

Preguntas más frecuentes:

1. ¿En qué consiste la solución Trend Micro Web Application Security?
2. ¿Por qué necesito proteger mis sitios Web de los ataques?
3. ¿Cómo pueden dañar el malware o los hackers mi sitio Web y mi negocio?
4. ¿Cómo puedo saber si Web Application Security es adecuado para mi negocio?
5. ¿Qué es el logotipo de marca de confianza de SecureSite?
6. ¿Cómo comprueba Trend Micro si mi sitio Web ha sido pirateado?
7. ¿Puedo evaluar Trend Micro Web Application Security?
8. ¿Cómo funciona la solución Web Application Security?
9. ¿Qué tipos de componentes de aplicaciones de sitios Web explora Web Application Security?
10. ¿Cómo me pueden configurar el servicio para explorar mis servidores Web?
11. ¿Funciona Web Application Security con un cortafuegos?
12. ¿Web Application Security explora todo mi dominio o solo una parte del sitio Web?
13. ¿Cuáles son las vulnerabilidades que busca Web Application Security?
14. ¿Cuánto tiempo se invierte en una exploración?
15. ¿Cómo afectan las exploraciones a mis servidores Web?
16. ¿Qué tipos de informes sobre vulnerabilidades hay disponibles?
17. ¿Pueden recibir los usuarios notificaciones por correo de los resultados de la exploración de seguridad?
18. ¿Qué formatos de archivos de informes puede generar Web Application Security?
19. ¿Cómo se valora la gravedad en los informes?
20. ¿Cómo se asocian las amenazas críticas/graves/moderadas a CVSS?
21. ¿Qué significan los distintos niveles de gravedad en los informes sobre valoración de vulnerabilidades?

General

1. **Pregunta:** ¿En qué consiste la solución Trend Micro Web Application Security?

Respuesta: La solución Trend Micro Web Application Security ayuda a las organizaciones a proteger sus sitios Web antes de que sus sistemas estén en peligro y busca permanentemente indicios de posibles ataques de piratería en los sitios Web a fin de poder tomar las acciones pertinentes. Esto lo consigue gracias a un servicio alojado que ofrece las funciones siguientes:



Web Application Security reduce drásticamente el tiempo, los riesgos y los costes que implica la protección de un sitio Web mediante la búsqueda automática de vulnerabilidades y puntos débiles en todas las aplicaciones Web, redes y sistemas operativos alojados, y la generación de informes resolutivos de expertos a través de un servicio alojado. Para certificar los dominios de comercio electrónico, se puede mostrar un logotipo opcional de marca de confianza de Trend Micro SecureSite para reforzar así la certificación de seguridad de su sitio Web.

Un componente del servicio de supervisión de Web Application Security comprueba de forma continua la red Trend Micro Smart Protection Network en busca de indicios de acciones maliciosas en sus sitios Web. Si su sitio Web ha sido pirateado, recibirá de inmediato una alerta sobre la presencia de contenido malicioso.

Y, en breve, el servicio Advanced ofrecerá informes detallados sobre cumplimiento de normativas (como PCI, SOX y HIPAA) que identifican las infracciones de las normativas existentes y las acciones de reparación necesarias para volver rápidamente al estado de cumplimiento.

Actividades del servicio - versión 1.0	Standard	Advanced -Muy pronto disponible
Exploraciones de vulnerabilidades de las aplicaciones Web	X	X
Exploraciones de vulnerabilidades del Host	X	X
Servicio de marca de confianza de SecureSite	X	X
Alertas de infiltración	X	X
Exploraciones a petición*	X	X
Informes	X	X
Exploraciones e informes de cumplimiento de normativas (se incluyen PCI, SOX y HIPAA)		X

*5 exploraciones anuales en la versión Standard. Exploraciones a petición adicionales disponibles como complemento.

2. **Pregunta:** ¿Por qué necesito proteger mis sitios Web de los ataques?

