Akamai

WHITE PAPER

Estrategia contra los 10 principales riesgos de seguridad de las API según OWASP

Cómo le ayuda Akamai a mitigar las vulnerabilidades y amenazas comunes de las API

10 principales riesgos de seguridad de las API según OWASP		¿Puede ayudarle Akamai?
API1:2023	Autorización a nivel de objeto comprometida	☑
API2:2023	Autenticación comprometida	☑
API3:2023	Autorización a nivel de propiedad de objeto comprometida	☑
API4:2023	Uso de recursos sin restricciones	☑
API5:2023	Autorización a nivel de función comprometida	☑
API6:2023	Acceso sin restricciones a flujos empresariales confidenciales	☑
API7:2023	Falsificación de solicitudes del lado del servidor	☑
API8:2023	Configuración de seguridad incorrecta	☑
API9:2023	Gestión del inventario inadecuada	☑
API10:2023	Uso inseguro de API	☑

Las API tienen una importancia central en los productos digitales, servicios y entornos de nube de las empresas. Asimismo, se han convertido en el estándar para crear y conectar aplicaciones, pues cada vez son más las organizaciones que utilizan arquitecturas basadas en microservicios para desarrollar sus aplicaciones. Sin embargo, su acceso constante a los datos y los sistemas críticos las convierte no solo en un factor de ingresos, sino también en un riesgo operativo.

Las API expuestas o mal configuradas son muy comunes, fáciles de vulnerar, y a menudo no están protegidas. Y la vulneración de una sola API puede provocar el robo de millones de registros.

Dado que el 78 % de las organizaciones afirma haber sufrido incidentes de seguridad de API en un año, está claro que protegerlas debería ser una prioridad. La superficie de ataque de las API se ha convertido rápidamente en uno de los objetivos predilectos de los atacantes, tan rápido que muchas empresas no han tenido tiempo de comprender este fenómeno y sus particularidades:

Riesgos de las API

Métodos de ataque a las API

Funciones y controles de seguridad de API

¿Qué incluye la superficie de ataque de API? Resumiendo, es mucho más amplia de lo que muchas organizaciones creen. Nuestra concepción tradicional de las API (por ejemplo, las API para comunicación de máquina a máquina o las API de terceros) puede y debe ampliarse para incluir los servicios de aplicaciones web y móviles dentro de la arquitectura basada en microservicios. En otras palabras, una solicitud web dentro de la arquitectura es una API que funciona como una llamada dentro de una serie de llamadas a varios microservicios.

78 %

Así de alto es el porcentaje de organizaciones que afirman haber sufrido incidentes de seguridad relacionados con las API en el último año. Evidentemente, la protección de las API debería ser una prioridad.

El 5 de junio de 2023, el prestigioso Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP) publicó la primera actualización importante a su lista inicial de los 10 principales riesgos de seguridad de las API, publicada en 2019. La lista actualizada analiza cómo cada una de estas llamadas a API puede abrir posibles brechas de seguridad y producir riesgos de privacidad, entre los que se incluyen:

Validación de datos deficiente

Errores de configuración

Fallos de implementación

Brechas de integración entre los componentes de seguridad

Siga leyendo para conocer los riesgos clave identificados por OWASP y descubrir cómo las soluciones de seguridad de API de Akamai pueden ayudarle a mitigarlos.

El problema es que incluso las organizaciones que afirman tener inventarios completos de API son altamente vulnerables:

Solo **4 de cada 10** saben cuáles de sus API devuelven datos confidenciales cuando reciben una llamada.

API1:2023 — Autorización a nivel de objeto comprometida

Las vulnerabilidades de autorización a nivel de objeto comprometida (Broken Object Level Authorization, BOLA) están presentes cuando la autorización de un cliente no se valida de forma adecuada para acceder a los ID de objeto. Esta vulnerabilidad puede ofrecer a los atacantes la posibilidad de acceder a los recursos directamente, omitiendo el flujo de trabajo de la aplicación previsto y obteniendo acceso no autorizado a datos confidenciales. Las organizaciones pueden reducir este riesgo evitando fiarse en exclusiva de los ID de objeto que los clientes envían en sus solicitudes. En lugar de esto, las organizaciones pueden asignar ID aleatorios no adivinables a los objetos para garantizar una validación adecuada de cada uno de ellos. Cuando sea necesario, enmascarar el ID real de los objetos puede proporcionar una capa adicional de seguridad.

Cómo puede ayudar Akamai

Los sistemas de vigilancia siempre alerta de Akamai realizan un seguimiento de las amenazas y generan alertas en caso de intento de ataques de BOLA, lo que garantiza una atención y acción inmediatas.

Akamai mitiga este riesgo:

- Identificando los intentos de ataques de BOLA.
- Clasificando los terminales de API susceptibles de sufrir ataques de BOLA en función de la información recibida (por ejemplo, parámetros enumerables), así como de las relaciones entre los objetos y las propiedades de API.
- Generando alertas sobre los ataques de BOLA perpetrados, tanto si han logrado su objetivo como si no.

API2:2023 — Autenticación comprometida

La autenticación comprometida hace referencia a un amplio número de vulnerabilidades en el proceso de autenticación, que exponen el sistema a atacantes que pueden explotar estos puntos débiles para quebrantar la protección de los objetos de API. Normalmente, los atacantes que aprovechan las vulnerabilidades de autenticación comprometida manipulan las brechas del sistema, como las contraseñas poco seguras o la reproducción de sesiones. Para protegerse frente a vulnerabilidades de autenticación comprometida, las organizaciones pueden aplicar mecanismos de autenticación más sólidos, como políticas de contraseñas seguras, rotación de claves, firmas de token fiables y claves de cifrado. La aplicación de estas estrictas políticas en toda la organización puede reducir significativamente el riesgo.

Cómo puede ayudar Akamai

Akamai refuerza la seguridad de las API mediante la identificación y corrección de los puntos débiles de autenticación, la neutralización de ataques automatizados y las alertas proactivas sobre intentos de ataques.

Akamai mitiga este riesgo:

- Identificando los terminales de API que no necesitan autenticación o que no se ajustan a las prácticas recomendadas, como firmas de token o claves de cifrado poco seguras y la aceptación de tokens de autenticación caducados.
- Protegiendo contra ataques automatizados de diccionario o de Credential Stuffing gracias a sus funciones de gestión de bots.
- Gestionando la autorización de JSON Web Tokens aplicando firmas de token seguras con API Gateway.
- Generando alertas en caso de intentos de ataques de autenticación de usuario comprometida.

API3:2023 — Autorización a nivel de propiedad de objeto comprometida

La autorización a nivel de propiedad de objeto comprometida (Broken Object Property Level Authorization, BOPLA) es un defecto de seguridad que permite a un terminal de API exponer innecesariamente más propiedades de datos de las necesarias para su funcionamiento, sin tener en cuenta el principio de privilegio mínimo.

Este defecto puede proporcionar a los atacantes, accidentalmente, un exceso de datos que pueden servir para detectar otras posibles vulnerabilidades o para extraer datos confidenciales. Aquí se incluyen casos en los que propiedades asociadas exclusivamente con el acceso de nivel de administrador pueden ser manipuladas por usuarios no autorizados, lo que pone aún más en peligro la integridad del sistema. Para garantizar la seguridad y evitar que los atacantes obtengan o manipulen la información excedente, es fundamental proporcionar niveles de acceso y exposición de datos adecuados, lo que impide que los posibles atacantes aprovechen estos descuidos.

Cómo puede ayudar Akamai

Gracias a las completas tácticas de Akamai, las empresas pueden mitigar los riesgos de BOPLA mediante la identificación y catalogación de los terminales de API y sus propiedades asociadas.

Akamai mitiga este riesgo:

- Identificando y etiquetando todos los terminales y las propiedades de API que exponen, como la información de identificación personal (PII).
- Identificando terminales, objetos y propiedades de API ocultos o no documentados, así como propiedades anómalas.
- Aplicando políticas de seguridad en parámetros y propiedades aceptables y definidos para garantizar el saneamiento de los datos.
- Aplicando políticas de seguridad basadas en la especificación completa de OpenAPI/Swagger y permitiendo que solo los terminales y métodos de API con la configuración correcta accedan a los objetos y a las propiedades correspondientes.
- Generando alertas sobre intentos de ataques de BOPLA.

API4:2023 — Uso de recursos sin restricciones

El uso de recursos sin restricciones (a veces denominado agotamiento de recursos de API) es un tipo de vulnerabilidad en el que las API no limitan el número de solicitudes o el volumen de datos que atienden en un periodo determinado. Este descuido puede abrir la puerta a ataques de denegación de servicio (DoS), que pueden dejar el sistema no disponible para los usuarios legítimos. Estos ataques pueden tener importantes implicaciones empresariales, y traducirse en interrupciones de la disponibilidad del servicio, descontento de los clientes y posibles pérdidas de ingresos, en función de la duración y el alcance de la interrupción. Es fundamental contar con medidas en vigor que limiten la tasa de solicitudes de API y el tamaño de las devoluciones de datos para evitar la pérdida de servicio.

