JUSTIFICACIÓN (*)

Actualmente las aplicaciones web son cada vez más diversas por lo que a su vez también aumenta su complejidad. Se han vuelto frecuentes los ataques a través de navegadores web por lo que en algunas de estas aplicaciones la data del cliente pudiese estar comprometida si se realizara un ataque.

OBJETIVO GENERAL (*)

- Conocer las principales mejoras y oportunidades brindadas por este lenguaje de programación facilitando así el aumento de la seguridad de las aplicaciones o herramientas desarrolladas en este lenguaje.

OBJETIVOS ESPECIFICOS

- Identificar ataques realizados a las aplicaciones web
- Conocer el riesgo de funciones peligrosas y limitar su uso
- Aprender técnicas de programación segura en PHP
- Conocer las buenas prácticas para asegurar el entorno de las aplicaciones desarrolladas en PHP.

DESCRIPCION GENERAL DE LA ESTRUCTURA DEL PROGRAMA (*)

Curso 1: Validaciones y Contramedidas
1.1 Módulo 1: Validación de Datos
1.2 Módulo 2: Inyección CRLF (HTTP Response splitting)
1.3 Módulo 3: Listas Negras y Listas Blancas
1.4 Módulo 4: Contramedidas Específicas OWASP

Curso 2: Seguridad de Datos y Comercio Electrónico
2.1 Módulo 1: Cross-Site Request Forgery (CSRF)
2.2 Módulo 2: Seguridad del Framework
2.3 Módulo 3: Desbordamiento de Datos y Threading
2.4 Módulo 4: Comercio Electrónico Seguro

Curso 3: Programación Segura
3.1 Módulo 1: Programación Segura: Cliente
3.2 Módulo 2: Ataques MiTM
3.3 Módulo 3: Programación Segura: Web
3.4 Módulo 4: Criptografía Avanzada

Curso 4: Encriptado y Auditorías de Código

4.1 Módulo 1: Criptoanálisis
4.2 Módulo 2: Estándares de Encriptado
4.3 Módulo 3: Auditoría de Código
4.4 Módulo 4: Auditoría de Código Fuente