Akamai

WHITE PAPER

Las 10 principales vulnerabilidades según OWASP

Cómo Akamai ayuda a proteger contra las vulnerabilidades comunes

Introducción

En la lista 10 principales vulnerabilidades según OWASP (Proyecto abierto de seguridad de aplicaciones web) se clasifican las vulnerabilidades más frecuentemente vistas en las aplicaciones web, lo que permite concienciar a las organizaciones. Para sacar el máximo partido de la lista de las 10 principales vulnerabilidades según OWASP, es necesario comprender dónde, cómo y cuánto pueden ayudarle los proveedores de seguridad a mejorar sus prácticas de desarrollo. En el siguiente desglose de las 10 principales vulnerabilidades según OWASP se describe cada una de ellas, además de explicarse cómo Akamai puede ayudar a las organizaciones con soluciones de seguridad en el Edge, servicios gestionados y la plataforma inteligente de Edge más grande del mundo.

Productos de Akamai

10 principales vulnerabilidades según OWASP		Account Protector	Akamai Guardicore Segmentation	App & API Protector	Bot Manager	Enterprise Application Access	Enterprise Threat Protector	Identity Cloud	Servicios de seguridad gestionados	Akamai MFA	Page Integrity Manager
Control de acceso comprometido	A01			✓	✓	✓		✓		✓	
Fallos criptográficos	A02			✓		✓	✓				✓
Inyección	A03			✓							
Diseño inseguro	A04			✓		✓					
Configuración de seguridad incorrecta	A05		✓	✓	✓						
Componentes vulnerables y obsoletos	A06		✓	✓							✓
Fallos de identificación y autenticación	A07	✓		✓	✓	✓		✓		✓	
Fallos de integridad de datos y software	A08		✓	✓			✓				✓
Fallos de registro y de supervisión de la seguridad	A09		✓	✓		✓	✓		✓		
Falsificación de solicitudes del lado del servidor	A10		✓	✓							

Las 10 principales vulnerabilidades según OWASP son categorías de riesgos, no riesgos individuales. Las soluciones de Akamai abordan estas categorías de riesgo de varias maneras. Lea el white paper para obtener más información.

A01: Control de acceso comprometido

> "El control de acceso aplica la política de modo que los usuarios no puedan actuar sobrepasando los permisos que tengan. Los fallos suelen provocar la divulgación o modificación de información no autorizada, o bien la destrucción de todos los datos o la posibilidad de realizar una función comercial que va más allá de los límites del usuario".
>
> — Fuente: owasp.org

Cómo ayuda Akamai

Aunque corresponde a las organizaciones corregir su modelo de control de acceso para solucionar plenamente la vulnerabilidad Control de acceso comprometido, la experiencia de Akamai en protección de API y aplicaciones web (WAAP) puede ayudarle a detectar y protegerse frente a algunos de los vectores de ataque que intentan explotarla:

- **Enterprise Application Access** pone a disposición de los usuarios empresariales un modelo de acceso con mínimos privilegios, gracias al cual solo los usuarios autenticados pueden ver y acceder a las aplicaciones autorizadas y es compatible con un modelo de seguridad Zero Trust.
- **Akamai MFA** ofrece servicios de autenticación estricta basados en estándares de tecnología FIDO2 resistentes a los ataques de phishing.
- **App & API Protector**, la solución WAAP de Akamai, puede ayudar a bloquear ataques intensos al navegador mediante la comprobación del encabezado de referencia, así como a aplicar la autenticación para que las API refuercen el control de acceso con Akamai API Gateway.
- **Identity Cloud** proporciona controles de acceso detallados a los datos del usuario final, lo que permite el acceso con mínimos privilegios por usuario o sistema internos.
- **Bot Manager** evita los ataques automatizados de herramientas y los ataques de inicio de sesión.

