WHITE PAPER

Cómo mejorar con Akamai las prácticas de seguridad para mitigar los 10 principales riesgos

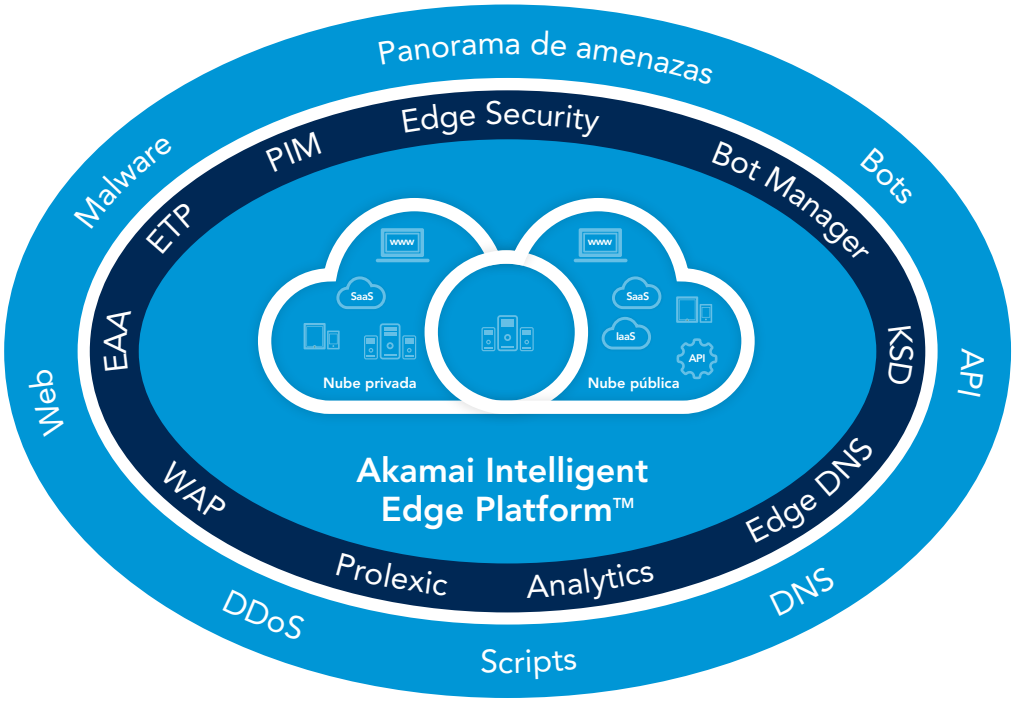
Akamai

Introducción

Las 10 principales vulnerabilidades según OWASP engloban los tipos de vulnerabilidades más frecuentes que se observan en las aplicaciones web. Para evitar la percepción errónea que suelen perpetuar los proveedores de seguridad, no constituyen una lista de comprobación de los vectores de ataque que pueden bloquearse simplemente a través de un firewall de aplicaciones web (WAF). En cambio, su objetivo es concienciar sobre las vulnerabilidades de seguridad más habituales que deben tener en cuenta los desarrolladores de aplicaciones, mejorar dicha concienciación en una serie de prácticas de desarrollo y ayudar a inculcar una cultura de desarrollo seguro.

Para abordar las 10 principales vulnerabilidades según OWASP, es necesario que comprenda el papel que desempeñan tanto los proveedores de seguridad como su propia organización a la hora de proteger las aplicaciones web. Algunas áreas de riesgo solo podrán abordarlas los propios desarrolladores de aplicaciones. Aunque muchos proveedores de seguridad puedan ser de ayuda en determinadas áreas, no suelen ofrecer una total cobertura o la mejor cobertura posible contra una vulnerabilidad. Las mejores soluciones incluyen una combinación de personas, procesos y tecnologías para mitigar los riesgos asociados con las 10 principales vulnerabilidades.

Para sacar el máximo partido de la lista de las 10 principales vulnerabilidades según OWASP, es necesario comprender dónde, cómo y cuánto pueden ayudar los proveedores de seguridad a ampliar las mejoras de sus propias prácticas de desarrollo. A continuación se describe el papel que puede desempeñar Akamai para ayudarle en su tarea con nuestras soluciones de seguridad en el borde de Internet[1], servicios gestionados[2] y plataforma segura en el borde de Internet[3].