Cómo puede ayudar Akamai

Akamai protege sus API frente a las amenazas de uso de recursos sin restricciones:

- Identificando los terminales vulnerables y proporcionando alertas en tiempo real sobre los intentos de ataques volumétricos.
- Detectando los excesos de errores, intentos de inicio de sesión o comportamientos atípicos que indican riesgos.

Akamai mitiga este riesgo:

- Identificando los terminales de API que no cuentan con limitaciones de velocidad o que están sufriendo ataques a través de grandes diccionarios volumétricos o Credential Stuffing.
- Iniciando flujos de trabajo para ralentizar o bloquear los ataques volumétricos.
- Generando alertas sobre intentos de ataques volumétricos.

API5:2023 — Autorización a nivel de función comprometida

La autorización a nivel de función comprometida (Broken Function Level Authorization, BFLA) puede producirse cuando los modelos de control de acceso para los terminales de API no se implementan correctamente. Los métodos de control de acceso incorrectos u obsoletos puede que no restrinjan adecuadamente el acceso no autorizado, lo que permite a los atacantes acceder a información confidencial o al sistema en su conjunto. Para mitigar este riesgo, las empresas pueden adoptar el principio del privilegio mínimo, que garantiza que, a todas las funciones, especialmente a las funciones administrativas, solo puedan acceder los usuarios que tengan los permisos adecuados.

Cómo puede ayudar Akamai

Mediante el seguimiento de los plazos de comportamiento, la aplicación de políticas de seguridad a funciones confidenciales, la gestión de la rotación y revocación de claves, y la alerta inmediata de cualquier intento sospechoso, Akamai puede ayudar a fortalecer la estrategia de prevención y respuesta de las organizaciones frente a la vulnerabilidad BFLA.

Akamai mitiga este riesgo:

- Identificando los plazos de comportamiento en el acceso a los terminales de API mediante la captura de datos de usuarios, claves de API, tokens de acceso, ID de sesión, etc.
- Aplicando la rotación de claves o la revocación de claves expuestas a través de API Gateway.
- Generando alertas sobre intentos sospechosos de acceso a funciones administrativas.

API6:2023 — Acceso sin restricciones a flujos empresariales confidenciales

Este problema de acceso surge cuando una API expone operaciones críticas, como la lógica empresarial, sin un control suficiente. Esto puede generar un acceso y explotación no autorizados, lo que puede provocar daños importantes a una empresa. Llevar a cabo un ataque suele implicar conocer el modelo de negocio respaldado por la API, identificar flujos empresariales confidenciales y aprovechar las brechas de estos flujos. Esto puede tener consecuencias, como impedir que los usuarios legítimos compren un producto.

Cómo puede ayudar Akamai

Proteja su empresa con las completas soluciones de protección de API de Akamai, que ofrecen identificación de los terminales confidenciales, alertas de ataques en tiempo real y asesoramiento de expertos para salvaguardar sus operaciones y datos clave.

Akamai mitiga este riesgo:

- Identificando los terminales de API confidenciales, como los flujos de pago o los terminales con PII.
- Generando alertas sobre una serie de posibles explotaciones, que van desde la exfiltración o la manipulación de datos hasta los intentos sospechosos en estos terminales de API confidenciales.

API7:2023 — Falsificación de solicitudes del lado del servidor

La falsificación de solicitudes del lado del servidor (Server Side Request Forgery, SSRF) permite a un atacante inducir a la aplicación del servidor a que envíe solicitudes HTTPS a un dominio arbitrario elegido por el propio atacante. En un ataque de SSRF típico, el atacante engaña al servidor para que realice una solicitud a los recursos internos, evitando así los firewalls y obteniendo acceso a los servicios internos, lo que puede provocar la exposición de datos o la ejecución remota de código. Para mitigar este riesgo, resulta fundamental validar, filtrar o limpiar los datos introducidos por el usuario, así como limitar las conexiones de salida que el servidor puede realizar, garantizando que solo se comunique con los servicios esenciales.

Cómo puede ayudar Akamai

Refuerce su estrategia de seguridad con Akamai mediante la detección de anomalías en conexiones API fiables, una gestión eficaz de las claves y notificaciones inmediatas sobre intentos de ataques de SSRF.

Akamai mitiga este riesgo:

- Mejorando la defensa mediante políticas de protección de API y aplicaciones web para ataques de SSRF.
- Aplicando la rotación de claves o la revocación de claves expuestas a través de API Gateway.