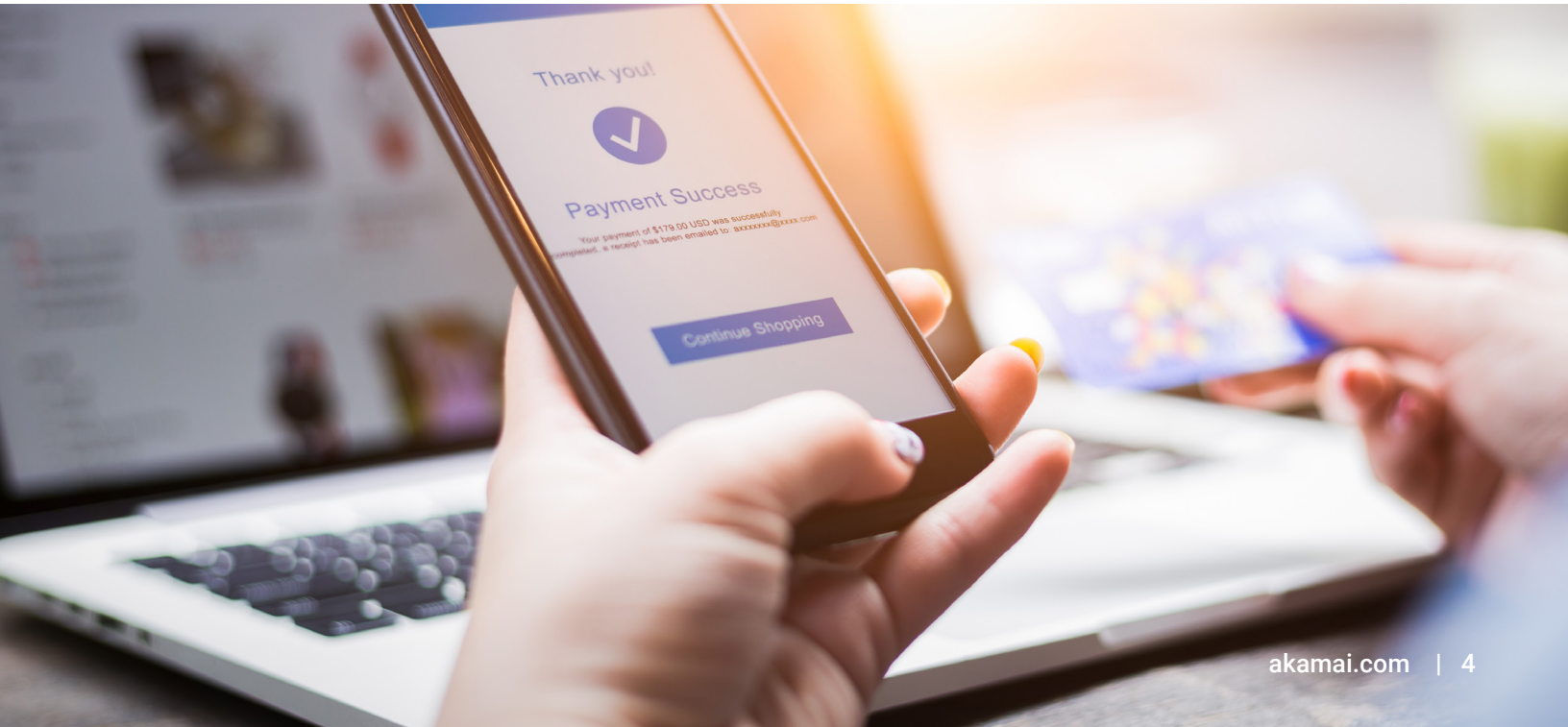
A02: Fallos criptográficos

> "Lo más importante son los fallos relacionados con la criptografía (o la falta de esta), lo que, a menudo, puede derivar en la exposición de datos confidenciales. … Por ejemplo, contraseñas, números de tarjetas de crédito, expedientes médicos, información personal y secretos comerciales requieren una protección adicional, principalmente si esos datos se rigen por las leyes de privacidad".
>
> — Fuente: owasp.org

Cómo ayuda Akamai

Las organizaciones no pueden protegerse completamente de los fallos criptográficos por medio de una única solución de seguridad. Sin embargo, la combinación de varias soluciones puede servir para abordar algunos aspectos de esta vulnerabilidad. Por ejemplo:

- **App & API Protector** cifra y protege los datos confidenciales en tránsito con las últimas versiones de TLS y cifrados potentes. También permite:
  - Garantizar el cumplimiento de las normas del sector de las tarjetas de pago (PCI), ya que funciona exclusivamente desde una red de distribución de contenido (CDN) segura, compatible con todos los certificados TLS de marca y que protege las claves privadas del cliente.
  - Ofrecer una CDN que cuente con protección mediante seguridad física y operativa, como bastidores aislados y detectores de movimiento, que garantice que solo el personal autorizado pueda acceder a los servidores.
  - Localizar y evitar filtraciones de datos confidenciales mediante el aprendizaje de la información de identificación personal (PII) de la API.
- **Enterprise Application Access** puede proteger el acceso remoto cifrando la comunicación, así como ocultando los datos confidenciales a los intrusos de la red.
- **Enterprise Threat Protector** puede ayudar a prevenir la exposición de datos confidenciales.
- **Page Integrity Manager** también puede detectar filtraciones de PII mediante el uso indebido de código JavaScript que podrían ser consecuencia de fallos criptográficos.