A1: Inyección

Impacto: grave	**Prevalencia:** común	**Explotabilidad:** fácil

Los defectos de inyección, como la inyección SQL, NoSQL, OS y LDAP, se producen cuando se envían datos que no son de confianza a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute comandos no intencionados o acceder a datos sin la debida autorización.

Cómo puede ayudar Akamai

Las organizaciones pueden utilizar una solución de seguridad de WAF para proteger las aplicaciones web y las API contra defectos de inyección. Sin embargo, deben siempre reparar las aplicaciones web para abordar cualquier vulnerabilidad detectada en función de su ciclo de vida de desarrollo.

- El WAF[4] de Akamai proporciona una amplia protección contra ataques de inyección mediante las reglas preconfiguradas existentes.
- Los parches virtuales con reglas personalizadas pueden ayudar a abordar con rapidez las vulnerabilidades de inyección emergentes o las nuevas vulnerabilidades expuestas a partir de cambios en las aplicaciones, hasta que la aplicación se pueda reparar. Los parches virtuales también pueden automatizarse e integrarse en los procesos DevSecOps, que aprovechan las funciones de API OPEN de Akamai.
- Client Reputation[5] proporciona una puntuación de riesgo para clientes maliciosos de actividad elevada en la categoría de atacantes web, con el fin de ayudar a identificar y bloquear los ataques de inyección.
- Los ataques de inyección también pueden analizarse en más profundidad por el WAF con un modo de alerta para el área de penalización.

A2: Autenticación comprometida

Impacto: grave	**Prevalencia:** común	**Explotabilidad:** fácil

Las funciones de las aplicaciones relacionadas con la autenticación y la gestión de sesiones suelen implementarse de forma incorrecta, lo que permite a los atacantes poner en riesgo contraseñas, claves o tokens de sesión, o explotar otros fallos de implementación para asumir las identidades de otros usuarios de forma temporal o permanente.

Cómo puede ayudar Akamai

Aunque corresponde a las organizaciones corregir el proceso de autenticación comprometido para solucionar plenamente esta vulnerabilidad, Akamai puede ayudar a detectar y proteger frente a muchos de los vectores de ataque que intentan explotarla:

- El WAF de Akamai ofrece una función de control de frecuencia, que puede gestionar ataques de fuerza bruta.
- Las soluciones de gestión de bots[6] pueden detectar y gestionar la automatización utilizada para los ataques de Credential Stuffing.
- Las cookies de HTTP pueden cifrarse en la plataforma de Akamai[7] para evitar la alteración y modificación de cookies, lo que refuerza el proceso de autenticación.
- Enterprise Application Access (EAA)[8] puede acceder mediante proxy a las aplicaciones a través de un "modelo de acceso con mínimos privilegios", lo que reduce la superficie de ataque de la aplicación y mejora el acceso con funciones de autenticación de dos factores (2FA) y de varios factores (MFA).

A3: Exposición de datos confidenciales

Impacto: grave	**Prevalencia:** generalizada	**Explotabilidad:** media

Muchas aplicaciones web y API no protegen correctamente los datos confidenciales, como datos financieros, de salud y la información de identificación personal. Los atacantes pueden robar o modificar esos datos de escasa protección para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Sin protección adicional, como el cifrado en reposo o en tránsito, los datos confidenciales podrían estar en peligro y requieren precauciones especiales al intercambiarlos en el navegador.

Cómo puede ayudar Akamai

La exposición de datos confidenciales cubre muchos aspectos de cómo se transmiten, almacenan y comparten los datos, incluida la exposición accidental de los datos de una página web sin protección, y no puede quedar totalmente protegida por una única solución de seguridad. Sin embargo, existen varias soluciones que sirven para abordar algunos aspectos de esta vulnerabilidad. Por ejemplo:

- Akamai cifra y protege los datos confidenciales en tránsito y ayuda a mantener el cumplimiento del PCI, ya que funciona exclusivamente desde una CDN segura con bastidores aislados, compatibles con todos los certificados SSL de marca y protege las claves privadas de un cliente.
- Enterprise Application Access puede proteger el acceso remoto cifrando la comunicación y ocultando los datos confidenciales a los intrusos de la red.
- Enterprise Application Access también puede integrarse con las soluciones de prevención de pérdida de datos (DLP, por sus siglas en inglés) mediante ICAP para proteger aún más los datos sensibles de la exposición.
- Enterprise Threat Protector (ETP)[9] puede ser útil con la exposición de datos confidenciales.

