# Tema: Discovering Security Vulnerabilities and Leaks in ASP.NET Websites

## Síntesis:

Las vulnerabilidades de seguridad no pueden ser detectados tan fácilmente por el propietario del sitio web, en este artículo se describe un algoritmo que tiene como objetivo la detección de vulnerabilidades de seguridad, en este caso de “.net”. El algoritmo tiene como objetivo ayudar a la organización, corregir las vulnerabilidades y mejorar la seguridad en general

Este es un programa escrito con la intención de generar un informe que describe la mayoría de las fugas y los tipos de vulnerabilidades mencionando el nombre del archivo, la descripción de la fuga y su ubicación. Prácticamente este código se base en estudiar el Código fuente de la aplicación a cargo de los archivos ASP.

.Net nos sirve para montar sitios web dinámicos, aplicaciones web y servicios web. Esto es debido a que posee mejor soporte de lenguaje y sus características distintivas como programación impulsada por controles de servidor fácil y rápido en el uso de su entorno de desarrollo.

Actualmente muchas organizaciones e individuos dependen de sitios web en .Net, lo que permite a un usuario malintencionado explotar las debilidades del sitio web buscando una vulnerabilidad de seguridad para inyectar su Código malicioso. De aquí surge la necesidad de una herramienta para probar sitios web aplicaciones escritas en el lenguaje ASP.

Al presente, existen muchos tipos de vulnerabilidades que varían en términos de complejidad, detección y recuperación. Un claro ejemlo son las inyecciones SQL, la cual es una forma de ataque que puede ocurrir cuando una aplicación usa una entrada del usuario que no ha sido verificada en el sitio para ver si es válida.

Por otra parte, el Cross Site Scripting ('XSS'), es uno de los ataques a la capa de aplicación más comunes, este se aprovecha de una vulnerabilidad del sitio web en la que el sitio muestra contenido que incluye datos no desinfectados proporcionados por el usuario. Normalmente sucede en páginas web dinámicas que mezclan datos del navegador (HTML) con el código (etiqueta <script>) que está incrustado en los datos.

Es necesario reducir las vulnerabilidades de seguridad en nuestros, para lograrlo, el desarrollador debe de ser consciente de la gran responsabilidad de seguridad en la aplicación desde la iniciación en la programación.

Referencia: Al-Amro H., El-Qawasmeh, E., “Discovering Security Vulnerabilities and Leaks in ASP.NET Websites”, Information Systems Department King Saud University, KSU Riyadh, pp. 329 – 333.