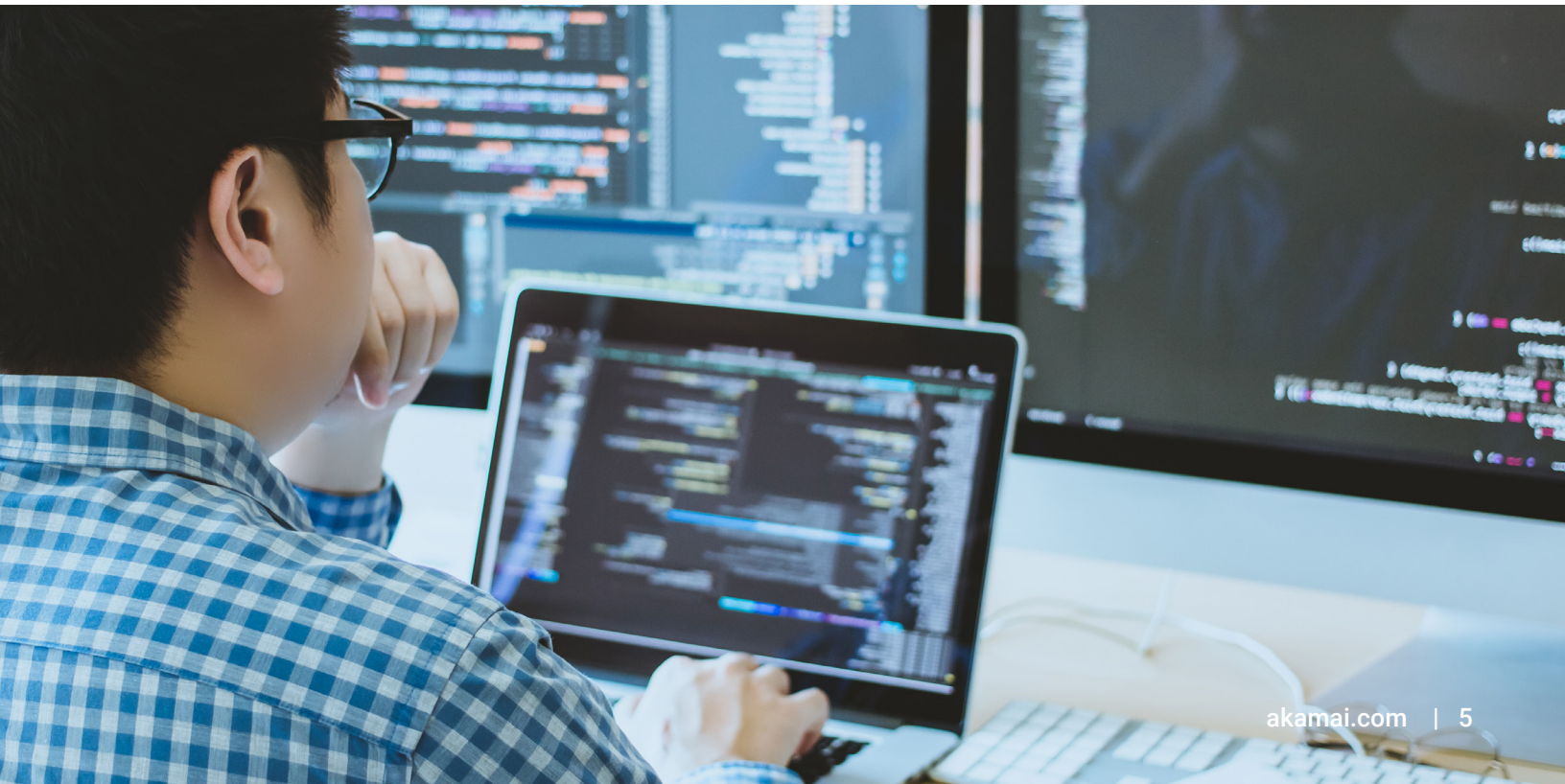
A03: Inyección

> "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".
>
> — Fuente: Akamai

Cómo ayuda Akamai

Use WAAP para mitigar el riesgo de ataques de inyección a las aplicaciones web y API. Sin embargo, las organizaciones deben siempre aplicar los parches necesarios a las aplicaciones web para abordar cualquier vulnerabilidad detectada durante sus ciclos de desarrollo respectivos.