A4: Entidades externas XML (XXE)

Impacto: grave	**Prevalencia:** común	**Explotabilidad:** media

Muchos procesadores XML antiguos o mal configurados evalúan las referencias de entidades externas en los documentos XML. Las entidades externas pueden utilizarse para divulgar archivos internos mediante el gestor de URI de archivos, los recursos compartidos de archivos internos, el análisis de puertos internos, la ejecución de código remoto y los ataques de denegación de servicio.

Cómo puede ayudar Akamai

- El WAF de Akamai incluye reglas que pueden detectar y detener ataques XXE antes de que el analizador XML procese a la entidad externa peligrosa.
- El WAF de Akamai incluye funciones de protección de API con limitaciones de solicitud de API que se pueden utilizar para validar XML y JSON mediante formatos predefinidos para bloquear los ataques XXE.

A5: Control de acceso comprometido

Impacto: grave	**Prevalencia:** común	**Explotabilidad:** media

Las restricciones sobre lo que los usuarios autenticados tienen permitido hacer no suelen aplicarse correctamente. Los atacantes pueden aprovechar estos fallos para vulnerar funciones o datos no autorizados, y acceder a cuentas de otros usuarios, ver archivos confidenciales, modificar datos, cambiar derechos de acceso, etc.

Cómo puede ayudar Akamai

Aunque corresponde a las organizaciones corregir su modelo de control de acceso para solucionar plenamente esta vulnerabilidad, Akamai puede ayudar a detectar y proteger frente a algunos de los vectores de ataque que intentan explotarla:

- Enterprise Application Access brinda un modelo de acceso con mínimos privilegios a usuarios empresariales, lo que permite la visibilidad y el acceso solo a las aplicaciones autorizadas por usuarios autenticados, lo cual es compatible con un modelo de seguridad Zero Trust.
- API Gateway[10] puede aplicar la autenticación para que las API refuercen el control de acceso.
- El WAF de Akamai puede ayudar a bloquear ataques intensos al navegador mediante la comprobación de referencias.
- Las cookies de HTTP se pueden cifrar en la plataforma Akamai, lo que refuerza el control de acceso.

A6: Configuración de seguridad incorrecta

Impacto: moderado	**Prevalencia:** generalizada	**Explotabilidad:** fácil

La configuración de seguridad incorrecta es el problema que se observa con más frecuencia. A menudo es la consecuencia de unas configuraciones predeterminadas inseguras, unas configuraciones incompletas o ad hoc, el almacenamiento en nube abierta, encabezados HTTP mal configurados o mensajes de error descriptivos que contienen información confidencial. Todos los sistemas operativos, marcos, bibliotecas y aplicaciones deben configurarse de forma segura pero, además, deben repararse y actualizarse puntualmente.

Cómo puede ayudar Akamai

Por definición, la configuración de seguridad incorrecta (a.) cubre varios aspectos de la seguridad de las aplicaciones y (b.) requiere que las organizaciones configuren correctamente los controles de seguridad. Aunque no sustituye a una configuración adecuada, Akamai puede ayudar a protegerse contra la fuga de datos:

- El WAF de Akamai incluye un grupo saliente de ataque de anomalías para capturar fugas de información, como códigos de error, así como el código fuente que se genera de la configuración incorrecta de serie de la seguridad.
- Los parches virtuales con reglas personalizadas pueden ayudar a abordar con rapidez las fugas de datos detectadas hasta que la aplicación se pueda reparar.
- Los ataques de fuerza bruta con el uso de credenciales predeterminadas pueden protegerse con controles de frecuencia.
- La configuración de seguridad débil en los encabezados de la política de seguridad de contenido puede reforzarse en la plataforma Akamai.

