



¿ESTÁ SU SITIO WEB
A SALVO DE HACKERS?

Realice auditorías de seguridad con Acunetix

Hasta el 70% de los sitios Web tienen vulnerabilidades que podrían llevar al robo de información sensible de las empresas tal como información de tarjetas de crédito y listados de sus clientes.

Los hackers están concentrando sus esfuerzos en aplicaciones basadas en Web - carritos de la compra, formularios, acceso restringido a páginas, contenido dinámico, etc. Accesible 24/7 desde cualquier parte del mundo, las aplicaciones Web inseguras facilitan el acceso a bases de datos corporativas y permiten también acceder a los hackers para llevar a cabo actividades ilegales utilizando el sitio atacado.

Firewalls, seguridad SSL y bloqueo de servidores son inútiles contra hackeos de servidores Web

Ataques enfocados a aplicaciones Web, lanzados contra el puerto 80/443 pasan directamente a través del cortafuegos, saltándose la seguridad a nivel de la red y del sistema operativo y se dirigen directamente al corazón de su aplicación y los datos corporativos. Las aplicaciones Web hechas a medida son a menudo insuficientemente testeadas, tienen vulnerabilidades por descubrir y por lo tanto son presa fácil para los hackers.

Averigüe si su sitio es seguro antes de que los piratas informáticos descarguen datos sensibles, cometan un delito utilizando de su sitio Web como plataforma de lanzamiento y pongan en peligro su negocio. Acunetix Web Vulnerability Scanner rastrea su sitio Web, analiza automáticamente sus aplicaciones Web y encuentra vulnerabilidades por inyección de SQL, Cross Site Scripting y otras vulnerabilidades que puedan dejar expuesto su negocio online. Informes concisos permiten identificar en que punto necesitan ser parcheadas sus aplicaciones Web y permitiendo por tanto proteger su negocio de inminentes ataques de piratas informáticos.

ANÁLISIS EXHAUSTIVO para SQL Injection y vulnerabilidades Cross Site Scripting (XSS)

Acunetix es líder en detección de SQL Injection y vulnerabilidades XSS. Acunetix tiene un índice de detección muy alto para los dos mayores defectos - SQL injection y Cross Site Scripting; al tener una tasa tan baja de falsos positivos permite a los analistas de seguridad discutir sobre las amenazas reales.

No todo el mundo puede presumir de detectar las últimas amenazas XSS Como Blind XSS y DOM-based XSS. La detección de estas vulnerabilidades requiere de un analizador sofisticado. El indexado tradicional y las tecnologías de análisis son simplemente insuficientes. Acunetix hace uso de **AcuMonitor** para ir un paso más allá que los hackers y detectar vulnerabilidades sofisticadas como Blind XSS y Mail Header Injection..

REMEDIACIÓN MÁS RÁPIDA con la tecnología AcuSensor

Esta tecnología de seguridad propietaria garantiza un mayor nivel de detección de vulnerabilidades y reducción de falsos positivos junto con la detección precisa del lugar dónde se encuentra la vulnerabilidad en el código fuente. El resultado es una remediación más rápida de las Vulnerabilidades comparado con otros analizadores del mercado.

SOPORTE HTML5 COMPLETO con Acunetix DeepScan

Impulsado por el motor de renderizado utilizado en Chrome y Safari, Acunetix DeepScan permite que nuestros analizadores interpreten por completo los sitios web, aplicaciones web y sitios web móviles, incluyendo los sitios implementados con HTML5 y tecnologías basadas en JavaScript como AJAX y Single Page Applications. Mediante su interpretación avanzada de JavaScript, Acunetix DeepScan se utiliza de forma automática para detectar vulnerabilidades DOM-based y XSS.

ANALICE ÁREAS PROTEGIDAS POR CONTRASEÑA Automáticamente

Acunetix es capaz de rellenar automáticamente formularios web y autenticarse con Un login. Muchos analizadores son incapaces de hacerlo o bien requieren de scripts complejos. Utilizando la herramienta de Acunetix, Login Sequence Recorder, se puede grabar la secuencia de login, relleno de campos o una secuencia específica de indexado. El analizador reproduce la secuencia durante el proceso de análisis y Rellena los formularios web y se valida en las áreas protegidas por contraseña automáticamente.

ANALICE MÚLTIPLES SITIOS WEB En cualquier lugar y momento

Lance análisis contra todos sus sitios web. Con las soluciones Acunetix en local y online podrá lanzar análisis inmediatos o planificarlos para más tarde, y recoger Los resultados desde cualquier lugar y en cualquier momento.