- **App & API Protector** ofrece una solución WAAP líder en el sector con un motor de seguridad adaptable (ASE), que proporciona una amplia protección contra ataques de inyección mediante las reglas preconfiguradas existentes. El área de penalización del ASE puede bloquear temporalmente mediante WAAP cualquier tráfico procedente de clientes que recientemente hayan intentado llevar a cabo un ataque de inyección.
- 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 equipos de seguridad también pueden automatizar los parches virtuales e integrarlos en los procesos DevSecOps mediante el aprovechamiento de las funciones API de Akamai.
- **Client Reputation** puede ayudar a identificar y bloquear los ataques de inyección. Asimismo, proporciona una puntuación de riesgo para clientes maliciosos de actividad elevada en la categoría de atacantes web.



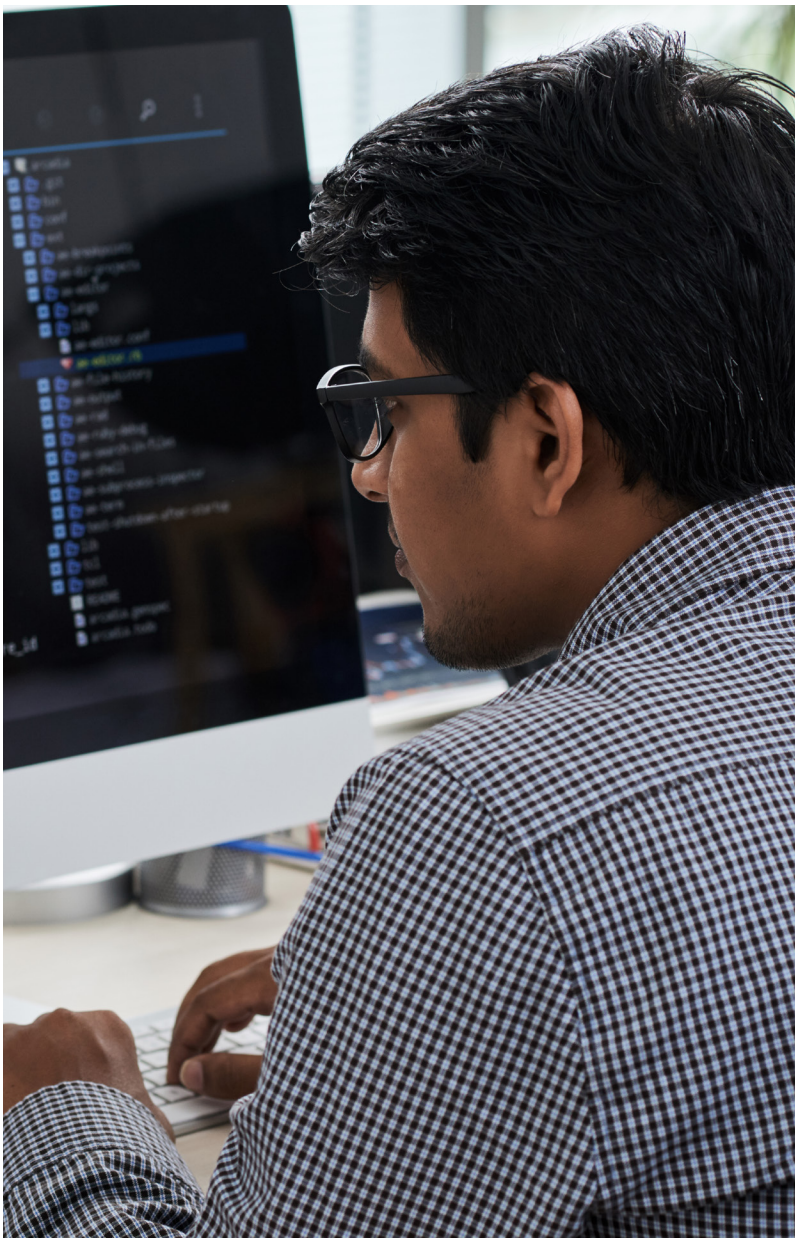
A04: Diseño inseguro

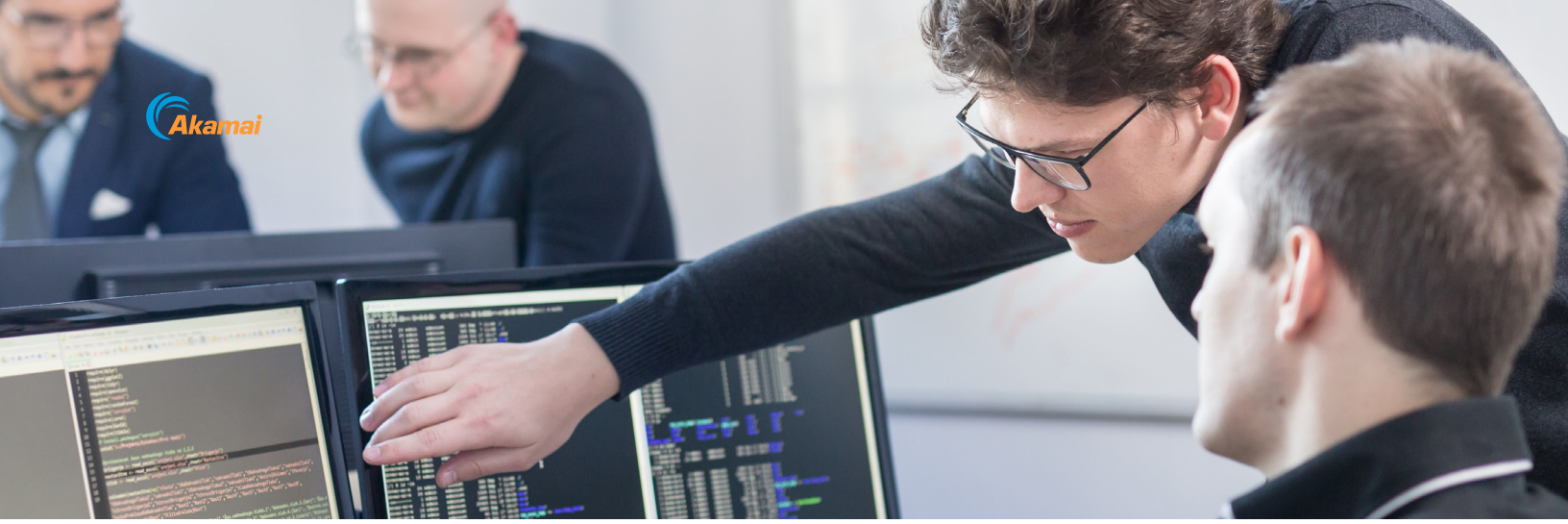
> "El diseño inseguro es una categoría amplia que representa diferentes deficiencias, lo que se expresa como 'falta el diseño de control o este no es eficaz'. Existe una diferencia entre un diseño inseguro y una implementación insegura. Un diseño seguro aún puede tener defectos de implementación que provoquen vulnerabilidades que se puedan aprovechar. Un diseño inseguro no puede corregirse mediante una implementación perfecta, ya que, por definición, los controles de seguridad necesarios nunca se han creado para defenderse frente a ataques específicos".
>
> — Fuente: owasp.org

Cómo ayuda Akamai

Las organizaciones deben integrar la seguridad desde las primeras etapas del diseño. Sin embargo, puede que los equipos de desarrollo tengan dificultades para lograr esto si la seguridad es difícil de incorporar. Los productos de Akamai ayudan a las organizaciones a detectar de forma más rápida problemas en las fases iniciales para evitar que los diseños inseguros pongan en peligro sus aplicaciones y API.

- **App & API Protector**, que incluye nuestra solución WAAP y ASE, también puede detectar y solucionar algunos defectos de diseño que podrían llegar a la fase de producción. También aprovecha la automatización para descongestionar y simplificar las tareas rutinarias, dejando para los humanos aquellas en las que se requiere el análisis humano. Esta automatización incluye actualizaciones automáticas, ajuste automático, detección de API, programabilidad simplificada y experiencia del usuario.
- **Enterprise Application Access** garantiza que solo los usuarios autorizados puedan acceder a las aplicaciones. Este enfoque de mínimos privilegios evita el movimiento lateral a otras aplicaciones, lo que puede producirse fácilmente con soluciones de acceso a la red, como las redes privadas virtuales (VPN).





