Máster en Ingeniería de Sistemas e Informática
62612 - Diseño de aplicaciones seguras

Guía docente para el curso 2010 - 2011

Curso: 1, Semestre: 1, Créditos: 4.0

Información básica

Profesores

- **Unai Arronategui Arribalzaga** unai@unizar.es
- **Fernando Tricas García** ftricas@unizar.es
- **Elvira Mayordomo Cámara** elvira@unizar.es

Recomendaciones para cursar esta asignatura

Estudiantes interesados en complementar su visión del desarrollo de programas pensando en su seguridad.

Actividades y fechas clave de la asignatura

Ver el horario del máster.

Inicio

Resultados de aprendizaje que definen la asignatura

El estudiante, para superar esta asignatura, deberá demostrar los siguientes resultados...

1:
Conoce los problemas de seguridad mas habituales en los programas, asi como las medidas preventivas necesarias

2:
Entiende que las medidas de seguridad en los programas no sólo afectan a la programción y codificación, sino también a la forma en que se diseña el sistema globallmente.

3:
Conoce los principios básicos de seguridad en sistemas.

4:

Conoce los principios básicos de la criptografía.

Introducción

Breve presentación de la asignatura

El desarrollo de aplicaciones pensando en la seguridad es una preocupación bastante reciente en la industria del desarrollo de programas. Todas las empresas más importantes tenen sus propios programas de desarrollo pensando en la seguridad y empieza a existir una buena base de conocimientos que nos permitirán mejorar la forma en que desarrollamos software.

En este curso se presenta una introducción a los aspectos mas importantes del desarrollo de programas pensando en la seguridad, tanto desde el punto de vista de los sistemas subyacentes, como de las cuestiones relacionadas con la programación y el propio diseño de las aplicaciones, sin olvidar algunas herramientas útiles y necesarias como la criptografía.

Contexto y competencias

Sentido, contexto, relevancia y objetivos generales de la asignatura

La asignatura y sus resultados previstos responden a los siguientes planteamientos y objetivos:

A la hora de desarrollar programas que han de ejecutarse en cualquier contexto (dentro de la propia empresa u organización, como productos para otras empresas o incluso como parte de un servicio que comercializamos o ponemos a disposición de otros) es fundamental tener en cuenta que habrá personas que traten de sacar partido de los posibles defectos de los mismos: bien para obtener información, para obtener algún tipo de beneficio o para atacar a terceros.

Esta asignatura pretende hacer conscientes a los estudiantes del problema y mostrarles las formas más habituales en las que se pueden producir este tipo de problemas, junto con la forma de tratar de evitarlos.

Contexto y sentido de la asignatura en la titulación

El Máster en Ingeniería de Sistemas e Informática tiene un bloque de asignaturas que forma al alumno en tecnologías de servicios web, diseño de aplicaciones seguras y sistemas distribuidos. No tiene sentido hoy en día pensar en diseñar cualquier tipo de sistema que incluya el desarrollo de aplicaciones sin tener en cuenta los aspectos de seguridad.

Al superar la asignatura, el estudiante será más competente para...

1:
Comprender el problema de la seguridad en el desarrollo de programas y su aplicación a la propia labor en la informática.

2:
Tener en cuenta la seguridad de los programas a la hora de diseñarlos, añadiendo esta característica a las ya habituales de fiabilidad, robustez, eficiencia, ...

3:
Conocer los principales problemas de seguridad que afectan a los programas en todas las fases de su desarollo, así como las medidas que ayudaran a evitarlos.

4:
Comprender que los programas se ejecutan dentro de sistemas más complejos y que eso también ha de ser tenido en cuenta.

5:
Conocer los principios básicos de la criptografía, que les permitirán identificar la necesidad y utilizarla adecuadamente.

Importancia de los resultados de aprendizaje que se obtienen en la asignatura:

La industria se ha dado cuenta de que ya no es posible desarrollar programas sin tener en cuenta los aspectos de seguridad: el coste puede ser de tiempo perdido, pero también puede afectar a recursos e incluso a personas.

Evaluación

Actividades de evaluación

El estudiante deberá demostrar que ha alcanzado los resultados de aprendizaje previstos mediante las siguientes actividades de evaluacion

1:
De manera individual, cada estudiante elegirá un tema (de los tratados en la asignatura o relacionados) y estudiará algunos artículos relevantes sobre el tema elegido (los profesores ayudarán en la fase de selección de los artículos y a la hora de acotar el trabajo). Con el conocimiento adquirido elaborará un informe de alrededor de 6 u 8 páginas y hará una exposición oral ante los profesores y el resto de la clase donde demostrará la comprensión del tema y la justificación de las decisiones adoptadas a la hora de exponerlo.

Actividades y recursos

Presentación metodológica general

El proceso de aprendizaje que se ha diseñado para esta asignatura se basa en lo siguiente:

1. La presentación de los contenidos de la asignatura en clases magistrales por parte de los profesores.
2. El estudio personal de la asignatura por parte de los alumnos y la presentación de los resultados en clases o seminarios.

Actividades de aprendizaje programadas (Se incluye programa)

El programa que se ofrece al estudiante para ayudarle a lograr los resultados previstos comprende las siguientes actividades...

1: Introducción a la seguridad en Sistemas

2: Introducción a la criptografía

3:
Desarrollo de aplicaciones seguras

- Gestión de riesgos
- Selección de tecnologías
- Principios básicos
- Auditoría de programas
- Desbordamiento de memoria
- Control de acceso
- Condiciones de carrera
- Aleatoriedad y determinismo
- Aplicación de la criptografía
- Gestión de la confianza y validación de entradas
- Autentificación con claves

- Seguridad en bases de datos
- Seguridad en el cliente en la web

Planificación y calendario

Calendario de sesiones presenciales y presentación de trabajos

Pendiente de planificar. Corresponde al horario asignado al curso y una fecha que se fija en cada una de las convocatorias para la presentación del trabajo escrito y su posterior presentación oral.

Bibliografía y documentos de referencia

Bibliografía

- John Viega and Gary McGraw. Building Secure Software. Addison-Wesley
  Se puede considerar el primero que se estableció como un texto completo dedicado a la seguridad en el desarrollo de programas. Más orientado hacia Unix, pero aprovechable por cualquiera. No habla prácticamente nada de la programación web. También en Building Secure Software.
- Michael Howard, David C. LeBlanc. Writing Secure Code. Microsoft Press. Second Edition.
  El libro de Microsoft. Bastante bueno, orientado a Windows y, como es un poco mas moderno, ya habla de los problemas relacioados con la programación web.
- Sverre H. Huseby. Innocent Code. A security wake-up call for web programmers. Wiley.
  Un libro orientado a la programación web. Cortito, se lee muy bien y se aprende mucho.
- Ross Anderson. Security Engineering. Wiley.

Además, los profesores mantienen la página web sobre Diseño de Aplicaciones Seguras, donde se proporcionan enlaces a documentos y otra información relevante, así como las presentaciones utilizadas en clase.

Referencias bibliográficas de la bibliografía recomendada