CYBER THREATS WON'T WAIT
WHY SHOULD YOU?

Security shouldn't slow you down—it should accelerate your innovation. Testify isn't just a security tool; it's an innovation catalyst that transforms cybersecurity from a hurdle into an advantage. Step into the future of API security with Testify and fortify your digital infrastructure like never before.

Only 38% of APIs, on average, undergo vulnerability testing.

Only 37% can understand the context of their APIs.

As a result, many organizations are expressing low confidence in their security posture.

TESTIFY HARNESSING FUZZING ALGORITHMS

Unlike legacy security solutions that rely on static, manual testing, Testify proactively probes APIs for vulnerabilities, identifying code weaknesses before they become attack vectors. This automation-first approach eliminates bottlenecks, ensuring security is not just reactive, but predictive.

BUILT FOR DEVELOPERS, LOVED BY ENTERPRISES

Testify seamlessly integrates into DevSecOps pipelines, working silently yet powerfully in the background. Industry may vary, Testify's performance doesn't. Testify adapts to your ecosystem, strengthening your security posture without disrupting operations.

Testify Empowers businesses spanning a vast spectrum of industries spanning

- Banking, Finance & Insurance (BFSI)
- Manufacturing & Automotive
- Government & Public Services
- Healthcare & Pharmaceuticals
- Retail & eCommerce

www.icyberpro.com 011-40586135 info@icyberpro.com

API SECURITY BOTTLENECKS

CURRENT SECURITY CHALLENGES

- Cost-Intensive
- Inadequate Vulnerability Mapping
- Status Code Incompatibility
- Delayed Threat Detection
- Limited Payload Flexibility
- Lack of Performance Insights
- Uncatalogued Endpoints
- Weak Threat Mitigation Strategies
- Non-Compliance with Industry Standards
- API Structures Loopholes
- Unidentified Injection Risks
- Object-Level Access Gaps
- Insecure Mass Data Handling
- Function-Level Access Loopholes
- Client Dependency
- Limited API Integration Flexibility
- Inefficient API Lifecycle Management
- Manual Security Assessment Bottlenecks
- Incomplete SBOM Visibility
- Inconsistent API Classification
- Generic Testing Procedures
- Obsolete API Versions
- Inaccurate API Testing
- Disconnected Security Workflows
- Zero-Day Vulnerability Detection Gaps
- Expertise Crunch

WHY TESTIFY ?

PREVENTING IS PROTECTING

- Cost-Effective Security
- Tailored Test Case Integration
- Fuzzing-Driven Vulnerability Mapping
- Threat Detection at the Source
- Dynamic Payload Capability
- In-depth Performance Analytics
- OWASP Guidelines (2019 & 2023) Compatibility
- Optimized REST API Standard
- Code Injection Vulnerabilities Detection
- Object-Level Access Control Flaws Resolution
- Mass Data Assignment Safeguards
- Function-Level Access Gaps Elimination
- No-Client Environment Compatibility
- API Ingestion via multiple methods
- Manage your API Lifecycle
- Automated Security Assessmen
- Generate API bill of material
- Classify APIs as Custom or Third-Part
- Check for Outdated API Versions
- Targeted API Evaluations for Precise Testing
- Effortless Security Pipeline Sync
- Obsolete API Versions
- Zero-Day Threat Discovery Mechanisms

www.icyberpro.com 011-40586135 info@icyberpro.com