Depués de más de 20 años en desarrollo, las API ya se utilizan en todas partes. En una encuesta de 2021, el 73% de las empresas informaron que ya publican más de 50 API, y este número crece constantemente.

Las API tienen funciones cruciales que desempeñar en casi todas las industrias de la actualidad, y su importancia aumenta de forma constante a medida que pasan a la vanguardia de las estrategias comerciales. Esto debido a que las API conectan sin problemas aplicaciones y dispositivos dispares, brindando sinergias y eficiencias comerciales nunca antes vistas.

Sin embargo, las API tienen vulnerabilidades como cualquier otro componente del software. Además, si no se prueban de forma rigurosa desde el punto de vista de la seguridad, también pueden introducir una gama completamente nueva de superficies de ataque y exponerlo a riesgos sin precedentes. Si se espera hasta la producción para descubrir vulnerabilidades de API, pueden ocurrir retrasos sustanciales.

Se debe tener en cuenta que las API hacen más que simplemente conectar las aplicaciones, cambian la funcionalidad de formas impredecibles. Muchas de las debilidades únicas que pueden introducir las API son bien conocidas por los hackers, que han desarrollado distintos métodos para atacar sus API con el fin de acceder a los datos y la funcionalidad subyacentes.

Según OWASTOP API Top 10, no es raro que los usuarios legítimos y autenticas exploten la API utilizando llamadas que parecen legítimas pero que en realidad están destinadas a manipular la API. Este tipo de ataques, cuyo objetivo es manipular la lógica empresarial y aprovechar las fallas de diseño, resultan atractivos para los atacantes.

Cada API es única y propietaria. Como tal, sus errores y vulnerabilidades de software son únicos y también *«desconocidos»*. El tipo de errores que conducen a ataques a nivel de la lógica empresarial o del proceso empresarial resultan prácticamente en hacer difícil el proceso de identificar como un defensor.

Prueba de seguridad de API

La seguridad Shift-left ya está ampliamente aceptada en muchas organizaciones, lo que permite realizar pruebas continuas durante todo el desarrollo. Sin embargo, las pruebas de seguridad de API por lo general fracasan o se realizan sin una comprensión suficiente de los riesgos involucrados. Estas son algunas razones de esto:

- Las herramientas de prueba de seguridad de aplicaciones existentes son genéricas y apuntan a las vulnerabilidades de las aplicaciones web tradicionales, y no pueden manejar de forma efectiva las complejidades de la lógica empresarial de una API.
- Debido a que las API no tienen una interfaz de usuario, es común que las empresas prueben la web, la aplicación y los dispositivos móviles por separado, pero no la API en sí.
- Las API de prueba pueden ser intensivas manualmente y no son escalables cuando se tienen cientos de ellas.
- La experiencia y los conocimientos pertinentes pueden ser escasos, ya que las pruebas de API son más complicadas que otros tipos de pruebas.
- Con las API heredadas, es posible que no conozca las API ya implementadas o la documentación.

Por lo tanto, aunque muchas organizaciones ya valoran la seguridad de desplazamiento a la izquierda, las pruebas de seguridad de API por lo general se dejan fuera del panorama general de DevSecOps.

Esto es lamentable, ya que las vulnerabilidades de API requieren más tiempo para subsanarse que las vulnerabilidades de aplicaciones tradicionales. En una encuesta reciente, el 63% de los encuestados informó que se necesita más tiempo para subsanar las vulnerabilidades de API. También es probable que este número aumente debido a la rápida adopción y dependencia de las aplicaciones de las API.

Aunque la mayoría de los líderes en seguridad son conscientes de la importancia de las pruebas de seguridad de API, poco menos de la mitad dice que aún no tienen una solución de

prueba de seguridad de API completamente integrada en su canal de desarrollo.

Como primer paso para un enfoque integral, es importante examinar las actitudes más comunes hacia las pruebas de seguridad de aplicaciones actualmente: pruebas de seguridad estáticas y pruebas de seguridad dinámicas.

Las pruebas de seguridad estáticas adoptan un enfoque de caja blanca, creando pruebas basadas en la funcionalidad conocida de la aplicación mediante la revisión del diseño, la arquitectura o el código, incluidas las muchas rutas complejas que los datos pueden tomar a medida que pasan por la aplicación.

Las pruebas de seguridad dinámicas adoptan un enfoque de caja negra, creando pruebas basadas en el rendimiento esperado de la aplicación dado un conjunto particular de entradas, sin tener en cuenta el procesamiento interno o el conocimiento del código subyacente.

Cuando se trata de API, los desarrolladores y los equipos de seguridad frecuentemente discuten sobre cuál de los dos métodos es el más apropiado, con el principal razonamiento a favor de cada uno:

- Las pruebas estáticas son el único método que tiene sentido: debido a que no hay una interfaz de usuario para las API, debe saber qué sucede dentro de la lógica empresarial.
- Las pruebas dinámicas son todo lo que se necesita, ya que las pruebas unitarias utilizan modelos estáticos y ya se completaron en una etapa anterior del proceso.

Las pruebas de seguridad API de *«caja gris»* pueden ofrecer una alternativa interesante. Debido a que no existe una interfaz de usuario, tener conocimiento del funcionamiento interno de la aplicación puede ayudar a crear pruebas funcionales de forma eficiente que se centren en la lógica empresarial.

Además de su creciente popularidad, las API también crean una mayor vulnerabilidad para las aplicaciones web. Un gran número de organizaciones ni siquiera saben cuál es el alcance

de sus API y vulnerabilidades. Los hackers pueden probar fácilmente las debilidades conocidas y desconocidas por medio de las API disponibles.

Una combinación de procesamiento de lenguaje natural e inteligencia artificial (AI) ofrece una opción viable de *«caja gris»* que automatiza, escala y simplifica el complejo proceso de pruebas de seguridad API.