wib. | Whitepaper

Why API Security must be holistic

Introducing Wib Fusion Platform - For advanced API Security

Beware the false sense of API Security

APIs are everywhere and growing within organizations at an incredible rate, generating more and more API security blind spots that few, if any, existing security programs are equipped to handle. No wonder that APIs are the preferred attack vector to achieve any malicious objective.

Eliminating API security issues requires a multi-lens disciplinary approach ranging from the code which introduces the vulnerabilities, to vulnerability management programs to Security Operations Center (SOC) and Instant Response (IR). Failing to address the problem holistically, creates a false sense of security; a reality acknowledged by Gartner in its "Innovation insight for API protection" that calls for a "...composite solution for discovery, API testing, posture management, and real time protection."

Liberating innovation from API risk

This paper details how Wib's API Security Fusion Platform, helps organizations safeguard their assets and any aspects of digital innovation by identifying, addressing, and minimizing API risk.

We examine API Security threats and how they manifest themselves from inception to remediation. It is intended to help CISOs, business leaders and IT professionals in the process of dealing with their API exposure and looking for a solution that integrates into existing workflows within their security programs.

APIs take 'center stage' on the security agenda

API security is a top-of-mind concern for most organizations because APIs are mission-critical, their lifecycle makes them open to various forms of compromise and attackers are having a 'field day' exploiting them.

Organizations rely on APIs and cloud technologies to innovate and meet business objectives quickly; they are central in the facilitation of data movement and communication exchange with partners, customers, internal teams and systems.

The resulting API boom harbors an ever-growing number of blind spots such as unmonitored shadow APIs or unmanaged zombie APIs that the existing security stack is not equipped to handle.

The public availability of APIs combined with their direct access to company resources and assets - minimize the need for attackers to gain a foothold in the target's environment to achieve any objective, from data exfiltration to service disruption, service scalping and many others.

This growing threat is a pressing issue for organizations as APIs grow in sophistication and form a vital component of businesses' operations.

APIs lifecycle can make them vulnerable to different types of compromise presenting opportunities for attackers to take advantage.

Turning APIs from an exposed attack surface to a robust security practice is a challenge that requires a comprehensive approach, that considers all aspect of the API design, testing, deployment, and management.

How attackers exploit API security vulnerabilities

API security threats can originate from several areas on the development pipeline, but it usually starts with the attacker studying the behavior of the API, understanding the logic behind it from a business process perspective, and finding faults or misconfigurations to exploit. A skilled attacker can identify vulnerabilities from seemingly regular use and can move undetected within the application. Some examples of these cases outlined:

- **Attackers exploited several security flaws in a social network API** such as missing authentication to user data and sequential identifiers for content. They successfully scraped 70 TB of user data including media files with geotagging just by sending regular requests enumerating the sequential identifier.
- **An attacker discovered that an API handling currency exchange was vulnerable to mass assignment** due to not applying sufficient input validation, combined with internal logic that automatically rounded up any amount after the second decimal point. The attacker was able to increase their account balance into millions of dollars simply by creating huge numbers of tiny transactions that were all rounded up.
- **An attacker abused the lack of rate limiting in an e-commerce site** to clear an entire inventory as soon as it was restocked, leaving products unavailable for long periods and harming the store's reputation.
- **Attackers gain access through a shadow API to expose personal data of millions of social media users,** in one of the most publicly covered cases in recent years resulting in a $5 billion fine by the Federal Trade Commission (FTC). In this exploit, a political consulting firm, is able to access the personal data of millions of users of a large social media network, through a shadow API created by a company employee. Developed to allow quick, easy, and efficient access to data for developers and employees, this Shadow API ended up a 'culprit' in exposing access to personal data of millions of users without their knowledge or consent.

Wib's advanced API security – for Holistic protection

To eliminate and effectively protect against API threats, Wib has embraced a multi-lens disciplinary approach that achieves end-to-end coverage.

This is significantly preferable to any solution focused only on one aspect of the API lifecycle such as production traffic, which in most cases provides less than inadequate protection completely overpassing potential vulnerabilities that could be developed at coding or identified during testing, leaving organizations completely exposed.

Wib's holistic API Fusion platform helps organizations reduce the risk of these types of attacks by providing a comprehensive solution for discovery, vulnerability validation, posture management, early-stage prevention and real-time protection with frictionless shift left.

