acunetix

¿ESTÁ SU SITIO WEB A SALVO DE HACKERS?

Verifíquelo con Acunetix Web Vulnerability Scanner

Realice auditorías de seguridad de su sitio Web con Acunetix Web Vulnerability Scanner

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. Una Web víctima de un ataque puede ser utilizada para poner en marcha actividades delictivas como el alojamiento de sitios de phishing o transferir contenidos ilícitos, mientras que abusa del ancho de banda de la página Web y hace a su titular responsable de estos actos.

Los cortafuegos, seguridad SSL y bloqueo de servidores son inútiles contra los ataques a servidores de aplicaciones 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 probadas, 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.

Acunetix - 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.

Acunetix Web Vulnerability Scanner incluye varias características innovadoras:

- Un analizador automático de JavaScript que permite realizar pruebas de seguridad de Ajax y aplicaciones Web 2.0
- Dispone de los test más avanzados y profundos de análisis y pruebas de Inyección de SQL y Cross Site Scripting.
- El grabador de macros hace que las pruebas sobre los formularios de las áreas protegidas de la Web sean más fáciles.
- Diversos tipos de informes, incluidos informes de conformidad VISA PCI.
- El analizador de vulnerabilidades, rapidísimo y multitarea, rastrea cientos de miles de páginas con facilidad.
- Pruebas de vulnerabilidad de carga automatizada de informes.
- Acunetix rastrea y analiza los sitios Web incluyendo el contenido de Flash, AJAX y SOAP
- Innovadora Tecnología AcuSensor que permite la exploración precisa de muchas vulnerabilidades.
- Análisis de puertos red y alertas contra el servidor Web para complejos controles de seguridad.

Clientes de Acunetix

NASA
US Army
US Air Force
KPMG
Disney
Bank of China
Fujitsu
Hewlett Packard
AmSouth Bank
US Department of Energy
California Department of Justice
Wescom Credit Union
Trend Micro
State of North Carolina
US Geological Service
France Telecom
ActionAid UK
University of Reading
PricewaterhouseCoopers Australia
CERN, Switzerland
Panasonic Asia Pacific
The Armed Forces of Norway
Credit Suisse

En la prensa:

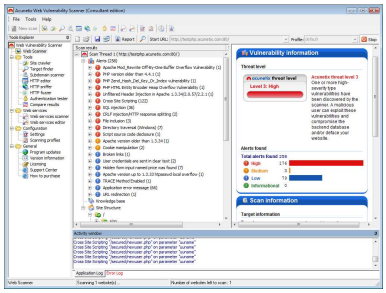
"Acunetix WVS no sólo le muestra las vulnerabilidades de su sitio Web. También ofrece información y herramientas que le permitirán realizar verificaciones en sus aplicaciones Web. Es una herramienta importante para desarrolladores Web. Personalizable y, por lo tanto, se presta muy bien a pruebas en profundidad."

Help Net Security

Análisis en profundidad para comprobar vulnerabilidades de Inyección de SQL, Cross Site Scripting (XSS) y otros utilizando la innovadora Tecnología AcuSensor

Acunetix analiza todas las puntos vulnerables de la Web incluyendo Inyecciones de SQL, Cross Site Scripting y otros. La Inyección de SQL es una técnica de hacking que modifica las consultas SQL a fin de obtener acceso a los datos de la base de datos. Los ataques de Cross Site Scripting permiten que un hacker ejecute un script malicioso en el navegador Web de sus visitantes.

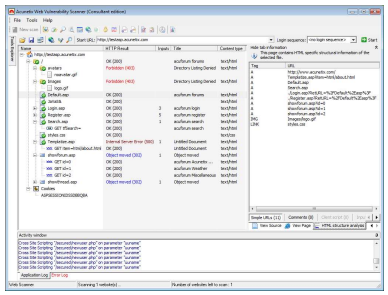
La detección de estas vulnerabilidades requieren de un sofisticado motor de detección.
Pero más importante que el análisis de vulnerabilidades Web no es la cantidad de ataques que puede analizar si no la complejidad y el rigor con el que el analizador lanza ataques de Inyección de SQL, Cross Site Scripting y otros ataques.
Acunetix tiene un avanzado motor de detección de la vulnerabilidades que utilizar la **tecnología pionera AcuSensor**. Esta es una tecnología de seguridad única que detecta rápidamente vulnerabilidades con un bajo número de falsos positivos, indica dónde se encuentra la vulnerabilidad en el código y realiza informes de depuración. También es capaz de localizar Inyecciones CRLF, ejecución de código, Directory Traversal, inclusión de archivos, vulnerabilidades de autenticación y otras muchas más.