Respuesta: Los sitios Web son una puerta abierta a su negocio, un medio tanto de visibilidad como de ingresos. Sin embargo, muchos sitios Web presentan vulnerabilidades imperceptibles para la empresa pero que exponen a sus clientes y datos a posibles ataques. Para complicar más las cosas, en muchas ocasiones el desarrollo y el alojamiento de estos sitios Web son gestionados por otras empresas. Diversas investigaciones revelan el gran número de sitios Web vulnerables:

- Más del 79% de los sitios Web que contienen código malicioso son legítimos, es decir, han sido atacados por hackers (ZDNet, abril de 2008)
- Se han identificado más de 28.000 vulnerabilidades de XSS conocidas en los mencionados sitios Web, de las cuales solo se ha solucionado un 5% (fuente: XSSed.com, agosto de 2008)
- Más del 40% de los incidentes de amenazas Web han implicado a sitios legítimos en la distribución de malware sin el conocimiento de estos últimos (fuente: TrendLabs, 2008)

3. **Pregunta:** ¿Cómo pueden dañar el malware o los hackers mi sitio Web y mi negocio?

Respuesta: Los hackers y los ciberdelincuentes ganan dinero a costa de las debilidades de la Web y robando información confidencial como números de tarjetas de crédito. Los nuevos ataques a los sitios de comercio electrónico aumentan cada día. Para la mayoría de las empresas, conocer y comprender amenazas como las vulnerabilidades de Web2.0, SQL Injections y otros tipos de vulnerabilidades de sitios cruzados es una tarea tediosa y desbordante. Sin embargo, proteger la información confidencial es responsabilidad de la organización, ya sean datos de los empleados, clientes o socios comerciales. Pero los esfuerzos de seguridad para proteger los sitios Web acaparan la atención en detrimento del desarrollo comercial, hecho que origina un círculo vicioso. La pérdida de confianza de estos elementos menoscaba la reputación empresarial y pone en peligro las actividades que generan ingresos. De hecho, muchos millones de consumidores son reticentes a usar sus tarjetas de crédito en la Web por el miedo al fraude y al robo de identidades.

4. **Pregunta:** ¿Cómo puedo saber si Web Application Security es adecuado para mi negocio?

Respuesta: Considere usar Web Application Security si desea:

- Reducir el tiempo, el riesgo y el coste de buscar y reparar las vulnerabilidades de seguridad de sus sitios Web
- Encontrar una forma sencilla y rentable de valorar y supervisar la seguridad de sus sitios Web
- Contar con una ayuda fiable por parte de expertos y proporcionar una experiencia en línea más segura para sus posibles clientes, clientes existentes, socios empresariales y empleados

- Desarrollar prácticas sólidas de seguridad de datos y garantizar la protección de aplicaciones y sistemas Web públicos
- Solucionar posibles problemas de seguridad antes de que tengan un impacto en su organización
- Eliminar el gasto en la adquisición y el mantenimiento de múltiples productos
- Simplificar la implementación con una distribución basada en el software como servicio, sin necesidad de tener hardware o software adicional

5. **Pregunta:** ¿Qué es el logotipo de marca de confianza de SecureSite?



Respuesta: El logotipo de marca de confianza opcional de SecureSite Tested: 2 Sept, 2008 es un sello de aprobación externo que permitirá a los clientes de su comercio electrónico saber que ha tomado las acciones necesarias para proteger su información. Se trata de un servicio opcional disponible con una exploración diaria que examina los sitios Web en busca de vulnerabilidades, contenido peligroso y enlaces que expongan los equipos y la información personal de los consumidores a un uso malintencionado. Los sitios Web que cumplan las políticas de seguridad podrán incluir el logotipo de marca de confianza de Trend Micro SecureSite en sus páginas Web para demostrar su preocupación e interés por las cuestiones de seguridad a los internautas. Los clientes de Web Application Security que elijan una frecuencia de exploración distinta a la diaria no podrán mostrar el logotipo de marca de confianza de SecureSite en sus sitios Web.

6. **Pregunta:** ¿Cómo comprueba Trend Micro si mi sitio Web ha sido pirateado?

