API Penetration Testing as a Service (PTaaS)

Security & Compliance: Simplified & Validated.

Every organization has two core things to protect - Revenue and Reputation. Both are directly impacted by businesses' ability to build and execute a reliable Security, Compliance and Risk Management strategy. And organizations with regulatory requirements must understand the direct impacts that security and compliance management have on their ability to defend and protect both revenue and brand reputation.

Pen Testing is a key first step to help you achieve both! Knowing what you're actually vulnerable to from the outside is a critical component of any security and risk program, and we believe every organization should have easy and simple access to comprehensive Pen Testing, on demand.

Wib's advanced application and API penetration testing service covers today's most rapidly expanding attack surface - APIs, and is Available Today!

To help our customers manage these changes and meet these new requirements, Wib is simplifying the process for organizations to become fully compliant and demonstrate rigorous risk management.

Wib API Pen Testing as a Service (PTaaS)

Our industry-first API pen testing service is a quick and simple way to ensure compliance with the new regulations by providing full pen testing capabilities or augmenting your existing pen testing solution with our API-specific security expertise.

Gartner®

According to Gartner

90% of web-enabled applications will expose more attack surface via APIs than in the user interface (UI), and API abuses will move from infrequent to the most-frequent attack vector during 2022.

PCI Compliance

In addition, all PCI covered entities will be required to transition to compliance with PCI DSS 4.0 over the next two years, and for the first time, PCI Data Security Standards now require specific **testing for API vulnerabilities, including logic-based attacks** (Section 6.4.1, PCI DSS v4.0).

What you get

Wib's unobtrusive API PTaaS offering is delivered within 3 weeks with minimal resource pressure and NO integration requirements:

1. Full risk and vulnerability assessment of your critical APIs (can include black, grey, or white box testing)
2. A risk severity score based on NIST cyber Matrix calculator
3. Contextual remediation report for all identified vulnerabilities
4. Remediation road map plan with implementation suggestions and professional validation of remediation as required by PCI DSS 4.0
5. Training and consultancy session with Wib's expert Offensive Security team
6. Testing tailored to GDPR, CCPA, SOC-2, ISO, NIST 800-30, HIPAA, CMA and other regulatory frameworks

What we test for:

1. OWASP API top 10 vulnerabilities
2. Business Logic Vulnerabilities, including sophisticated and chained attacks that automated tools miss
3. PCI- DSS Mandated requirements such as segmentation, AuthN, and AuthZ controls
4. GDPR, CCPA, SOC-2, ISO, NIST 800, HIPAA, and other regulatory framework requirements tailored to your company and industry needs

Consumption model

Flexible Offerings – Pick and Choose what fits your security program

1. Annual, Semi-Annual, Quarterly, or custom testing intervals
2. On-Demand testing for material changes to your architecture / attack surface, pre or post production - or both!
3. Specific, actionable remediation instructions and professional validation - so you KNOW your attack surfaces are hardened post-fix
4. No implementation / installation required – full assessment of your API attack surface with a testing process that is unobtrusive and hassle free.