



Esta formación está orientada a que los equipos de programadores conozcan y utilicen las buenas prácticas en el diseño y desarrollo de aplicaciones en PHP para evitar vulnerabilidades de seguridad. El objetivo del mismo es conocer como proteger la aplicación contra los fallos más comunes en PHP (SQL Injection, XSS, Command Execution, File Inclusion ...)

Descripción

Hoy en día las aplicaciones web son uno de los servicios más utilizados ya sea accediendo a un servidor web a través de internet o de una intranet.

El lenguaje PHP es versátil, sencillo de usar y permite crear soluciones de gran envergadura, como consecuencia PHP se ha convertido en un lenguaje de desarrollo relevante y en constante crecimiento.

Las aplicaciones escritas en este lenguaje están expuestas a diversas amenazas si no se toman las medidas adecuadas para evitarlo, por este motivo se resalta la importancia de la formación en seguridad que deberían de recibir todos los programadores.

Si no se procede de forma correcta, las aplicaciones web desarrolladas en este lenguaje pueden servir como puerta de entrada de un intruso a la red de la

empresa, por lo que la seguridad de este tipo de aplicaciones tiene que ser tomada como prioritaria para no exponer la seguridad de su negocio.

Esta formación está orientada a que los equipos de programadores conozcan y utilicen las buenas prácticas en el diseño y desarrollo de aplicaciones en PHP para evitar vulnerabilidades de seguridad.

El objetivo del mismo es conocer como proteger la aplicación contra los fallos más comunes en PHP (SQL Injection, XSS, Command Execution, File Inclusion ...)

Un curso imprescindible para asegurar la calidad y seguridad de las aplicaciones desarrolladas en este lenguaje.



Programa

- **Introducción.**
 - Principios de seguridad informática.
 - Vectores de ataque más comunes.
- **Procesado de la información.**
 - Formularios y URL's.
 - Errores en subida de ficheros.
 - Ataques CSS.
 - Spoofing en aplicaciones php.
- **Bases de datos.**
 - Introducción a SQL.
 - Inyección.
 - Fugas de información.
- **Autenticación.**
 - Ataques de fuerza bruta.
 - Otros ataques.
- **Cookies.**
 - Seguridad en cookies.
- **Sesiones.**
 - Fijación y seguridad en el manejo de sesiones.
- **Otros errores comunes.**
 - Inclusiones.
 - Ejecución de comandos.
 - Acceso a ficheros.
 - Acceso a código fuente.
- **Criptografía.**
 - Bases de criptografía.
 - Criptografía en bases de datos.
 - Encriptación de datos en la aplicación.
- **Hosting y configuración de Apache.**
 - Peligros de hosting compartido.
 - Configuración segura de Apache y php

Duración

Consultar

Lugar

Oficinas cliente
Centro de Formación

Contacto

formacion@aitsec.com
Telf.: 902 05 65 35