Respuesta: Trend Micro Smart Protection Network es una infraestructura de seguridad de contenidos por Internet de nueva generación compuesta por una red mundial de sensores, con bases de datos de amenazas correlacionadas continuamente actualizadas que ofrecen una protección exhaustiva frente a todos los tipos de amenazas, desde archivos maliciosos, spam, phishing y amenazas Web hasta ataques de denegación de servicio, vulnerabilidades Web y la pérdida de datos. Web Application Security supervisa permanentemente la actividad de Trend Micro Smart Protection Network para detectar si se ha puesto en peligro la seguridad de sus sitios Web. En el caso de que uno de sus sitios Web haya sido atacado, recibirá de inmediato una alerta por correo electrónico sobre la presencia de contenido malicioso para que pueda realizar las acciones necesarias y evitar así un daño mayor a los activos y la reputación de su empresa. El proceso de supervisión no requiere una exploración específica de sus sitios Web reales, sino que hace uso de la información en tiempo real sobre amenazas Web de Smart Protection Network. Además, si su sitio mantiene un estado de confianza o seguro, Trend Micro le enviará periódicamente un mensaje de correo confirmando este estado para que sepa que seguimos trabajando para usted.

7. **Pregunta:** ¿Puedo evaluar Trend Micro Web Application Security?

Respuesta: Sí. El servicio Web Application Security está disponible en versión de evaluación. La página de registro para evaluarlo es:

<http://es.trendmicro.com/es/solutions/enterprise/security-solutions/web-application-security/trial>

Para completar el registro deberá indicar un dominio accesible públicamente o una dirección IP del host junto con una dirección de correo válida. La posibilidad de definir la fecha y la hora de las exploraciones le permite planificarlas teniendo en cuenta sus necesidades. Tras completar el registro, recibirá un mensaje de confirmación que le pedirá que publique un pequeño fragmento de texto oculto en su sitio Web para comprobar que es propietario de ese dominio. Cuando finalice la exploración de evaluación, le enviaremos un mensaje de correo electrónico cuando pueda descargarse el informe sobre la búsqueda de vulnerabilidades. La confirmación incluirá información sobre la cuenta y la contraseña de la URL para acceder a los resúmenes ejecutivos y a los informes de soluciones (nota: para los clientes de producción, la información de la contraseña de la cuenta se comunicará vía telefónica para garantizar la privacidad). Estos informes estarán disponibles para

consulta durante 30 días en un portal Web seguro y privado. Con el servicio de evaluación, solo se explorará un dominio o dirección IP en busca de vulnerabilidades; no obstante, el servicio real admite organizaciones con hasta más de 16 dominios.

Aspectos técnicos

8. **Pregunta:** ¿Cómo funciona la aplicación Web Application Security?

Respuesta: Puesto que las búsquedas de vulnerabilidades de Web Application Security forman parte de un servicio Web alojado, empezar a proteger sus sitios Web es una tarea rápida y sencilla dado que no se requiere instalar hardware o software adicional. Además, gracias a la seguridad alojada gestionada por Trend Micro, siempre podrá contar con la tecnología más reciente y la mejor protección.

- Después de la inscripción, Web Application Security explorará su sitio Web según el programa que haya definido para valorar las debilidades y vulnerabilidades.
- Tras la exploración, Web Application Security valorará el riesgo y le ofrecerá informes para que pueda actuar rápidamente y mejorar su seguridad.
- Estos informes describen el estado de seguridad de su sitio Web; recogen las posibles vulnerabilidades, la gravedad de los problemas así como el consejo recomendado por los expertos para solucionarlos. Las exploraciones a petición se ejecutan cuando usted las solicita con el fin de validar el éxito de sus acciones para solucionar los problemas de seguridad de su sitio Web.
- Si elige programar exploraciones diarias y cumple con nuestros criterios de seguridad, tendrá derecho a mostrar en su página Web el logotipo de marca de confianza de SecureSite, una prueba para los visitantes de su Web de que se adoptan medidas adicionales para proteger sus datos y privacidad en línea.
- Web Application Security supervisa constantemente la red Trend Micro Smart Protection Network en busca de indicios de ataque a sus sitios Web y le alerta de inmediato de la detección de contenido malicioso.

9. **Pregunta:** ¿Qué tipos de componentes de aplicaciones de sitios Web explora Web Application Security?

