



PENETRATION TESTING

# API

Secure your API backbone with our comprehensive API penetration testing service.

## What is API penetration testing?

API penetration testing, or API pen testing, involves a security assessment that evaluates the strength of an application's APIs. APIs are commonly the foundation of modern applications, enabling data exchange between various software components. However, their accessibility to external users and systems makes them susceptible to different types of attacks. API pen testing aims to pinpoint and exploit vulnerabilities that permit unauthorised access, data theft, or service disruption.

## Why is API penetration testing important?

### Protect sensitive data

APIs handle sensitive data such as personal information, financial records, and proprietary business data. Securing these data channels prevents data breaches and maintains user trust.

### Compliance requirements

Many industries must comply with regulations such as GDPR, PCI-DSS, and HIPAA, which require regular security assessments. API pen testing helps organisations meet these compliance mandates.

### Identify hidden vulnerabilities

Regular security measures might not uncover deeper issues within APIs. Penetration testing exposes authentication, authorisation, input validation, and business logic flaws that threat actors could exploit.

### Prevent financial loss

Data breaches and service disruptions can lead to significant financial losses due to regulatory fines, legal fees, and damage to reputation. Regular API testing mitigates these risks by identifying vulnerabilities before they are exploited.

### Safeguard business reputation

Earning ISO 42001 certification differentiates Proactively identifying and addressing security vulnerabilities helps protect your reputation by preventing security incidents that could lead to loss of customer trust and business

opportunities.

## Our API penetration testing methodology

We usually follow but do not limit our test cases to the OWASP API Top 10, a list of the ten most critical security risks for APIs. These risks are ranked based on their likelihood of occurrence and their potential impact on an organisation's security.

## SmartView takes care of your reporting

Cognisys' SmartView Portal is a comprehensive, centralised solution for managing projects and vulnerabilities effectively. This powerful platform allows clients to seamlessly track the status of identified security issues, assign tasks to appropriate team members, and oversee the progress of remediation efforts. By providing real-time insights and a structured workflow, the SmartView Portal ensures that vulnerabilities are prioritised and resolved promptly, minimising potential risks.

Additionally, the portal's user-friendly interface enhances collaboration and communication among team members, leading to a more coordinated and proactive approach to security. Ultimately, this results in a strengthened security posture for web applications and an improved overall risk management strategy.

## Why choose Cognisys' API penetration testing?

With the rise in API usage, the need for robust security measures has never been more critical. Our API penetration testing services stand out because of our expertise, thoroughness, and, most importantly, our commitment to your security. We don't just identify vulnerabilities; we partner with you to understand your specific risks and guide you through the remediation process. By choosing us, you ensure that your APIs are secure and optimised for performance and compliance.

[BACK TO CONTENTS](#)

