ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2020/2021

Máster en Ingeniería Informática (Plan 2018)

DATOS DE LA ASIGNATURA			
Nombre:			
Seguridad Web			
Denominación en inglés:			
Web Security			
Código:		**Carácter:**	
1180423		Optativo	
Horas:			
	Totales	**Presenciales**	**No presenciales**
Trabajo estimado:	75	30	45
Créditos:			
	Grupos reducidos		
Grupos grandes	**Aula estándar**	**Laboratorio**	**Prácticas de campo**	**Aula de informática**
1.5	0	0	0	1.5
Departamentos:		**Áreas de Conocimiento:**	
Tecnologías de la Información		Lenguajes y Sistemas Informáticos	
Curso:		**Cuatrimestre:**	
1º - Primero		Segundo cuatrimestre	

DATOS DE LOS PROFESORES			
Nombre:	**E-Mail:**	**Teléfono:**	**Despacho:**
Pachón Álvarez, Victoria	vpachon@uhu.es	87373	119 Edificio de la Escuela Técnica Superior de Ingeniería
*Fernández de Viana y González, Iñaki	i.fviana@dti.uhu.es	87378	Despacho 128. Escuela Técnica Superior de Ingeniería

*Profesor coordinador de la asignatura

Consultar los horarios de la asignatura

DATOS ESPECÍFICOS DE LA ASIGNATURA

1. Descripción de contenidos

1.1. Breve descripción (en castellano):

- Fuzzing Tecnologías Web
- Ejecución de código en el lado del Servidor Web
- Ejecución de código en el lado del Cliente Web
- Inyección SQL
- Info Leaks
- Inyección Xpath y Blind Xpath
- Inyección NoSQL

1.2. Breve descripción (en inglés):

This subject is focus on Fuzzing Web Technologies, execution of code on the Web Server side, execution of code on the web client side, SQL injection, info leaks, blind Xpath and Xpath injection and NoSQL injection.

2. Situación de la asignatura

2.1. Contexto dentro de la titulación:

La asignatura se imparte en el segundo cuatrimestre del Márter en Ingeniería Informática y tiene un caracter optativo. Se complementa con el resto de asignaturas del máster que abordarn temas de seguridad centrándose en aspectos de seguridad relacionados con servidores y clientes web.

2.2. Recomendaciones:

Se recomienda que el alumno tenga conocimientos básicos de administración de servidores, lenguajes de programación orientados al desarrollo de aplicaciones web y de base de datos tanto relacionales como no relacionales

3. Objetivos (Expresados como resultados del aprendizaje):

La aparición de la Web 2.0, el intercambio de información a través de redes sociales y el crecimiento de los negocios en la adopción de la Web como un medio para hacer negocios y ofrecer servicios, ha llevado a dotar a la Web de los mecanismos de seguridad oportunos que nos garanticen el adecuado desempeño de aplicaciones Web intrínsecamente insegura.
Con esta asignatura el alumno comprenderá los principios fundamentales de seguridad web, estudiará los ataques web más comunes y aprenderá cómo defenderse de dichos ataques que buscan comprometer a las empresas y usuarios accediendo a los sitios web para fines no lícitos.

4. Competencias a adquirir por los estudiantes

4.1. Competencias específicas:

4.2. Competencias básicas, generales o transversales:

- **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
- **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
- **CG8:** Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y mulitidisciplinares, siendo capaces de integrar estos conocimientos
- **CT1:** Gestionar adecuadamente la información adquirida expresando conocimientos avanzados y demostrando, en un contexto de investigación científica y tecnológica o altamente especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en el campo de estudio.
- **CT3:** Desarrollar una actitud y una aptitud de búsqueda permanente de la excelencia en el quehacer académico y en el ejercicio profesional futuro.
- **CT5:** Utilizar de manera avanzada las tecnologías de la información y la comunicación, desarrollando, al nivel requerido, las Competencias Informáticas e Informacionales ('CI2).

5. Actividades Formativas y Metodologías Docentes

5.1. Actividades formativas:

- Sesiones de Teoría sobre los contenidos del Programa.
- Sesiones Prácticas en Laboratorios Especializados o en Aulas de Informática.
- Actividades Académicamente Dirigidas por el Profesorado: seminarios, conferencias, desarrollo de trabajos, debates, tutorías colectivas, actividades de evaluación y autoevaluación.

5.2. Metologías docentes:

- Clase Magistral Participativa.
- Desarrollo de Prácticas en Laboratorios Especializados o Aulas de Informática en grupos reducidos.
- Resolución de Problemas y Ejercicios Prácticos.
- Tutorías Individuales o Colectivas. Interacción directa profesorado-estudiantes.
- Planteamiento, Realización, Tutorización y Presentación de Trabajos.
- Conferencias y Seminarios.
- Evaluaciones y Exámenes.