Respuesta:

Explora	Ejemplos	Protege frente a
Capa de aplicaciones	<p><u>Infraestructura Web:</u> Apache, Apache Tomcat, Microsoft Internet Explorer, Mozilla Firefox, Microsoft IIS, FTP, BEA Weblogic, Adobe ColdFusion, SSH, TELNET y cestas de la compra</p> <p><u>Web 2.0:</u> Aplicaciones JavaScript, AJAX y Adobe Flash</p> <p><u>Páginas Web:</u> Formularios y contenido residentes en el sitio Web</p>	<ul style="list-style-type: none"> • Peligro en los sitios Web por vulnerabilidades de secuencias de sitios cruzados (XSS) • Falseamiento de contenido • Rutinas de malware Javascript • Vulnerabilidades que pueden causar la denegación de servicios (DoS) en el sitio Web • Daño o sustracción de datos e identidades
Bases de datos	Oracle Microsoft SQL Server Sybase PostgreSQL Sun MySQL IBM DB2 IBM DB2/400 Lotus Notes/Lotus Domino	<ul style="list-style-type: none"> • Ataques SQL Injection destinados a robar datos de tarjetas de crédito e identidades • Problemas de configuración e incumplimiento de políticas

Sistemas de redes	Cortafuegos Cisco, IPSec, PPTP, Network File System (NFS), DHCP, DNS, LDAP, SNMP	<ul style="list-style-type: none"> • Problemas de configuración del sistema (por ej., contraseñas poco seguras) • Acceso no autorizado a los sistemas
Sistemas operativos	Microsoft Windows, Linux, Unix, Sun Solaris, Mac OS, BSC, IBM AIX, IBM AS/400, Novell NetWare	<ul style="list-style-type: none"> • Acceso al sistema operativo o puesta en peligro del mismo por infracciones de políticas como contraseñas fácilmente adivinables, permisos de archivos o acceso inadecuado a las cuentas

10. **Pregunta:** ¿Cómo me pueden configurar el servicio para explorar mis servidores Web?

Respuesta: Nuestro equipo de operaciones le enviará un formulario de configuración de Web Application Security donde podrá registrar los dominios o direcciones IP que desea que exploremos en busca de vulnerabilidades y de contenido malicioso.

11. **Pregunta:** ¿Funciona Web Application Security con un cortafuegos?

Respuesta: Sí. Aunque puede ser necesario que introduzca en la lista blanca de su cortafuegos/IDS/IPS la dirección IP del servidor de exploración de Trend Micro para evitar que la exploración se bloquee como un ataque malicioso.

12. **Pregunta:** ¿Web Application Security explora todo mi dominio o solo una parte del sitio Web?

Respuesta: La exploración seguirá los enlaces a todas las páginas del sitio Web que aparecen enumeradas bajo el dominio solicitado. No se realiza un seguimiento de los enlaces externos.

13. **Pregunta:** ¿Cuáles son las vulnerabilidades que busca Web Application Security?

Respuesta:

Habilitadores de fraudes/phishing	
Secuencias de sitios cruzados	Timan a los usuarios: La mayoría de los expertos e investigadores del sector coinciden en que las secuencias de sitios cruzados (XSS) siguen siendo la vulnerabilidad más habitual de los sitios Web. Según el sitio Web, las XSS pueden ser especialmente dañinas para las empresas y los consumidores. Los nuevos vectores de ataque empleados son responsables de fraudes por phishing muy efectivos y gusanos Web que son resistentes a los métodos de protección comúnmente aceptados. La evolución como rutina maliciosa del malware de JavaScript más reciente ha causado que la detección y la solución de esta vulnerabilidad sean más importantes que nunca antes.
Filtraciones de datos	
Filtraciones de información	Sustraen información de carácter privado: Las filtraciones de información tienen lugar cuando un sitio Web revela accidentalmente (o es manipulada para revelar) información confidencial como comentarios de los desarrolladores, información sobre los usuarios, direcciones IP internas, código fuente, números de revisión, mensajes/códigos de error, etc., que pueden ser de utilidad para un ciberdelincuente.

