Acunetix Web Vulnerability Scanner es una herramienta de seguridad de aplicaciones Web automatizada. Acunetix WVS es capaz de escanear cualquier sitio Web o aplicación Web que es accesible a través del protocolo HTTP / HTTPS. Sin embargo, no todas las pruebas se puede realizar de forma automática, y por lo tanto Acunetix WVS proporciona herramientas de Penetración manuales para pruebas particulares.

- Acunetix es una herramienta automatizada de pruebas de seguridad de aplicaciones Web
- Comprueba diferentes vulnerabilidades (por ejemplo inyección de SQL, Cross Site Scripting). Hasta la fecha Acunetix comprueba sobre más de 500 tipos diferentes de vulnerabilidades.
- Acunetix puede escanear cualquier sitio Web que es accesible a través del protocolo HTTP / HTTPS, básicamente, si el sitio Web se puede ver en un navegador, Acunetix puede escanearlo.
- Nuestra herramienta también proporciona herramientas de pruebas de penetración manuales que aumentan y contribuyen a las pruebas automatizadas, así como ayudar con la prueba de vulnerabilidades lógicas

Tecnologías propiedad de Acunetix

AcuMonitor: Es un servicio intermediario que ayuda al usuario a detectar vulnerabilidades que han podido ser inyectadas en la Website pero no son aparentes hasta que se ejecuta algo específico de la Website y hace que la vulnerabilidad se active. En este caso se envía inmediatamente un email al usuario informando de los detalles de la vulnerabilidad.

Acusensor: Es un plug- in que obtiene más información del código; de como las Websites se han creado y lo envía a WVS. Ayuda a detectar más vulnerabilidades mientras genera menos falsos positivos. Además indica exactamente donde en el código esta la vulnerabilidad e informa como depurarlo.

DeepScan: Es la última tecnología revolucionaria de Acunetix Web Vulnerability Scanner, puede escanear y analizar HTML5 y aplicaciones Web basadas en JavaScript. Es el único escáner de vulnerabilidades Web en el mercado capaz de realizar esto. Las Aplicaciones Web basadas en HTML5 están utilizando una gran variedad de bibliotecas complejas de JavaScript como AngularJS, Backbone.js, Ember.js y SproutCore. DeepScan también permite el escaneo de Aplicaciones Single Page (SPA), además de mejorar la detención de vulnerabilidades Cross Site Scripting basados en DOM.

Como funciona Acunetix WVS

1. ***Crawling (rastreador)*** - El rastreador analiza la Website entera desde la URL inicial para descubrir todos los directorios y archivos. A continuación, revisará y analizará la estructura completa de directorios del sitio Web.

2. ***Después Acunetix lanza un Escaneo de vulnerabilidades*** - Acunetix WVS lanzará una serie de ataques de vulnerabilidades en cada página. A continuación Acunetix lanzará pruebas en contra de los controles en cada página, similar a lo que los hackers podrían hacer para atacar a un sitio Web.

3. ***Esta exploración o escaneo producirá resultados que se muestran en el nodo de Alertas -*** Todas las vulnerabilidades encontradas se mostrarán con información detallada en la interfaz gráfica del software en la zona de alerta (AlertsNode). Cada alerta contiene información acerca de la vulnerabilidad, ejemplos posibles para su solución, y CVE, CWE, e información CVSS.

4. ***Por último, el usuario puede crear diferentes Informes y Remediación -*** Acunetix es capaz de exportar las vulnerabilidades encontradas en una variedad de informes diferentes. Y la comprobación o escaneo de alertas específicas permite fijar y probar las vulnerabilidades de forma individual en lugar de volver a ejecutar una exploración o escaneo completo.