It utilizes a comprehensive, multi-lens approach, powered by Wib's proprietary Fusion Engine, to assess the security posture of APIs, minimize risk, and quickly address cybersecurity incidents throughout the entire development process - from code to testing and production – further enabling incident response and vulnerability management via **Wib's Fusion Defense layer.**

Discovery: Wib's API discovery tool uses multiple sources of data from code analysis, traffic inspection, and API testing that in turn fuses them together to help organizations identify and inventory all APIs and their vulnerabilities, making it easier to manage and secure them.

Vulnerability validation: A fully automated API testing process ensures that every vulnerability detected by the Fusion Engine is a genuine threat that needs to be addressed.

Posture management: Using the analyzed data from the Fusion Engine, Wib's posture management tools calculate the risk and business impact using industry standards such as NIST to help organizations assess the security posture of their APIs; and using API testing tools to identify and validate any vulnerabilities.

Early-stage prevention: By integrating to the CI/CD pipeline, Wib's code analysis and API testing tools can detect vulnerabilities in the early stages of development, allowing possible threats to be fixed and prevented long before code is deployed to production.

Real-time protection: Wib's real-time protection tools monitor API traffic and detect any suspicious activity, enabling security teams to apply block rules and helping prevent API attacks.

Frictionless workflow integrations: Wib's Fusion Platform integrates with existing tools and workflows, whether creating tickets, reporting to Security Operations Center or applying protection rules. It gives teams what they need, when they need it – without changing their internal processes and procedures.

Risk management with Wib Fusion Platform

API risk management can be especially challenging with API inventories that grow daily and can be hard to keep track of.

A common practice for countering this challenge is creating and maintaining Open API specifications (OAS) that can then be used by traditional security tools. While this solution works in mapping the API inventory it requires considerable overhead to create and maintain properly and often a gradual drift occurs between the documentation and the actual code.

Another challenge, due to the rate of change in the API inventory, which impacts the ability to identify vulnerabilities within the APIs. Some organizations may use red teams or external pen-testers to hunt for possible vulnerabilities, but these actions are not performed at the same frequency as API deployment, leaving possible new vulnerabilities exposed until the next planned cycle of pen testing.

Wib understands these challenges and takes a fully automated approach for creating and continuously maintaining the API inventory – regardless of whether the organization has an OAS - by analyzing both code and traffic to identify and analyze possible threats. Wib's Fusion Platform does this by connecting directly to the source code. It additionally uses traffic to verify what precisely is out there and whether all APIs are accounted for (thereby uncovering blind spots). Additionally, WIb's API testing and code analysis tools allow for rapid vulnerability detection, testing APIs before, during and after they are deployed.

The platform is designed to integrate into existing workflows for all solution beneficiaries. For instance, vulnerabilities will be introduced to the vulnerability management team, while active validated threats will be sent to the security operations center and instant response teams. Wib's Fusion Platform is designed with frictionless integration in mind, allowing organizations to simply focus on eliminating risks.

Wib Fusion Platform for frictionless integration

Solutions that do not add responsibilities to developers or require additional synchronization processes from the team can significantly accelerate the time it takes to realize value and decrease total cost of ownership. With the ever-growing security stack that organizations are managing, it is vital to choose solutions that integrate seamlessly into existing workflows.

Wib's Fusion Platform is pioneering a new era in API security and is designed to do just that. With a variety of integrations with common key tools, such as code repositories, ticketing systems, and reporting tools, it provides developers, DevOps, and SecOps teams with the necessary functionality without adding friction to their existing workflows. Integrating into the CI/CD pipeline enables DevOps team to infuse security testing at the earliest stage of the API development lifecycle significantly reducing bottlenecks and resource wastage.

This seamless and comprehensive approach allows teams to shift-left and focus on their responsibilities while ensuring that security is integrated into their processes without disruption.

Conclusion

APIs are an integral part of organization's infrastructure, connecting systems and sharing services with partners and customers. However, the rapid growth of APIs has invited the attention of bad actors who in turn exploit faults in the business logic that are in the blind spots of traditional defenses, making it one of the most frequent attack vectors organizations now face.

Wib's Fusion Platform with its advanced API Security capability, addresses this problem by taking a holistic approach that covers the API lifecycle end to end, from discovery through early-stage prevention, to real-time protection. The platform tests and validates vulnerabilities early on, enabling organizations to fortify their posture and APIs before deployment. Additionally, Wib's detection tools allow organizations to respond to real-time logic-based attacks all while keeping existing workflows intact and achieving shift-left for development, SecOps, and DevOps teams by supplying frictionless integrations.

Visit www.wib.com for more