AppSentinels.ai
Application Security Re-invented

Why current DAST/IAST products are inadequate against API vulnerabilities

During our various customer interactions, customers using Dynamic Application Security Testing (DAST) or Interactive Application Security Testing (IAST) often ask how AppSentinels solution is different compared to their existing tool:

The core difference is AppSentinels API Security Platform understands the context of the Application it is protecting while DAST/IAST products unfortunately don't.

Let me explain why I am saying this and why this is important:

DAST products started appearing in the market around a decade+ ago to find vulnerabilities in web applications. They focussed on web attacks understanding that was existing then – OWASP Top-10 attacks. As there is no standard way to describe what a web application does and how to interact with it, DAST products comes packaged with a spider/crawler that scans through various URLs in the web-application. These products will then insert signatures/regex patterns of known attacks mostly OWASP TOP-10 attacks like SQLi, LFI/RFI, RCE and other in the discovered URL's. While such an approach worked for web-applications, it falls flat with API based applications due to multiple reasons.

First, there's no way to discover API endpoints by crawling, thereby severely limiting efficiency of these tools in finding security issues in the application. To avoid this limitation, DAST tools started adding capability to inspect APIs using customer provided OpenAPI/Swagger schema. Relying on this approach for API security testing has serious limitations as majority of the organizations struggle with basic visibility of APIs and their API documentation is lagging or incomplete, rendering schema-based API tests irrelevant and noisy.

Second, and perhaps much bigger challenge that limits usefulness of DAST/IAST for API vulnerabilities is the complex nature of API attacks – a problem that also limits efficacy of other tools like WAF to effectively protect against API attacks.

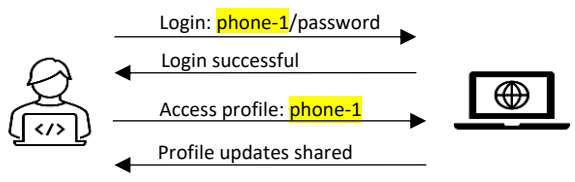
API attacks are business logic exploits. Business logic are unique to every organization and depends on how the organization has designed or implemented their APIs. The code that represents business logic doesn't follow well-defined patterns where signatures or rules can be built. DAST/IAST products have no capability to understand an application behaviour and derive its business logic.

In summary, DAST/IAST tools can at best identify very small number of generic vulnerabilities (mostly OWASP Top-10) but none of the OWASP API Top-10 vulnerabilities or business logic exploits that mars API landscape.

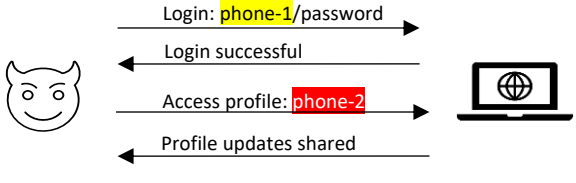
How AppSentinels Intelligent Stateful API-DAST is different?

Before we see how AppSentinels API-DAST is different, let's see what an API business logic exploit looks like with a very simple illustration. Below is a real BOLA attack scenario against a famous social network in 2019:

Normal scenario:



Malicious scenario:

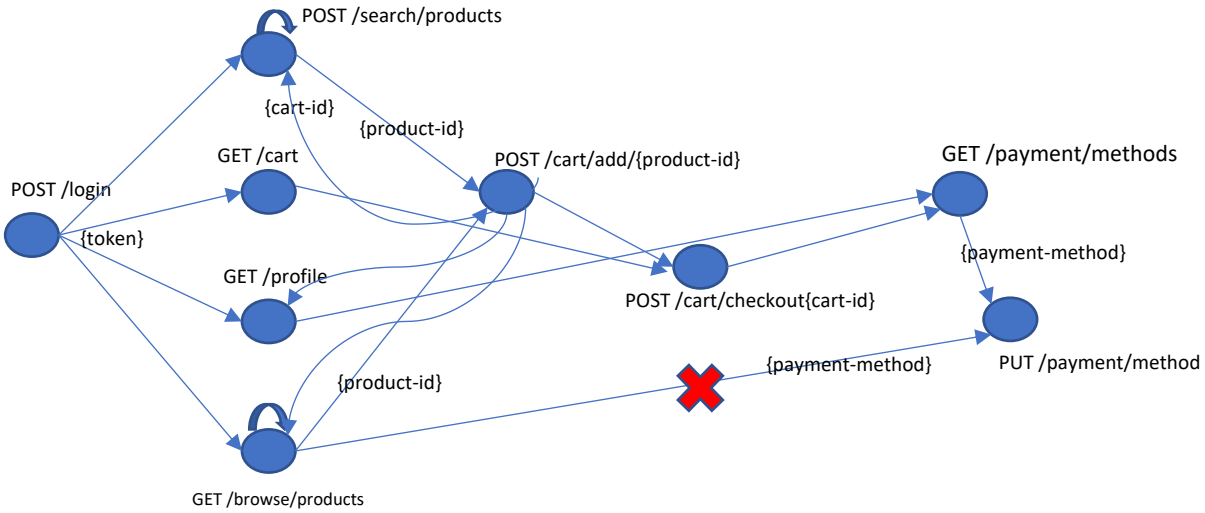


As you see from this example, group of two API's and two objects (highlighted) were involved in the breach. The two APIs were chained/connected. Individually each of the API calls are benign. However, the change of object value while calling the second API in the malicious scenario, results in the attack. If the second API implementation doesn't do sufficient security checks, it will result in unauthorized access, thereby breaching the logic built across the two APIs. Finding and blocking such API attacks require building deep understanding of the application behaviour and user context. At max, DAST/IAST solutions have narrow view of a single API and doesn't have right architecture foundation to build deeper understanding of the application logic. Without the relevant context, these tools can't detect such API attacks.

Right architecture is foundational to do SHIFT LEFT Right!

To catch API business logic breach like the scenario above, security platform has to build deep understanding of application behavior and understand how users are accessing the application. Solutions need context that cannot be learned looking at each transaction in silos. Solutions must analyse and stitch data to understand normal behaviour, identify outliers, and put together the pieces to form a bigger picture. Traditional tools lack big data, AI and ML and don't have ability to gather and stitch these events to come up with complete picture.

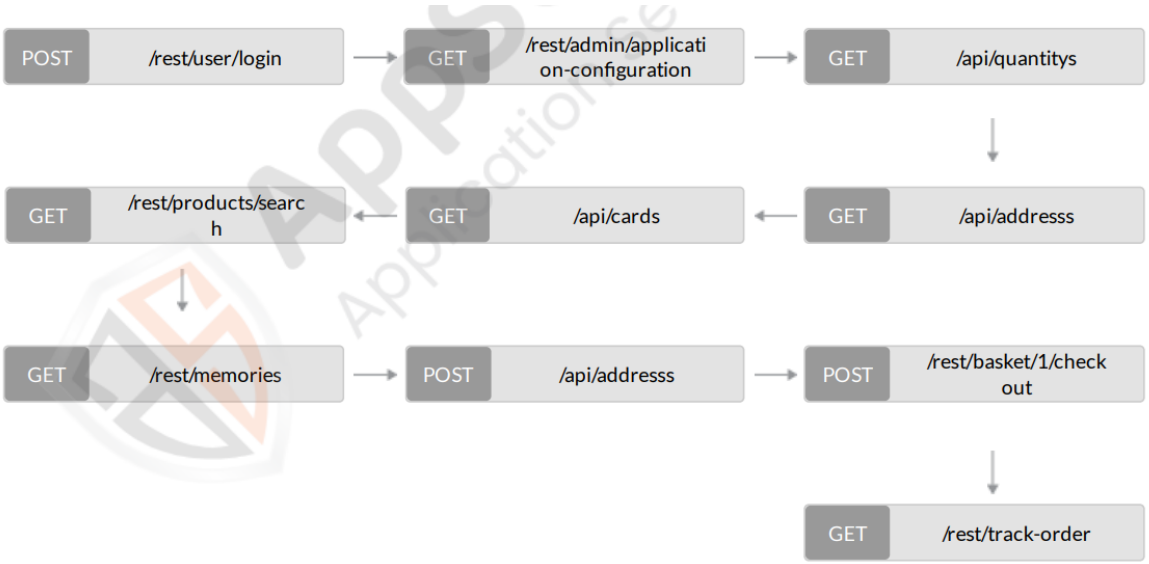
By analyzing complete API workflows, AppSentinels creates baseline of normal behaviour, models complex relationship within the application to discover happy path workflows and can construct exception path workflows that hackers generally go after. With such a deep context, it generates numerous AI/ML backed security tests that can cover the application inside-out including many hard-to-find corner cases. See this with an example below:



The platform can perform extensive happy/exception path coverage including:

- Session aware tests with authorization token, cookies etc
- Object ownership access evaluation with multiple users
- Function access evaluation across various roles
- Pagination controls exploits for excessive data exposure
- Intelligent guess of potential mass assignment inputs
- Authentication bypass, Token reuse & replay, weak JWT etc
- Exploits for potential crashes, double-free, use-after-free etc
- Sensitive data and PII detection in application crashes
- Enhance testing with real-world traffic and simulated attacks

Every security test-case API-DAST generates will simulate a happy or exception path scenario, with complete session consisting of multiple API's called in the right order with the correct payload like shown in the example. It augments your existing team's testing capabilities.



Note on OWASP API Security Top-10 of DAST/IAST Tools

Below table provides coverage of OWASP API Top-10 coverage of AppSentinels vs DAST & IAST tools:

OWASP API Protection	AppSentinels API-DAST	DAST	IAST
OWASP API-1 Broken Object Level Authorization	**Complete**	None	None
OWASP API-2 Broken User Authentication	**Complete**	Partial	Partial
OWASP API-3 Excessive Data Exposure	**Complete**	None	None
OWASP API-4 Lack of resources and rate limiting	**Complete**	Partial	Partial
OWASP API-5 Broken Function Level Authorization	**Complete**	None	None
OWASP API-6 Mass Assignment	**Compete**	None	None
OWASP API-7 Security Mis-configuration	**Complete**	None	None
OWASP API-8 Injection	**Complete**	Complete	Complete
OWASP API-9 Improper Assets Management	**Complete**	None	None
OWASP API-10 Insufficient Logging & Monitoring	**Partial**	None	None

Summary

AppSentinels API-DAST outclasses any other DAST/IAST solution existing in the market by building very deep understanding of the application context and using it to test various happy/exception path workflows in the application. **It augments testing capability of the organizations. It also is a viable replacement for milestone based manual VAPT or costly bug-bounty programs that can't move with the speed of dev-ops.**

Integrating AppSentinels API-DAST can help organization transform their security posture to pro-active security and benefit from the SHIFT-LEFT efforts by selecting the right tool for the job.

About AppSentinels.ai

AppSentinels is next generation API security company that is redefining the way Application Security is done in organizations.

- With it's continuous discovery, AppSentinels helps bring complete visibility of API's along with sensitive data exposure even when applications are evolving.

- With multi-layer defence shield – it protects organizations against all known and unknown attacks in production environment.
- With remediation, it helps developers address issues with pin-pointed accuracy. It also helps Security operations respond faster and better with the context and fewer false-positives.
- It's Intelligent Stateful API-DAST uncovers yet to be exploited API business logic issues and helps transform organization from reactive to pro-active security posture.

Application Security must evolve with the changing Application architectures. We at AppSentinels have built a product that addresses many of the challenges organizations are facing today.

Have any questions or want to try AppSentinels Intelligent Stateful DAST for your application, please reach out to: contact@appsentinels.ai