A05: Configuración de seguridad incorrecta

> "[Desde] la edición anterior, se ha analizado el 90 % de las aplicaciones para detectar alguna posible forma de configuración incorrecta, con una tasa de incidencia media del 4 % y más de 208 000 casos de una Common Weakness Enumeration (CWE) en esta categoría de riesgo. Sin un proceso concertado y repetible para configurar la seguridad de las aplicaciones, los sistemas están sometidos a un mayor riesgo".
>
> — Fuente: owasp.org

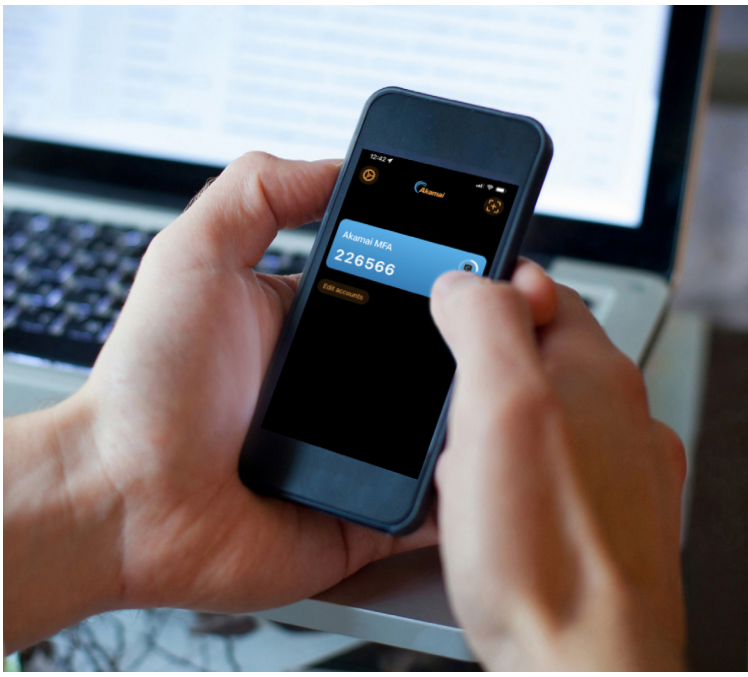
Cómo ayuda Akamai

Por definición, la configuración de seguridad incorrecta abarca varios aspectos de la seguridad de las aplicaciones. También se requiere que las organizaciones configuren adecuadamente los controles de seguridad. Los productos de Akamai ayudan de las siguientes maneras:

- Aunque no sustituye a una configuración adecuada, **App & API Protector** puede ayudar mediante:
  1. El uso de grupos de ataque contra anomalías salientes para capturar fugas de información, como códigos de error, así como el código fuente resultante de una configuración incorrecta de la seguridad.
  2. La aplicación de reglas que pueden detectar y detener ataques XXE antes de que el analizador XML procese la entidad externa peligrosa.
  3. La aplicación de reglas que puedan detectar el acceso a archivos confidenciales conocidos que dejen los desarrolladores en los servidores de producción.
- **Akamai Guardicore Segmentation** ayuda a protegerse de la fuga de datos debido a errores de configuración, al proporcionar tanto visibilidad como un control detallado de cualquier comunicación no autorizada o no planificada entre sus aplicaciones e Internet.
- Los parches virtuales con reglas personalizadas pueden ayudar a abordar con rapidez las fugas de datos detectadas hasta que el equipo pueda reparar la aplicación.
- Con **App & API Protector** y **Bot Manager**, es posible protegerse, mediante controles de frecuencia, de los ataques de fuerza bruta que utilizan credenciales predeterminadas.
- Una configuración débil en la política de seguridad de contenido y otros encabezados HTTP relacionados con la seguridad puede reforzarse en la plataforma Akamai.
- La detección automática de API que ofrece **App & API Protector** le permite detectar y clasificar de forma automática y continua sus API, incluidos los terminales, las definiciones y las características de los recursos y el tráfico.

