and Reporting

Every finding was manually validated by experienced consultants, with proof-of-concept requests captured to demonstrate real-world impact, followed by a comprehensive technical report and executive summary mapped to the OWASP API Security Top 10.

Business Value Delivered

The API Security Assessment gave the client comprehensive visibility into authorization weaknesses that automated scanning alone would not have identified, particularly around object-level access to patient data.

The engagement strengthened the organization's confidence in protecting sensitive health information, supported safer expansion of its partner integration program, and improved trust with healthcare partners handling shared patient data.

By addressing authorization and business logic gaps early, the client reduced the risk of regulatory exposure and reputational harm associated with unauthorized data access.

Why Woollemia Infosec

Woollemia Infosec delivers specialized API security assessments that go beyond generic vulnerability scanning, with deep expertise in object-level authorization testing, business logic analysis, and modern API authentication frameworks.

Our consultants work closely with engineering teams to provide practical, prioritized recommendations that strengthen API security without disrupting ongoing feature development.

Conclusion

This representative engagement demonstrates Woollemia Infosec's ability to perform comprehensive API Security Assessments for complex, multi-consumer API ecosystems handling sensitive data.

By evaluating authentication, authorization, business logic, and gateway configuration, we helped the client establish a stronger security foundation for its growing digital health platform.