Acunetix realiza ataques automatizados y muestra las vulnerabilidades encontradas

Analice AJAX y la Web 2.0 en busca de vulnerabilidades

El motor de análisis CSA (analizador de secuencia de comandos de cliente) le permite realizar una exploración exhaustiva de las más actuales y complejas aplicaciones Web en AJAX / Web 2.0 y detectar vulnerabilidades.



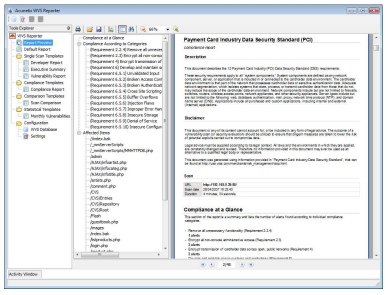
Acunetix analiza automáticamente el sitio web y muestra su estructura

Análisis de puertos y alertas de red

Acunetix Web Vulnerability Scanner también puede lanzar, opcionalmente, análisis de puertos contra el servidor Web cuando el sitio está alojado, e identifica automáticamente el servicio de red que se está ejecutando en un puerto abierto, lanzando una serie de pruebas de seguridad contra el servicio Web. Se pueden desarrollar también alertas de red personalizadas siguiendo la documentación detallada proporcionada por Acunetix.
Los controles de seguridad que se incluyen con el producto son: pruebas de fortaleza de contraseñas de FTP, IMAP, servidores SQL, Socks, SSH, Telnet y otras vulnerabilidades de servidores DNS como Open Zone Transfer, Open Recursion, Caché Poisoning, así como pruebas de acceso FTP anónimo como si se permitiese el acceso y el listado de directorios FTP, tests de seguridad para servidores Proxy mal configurados, controla debilidades de SNMP Community String, algoritmos de cifrado SSL débiles, y otros controles de seguridad sofisticados.

Los informes detallados le permiten cumplir normativas Jurídicas y de Conformidad.

Acunetix Web Vulnerability Scanner incluye un amplio módulo de reporting que permite generar informes que indiquen si sus aplicaciones Web satisfacen los nuevos requisitos de VISA PCI Data Compliance entre otros.



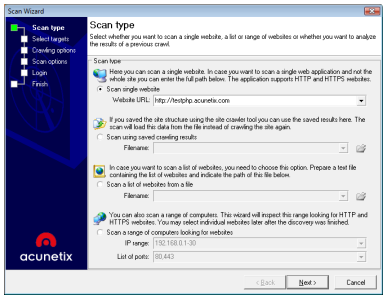
Múltiples informes incluyendo conformidad VISA PCI

Analiza su sitio utilizando la base de datos de Google Hacking

La Google Hacking Database (GHDB) es una base de datos de consultas utilizada por los hackers para identificar datos sensibles en su sitio Web tales como páginas de inicio de sesión de portales, registros de información de seguridad de la red y así sucesivamente.
Acunetix lanza las consultas almacenadas en la base de datos de Hacking de Google contra todo el contenido de su sitio Web e identifica los datos sensibles y objetivos fácilmente explotables antes de que un "motor de búsqueda de hackers" lo haga.

Realice pruebas de áreas protegidas por contraseñas y formularios web con relleno automático de formularios HTML

Acunetix Web Vulnerability Scanner es capaz de rellenar automáticamente formularios Web y autenticarse contra accesos Web. La mayoría de los escáneres de vulnerabilidad Web no son capaces de realizar estas operaciones o requieren complejas secuencias de comandos para realizar pruebas en estas páginas. No así con Acunetix: Utilizando la herramienta de grabación de macros se puede grabar un inicio de sesión o un proceso de rellenado de formulario y almacenar la secuencia. El escáner puede entonces reproducir esta secuencia durante el proceso de análisis y rellenar automáticamente formularios Web o contraseñas o iniciar sesiones en las áreas protegidas.



