Vulnerabilidades y filtraciones en webs con ASP.NET

Brandon David Meza Vargas - 3CV11

Hoy en día hay muchos sitios hechos con ASP.NET debido al amplio soporte de este lenguaje así como sus diversas funcionalidades. Es muy usado para crear sitios web dinámicos. De esta manera se propone un algoritmo para mejorar la seguridad de sitios hechos con ASP.NET

TIPOS DE VULNERABILIDADES

SQL INJECTION

Este tipo de ataques puede ocurrir cuando las entradas de los usuarios no son verificadas para saber si son válidas, los hackers pueden introducir entradas maliciosasque pueden ejecutar acciones en la base de datos, por ejemplo pueden borrar la base de datos u obtener información valiosa de ella

CROSS-SITE SCRIPTING

Estos ataques suceden principalmente en sitios dinámicos que son una mezcla de datos del navegador con el código <script> que esta embebido en los datos. Su objetivo es manipular los scripts del lado del cliente

ALGORITMO PARA MEJORAR LA SEGURIDAD

A continuación se presenta un algoritmo de 12 pasos donde cada apso maneja cada filtración

1. Validar si "ValidateRequest" en el web.config existe y si tiene un valor falso, despues reportar que hay una filtración
2. Verificar si el atributo "Debug" no existe, esto significa que su valor es verdadero y reportar que hay una filtración
3. Verificar que el atributo "Debug" no existe en wl web.config
4. Verificar si el atributo "customErrors" en el web.config exista y tega el valor off
5. Verificar si el atributo "customErrors" no existe en el web.config y reportar que hay una filtración
6. Verificar si el atributo "validateRequest" en .aspx existe y tiene el valor de false
7. Verificar si algun nombre de ID de una TextBox en .aspx no esta validada usando RegularExpressionValidator
8. Verificar si hay alguna concatenación con algún query
9. Definir metodos anti XSS que códifique los elementos HTML
10. Verificar si el comando "Response.Write" y el comando "<%=%>" no tienen algun método anti XSS y reportar que hay una filtración
11. Verificar que los comandos "Request.Params, Request.Form, Request.QueryString, Request.Cookies, Request" no tenga algún método anti XSS y reportarlo
12. Verificar si el comando "<%=%>" tiene la función Eval