A06: Componentes vulnerables y obsoletos

> "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 dar lugar a una pérdida grave de datos o la toma del control del servidor".
>
> — Fuente: Akamai



Cómo ayuda Akamai

A menudo, las organizaciones pierden la cuenta de los componentes de terceros que existen en sus aplicaciones (y los equipos de seguridad suelen desconocerlo por completo). Además, las organizaciones no tienen ningún control sobre el tiempo que tardará, si lo hace, el tercero en abordar las vulnerabilidades recién detectadas. Para mitigar esta falta de visibilidad y certeza se debe usar una solución de seguridad como WAAP y protección de scripts, como las siguientes:

- **App & API Protector** incluye varias reglas diseñadas para abordar vulnerabilidades conocidas, ya sea específicamente en sus aplicaciones o en componentes de terceros. También proporciona funciones para proteger las API, incluso cuando los componentes de terceros incorporados a esas API abren la puerta a que se cometan abusos.
- El módulo Insight de **Akamai Guardicore Segmentation** le permite consultar cualquier activo de su red que pueda ser vulnerable. La aplicación detallada incluida le permite acordonar aún más los activos afectados hasta que se haya aplicado un parche.
- Los parches virtuales con reglas personalizadas ayudan 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.
- **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** analiza constantemente el comportamiento de la ejecución de scripts, en sesiones de usuarios reales, para identificar comportamientos sospechosos o maliciosos. También 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.

A07: Fallos de identificación y autenticación

> "Las funciones de las aplicaciones relacionadas con la autenticación y la gestión de sesiones a menudo se implementan 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".
>
> — Fuente: Akamai

Cómo ayuda Akamai

Las organizaciones deben corregir sus fallos para solucionar plenamente esta vulnerabilidad. No obstante, las soluciones de Akamai que se enumeran a continuación pueden ayudar a detectar y proteger frente a muchos de los vectores de ataque que intentan aprovechar los errores de identificación y autenticación:

- **Bot Manager** puede detectar y mitigar ataques automatizados, como los que se utilizan en los ataques de Credential Stuffing.
- **Account Protector** mitiga los intentos de apropiación de cuentas, donde los impostores intentan obtener acceso no autorizado a las cuentas de usuario.
- **Enterprise Application Access** 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.
- **Akamai MFA** ofrece una autenticación estricta mediante la tecnología FIDO2 resistente a los ataques de phishing.
- **App & API Protector** ofrece una función de control de frecuencia, que puede gestionar ataques de fuerza bruta.
- **Identity Cloud** proporciona una gestión segura de las credenciales de usuario final y la información de perfil protegida por la autenticación de dos factores y las funciones de autenticación basadas en el riesgo.

A08: Fallos de integridad de datos y software

> "Los fallos de integridad de los datos y el software están relacionados con código e infraestructura que no protegen contra las violaciones de la integridad. Un ejemplo de ello es cuando una aplicación se apoya en complementos, bibliotecas o módulos de fuentes, repositorios y redes de entrega de contenido (CDN) que no gozan de confianza. Un canal de CI/CD inseguro puede introducir la posibilidad de acceso no autorizado, código malicioso o riesgo para el sistema".
>
> — Fuente: owasp.org

Cómo ayuda Akamai

Las organizaciones pueden utilizar WAAP para proteger las aplicaciones web y las API frente a fallos de integridad de datos y software. Sin embargo, deben siempre aplicar los parches necesarios a las aplicaciones web para abordar cualquier vulnerabilidad detectada durante sus ciclos de desarrollo respectivos.

- **App & API Protector**
  - Proporciona una protección sólida contra los ataques de deserialización.
  - Impide los ataques de máquina intermediaria que pueden generar problemas de integridad de datos a través de la implementación de las últimas versiones de TLS y de cifrados potentes.
  - Garantiza la autenticación del origen de los datos y la protección de la integridad de los datos de los registros de DNS mediante la implementación de DNSSEC con Edge DNS. Esto evita la manipulación de registros de DNS que pueden dirigir a los usuarios a fuentes que no gozan de confianza.
- El módulo Insight de **Akamai Guardicore Segmentation** le permite consultar cualquier activo de su red que haya recibido la actualización con fallos. La aplicación detallada incluida le permite acordonar aún más esos activos afectados hasta que se haya creado una corrección.
- **Enterprise Threat Protector** detecta ataques de phishing, que pueden atraer a los administradores y superusuarios de las aplicaciones a entornos hostiles o fuentes no fiables.
- Los parches virtuales con reglas personalizadas pueden ayudar a abordar con rapidez nuevos defectos de deserialización hasta que la aplicación se pueda reparar.
- **Page Integrity Manager** detecta scripts de terceros, los supervisa para detectar los posibles cambios y, a continuación, toma las medidas necesarias en los scripts que se hayan visto comprometidos.