Asistente fácil y rápido para lanzar un análisis

Avanzadas herramientas de pruebas de penetración incluidas

Además de su motor de búsqueda automatizada, Acunetix incluye herramientas avanzadas para permitir a los testers de pruebas de penetración afinar las pruebas de seguridad de aplicaciones Web:

- Editor HTTP - Con esta herramienta puede crear fácilmente solicitudes HTTP / HTTPS y analizar las respuestas del servidor Web.
- HTTP Sniffer - Intercepte, registre y modifique todo el tráfico HTTP / HTTPS revelando todos los datos enviados por una aplicación Web.
- HTTP Fuzzer - Realice pruebas sofisticadas contra desbordamientos de memoria y de validación de entrada. Pruebe miles de variables de entrada con el constructor de reglas HTTP Fuzzer. Pruebas que necesitarían normalmente días para realizarse pueden hacerse en minutos.
- Cree ataques personalizados o modifique los existentes con el Editor de Vulnerabilidades .
- Blind SQL Injector - Una base de datos de extracción de datos automatizada ideal para realizar pruebas de penetración para testers que deseen realizar más pruebas manualmente.

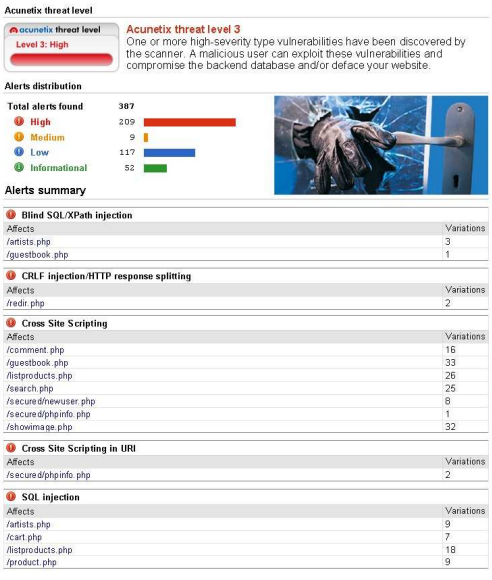
Muchas más funciones avanzadas

Analizar perfiles para escanear páginas Web fácilmente con diferentes opciones de exploración y de identidades:

- Generador de informes personalizados
- Compare exploraciones y encuentre las diferencias con las realizadas anteriormente
- Realiza fácilmente auditorías de los cambios realizados en la Web
- Descubre directorios con permisos débiles
- Analiza aplicaciones Web populares (por ejemplo, foros, carritos de la compra), y detecta sus versiones vulnerables
- Detecta si hay métodos HTTP peligrosos habilitados en su servidor Web
- Genera una lista de respuestas http poco comunes tales como Error interno del servidor, HTTP 500, etc.
- Personaliza la lista de falsos positivos

Versiones disponibles – Small Business, Enterprise y Consultant

Acunetix Web Vulnerability Scanner está disponible en tres versiones: Una versión de Small Business para un sitio Web designado, una versión Enterprise para permitir el análisis de un número ilimitado de sitios Web y una versión Consultor que permite usar Acunetix WVS para realizar pruebas de penetración a terceros.



Acunetix threat level

Acunetix threat level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	387
High	209
Medium	9
Low	117
Informational	52

Alerts summary

Blind SQL/XPath injection

Affects	Variations
/artists.php	3
/guestbook.php	1

CRLF injection/HTTP response splitting

Affects	Variations
/redir.php	2

Cross Site Scripting

Affects	Variations
/comment.php	16
/guestbook.php	33
/listproducts.php	26
/search.php	25
/secured/newuser.php	8
/secured/phpinfo.php	1
/showimage.php	32

Cross Site Scripting in URI

Affects	Variations
/secured/phpinfo.php	2

SQL injection

Affects	Variations
/artists.php	9
/cart.php	7
/listproducts.php	18
/product.php	9

Ejemplo de un resultado de análisis

"Acunetix WVS ha jugado un papel muy importante a la hora de identificar y mitigar fallos en aplicaciones Web. El gasto ha merecido la pena."

