TA-004: Desarrollo Código Seguro OWASP & .NET

Antecedentes

La relación tan estrecha que tenemos con la tecnología nos obliga a tener un esquema de interacción seguro con todo el software que integramos en nuestra vida diaria. El riesgo de utilizar software inseguro sin duda tiene impacto en sectores críticos de nuestra sociedad: sea el sector financiero, de salud, defensa, energía y otras infraestructuras, todos expuestos a riesgos graves y significativos con pérdidas económicas incalculables.

Por esta y más razones no nos podemos dar el lujo de tolerar problemas de seguridad relativamente sencillos, como los que son parte del día a día; es así que con el objetivo de disminuir el impacto contra estos riesgos, contamos con el apoyo de un proyecto abierto que es el OWASP Top 10, que tiene como objetivo crear conciencia acerca de la seguridad en aplicaciones mediante la identificación de los riesgos más críticos que enfrentan las organizaciones.

En esta capacitación, el propósito es detallar este proyecto de OWASP Top 10 y su relación con su implementación práctica en el desarrollo con la plataforma .NET.

Objetivo General del Curso

El objetivo de este programa de estudios es que los participantes conozcan la definición vigente de OWASP y su implementación práctica en el desarrollo de aplicaciones con .NET.

Duración

- 35 horas

Audiencia

- Desarrolladores de aplicaciones

Prerrequisitos

- Dominio de un lenguaje orientado a objetos (VB.NET, C#)
- Familiaridad con un IDE (Visual Studio)
- Conocimiento del ciclo de vida del desarrollo de software
- Conocimientos básicos de seguridad

Contenido

1. **Introducción**
   - Objetivo del Workshop
   - Contexto de la Seguridad

- Protección de datos en México
- Introducción a OWASP

2. **Seguridad en .NET**
   - Ataques Comunes y Estadísticas
   - ¿Por qué desarrollar Código Seguro?
   - Arquitectura de seguridad en .NET

3. **OWASP Top 10**
   - Injection
   - Broken Authentication and Session Management
   - Cross-Site Scripting (XSS) Attacks
   - Insecure Direct Object References
   - Security Misconfiguration
   - Sensitive Data Exposure
   - Missing Function Level Access Control
   - Cross-Site Request Forgery (CSRF) Attack
   - Using Components with Known Vulnerabilities
   - Unvalidated Redirects and Forwards

4. **Ciclo de vida del desarrollo seguro (SDL)**
   - Fases del SDL
   - Proceso e integración en el SDLC
   - Modelado de Amenazas
     - STRIDE
     - DREAD
   - Guías para implementación

5. **Seguridad en .NET Framework**
   - Modelos de Seguridad en .NET
     - RBS. Seguridad basada en roles
     - CAS. Acceso seguro al código
     - Application Domains
     - Criptografía

6. **Seguridad basada en Roles**
   - Autenticación
   - Autorización
   - Ataques comunes y técnicas defensivas

7. **Acceso seguro al código**
   - Actualización al modelo de seguridad
   - CAS el modelo a partir de CLR 4.0
   - CAS soporte a aplicaciones Legacy

8. **Criptografía**
   - Panorama
   - Algoritmos simétricos
   - Algoritmos asimétricos
   - Algoritmos Hash
   - Firmas digitales

9. **Seguridad en Manejo de Estado**
   - Técnicas del lado del cliente
   - Técnicas de servidor
   - Ataques comunes y técnicas defensivas

10. **Seguridad en .NET Framework**
    - Validación de Entrada
    - Manejo de Archivos
    - Application Domains
    - Manejo de Errores
    - Administración de la Configuración