LISTA DE COMPROBACIÓN DE AKAMAI

10 principales vulnerabilidades de seguridad de las API según OWASP

Las API se han convertido en el estándar para crear y conectar aplicaciones modernas, especialmente con el paso, cada vez mayor, a arquitecturas basadas en microservicios. Por ello, es importante proteger su organización de los riesgos de seguridad de API más comunes identificados por el Proyecto Mundial Abierto de Seguridad de Aplicaciones (OWASP). Consulte la lista actualizada de 2023 para obtener información que le ayude a proteger sus API.

Cobertura de Akamai de las 10 principales vulnerabilidades de las API según OWASP

- ☑ **API1:2023 — Autorización a nivel de objeto comprometida (Broken Object Level Authorization, BOLA):** las vulnerabilidades de BOLA están presentes cuando la autorización de un cliente no se valida de forma adecuada para acceder a los ID de objeto.
- ☑ **API2:2023 — Autenticación comprometida (Broken Authentication, BA):** BA hace referencia a un amplio número de vulnerabilidades en el proceso de autenticación, lo que expone el sistema a atacantes que pueden explotar estos puntos débiles para quebrantar la protección de los objetos de API.
- ☑ **API3:2023 — Autorización a nivel de propiedad de objeto comprometida (Broken Object Property Level Authorization, BOPLA):** BOPLA es un defecto de seguridad en el que un terminal de API expone innecesariamente más propiedades de datos de las necesarias para su funcionamiento, sin tener en cuenta el principio de privilegio mínimo.
- ☑ **API4:2023 — Uso de recursos sin restricciones:** se trata de un tipo de vulnerabilidad, a veces denominada "agotamiento de recursos de API", en el que las API no limitan el número de solicitudes ni el volumen de datos que sirven en un tiempo determinado.
- ☑ **API5:2023 — Autorización a nivel de función comprometida (Broken Function Level Authorization, BFLA):** una BFLA puede producirse cuando los modelos de control de acceso para los terminales de API no se implementan correctamente.
- ☑ **API6:2023 — Acceso sin restricciones a flujos empresariales confidenciales:** este riesgo surge cuando una API expone operaciones críticas, como la lógica empresarial, sin un control de acceso suficiente.
- ☑ **API7:2023 — Falsificación de solicitudes del lado del servidor (Server Side Request Forgery, SSRF):** este riesgo permite a un atacante inducir a la aplicación del servidor a que envíe solicitudes HTTPS a un dominio arbitrario elegido por el propio atacante.
- ☑ **API8:2023 — Configuración de seguridad incorrecta:** se refiere a una configuración inadecuada de los controles de seguridad, que puede dejar un sistema vulnerable ante los ataques.
- ☑ **API9:2023 — Gestión inadecuada del inventario:** supone un reto para todas las organizaciones que gestionan API. Las soluciones de seguridad de API pueden proteger las API conocidas, pero las desconocidas (incluidas las API obsoletas, heredadas o desfasadas) tal vez queden sin corregir y ser vulnerables a ataques.
- ☑ **API10:2023 — Uso inseguro de API:** hace referencia a los riesgos asociados al uso de API de terceros sin aplicar las medidas de seguridad adecuadas.

¿Desea obtener más información sobre la diferencia entre las listas del 2019 y del 2023 de los 10 principales riesgos de seguridad de API según OWASP? Consulte esta entrada del blog.

Trabaje con nosotros

Las organizaciones y sus proveedores de seguridad deben colaborar estrechamente y alinear personas, procesos y tecnologías para establecer una sólida protección contra los riesgos de seguridad descritos en los 10 principales riesgos de seguridad de las API según OWASP.

Acerca de Akamai

Akamai ofrece soluciones de seguridad líderes del sector, expertos de elevada experiencia y Akamai Connected Cloud, que obtiene información de millones de ataques a aplicaciones web, miles de millones de solicitudes de bots y billones de solicitudes de API cada día. Las soluciones de seguridad para aplicaciones web y API de Akamai le ayudarán a proteger su organización frente a los ataques distribuidos de denegación de servicio (DDoS) y frente a los ataques contra aplicaciones web y API más avanzados.

 | Publicado en 08/23