AUDACIX
OUTPERFORM YOUR NOW

Penetration Testing Case Study

Cloud ERP Application With Extensive API Integrations

Tech Stack

Python
C#
Java
React
Ruby On Rails
MySQL

Challenge

Enable secure integrations with 3rd party apps without slowing down speed of development

Result

Doubling of available APIs within 12 months + downward sloping API vulnerability trajectory

Client Story

Our client always had a strong security focus with PCI accreditation, because of the sensitive nature of data they stored. When a commercial decision required them to focus on 3rd-party integrations by expanding their API layer, they wanted AppSec partners who could help stay resilient, while they kept pace with a demanding development schedule.

The Challenge

This client had a strong engineering team with a well developed security culture. They did not want their security resilience compromised during the development surge.

So in addition to regular external web application and API penetration testing, our client required an enhanced API security structure that wouldn’t slow down their Engineers, but one that would also keep their customers’ data secure during transit.

The Solution

Audacix’s AppSec team applies a customised quarterly white-box penetration testing plan to the web application, infrastructure and APIs to help it satisfy PCI DSS 11.3 requirements.

Among other security protocols, all automated deployment pipelines mandatorily include vulnerability scans for OWASP Top 10 vulnerabilities. This extends to the API layer and ensures that all security controls are applied before each new API becomes publicly available.

Our client’s “shift left” with security allows them to apply the benefits of tools like our Cyber Chief application & API vulnerability scanner to find and patch vulnerability regressions before each release. This is a key part of maintaining their ISO27001 and PCI accreditation.

The thoroughness of the AppSec system means our quarterly penetration tests are not just for finding vulnerabilities, but also for simplying and speeding up security protocols.