A7: Filtros de scripts de sitios (XSS)

Impacto: moderado	**Prevalencia:** generalizada	**Explotabilidad:** fácil

Los fallos de XSS se producen cada vez que una aplicación (a.) incluye datos que no son de confianza en una nueva página web sin la validación o escape adecuados o (b.) actualiza una página web existente con datos proporcionados por el usuario mediante una API de navegador que puede crear HTML o JavaScript. XSS permite a los atacantes ejecutar scripts en el navegador de la víctima y secuestrar sesiones de usuario, deteriorar sitios web o redirigir al usuario a sitios maliciosos.

Cómo puede ayudar Akamai

Las organizaciones pueden utilizar una solución de seguridad de WAF para proteger las aplicaciones web contra fallos de XSS. Sin embargo, deben siempre reparar las aplicaciones web para abordar cualquier vulnerabilidad detectada en función de su ciclo de vida de desarrollo.

- Los productos WAF de Akamai cuentan con reglas de WAF de XSS existentes listas para usar destinadas a identificar y detener los ataques XSS.
- Los parches virtuales con reglas personalizadas pueden ayudar a abordar con rapidez las vulnerabilidades emergentes de XSS o las nuevas vulnerabilidades expuestas a partir de cambios en las aplicaciones, hasta que la aplicación se pueda reparar.
- Client Reputation proporciona una puntuación de riesgo para clientes maliciosos en la categoría de atacantes web con el fin de bloquear los ataques de XSS.
- La plataforma de Akamai puede definir encabezados de política de respuesta de seguridad sobre la marcha para protegerse de los ataques de XSS.

A8: Deserialización insegura

Impacto: grave	**Prevalencia:** común	**Explotabilidad:** difícil

La deserialización suele dar lugar a la ejecución de código remoto. Aunque los defectos de deserialización no tengan como resultado la ejecución de código remoto, pueden utilizarse para efectuar ataques como los ataques de repetición, ataques de inyección y ataques de escalada de privilegios.

Cómo puede ayudar Akamai

Las organizaciones pueden utilizar una solución de seguridad de WAF para proteger las aplicaciones web y las API contra defectos de deserialización inseguros. Sin embargo, deben siempre reparar las aplicaciones web para abordar cualquier vulnerabilidad detectada en función de su ciclo de vida de desarrollo.

- Las reglas del WAF de Akamai detectan los ataques de deserialización.
- Los parches virtuales con reglas personalizadas pueden ayudar a abordar con rapidez nuevos defectos de deserialización hasta que la aplicación se pueda reparar.
- El WAF de Akamai incluye funciones de protección API con un modelo de seguridad positivo que define formatos de objeto JSON y XML aceptables para excluir XML y JSON de diseño malicioso.

A9: Uso de componentes con vulnerabilidades conocidas

Impacto: moderado	**Prevalencia:** generalizada	**Explotabilidad:** media

Componentes como las bibliotecas, los marcos y otros módulos de software se ejecutan con los mismos privilegios que la aplicación. Además, los scripts actúan como recursos de aplicación de confianza con acceso completo a los datos de la aplicación. Si se explotan componentes vulnerables, este tipo de ataque puede facilitar una pérdida grave de datos o la toma del control del servidor. Las aplicaciones y las API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.

Cómo puede ayudar Akamai

Aunque resulten populares y se utilicen de forma generalizada para reducir los tiempos y los costes de desarrollo, los componentes de terceros son un punto de entrada muy habitual para las vulnerabilidades incluso en sus aplicaciones más exclusivas. Existen numerosos riesgos. A menudo, las organizaciones pierden la cuenta de los componentes de terceros que se usan en sus aplicaciones (y los equipos de seguridad suelen desconocerlo por completo). Además, las organizaciones no tienen ningún control sobre la rapidez o el momento en que las entidades de terceros abordan las vulnerabilidades recién detectadas. Como consecuencia, la reparación de aplicaciones en el momento oportuno puede resultar difícil o imposible, lo que exige el uso de una solución de seguridad, como el WAF y la protección de scripts:

- El WAF de Akamai incluye varias reglas diseñadas para abordar vulnerabilidades conocidas, ya sea específicamente en sus aplicaciones o en componentes de terceros.
- Los parches virtuales con reglas personalizadas pueden ayudar a abordar con rapidez las vulnerabilidades emergentes o las nuevas vulnerabilidades expuestas a partir de cambios en las aplicaciones, hasta que la aplicación se pueda reparar.
- El WAF de Akamai ofrece funciones de protección API para blindar las API de componentes de terceros frente a ataques que aprovechan vulnerabilidades conocidas.
- Client Reputation proporciona una puntuación de riesgo para clientes maliciosos en la categoría de análisis web para proteger frente a la explotación de nuevas vulnerabilidades.
- Page Integrity Manager protege las aplicaciones web frente a nuevas amenazas, como el robo de información web, el formjacking y los ataques de Magecart, mediante la detección de comportamientos de scripts sospechosos y la entrega de información procesable para bloquear actividades maliciosas.
- Page Integrity Manager bloquea la exfiltración de datos de scripts propios y de terceros a URL con vulnerabilidades conocidas, a través de una base de datos de vulnerabilidades y exposiciones comunes (CVE) que se actualiza constantemente.

A10: Registro y supervisión insuficientes

Impacto: moderado	**Prevalencia:** generalizada	**Explotabilidad:** media

El registro y la supervisión insuficientes, junto con la ausencia de integración o una integración ineficaz con la respuesta a incidentes, permiten a los atacantes vulnerar aún más los sistemas, mantener la persistencia, cambiar a más sistemas y alterar, extraer o destruir los datos. La mayoría de los estudios sobre filtraciones indican que el tiempo que se tarda en detectarlas suele superar los 200 días y que tales filtraciones suelen ser detectadas por partes externas en lugar de procesos o supervisiones internos.

Cómo puede ayudar Akamai

El registro y la supervisión insuficientes no describe una vulnerabilidad en sí misma, sino una brecha en la capacidad de una organización de resolver las vulnerabilidades y los intentos de explotarlas. Akamai ofrece varias funciones para proporcionar a las organizaciones una mayor visibilidad de los ataques, lo que incluye:

- Akamai cuenta con paneles y herramientas de generación de informes en la interfaz gráfica de usuario de Luna Control Center[11] de Akamai.
- Akamai se integra con la infraestructura SIEM de las organizaciones existentes para correlacionar los eventos detectados por Akamai con los de otros proveedores de seguridad.
- Los servicios de seguridad administrados de Akamai proporcionan funciones ininterrumpidas de análisis y respuesta.
- El WAF de Akamai incluye una función de área de penalización que permite un mayor registro de las sesiones sospechosas para un análisis más detallado.
- Enterprise Application Access de Akamai proporciona una solución de gestión de identidad integrada para autenticar y controlar el acceso a todas las aplicaciones empresariales. Cuando se combina con su función de proxy con reconocimiento de identidades, las organizaciones pueden obtener una visibilidad detallada de las acciones de los usuarios e incluir la visibilidad de todas las acciones GET/POST.
- Akamai Enterprise Threat Protector permite una visibilidad completa de todas las solicitudes de DNS externas de una empresa, tanto malintencionadas como inofensivas.

Conclusión

La mejor defensa contra las 10 principales vulnerabilidades según OWASP puede lograrse cuando las organizaciones y sus proveedores de seguridad trabajan juntos para coordinar personas, procesos y tecnologías. Akamai le ofrece tecnología líder del sector y personal con gran experiencia que se adaptan a sus procesos. Para obtener más información acerca de la cartera de productos de seguridad en el borde de internet de Akamai, eche un vistazo a la información más detallada de nuestro sitio web. Si desea comentar y explorar con más detalle cómo podemos asociarnos para crear la mejor protección para su negocio, póngase en contacto con el representante de ventas de Akamai.

Fuentes

1. Seguridad en el borde de Internet
2. Servicios y asistencia
3. Akamai Intelligent Edge Platform™
4. Kona Site Defender (KSD) y Web Application Protector (WAP)
5. Client Reputation
6. Bot Manager
7. Secure CDN
8. Enterprise Application Access
9. Enterprise Threat Protector
10. API Gateway
11. Luna Control Center

Akamai Experience the Edge