URL predecible	<p>Usa información pirateada de Google: Por lo general, el único mecanismo que protege la información confidencial es la predictibilidad de la URL. Los exploradores automáticos se han convertido en expertos en descubrir estos archivos realizando miles de intentos. Además, mediante un proceso denominado “Google Hacking” que consiste en piratear información de las bases de datos de este explorador, los ciberdelincuentes usan motores de búsqueda para detectar información confidencial mediante enlaces olvidados de un sitio Web.</p> <p>Encuentra páginas ocultas: Con el tiempo, muchas páginas de un sitio Web dejan de estar enlazadas, quedando huérfanas y olvidadas. Estas páginas Web suelen contener registros de pagos, copias de seguridad de software, futuras notas de prensa, mensajes de depuración o código fuente.</p>
SQL Injection	<p>Sustraer el contenido de bases de datos: El ataque SQL Injection ha estado involucrado en algunos de los sucesos más importantes de robo de identidades y de tarjetas de crédito. Las bases de datos actuales de los sitios Web almacenan información extremadamente confidencial, convirtiéndolas en un objetivo evidente y atractivo para los hackers maliciosos. En estos casos, son vulnerables al robo nombres, direcciones, números de teléfono, contraseñas, fechas de nacimiento, propiedad intelectual, secretos comerciales, claves de cifrado y otros muchos tipos de datos. Con tan solo colocar bien unas comillas, unos puntos y coma y unos comandos SQL toda una base de datos puede acabar en las manos equivocadas.</p>
Índices de directorios	<p>Encuentran páginas de carácter privado: Como una función de los servidores Web más utilizados, los índices de directorios enumeran los componentes de un directorio si no se ha creado un nombre de archivo específico o no tiene un archivo de índice (por ejemplo: index.html). Los listados de directorios pueden revelar información confidencial no destinada al público, como páginas Web previas a la publicación, archivos de registro, archivos temporales, archivos de copia de seguridad, etc.</p>
XPath Injection	<p>Extrae datos confidenciales: XPath Injection es una técnica de ataque, similar a SQL Injection, usada para aprovecharse de sitios Web que crean consultas XPath desde una entrada realizada por el usuario. Si un ciberdelincuente puede modificar una consulta XPath, podrá obtener información confidencial de un documento XML que, de lo contrario, no estaría a su alcance.</p>
Uso no autorizado	
Autenticación insuficiente	<p>Permite el acceso fraudulento: Los errores por autenticación insuficiente se suelen encontrar dentro de la lógica empresarial de una aplicación. Un ataque realizado correctamente permite al ciberdelincuente obtener acceso no autorizado a secciones protegidas de un sitio Web. Por ejemplo, con una sesión de usuario normal, un ciberdelincuente puede suplantar a otro usuario del sistema.</p>
Abuso de funcionalidad	<p>Usa las funciones del sitio Web contra el usuario/propietario: Como se indica en la clasificación de amenazas del Web Application Security Consortium, “El abuso de funcionalidad es una técnica de ataque que usa las propias capacidades y funcionalidades de un sitio Web para consumir, estafar o evadir mecanismos de control de acceso. Algunas funciones de un sitio Web, incluso funciones de seguridad, se pueden manipular para provocar un comportamiento inesperado. Cuando una función es vulnerable a su manipulación, un ciberdelincuente podría molestar a otros usuarios o estafar incluso a todo el sistema.”</p>
Desbordamiento del búfer	<p>Toma el control de los servidores: Se aprovecha de las vulnerabilidades del sitio Web para controlar un servidor y realizar actividades maliciosas.</p>

14. **Pregunta:** ¿Cuánto tiempo se invierte en una exploración?

Respuesta: El tiempo de exploración depende del tamaño de su sitio Web, del número de formularios del sitio Web y de la cantidad de vulnerabilidades detectadas en el mismo. La mayoría de las exploraciones de un solo dominio o dirección IP se puede realizar en menos de 15 minutos. Como parte del primer ciclo de la exploración, Trend Micro supervisará el tiempo de exploración de sus dominios y hosts para que usted pueda planificar de forma más eficaz las exploraciones futuras.

15. **Pregunta:** ¿Cómo afectan las exploraciones a mis servidores Web?

Respuesta: Web Application Security no utiliza técnicas de exploración que causen interrupciones en los servicios de la red. Sin embargo, ningún explorador de red puede garantizar que las exploraciones no causarán efectos colaterales ni alteraciones de todos los sistemas. Por ejemplo, explorar aplicaciones Web en busca de vulnerabilidades de secuencias de sitios cruzados y SQL Injection requiere que el servicio analice cada página del sitio Web de destino y envíe los formularios para la respuesta del servidor. Si tiene alguna pregunta al respecto, póngase en contacto con Trend Micro en wfss_support@trendmicro.com.

16. **Pregunta:** ¿Qué tipos de informes sobre vulnerabilidades hay disponibles?

