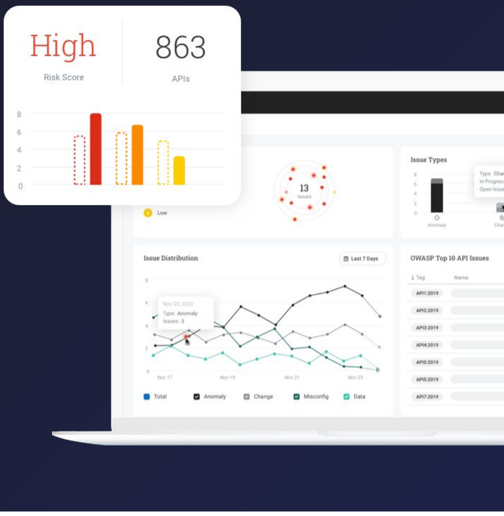
noname

Solution Brief

Addressing The OWASP API Top 10

The Noname API Security Platform helps you protect your APIs against the most critical API security vulnerabilities.



Protect Against The Most Critical API Vulnerabilities

Securing APIs continues to be a never-ending challenge for many organizations. Focusing on the most important security issues first is a great way to maximize your team's efficiency, but how do you know where to begin? The Open Web Application Security Project® (OWASP) API Security Top 10 is great resource. The list ranks the most critical API security risks for and provides a good starting point to help focus your security efforts. The table below details the OWASP API Security Top 10 and how the Noname API Security Platform helps your organization to reduce your API security risks.

	Overview	How Noname helps
API #1: **Broken object-level authorization**	BOLA vulnerable APIs can allow adversaries to access unauthorized data. This can be executed by manipulating a legitimate API request so that the target API returns data that should that the requester should not have authorization to access.	• API posture management analysis helps identify high-risk APIs (internet-facing, handles sensitive data) • Advanced machine learning (ML) and artificial intelligence (AI) build baseline API behaviors so that BOLA attack traffic can be detected and trigger policy-based remediation • Noname active API security testing can simulate BOLA attacks to identity vulnerable APIs in production and dev environments
API #2: **Broken user authentication**	Authentication controls are weak or easily defeated, allowing attackers to make requests to the API as the compromised user.	• API posture management analysis identifies and flags APIs that have inadequate access controls • Runtime protection detects brute force and credential stuffing attacks and triggers policy-based remediation • Active API security testing can simulate authentication attacks to identify vulnerable APIs in production and dev environments
API #3: **Excessive data exposure**	API responses return excessive unneeded data, adding unnecessary burden to resources and potentially exposing sensitive data.	• API posture management analysis flags APIs that handle sensitive data types and exposure to the internet so that they may be prioritized for review • Runtime protection detects excessive requests that in indicators of an attack such as data scraping • Active API security testing can test APIs for excessive data exposure
API #4: **Lack of resources & rate limiting**	Vulnerability to requests that may exhaust system resources causing the API to become unresponsive.	• API posture management analysis flags APIs without API rate-limiting configured in the API gateway • Runtime protection detects anomalous traffic surges and policy-based remediation can be automatically triggered • Active API security testing can test APIs traffic surges in pre-production environments
API #5: **Broken function-level authorization**	Inadequate or poorly configured APIs allow access to additional functions functions such as HTTP methods (e.g. POST, DELETE)	• API posture management analysis flags APIs with privileged API methods and public exposure • Runtime protection detects anomalous API requests such as admin methods or privileged API calls and trigger policy-based remediation • Active API security testing can simulate requests that should not be allowed and flag vulnerable APIs

	Overview	How Noname helps
API #6: **Mass assignment**	APIs that store data objects can be manipulated to store additional data, this could enable an attacker to modify or add privileges to user accounts.	• API posture management analysis helps identify high-risk APIs (internet-facing, handles sensitive data) that may require additional review • Granular runtime protection policies can detect transmission of sensitive data or added data elements (per API) and trigger response mechanisms such as blocking or deauthorization of the client • Active API security testing can test mass assignment susceptibility by fuzzing API endpoints and adding elements to API requests
API #7: **Security misconfiguration**	Security control gaps exist the supporting API delivery services or configurations, that could result in data leakage, theft, fraud, or abuse of the API.	• API posture management analysis combines runtime observations with configuration details to flag misconfigurations such as the handling of sensitive data types without or adequate authentication or gateway management • Runtime protection can detect when a misconfigured API is exploited and trigger response mechanisms • Active API security testing against pre-production environments can flag misconfigurations to be resolved before moving to production environments
API #8: **Injection**	Attackers inject code as part of the request that is then executed by the API endpoint. This enables attackers to run code on the target systems.	• API posture management analysis helps identify high-risk APIs that may require additional review • Runtime protection uses ML and AI to detect injections and trigger policy-based response mechanisms • Active API security testing can simulate injections so they may be addressed early in the dev pipeline
API #9: **Improper assets management**	Gaps in the understanding and documentation of the complete API inventory that results in inadequately protected or deprecated APIs being available and vulnerable.	• API posture management analysis automates the discovery of all APIs so that deprecated, rogue, and zombies APIs can be identified for more efficient asset management • Runtime protection can generate API specification documentation based on observed traffic so it can be compared to the actual specification and deltas can be addressed
API #10: **Insufficient logging & monitoring**	API issues including performance, abuse, attacks, and other anomalous traffic can not be easily determined with existing logging and monitoring tools.	• API posture management analysis helps identify business -critical API assets where logging/monitoring is essential • Runtime protection adds another layer of logging and monitoring along with API-specific policy violations and integration into SIEM

n noname

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022 GOLD API Security category North America

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022 GOLD Fastest Growing Cybersecurity Company North America

TOP 10 BLACK UNICORNS 2021 CYBER DEFENSE MAGAZINE

TOP 10 CYBERSECURITY EXPERTS 2021 CYBER DEFENSE MAGAZINE

About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across three pillars — Posture Management, Runtime Security, and Secure API SDLC. Noname Security is privately held, remote first with headquarters in Silicon Valley, with an office in Tel Aviv and Amsterdam.

Nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371