wib

OWASP API9:

Improper Asset Management

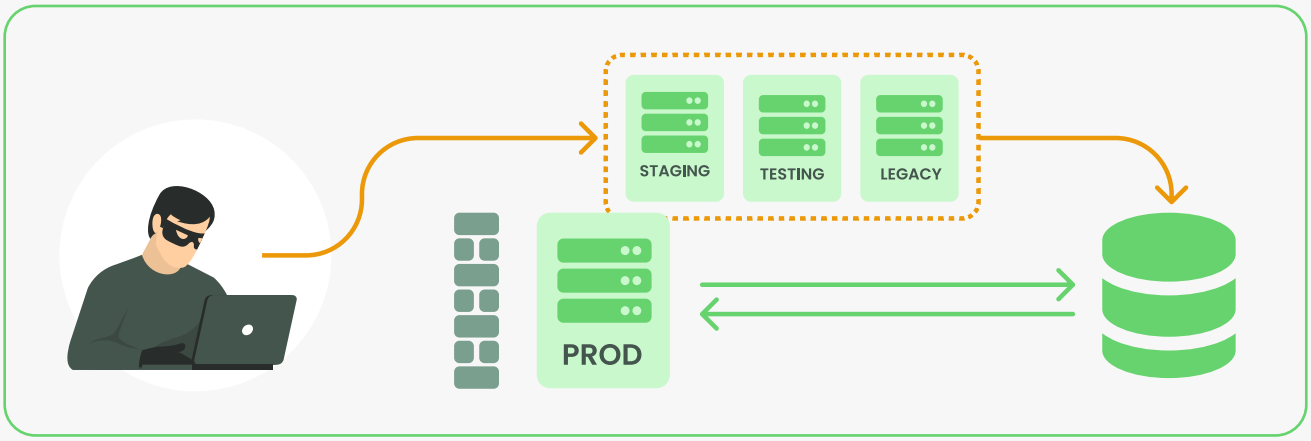
OWASP top 10

Unlike traditional web applications, APIs typically expose more endpoints and thus require structured, up-to-date documentation. Issues such as exposed debug endpoints and deprecated API versions can increase the attack surface. You can mitigate this risk by creating an inventory of deployed API versions and properly configured hosts.

Old API versions are usually unpatched, offering an easy way to compromise systems without fighting state-of-the-art security mechanisms. Understanding possible exposure and risk requires keeping an up-to-date API inventory with proper documentation.

How Hackers Exploit It

Security technologies rarely monitor or protect unknown APIs (also known as shadow APIs) and forgotten APIs (also known as zombie APIs. As a result, these APIs and the infrastructure that supports them are frequently vulnerable to attacks.



For example, imagine that an online business upgraded their search service after redesigning their applications but kept an old API version (api.serchingonline.com/versionnumber1) running, unsecured, and with access to the user database.

An attacker discovered the API address (api.serchingonline.com/versionnumber2) while targeting recently published applications.

By replacing versionnumber2 with versionnumber1 in the URL, the attacker gained access to the previous unprotected API, exposing all of the customers' personally identifiable information (PII).

Why You Should Care

Suppose an attacker is successful in discovering a shadow/forgotten API. In that case, they will have access to these APIs, updated versions, or potentially an entire server. As a result, they can access accounts in the system, retrieve users' personal data, and perform sensitive operations like sending personal messages, executing financial transactions, or blackmailing victims using their personal information by using these APIs or the server.

Traditional Tools Will Not Protect You

Traditional security tools like WAFs and API gateways only know what they are created for, requiring the import of API schema definitions to acquire a picture of the API environment. Therefore, if documentation is missing or erroneous, they have an incorrect understanding of the API environment. Moreover, these tools cannot discover and monitor APIs continually. As threats become more complicated and sophisticated, these tools miss attacks that target the logic of APIs.

How can you prevent it?

Because new APIs are launched and current APIs are updated often, it is difficult to detect and remedy vulnerabilities when documentation is out of date. Due to a lack of API inventory and retirement strategies, systems remain unpatched, resulting in sensitive data leakage.

You must do five things to protect your APIs from improper asset management threats:

1. Maintain an inventory of all APIs
2. Document all aspects of your APIs
3. Separate access to production and non-production data
4. Retire older API versions
5. Restrict access to information that should not be made public

However, an API security solution must also provide continuous discovery to maintain an up-to-date catalog of the API environment and accurate API documentation to prevent such attacks. For example, it must discover all host addresses, API endpoints, HTTP methods, API parameters and data types, and sensitive material.

How Wib Can Help You

Wib is a full-lifecycle API security platform, defending against API security threats. The platform ensures comprehensive protection across the entire API software lifecycle from development to testing to production.

Wib utilizes state-of-the-art proprietary AI and ML to analyze millions of requests in real-time. It provides complete visibility of existing APIs, with actionable insights and comprehensive protection across the entire lifecycle. It learns your APIs inside and out and can provide complete visibility of your existing APIs, analyze their integrity, identify vulnerabilities, and detect attacks in real-time.

If you are building or using APIs in your applications (and you probably are), sign up for a demo to see Wib in action and learn more.