Formulario de Aprobación Curso de Posgrado 2012

Asignatura: Seguridad en Aplicaciones

Profesor de la asignatura [1]:
Dr. Ing. Gustavo Betarte, Profesor Titular, Instituto de Computación
Msc. Ing. Felipe Zipitría, Profesor Adjunto, Instituto de Computación
Ing. Rodrigo Martínez, Ayudante, Instituto de Computación

Profesor Responsable Local [1]:

Otros docentes de la Facultad:

Docentes fuera de Facultad:

Instituto ó Unidad: Instituto de Computación
Departamento ó Area: Seguridad Informática

Fecha de inicio y finalización:
Horario y Salón:

Horas Presenciales: 39
(se deberán discriminar las mismas en el ítem Metodología de enseñanza)

Nº de Créditos: 5
(de acuerdo a la definición de la UdelaR, un crédito equivale a 15 horas de dedicación del estudiante según se detalla en el ítem metodología de la enseñanza)

Público objetivo y Cupos: Profesionales y estudiantes interesados en Seguridad Informática, en particular en el área de desarrollo, testing, gestión de proyectos, o seguridad.
No tiene cupo

Objetivos: El objetivo de este curso es introducir a los estudiantes en los principales conceptos y metodologías asociadas a la seguridad en el desarrollo de aplicaciones. Conocer los pilares fundamentales del enfoque en seguridad a la hora de proyectos de desarrollo de aplicaciones. Comprender y aplicar la gestión del riesgo en los proyectos de desarrollo, enfocados en la seguridad del producto, y la consistencia del proceso.

Conocimientos previos exigidos: Ninguno

Conocimientos previos recomendados: Conocimientos básicos de programación e Ingeniería de Software.

Metodología de enseñanza:
(comprende una descripción de las horas dedicadas por el estudiante a la asignatura y su distribución en horas presenciales -de clase práctica, teórico, laboratorio, consulta, etc.- y no presenciales de trabajo personal del estudiante)

- Horas clase (teórico): 20
- Horas clase (práctico):
- Horas clase (laboratorio): 8
- Horas consulta: 8

- Horas evaluación: 3
    - Subtotal horas presenciales: 39
- Horas estudio: 36
- Horas resolución ejercicios/prácticos:
- Horas proyecto final/monografía:
    - Total de horas de dedicación del estudiante: 75

Forma de evaluación: El curso se evaluará a partir de:

- los laboratorios
- un examen final de 2 hs.

Temario:

1. Introducción.
    1.1 Presentación, revisión de conceptos.
    1.2 Un framework para la gestión de riesgos

2. Siete hitos para la seguridad en el software
    2.1 Code review
    2.2 Análisis de riesgos en la arquitectura
    2.3 Tests de penetración
    2.4 Test de seguridad basado en los riesgos
    2.5 Casos de abuso
    2.6 Requerimientos de seguridad
    2.7 Operaciones de seguridad
    2.8 Análisis externo

3. Taxonomía de errores de codificación
    3.1 Validación de la entrada y codificación
    3.2 Abusos de API
    3.3 Funcionalidad de seguridad
    3.4 Tiempo y estado
    3.5 Manejo de errores
    3.6 Calidad del código
    3.7 Encapsulación, Entorno

4. Aplicaciones Web
    4.1 Autenticación/autorización
    4.2 Manejo de sesiones
    4.3 OWASP Top Ten, mapeo en la taxonomía

Bibliografía:

Gary McGraw, Addison-Wesly Software Security Series, Software Security: Building Security In, ISBN: 0-321-35670-5.

Open Web Application Security Project, OWASP, http://www.owasp.org