imperva

Protect APIs from business logic abuse in 5 easy steps

Developers publish APIs at a rapid pace and the margin for error is high. Cyber criminals are targeting design flaws in the business logic functionality of APIs to carry out malicious activity and steal sensitive data.

Here are 5 easy steps to protect your APIs from business logic abuse.

01 BLOCK APPLICATION LAYER ATTACKS WITH WAF

A WAF acts as a deterrent against business logic abuse as it blocks reconnaissance attacks like malicious web traffic and Distributed Denial of Service (DDoS attacks).

48% of API Developers conceive, implement, test, and deliver an API to production within 1 week (Source: Postman - 2022 State of the API Report)

02 PROTECT AGAINST BAD BOTS

The bad bot problem is getting worse with 38% of API attacks in 2022 consisting of bad bots abusing business logic and other automated threats. Bot protection prevents API manipulation by automated attacks.

(Source: Imperva 2023 Bad Bot Report)

86% of developers anticipate their usage of APIs to increase this year. (Source: Nylas - State of Developer Experience 2023 Report)

44% of developers have less than 2 years experience developing APIs (Source: Postman - 2022 State of the API Report)

03 DISCOVER, CLASSIFY AND PROTECT APIS

Business logic rules are unique to each API making them an ideal target for automated attacks. Discovery and classification gives you visibility of your risky APIs and helps protect against business logic abuse.

04 COMBINE API SECURITY AND BOT PROTECTION

Combining Advanced Bot Protection and API Security enables you to identify and protect APIs most at risk from bad bots which attackers use to identify API vulnerabilities like Broken Objective Level Authorization (BOLA).

05 PROTECT EVERYTHING IN ONE CONSOLE

Imperva's comprehensive single-stack application security platform combines Imperva API security and Advanced Bot Protection with WAF to provide the best protection for your applications and APIs against business logic abuse in one Unified Management Console.

OWASP

Imperva Cloud WAF protects against the OWASP Top 10 security threats.

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures

A10:2021-Server-Side Request Forgery