Mr Rodgers
IT Security Team
U.S. Air Force

"Las vulnerabilidades localizadas fueron de gran impacto; si hubiesen encontrado los agujeros de seguridad podrían haber hackeado un sitio Web de Joomla entero!"

Robin Muilvijk,
Member of the Quality & Testing Team,
Joomla!

"El uso de Acunetix WVS nos ha permitido programar análisis de sitios alojados en Betfair Group otorgando una gran visibilidad y capturando vulnerabilidades rápidamente en SDLC."

Jan Ettles
Betfair.com, UK

"Confiamos en Acunetix WVS para que nos dé unos buenos cimientos y proveer al mercado de servicios de seguridad y protección para nuestros clientes."

Jason Remillard
Founder and President
Sitesecuritymonitor.com

"Acunetix WVS realiza las pruebas de penetración más tediosas y recurrentes en un suspiro, reduciendo el tiempo necesario y aumentando la calidad de los tests"

Thierry Zoller
Telindus PSF
Luxembourg

Qué cambios ofrece la versión 7 de Acunetix Web Vulnerability Scanner?

La mayoría de los componentes principales de la versión 7 de Acunetix WVS han sido rediseñados.
Es un 75% más rápido utilizando un nuevo motor de análisis más rápido e inteligente.
En la versión 7 usted puede crear sus propios scripts de análisis de vulnerabilidades de red y Web puesto que la base de datos de vulnerabilidades ha sido migrada a script. El scripting también permite el uso de tests de seguridad más avanzados y flexibles al tiempo que reduce los falsos positivos.
La versión 7 también incluye tests de seguridad más meticulosos, algunos de los cuales no se podían realizar en versiones anteriores.

Resumen de nuevas funciones:

- Nuevo y revolucionario motor de análisis que permite detectar un mayor abanico de vulnerabilidades.
- Menos falsos positivos y negativos; utiliza técnicas de vulnerabilidades casi humanas!
- Soporte mejorado de aplicaciones Web 2.0; gestión mejorada de JSON y XML
- Mejora en la gestión y en las técnicas de detección de links y de parametros introducidos
- Consolidación de vulnerabilidades para facilitar la coordinación de soluciones de vulnerablidades
- Menos posibilidades de dejar sin servicio un sitio Web; análisis avanzado de capa presentación del sitio Web
- Mejoras en el manejo del gestor de sesiones de aplicaciones Web 2.0
- Nueva interfaz de estado de análisis con detalles granulares para el usuario
- Habilidad para reanalizar una vulnerabilidad específica para verificar la solución aplicada
- Configuración de Autenticación HTTP; soporta múltiples credenciales de autenticación
- Soporta un mayor abanico de tipos de contenido
- Gestión mejorada y más veloz del tráfico de red; soporte para DNS caching, keep-alive, etc
- Añadidas nuevas técnicas de auditoría de seguridad Web
- Se ha mejorado drásticamente los tests de seguridad de carga de ficheros
- Soporte para una mayor variedad de mecanismos de comunicación
- Nueva herramienta "Acunetix Scripting Tool" para asistir a la creación de nuevos scripts
- Habilidad para enviar y corregir automáticamente datos relevantes en web forms

Requisitos del Sistema:

- Windows XP, Vista, 2000, 2003 y 2008 server, Windows 7
- Internet Explorer 6 o superior
- 250 MB de espacio en disco
- 1GB de RAM

Acunetix Ltd
6th Floor
Portomaso Tower
PTM 01, Portomaso
Malta

Tel: (+356) 2316 8000
Fax: (+356) 2138 8099

Acunetix (USA)

Tel: (+1) 877 260 8931
Fax: (+1) 425 650 6873

Acunetix (UK)
Unit 2, St John Mews
St John Road, Hampton Wick
KT1 4AN
Kingston upon Thames
United Kingdom

Tel: (+44) 0800 0517577
Fax: (+44) 0844 8732291

Distribuido por:

SATINFO
Mayorista Oficial en España

c/Nápoles 335
08025 BARCELONA
www.satinfo.es
comercial@satinfo.es
Telf: 93 459 01 00
Fax: 93 207 39 59