23-24

MÁSTER UNIVERSITARIO EN
INGENIERÍA INFORMÁTICA

GUÍA DE ESTUDIO PÚBLICA

DESARROLLO DE SOFTWARE SEGURO (MÁSTER EN INGENIERÍA INFORMÁTICA)

CÓDIGO 31106205

UNED

23-24

DESARROLLO DE SOFTWARE SEGURO
(MÁSTER EN INGENIERÍA INFORMÁTICA)

CÓDIGO 31106205

ÍNDICE

Nombre de la asignatura	DESARROLLO DE SOFTWARE SEGURO (MÁSTER EN INGENIERÍA INFORMÁTICA)
Código	31106205
Curso académico	2023/2024
Título en que se imparte	MÁSTER UNIVERSITARIO EN INGENIERÍA INFORMÁTICA
Tipo	CONTENIDOS
Nº ETCS	6
Horas	150.0
Periodo	SEMESTRE 1
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

Lamentablemente los denominados “ciberataques” son noticia frecuente en los medios de comunicación. Según los datos publicados por el CERT (Computer Emergency Response Team) las vulnerabilidades de los sistemas informáticos reportadas cada año crecen y aumentan su grado de sofisticación.

En este curso se presentan métodos rigurosos, técnicas y herramientas para desarrollar e implantar software seguro. Los métodos incluyen el análisis de código para detectar las vulnerabilidades habituales, la revisión de código fuente mediante herramientas de análisis estático y buenas prácticas para desarrollar código seguro en lenguajes concretos de programación.

Los métodos y herramientas que se estudian sirven para la realización de pruebas, verificación y validación de software y sistemas, comprobando que se cumplen los requisitos funcionales y de seguridad. Con todos ellos, se aprende a validar y verificar el aseguramiento de la seguridad así como a establecer la diferencia entre vulnerabilidades y errores de programación. Las técnicas de test incluyen las pruebas de caja blanca, caja negra, pruebas contra ataques, amenazas y penetración, pruebas de resiliencia, etc.

La asignatura “Desarrollo de Software Seguro” se enmarca en el Máster Universitario en Ingeniería Informática, dentro del Módulo “Complementos en tecnología informática”. Es una asignatura optativa de 6 créditos que se imparte en el primer semestre. La relación con estas otras asignaturas del máster:

•Planificación y gestión de proyectos informáticos de I+D+i

•Sistemas empotrados

•Temas avanzados de redes e internet

•Cloud computing y gestión de los servicios de red

•Sistemas operativos de dispositivos móviles.

Se puede resumir indicando que esta asignatura de “Desarrollo de Software Seguro” supone una extensión de todas ellas cuando se trata de desarrollar un sistema software que debe tener la cualidad adicional de ser seguro. Obviamente esta cualidad debería ser exigible en cualquier desarrollo de software actual. Sin embargo, lamentablemente los aspectos de seguridad no son tenidos en cuenta y las vulnerabilidades de los sistemas aumentan cada día más.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

La formación previa que deberían tener los alumnos para el adecuado seguimiento de esta asignatura son los propios de ingreso al posgrado, haciendo especial recomendación en conocimientos de ingeniería de software y lenguajes de programación.
Es muy recomendable que se haya cursado la asignatura "Fundamentos de Programación" para facilitar la comprensión de los ejemplos de la bibliografía escritos en lenguaje C. Se recomienda que el alumno tenga preferiblemente alguna experiencia previa de programación con C++ para seguir los ejemplos de la bibliografía. Los conocimientos básicos de programación orientada a objetos se pueden obtener de la asignatura de Programación Orientada a Objetos perteneciente a la materia Fundamentos de la Programación.
Además es necesario dominar el inglés técnico (leer y escribir) para manejar con facilidad las fuentes bibliográficas.
Se recomienda realizar los ejercicios de los exámenes anteriores y después consultar las respuestas en la sección de exámenes anteriores corregidos.

EQUIPO DOCENTE

Nombre y Apellidos	DAVID JOSE FERNANDEZ AMOROS (Coordinador de asignatura)
Correo Electrónico	david@issi.uned.es
Teléfono	91398-8241
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	INGENIERÍA DE SOFTWARE Y SISTEMAS INFORMÁTICOS

Nombre y Apellidos	JOSE ANTONIO CERRADA SOMOLINOS
Correo Electrónico	jcerrada@issi.uned.es
Teléfono	91398-6478
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	INGENIERÍA DE SOFTWARE Y SISTEMAS INFORMÁTICOS

HORARIO DE ATENCIÓN AL ESTUDIANTE

La tutorización de los alumnos se llevará a cabo fundamentalmente a través de la plataforma aLF. Además se puede utilizar el correo electrónico y las consultas telefónicas:
Profesor: *David Fernández Amorós*
Horario: Jueves de 16:00 a 20:00
david@issi.uned.es,
Teléfono: 91 398 8241
Profesor: *José Antonio Cerrada*
Horario: Jueves de 16:00 a 20:00
jcerrada@issi.uned.es,
Teléfono: 91 398 6478
También es posible una asistencia personalizada (preferentemente previo aviso) en los días

y horas de tutorización en la siguiente dirección:
Dpto. de Ingeniería de Software y Sistemas Informáticos
ETSI Informática, UNED
C/ Juan del Rosal, 16
28040 MADRID

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

Competencias Básicas:
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

Competencias Generales:
G1 - Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería informática.
G2 - Capacidad para la dirección de obras e instalaciones de sistemas informáticos, cumpliendo la normativa vigente y asegurando la calidad del servicio.
G4 - Capacidad para el modelado matemático, cálculo y simulación en centros tecnológicos y de ingeniería de empresa, particularmente en tareas de investigación, desarrollo e innovación en todos los ámbitos relacionados con la Ingeniería en Informática.
G5 - Capacidad para la elaboración, planificación estratégica, dirección, coordinación y gestión técnica y económica de proyectos en todos los ámbitos de la Ingeniería en Informática siguiendo criterios de calidad y medioambientales.
G9 - Capacidad para comprender y aplicar la responsabilidad ética, la legislación y la deontología profesional de la actividad de la profesión de Ingeniero en Informática.

Competencias Transversales:
CT1 - Capacidad para emprender y liderar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.
CT2 - Capacidad para tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

Competencias Específicas:

DG2 - Capacidad para la planificación estratégica, elaboración, dirección, coordinación, y gestión técnica y económica en los ámbitos de la ingeniería informática relacionados, entre otros, con: sistemas, aplicaciones, servicios, redes, infraestructuras o instalaciones informáticas y centros o factorías de desarrollo de software, respetando el adecuado cumplimiento de los criterios de calidad y medioambientales y en entornos de trabajo multidisciplinares.

TI2 - Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de redes de nueva generación, los modelos de componentes, software intermediario y servicios.

TI3 - Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos.

TI4 - Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

TI11 - Capacidad para conceptualizar, diseñar, desarrollar y evaluar la interacción persona-ordenador de productos, sistemas, aplicaciones y servicios informáticos.

RESULTADOS DE APRENDIZAJE

La asignatura está enfocada al desarrollo y mantenimiento de software seguro y sin vulnerabilidades. Por tanto, los resultados de aprendizaje que se espera que el estudiante pueda alcanzar son:

- Identificar las principales causas de vulnerabilidad conocidas y desarrollar el código seguro que las evite.
- Conocer y saber aplicar un conjunto de métodos, técnicas y herramientas que permitan probar que el software desarrollado cumple los requisitos de funcionalidad y seguridad.
- Aplicar métodos para verificar formalmente la corrección de componentes de software crítico seguro.
- Realizar, junto con las pruebas tradicionales, otras adicionales específicas de seguridad.
- Usar modelos de penetración, patrones de ataque, de abuso o mal uso del sistema en la fase de pruebas.
- Conocer los procedimientos y programas de mantenimiento de software para que continúe cumpliendo con los requisitos de funcionalidad y seguridad.

CONTENIDOS

Tema 1: Estudio de Vulnerabilidades

Los aspectos estudiados en este tema son los siguientes:

•Errores de programación más peligrosos según el CWE/SANS Top 25

•Conceptos de seguridad

Tema 2: Prácticas de Desarrollo

Los aspectos estudiados en este tema son los siguientes:

•Buenas prácticas para análisis de requisitos, diseño arquitectónico y de detalle. Por ejemplo:

•Casos de uso/abuso

•Modelado de amenazas

•Análisis de riesgos

•Revisión de diseño

•Defensa en profundidad

Tema 3: Gestión de Memoria en C y C++

Los aspectos estudiados en este tema son los siguientes:

•Errores de manejo de strings

•Errores más comunes de gestión de memoria

•Buffer overflow

•Stack smashing

•Validación de entradas

•Memoria dinámica en C y C++

Tema 4: Strings, Punteros y Manejo de Enteros

Los aspectos estudiados en este tema son los siguientes:

•Errores de overflow de enteros

•Subterfugios con punteros

Tema 5: Otras vulnerabilidades en C y C++

Los aspectos estudiados en este tema son los siguientes:

•Errores de formateado de Entrada/Salida de datos

•Errores de secuenciado de Entrada/Salida de datos

•Errores de manejo de ficheros

METODOLOGÍA

La docencia de esta asignatura se impartirá a distancia, siguiendo el modelo educativo propio de la UNED. El principal instrumento docente será la plataforma aLF en la que se habilitarán diversos foros para canalizar las consultas y comentarios.
Las actividades a realizar por parte del alumno se desglosan de la siguiente manera:

Actividades formativas	Horas
Estudio de contenidos	60
Tutorías	10
Actividades en la plataforma virtual	5
Trabajos individuales	30
Trabajos en equipo	15
Prácticas informáticas	30
Elaboración de informes	0
Resolución de casos	0

Además, el estudiante podrá realizar consultas al equipo docente a través del correo, teléfono y presencialmente en los horarios establecidos para estas actividades. Ver apartado de ***Tutorización*** en esta guía docente.

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen de desarrollo
Preguntas desarrollo	4
Duración del examen	120 (minutos)

Material permitido en el examen

Todo tipo de material escrito.

Criterios de evaluación

El examen consiste en una serie de preguntas teóricas o correspondientes a un trozo de código. Se considerará la claridad en las respuestas, la adecuación de la respuesta a la pregunta y el uso de ejemplos ilustrativos, por ejemplo incluyendo fragmentos de código.

% del examen sobre la nota final	70
Nota del examen para aprobar sin PEC	0
Nota máxima que aporta el examen a la calificación final sin PEC	10
Nota mínima en el examen para sumar la PEC	5

Comentarios y observaciones

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad: Si

Descripción

Además de la convocatoria ordinaria, habrá una convocatoria extraordinaria en septiembre para los alumnos que no hayan aprobado en la convocatoria ordinaria o quieran subir nota.

Criterios de evaluación

Los mismos que para la prueba ordinaria.

Ponderación de la prueba presencial y/o los trabajos en la nota final: El mismo que para la prueba ordinaria

Fecha aproximada de entrega: Septiembre

Comentarios y observaciones

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?: Si,PEC no presencial

Descripción

Una prueba de tipo test en la herramienta correspondiente del curso virtual. Se dispondra de una semana para acceder y de dos horas para completarla. La realización de la PEC es voluntaria, pero si no se realiza se pierde la parte correspondiente de la nota para la evaluación final.

Criterios de evaluación

Hay diez preguntas. Cada pregunta correcta cuenta un punto. Las respuestas incorrectas no descuentan nota.

Ponderación de la PEC en la nota final: 30%

Fecha aproximada de entrega: La semana anterior a la primera semana de exámenes

Comentarios y observaciones

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s?: No

Descripción

Criterios de evaluación

Ponderación en la nota final

Fecha aproximada de entrega

Comentarios y observaciones

¿CÓMO SE OBTIENE LA NOTA FINAL?

La nota final se calculará multiplicando la nota de la PEC (de 0 a 10) por 0.3 y sumando la nota del examen (de 0 a 10) multiplicada por su peso 0.7. Es decir,

Nota final = PEC*0.3 + Examen * 0.7

BIBLIOGRAFÍA BÁSICA

ISBN(13):9780321822130
Título:SECURE CODING IN C AND C++ (Second Edition)
Autor/es:Robert C. Seacord ;
Editorial:ADDISON WESLEY

ISBN(13):9781439826966
Título:SECURE AND RESILENT SOFTWARE DEVELOPMENT
Autor/es:Mark S. Merkow And Lakshmikanth Raghavan ;
Editorial:CRC Press

Los dos libros están accesibles desde el portal de la UNED. Hay que autenticarse, y a partir de ahí.

- El libro de Seacord está aquí: (enlace). En este primer libro se estudian los aspectos generales relativos a todo el ciclo de vida del desarrollo de software seguro y sus particularidades.
- El libro de Merkow está aquí: (enlace). Este segundo libro está dedicado específicamente a estudiar las vulnerabilidades y las técnicas de programación segura en el lenguaje C y C++.

Hay un artículo que forma parte de la biblografía recomendada:

- Tsipenyuk, Katrina; Chess, Brian &McGraw, Gary. ***Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors.*** IEEE Security &Privacy, 2005

Este artículo se utiliza para clasificar los ciberataques y está disponible en la plataforma aLF de la asignatura.

BIBLIOGRAFÍA COMPLEMENTARIA

Aunque no se consideran necesarios para el estudio de la asignatura, los libros y documentos de esta bibliografía complementaria pueden ser muy interesantes para un estudio en mayor profundidad de la asignatura. La relación de documentos se incluye en la parte 2 de esta guia de la asignatura.

RECURSOS DE APOYO Y WEBGRAFÍA

Los alumnos tendrán a su disposición los siguientes recursos de apoyo al estudio:

- Guía de la asignatura: Incluye el plan de trabajo y orientaciones para su desarrollo. Esta guía será accesible desde el curso virtual.
- Curso virtual: A través de esta plataforma los alumnos pueden consultar información de la asignatura, acceder a material complementario, enunciados de ejercicios resueltos para que el alumno pueda autoevaluar sus conocimientos, realizar consultas al equipo docente y/o tutores a través de los foros correspondientes e intercambiar información con el resto de compañeros.

- Tutorías. En el Centro Asociado al que pertenezca el estudiante, éste deberá consultar si existe la posibilidad de disponer de una tutoría presencial con un tutor/a que le atienda presencialmente.
- Biblioteca: el acceso a las bibliotecas de los Centros Asociados y de la Sede Central permitirán al estudiante encontrar la bibliografía que podrá serle de utilidad durante el proceso de aprendizaje. De particular interés es el acceso electrónico a la colección de Safari Books Online a la que tienen acceso los estudiantes de la UNED.

Se ofrecerán las herramientas necesarias para que, tanto el equipo docente como el alumnado, encuentren la manera de compaginar el trabajo individual y el aprendizaje cooperativo (Skype, Moodle, Alf, etc.) si este se considerará necesario. Además de ello se podrá contactar con el equipo docente por teléfono y correo electrónico.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.