A09: Fallos de registro y de supervisión de la seguridad

"El registro, la detección, la supervisión y la respuesta activa insuficientes se producen en cualquier momento:

- Los eventos auditables, como inicios de sesión, inicios de sesión fallidos y transacciones de alto valor, no se registran.
- Las advertencias y los errores generan mensajes de registro inadecuados, poco claros o no generan este tipo de mensajes.
- Los registros de aplicaciones y las API no se supervisan para detectar posible actividad sospechosa.
- Los registros solo se almacenan localmente.
- No se han establecido los umbrales de alerta y los procedimientos de derivación de respuestas adecuados o no se aplican.
- Las pruebas de penetración y los análisis llevados a cabo con herramientas de pruebas de seguridad de aplicaciones dinámicas (DAST) no activan alertas.

La aplicación no puede detectar, escalar ni alertar sobre ataques activos en tiempo real o prácticamente en tiempo real".

— Fuente: owasp.org

Cómo ayuda Akamai

Los fallos de registro y de supervisión de la seguridad representan una carencia 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 Akamai Control Center.
- Los productos de seguridad de aplicaciones de Akamai se integran con la infraestructura SIEM existente de una organización para correlacionar los eventos detectados por Akamai con los de otros proveedores de seguridad.
- **Managed Security Service** proporciona funciones ininterrumpidas de análisis y respuesta.
- **App & API Protector** incluye una función de área de penalización que permite un mayor registro de aquellas direcciones IP donde se hayan detectado actividades maliciosas o sospechosas para un análisis más detallado.
- **Enterprise Application Access** integra una solución de gestión de identidades 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, en particular de las acciones GET/POST.
- **Enterprise Threat Protector** permite una visibilidad completa de todas las solicitudes de DNS externas de una empresa, tanto malintencionadas como inofensivas.
- **Akamai Guardicore Segmentation** proporciona una visibilidad profunda de los flujos de comunicación dentro de su red, de modo que las alertas se puedan activar cuando se produzca una comunicación no autorizada o inesperada. Además, se pueden aplicar políticas de seguridad al nivel de servicio o proceso individual para restringir esta comunicación. Con el módulo de detección de filtraciones agregado, las posibles amenazas pueden detectarse y neutralizarse rápidamente.

A10: Falsificación de solicitudes del lado del servidor

> "Las deficiencias de SSRF se producen cada vez que una aplicación web busca un recurso remoto sin validar la URL proporcionada por el usuario. Esto permite a un atacante forzar a la aplicación a que envíe una solicitud creada a un destino inesperado, incluso cuando esté protegida por un firewall, una VPN u otro tipo de lista de control de acceso (ACL) a la red".
>
> — Fuente: owasp.org

Cómo ayuda Akamai

Akamai WAAP incluye reglas que pueden buscar la inyección de URL. Esta función puede impedir que los atacantes induzcan al servidor a ir a otro lugar y a enviar una solicitud, es decir, para que sus analistas de seguridad crean que es una solicitud válida.

- Las reglas de **App & API Protector** ayudan a evitar que esas solicitudes de explotaciones lleguen al servidor vulnerable en primer lugar.
- **Akamai Guardicore Segmentation** puede supervisar y bloquear el tráfico saliente inesperado a nivel del servidor.

Conclusión

Para preparar la mejor defensa contra las 10 principales vulnerabilidades según OWASP, es necesario que las organizaciones y sus proveedores de seguridad trabajen juntos para detectar las vulnerabilidades tan pronto como sea posible e implementar soluciones para mitigarlas. Obtenga más información acerca de la cartera de productos de seguridad en el Edge de Akamai. Si desea tratar y explorar cómo podemos colaborar para crear la mejor protección para su negocio, póngase en contacto con su representante de ventas de Akamai.

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Gracias a la plataforma informática más distribuida del mundo, de la nube al Edge, nuestros clientes pueden desarrollar y ejecutar las aplicaciones con facilidad, mientras acercamos las experiencias a los usuarios y mantenemos las amenazas a raya. Para obtener más información acerca de las soluciones de seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado en octubre de 2022.