INFORMES EXHAUSTIVOS para Cumplimiento Legal y de Normativas

Su aplicación web y servidores perimetrales cumplen con las normativas de la Industria y con las regulaciones? Deje que Acunetix le ayude con su módulo de informes extensivo y detallado que cubre un amplio rango de estándares incluyendo:

- CWE/SANS Top 25 Most Dangerous Software Errors
- The Health Insurance Portability and Accountability Act (HIPAA)
- International Standard - ISO 27001
- NIST Special Publication 800-53 - Recommended Security Controls for Federal Information Systems
- OWASP TOP 10 2013
- Payment Card Industry Data Security Standard version 3.0
- Sarbanes-Oxley Act
- DISA STIG Web Security
- Web Application Security Consortium: Threat Classification

LÍDER MUNDIAL EN SEGURIDAD DE APLICACIONES WEB

Acunetix ha sido pionero en la tecnología de análisis de seguridad de aplicaciones Web: Sus ingenieros se centraron en seguridad Web en 1997 y han desarrollado una ingeniería de peso en el análisis de sitios Web y detección de vulnerabilidades.



ACABE CON LOS BUSCADORES DE VULNERABILIDADES DE HACKERS

Acunetix lanza consultas desde Google Hacking Database (GHDB) contra el contenido indexado de su sitio web, identificando datos sensibles o bien objetivos que puedan ser explotados antes de que lo haga el hacker.

IDENTIFICACIÓN AUTOMÁTICA de páginas de error 404

Determine automáticamente si una página de error personalizada está en uso e identifíquela sin necesidad de crear patrones de reconocimiento Antes del análisis

SERVIDOR DE SEGURIDAD PERIMETRAL

Acunetix lanza análisis de puertos contra el servidor que alberga la página web, identifica automáticamente servicios de red que se ejecuten en puertos abiertos y lanza una serie de test de seguridad contra los servicios de red. Existe la posibilidad de crear alertas de red utilizando el SDK de Acunetix.

Los test de seguridad incluidos en el producto son:

- Test para contraseñas débiles en servidores FTP, IMAP, SQL, POP3, Socks, SSH, Telnet y otras vulnerabilidades DNS como Open Zone Transfer, Open Recursion, Cache Poisoning,
- Test de acceso FTP como si se permitiese el acceso anónimo y el listado de directorios FTP escribibles, test de seguridad Servidores Proxy mal configurados
- Test para SNMP Community String,
- Test para cifrados SSL débiles,
- Y muchos otros test de seguridad sofisticados.

Adicionalmente la solución online utiliza OpenVAS – la red de análisis de vulnerabilidades líder y, por lo tanto, haciendo uso de de una base de datos de decenas de miles de test de seguridad de nivel de red.

HERRAMIENTAS DE PENETRACIÓN AVANZADA

Adicionalmente a su motor de análisis automatizado, Acunetix incluye herramientas avanzadas que permiten afinar las auditorías de aplicaciones web:

Editor HTTP – Construye peticiones HTTP/HTTPS y analiza la respuesta del servidor web.

HTTP Sniffer - Intercepta, registra y modifica todo el tráfico HTTP/HTTPS y revela los datos enviados por el navegador y por la aplicación web.

HTTP Fuzzer – Realiza pruebas difusas sofisticadas para probar la validación de input de aplicaciones web y la gestión de datos inválidos o inesperados Prueba miles de parámetros de entrada con el sencillo constructor de reglas de HTTP Fuzzer. Pruebas que necesitarían días para ejecutarse manualmente se realizan en minutos.

Blind SQL Injector – Una herramienta de extracción de datos automatizada ideal para pruebas de penetración para los que quieran ir más allá.

MÁS FUNCIONES AVANZADAS

- Detecta vulnerabilidades HTTP Parameter Pollution (HPP)
- Soporte para cabeceras HTTP personalizadas en análisis automatizados.
- Soporte para múltiples credenciales de autenticación HTTP.
- Perfiles de análisis para analizar sitios web con diferentes opciones de análisis e identidades.
- Generador de informes personalizado.
- Compara análisis y encuentra diferencias con análisis anteriores.
- Vuelve a auditar cambios de un sitio web de forma fácil con la opción Rescan.
- Soporte para CAPTCHA, Single Sign-On y autenticación que utilice mecanismos Two Factor
- Detecta directorios con permisos débiles y si se han habilitado métodos HTTP peligrosos.
- Genera una lista respuestas HTTP inusuales como error internos de servidor, HTTP 500, etc.
- Personaliza la lista de falsos positivos.
- Auditoría de seguridad de la configuración de servidor web.
- Auto-importación de reglas “rewrite” de IIS 7 desde web.config.file.
- Habilidad para re-analizar una vulnerabilidad específica tras su remediación.
- Automatiza el análisis de vulnerabilidades de formularios de carga de ficheros.



INFORMACIÓN DE CONTACTO:

