AppSentinels.ai

It’s all about business logic security!

In May'22, a major Indian payment gateway reported a fraud of 7.3 Crore (approx. 1 million US$). Few months earlier in Feb'22, world's top crypto-exchange – Coinbase had to suspend trading when a breach was reported where a user could sell cryptos without owning them. Similarly in Nov'21, white-hat hacker Alissa Knight reported 55 banking applications of large global banks had exploits that allowed anyone to change debit card PIN numbers as well as move money across accounts WITHOUT account owner authorizations.

These are examples of BUSINESS LOGIC EXPLOITS where hackers were able to bypass application business logic and carried out frauds, resulting in economic and reputation losses for the organizations.

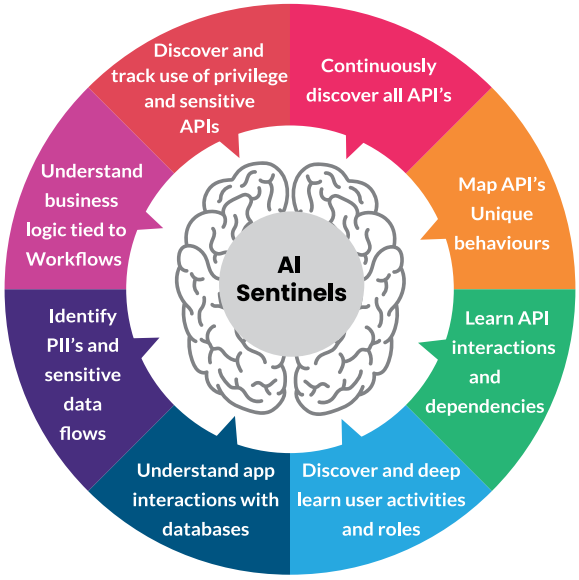
Let's see this with a simple illustration of a Broken Object Level Authorization (BOLA) attack which is part of OWASP API Top-10 list. Below is a real attack scenario against a famous social network in 2019:

A simple change of parameter in the second API (Access Profile API) resulted in massive data-breach. Ironically current generation security solutions like WAFs, NGFWs, API-GWs OR SAST/DAST are blind to Business-Logic attacks!

Protecting "Businesses" against business-logic exploits is not optional

With organizations becoming digital entities, protecting businesses and applications against business logic exploits, frauds, data-breaches are getting more important than ever. AppSentinels has built a platform that addresses all these challenges.

AppSentinels AI full life-cycle API security platform builds deep understanding of application behaviour. It tracks context of the user and identifies outliers using multitude of AI/ML and heuristics models.



Being Proactive is need of hour

Every organization is trying to deliver innovation as fast as possible. The pace of change is not an option but existential for organizations. However, it is exposing flaws in applications that hackers are exploiting. Organization's need a solution that can find security issues during the development pipeline so the issues can be fixed before the code gets deployed to Production. This is what AppSentinels Intelligent Stateful DAST achieves – finding OWASP API Top-10 issues and business logic exploits. It's like a 24×7 pen-tester for the application and helps organization deploy their code with confidence. It's world's first and only automated API security testing tool backed by AppSentinels powerful AI/ML models.

Summary

Gartner mentions by 2022, API will be the biggest attack vectors. The target of these attacks is Application's Business Logic. Current generation products-built decades ago like WAF, NGFW, Zero-Trust, RASP and SAST/DAST etc, cannot fight against the new generation of threats as is evident with the news of API breaches reported on a regular basis. Application Security must evolve with the changing Application architectures. Organization MUST include API security in their posture.

Why API Security?

AppSentinels is world's most comprehensive next generation full-life cycle API security platform that uses AI/ML to stop advance business-logic API attacks. Our deep learning models find attackers early in the attack phase and blocks them, protecting applications from breaches, frauds and data loss.

AppSentinels platform also includes world's first and only Intelligent Stateful DAST that helps find API security flaws including OWASP API Top-10 issues early in dev-cycle and provides actionable insights to developers to fix those issues. The platform discovers all APIs in real-time, provides catalogue of APIs, PII/Sensitive data flow via those APIs and risk score against the APIs.

AppSentinels is started with a vision of addressing major gaps in Application Security. The founding team at AppSentinels comes with more than 100 years of cumulative experience in building Security products in various verticals – cloud, network, endpoints, container etc. The products built by the founding team won many industry awards and were making more than half-a-billion US$ ARR for the organizations.