API8:2023 — Configuración de seguridad incorrecta

Este problema hace referencia a una configuración inadecuada de los controles de seguridad, que puede dejar un sistema vulnerable ante los ataques. Esto podría incluir configuraciones predeterminadas inseguras, unas configuraciones incompletas o ad hoc, el almacenamiento en nube abierta, encabezados HTTP(S) mal configurados y mensajes de error descriptivos que contienen información confidencial. Para mitigar los riesgos, resulta fundamental que las organizaciones se aseguren de haber configurado correctamente sus controles de seguridad en todos los aspectos de sus aplicaciones y API. Esto implica llevar a cabo actualizaciones periódicas, pruebas exhaustivas y una supervisión continua para identificar y corregir cualquier error de configuración de forma inmediata.

Cómo puede ayudar Akamai

Gane perspectiva mientras Akamai le ayuda a identificar terminales de API "en la sombra", "no autorizados" o "zombis"; asimismo, lo tendrá más fácil para respetar las prácticas de seguridad recomendadas, afianzar su implementación de HTTPS y recibir alertas instantáneas sobre las configuraciones de seguridad incorrectas.

Akamai mitiga este riesgo:

- Identificando terminales de API "en la sombra" que podrían dejar expuestos entornos de bajo nivel (por ejemplo, entornos de prueba y staging).
- Identificando y comparando los terminales, los objetos y las propiedades de API con las prácticas recomendadas y los estándares de configuración de seguridad.
- Aplicando políticas de seguridad mediante las prácticas de seguridad de API recomendadas, como solicitudes y respuestas HTTPS con el formato correcto, la configuración o eliminación de encabezados HTTP correctos, y un control total del intercambio de recursos de origen cruzado (CORS) y los encabezados de control de caché.
- Aplicando una implementación HTTPS adecuada a través de SSL/TLS, incluidos conjuntos de cifrado correctos y seguros.
- Generando alertas de configuración incorrecta o de incumplimiento de las prácticas y estándares recomendados para la seguridad de API.

API9:2023 — Gestión inadecuada del inventario

Gestionar de manera adecuada el inventario es un reto para cualquier empresa que gestione API. Las soluciones de seguridad de API son capaces de proteger las API conocidas, pero las desconocidas (incluidas las API "en la sombra") pueden quedar sin corregir y ser vulnerables a los ataques. Esto puede dar lugar a componentes desfasados, páginas o API no utilizadas y una divulgación innecesaria de información confidencial. Gestionar los servicios sin llevar a cabo un mantenimiento adecuado puede hacer que los sistemas queden expuestos a las amenazas, y los atacantes pueden obtener acceso a datos confidenciales o incluso al servidor a través de API desconocidas que estén conectadas a la misma base de datos. Los controles de acceso y las auditorías periódicas son esenciales para evitar que los componentes de los servicios de una organización estén cambiando todo el tiempo.

Cómo puede ayudar Akamai

Akamai supervisa constantemente el tráfico de API para detectar los terminales de API ocultos y las API en riesgo, proporcionando a las organizaciones un almacenamiento seguro de los datos, un análisis avanzado de las amenazas y alertas inmediatas sobre posibles ataques.

Akamai mitiga este riesgo:

- Supervisando de forma continua el tráfico de API expuesto de sus entornos, incluidos los terminales de API norte-sur que se comunican con API de acceso público y los terminales de API este-oeste internos.
- Identificando terminales de API "en la sombra" que podrían dejar expuestos entornos de bajo nivel (por ejemplo, entornos de prueba y staging) o versiones de API no documentadas o desfasadas.
- Creando un inventario de API actualizado basado en la puntuación de riesgo y la clasificación de datos.
- Generando alertas sobre una serie de posibles explotaciones, que van desde la exfiltración o la manipulación de datos hasta los intentos sospechosos en estos terminales de API confidenciales.