Respuesta: Web Application Security ofrece resúmenes ejecutivos e informes de soluciones.

- **Resumen ejecutivo:** Ofrece una visión general de alto nivel de los resultados de las auditorías de seguridad, con vistas resumidas y tablas que ilustran el estado de la red y los servidores Web, incluyendo las vulnerabilidades existentes por gravedad y categoría.
- **Informe de soluciones:** Ofrece una valoración detallada que identifica los riesgos de seguridad que pueden influir negativamente en sus operaciones y activos Web más importantes. En este informe se cuantifican los riesgos y se genera un índice de riesgos general para cada sistema, lo que le permite priorizar convenientemente sus actividades de resolución. Para cada host y vulnerabilidad se define un completo plan de solución y un conjunto de acciones recomendadas junto con el tiempo estimado necesario para resolver el problema.

17. **Pregunta:** ¿Pueden recibir los usuarios notificaciones por correo de los resultados de la exploración de seguridad?

Respuesta: Sí. Cuando Web Application Security acaba las exploraciones y publica los informes correspondientes en el portal Web el usuario recibe un mensaje de correo electrónico. Asimismo, si hay contenido malicioso en su sitio Web y Trend Micro Smart Protection Network lo detecta, el usuario recibe una alerta inmediata con los detalles del sitio Web infectado y del malware hallado.

18. **Pregunta:** ¿Qué formatos de archivos de informes puede generar Web Application Security?

Respuesta: Los informes se publican en formato PDF y únicamente se puede acceder a ellos mediante una cuenta en nuestro portal Web de seguridad en línea.

19. **Pregunta:** ¿Cómo se valora la gravedad en los informes?

Respuesta: Usamos el sistema de puntuación CVSS (Common Vulnerability Scoring System) que asigna una puntuación del 1 al 10 a cada vulnerabilidad: <http://nvd.nist.gov/cvss.cfm>. También asignamos nuestra escala del 1 al 10 a la escala PCI para poder crear informes PCI. Los informes PCI usarán la gravedad y categoría PCI, las cuales no suelen estar relacionadas con lo que nosotros consideramos gravedad (por ej., toda denegación de servicio = 3, todos los gusanos = 5, etc.).

20. **Pregunta:** ¿Cómo se asocian las amenazas críticas/graves/moderadas a CVSS?

Respuesta:

- **Crítica:** vulnerabilidad en un sistema que es fácilmente accesible, requiere poca o ninguna autenticación y ofrecerá la posibilidad de acceder a información confidencial, dañar/eliminar datos o crear un fallo en el sistema. Una puntuación entre 8 y 10 en el sistema CVSS. Ejemplos: No hay ninguna contraseña en la cuenta de administrador CIFS; los usuarios anónimos pueden obtener la política de contraseñas de Windows.

- **Grave:** vulnerabilidad en un sistema que es accesible con un nivel moderado de experiencia, puede o no requerir autenticación y ofrecerá acceso parcial a información restringida, acceso para destruir alguna información o desactivar los sistemas individuales de una red. Una puntuación entre 4 y 7 en el sistema CVSS. Ejemplos: FTP anónimo en el que se puede escribir; se permite un hash débil del administrador de la red.
- **Moderada:** vulnerabilidad en un sistema que es accesible de forma local, requiere autenticación y ofrecerá poco o ningún acceso a información restringida, no puede destruir o dañar información ni puede causar fallos en ningún sistema. Una puntuación entre 1 y 3 en el sistema CVSS. Ejemplos: Nombre de comunidad SNMP predeterminados o adivinables: público, vulnerabilidad de detección del estado interno de OpenSSL PRNG.

21. **Pregunta:** ¿Qué significan los distintos niveles de gravedad en los informes sobre valoración de vulnerabilidades?

Respuesta: Las vulnerabilidades críticas son aquellas que se pueden utilizar de forma remota, permiten acceso raíz o de administrador o tienen gusanos o virus circulando activamente. Las vulnerabilidades graves son aquellas que solo se pueden usar localmente, no permiten acceso raíz ni vulnerabilidades de denegación de servicio. Las vulnerabilidades moderadas son aquellas que filtran información potencialmente confidencial y podrían usarse junto con otras vulnerabilidades para lanzar un ataque.