API10:2023 — Uso inseguro de API

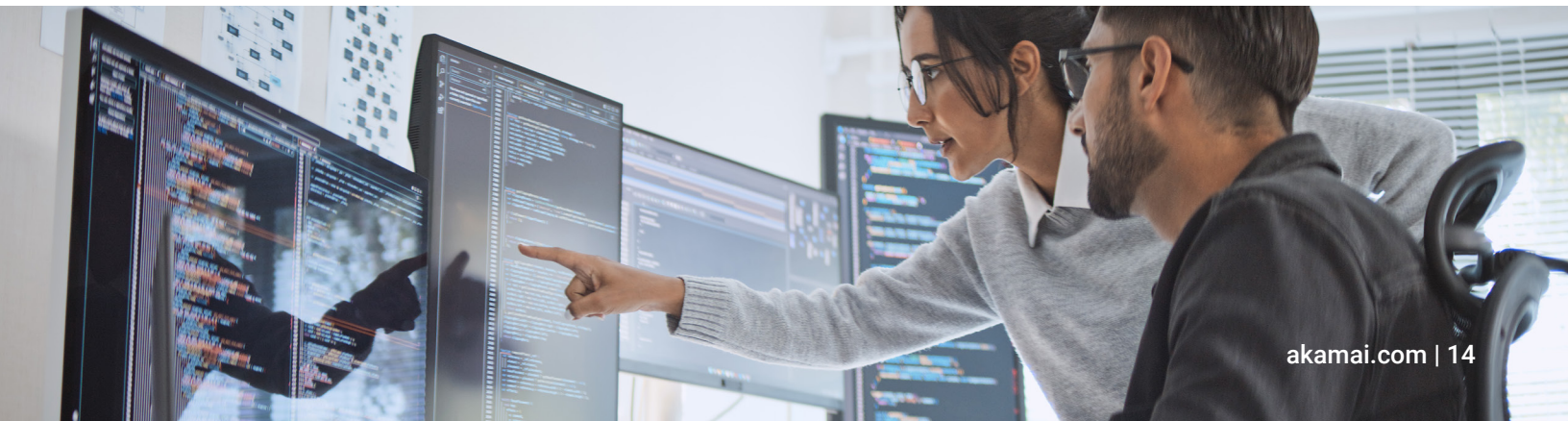
El uso inseguro hace referencia a los riesgos asociados al uso de API de terceros sin aplicar las medidas de seguridad adecuadas. Las organizaciones dependen cada vez más de las API de terceros para ampliar los servicios y las funcionalidades, por lo que estas API suelen ser de confianza de forma predeterminada. Esto puede dar lugar a importantes vulnerabilidades de seguridad. Si no se implementan los límites adecuados de consumo de recursos, saneamiento, validación de datos y cifrado, las empresas pueden quedar expuestas a importantes vulnerabilidades. Para mitigar estos riesgos, las organizaciones pueden implementar el cifrado de todos los datos transmitidos por la red, validar y sanear todos los datos introducidos y establecer límites razonables en el consumo de recursos.

Cómo puede ayudar Akamai

Proteja en todo momento sus sistemas mediante la supervisión y validación de sus servicios para garantizar la seguridad con los servicios de supervisión, alerta y consultoría de Akamai.

Akamai mitiga este riesgo:

- Supervisando de forma continua todo el tráfico de API expuesto de sus entornos, incluidas las API este-oeste y de salida que facilitan las integraciones empresa a empresa (B2B) o de terceros.
- Generando alertas sobre una serie de posibles explotaciones, que van desde la exfiltración o la manipulación de datos hasta los intentos sospechosos en estos terminales de API confidenciales.
- Aplicando políticas de protección de API y aplicaciones web para frustrar toda una serie de ataques de API estructurados en grupos.



Riesgos de seguridad adicionales de OWASP

El informe "10 principales riesgos de seguridad de las API según OWASP de 2023" fue la primera actualización importante realizada por la organización sin ánimo de lucro en su lista desde 2019. Recomendamos revisar la lista original, que aborda otros riesgos de seguridad, como los ataques de inyección, que aún son relevantes en el panorama actual.

Akamai puede ayudar a afrontar este riesgo de seguridad:

- Identificando terminales de API vulnerables a ataques de inyección mediante la comparación de firmas y la detección de anomalías.
- Aplicando políticas de seguridad a través de la inspección JSON y XML de solicitudes de API y el análisis de una serie de ataques de inyección, como SQLi, XSS, CMDi, RFI y LFI.
- Generando alertas sobre ataques de inyección.

OWASP también ha publicado otras listas con riesgos de seguridad relevantes, como los 10 principales riesgos de seguridad de aplicaciones web según OWASP. La cartera de productos de seguridad de Akamai también ayuda a mitigar estos riesgos de seguridad.

Estamos aquí para ayudarle

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.

Akamai ofrece soluciones de seguridad líderes del sector, expertos de elevada experiencia y una plataforma que obtiene información de millones de ataques a aplicaciones web y API, miles de millones de solicitudes de bots y hasta 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 DDoS, a las aplicaciones web y de API más avanzados. Además, Managed Security Service de Akamai ofrece funciones de supervisión permanente, gestión de la seguridad y mitigación de amenazas.

Para obtener más información sobre la cartera de productos de seguridad de Akamai, eche un vistazo a nuestro sitio web. Si desea tratar con más detalle cómo podemos colaborar para crear la mejor protección para su negocio, póngase en contacto con su representante de ventas de Akamai hoy mismo.

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Gracias a la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn. Publicado en septiembre de 2024.