5.3. Desarrollo y justificación:

Actividades Formativas no presenciales:

- Lectura de los contenidos de los temas
- Entrega de ejercicios/prácticas/trabajos evaluables
- Actividades de autoevaluación
- Tutorías colectivas a través de plataformas de enseñanza virtual (foros, wikis, chats)
- Trabajo individual/autónomo del estudiante
- Actividades no presenciales con evaluación por pares
- Desarrollo cooperativo de trabajos utilizando herramientas de discusión asíncrona. (foros, wikis…)

Metodologías docentes no presenciales:

- Visualización y escuchas de sesiones grabadas de seminarios ad hoc con entrevistas a expertos en algunos temas claves de la materia, o vídeos seleccionados que incentiven algunas competencias
- Tutorías en línea. Utilización de foros y otros medios de comunicación e interacción con el profesorado
- Trabajos colaborativos. Llevar a cabo una actividad basada en un objetivo común en el que el estudiante debe colaborar activamente para realizarla.
- Metodologías basadas en la acción. Revisión, planificación de las mejoras de trabajos con la participación de los estudiantes y el profesor.

Con respecto a las metodologías presenciales, en cada sesión académica de teoría, el profesor explicará los conceptos básicos de cada tema mediante una clase magistral participativa. Dichos contenidos deben ser trabajados previamente por el alumnos mediante una lectura compresiva de los temas. En las sesiones prácticas en laboratorio se planteará un problema de mayor complejidad que lo/as alumno/as deberán resolver durante varias sesiones. Durante las sesiones de prácticas, los alumnos desarrollarán su trabajo con ayuda del profesorado. Los enunciados y materiales están disponibles en la web de la asignatura; aún así se recomienda la utilización de libros, recursos y fuentes de conocimiento adicionales. Además, se llevarán a cabo actividades académicamente dirigidas que consistirán en trabajos en grupos reducidos o individuales y en la entrega de ejercicios y trabajos.
La asignatura dispone de una página web donde el alumno puede consultar el material para preparar cada clase, así como la documentación necesaria para cada sesión práctica. Se utilizarán todos los medios tecnológicos disponibles en el aula (vídeo-proyector, wi-fi, etc.). Los alumnos que lo deseen pueden traer material a la clase (libros, portátiles, etc.).

6. Temario desarrollado:

Tema 1. Introducción a las Seguridad Web
- Introducción
- Concepto de aplicación Web
- Conceptos básicos sobre servidores web
- Conceptos básicos sobre el protocolo HTTP
- Conceptos básico sobre hacking de aplicacones web

Tema 2. Seguridad en el lado del servidor web
- Introducción
- Reconocimiento
- Escaneo de puertos
- Escaneo de vulnerabilidades

Tema 3. Seguridad en el lado de la aplicación web
- Introduction
- Reconocimiento de aplicaciones web
- Escaneo de aplicaciones web
- Vulnerabilidades por injección: SQL- NOSQL, etc
- Vulnerabilidades de sesión y autentificación
- Otras vulnerabilidades

Tema 4. Seguridad en el lado del cliente Web
- Introduction
- Reconocimiento del cliente web
- Escaneo del cliente web
- Vulnerabilidades Cross-Site Scripting (XSS)
- Vulnerabilidades Cross-Site Request Forgery (CSRF)
- Vulnerabilidades basadas en ingeniería social

7. Bibliografía

7.1. Bibliografía básica:

- **Hacking web technologies 2ª Edición.** Pablo González... [et al.]. OxWORD, 2017
- *Hacking web applications : client-side attacks***.** Enrique Rando González. 0XWord, 2017
- *Hacking de aplicaciones web : SQL Injection 3º Edición.* Enrique Rando González, Chema Alonso y Pablo González**.** OxWord, 2016
- **The basics of web hacking: tools and techniques to attack the Web**. Josh Pauli y Scott White. Syngress, an imprint of Elsevier, 2013.
- *Hacking web apps: detecting and preventing web application security problems*. Mike Shema y Jorge Blanco Alcover. Syngress, 2012.

7.2. Bibliografía complementaria:

- *UNIX and Linux System Administration Handbook 5th edition*. Dan MackliN. Pearson Ft Prentice Hall, 2017.
- *Docker: Up & Running: Shipping Reliable Containers in Production, 2 edition.* Sean P Kane (Autor), Karl Matthias. O'Reilly Media, 2018.
- *VirtualBox Documentation*. Oracle. https://www.virtualbox.org/wiki/Documentation.
- *Php documentation*. The PHP Group. http://php.net/docs.php
- *Python documentation.* Python Software Foundation. https://docs.python.org/

8. Sistemas y criterios de evaluación.

8.1. Sistemas de evaluación:

- Examen de teoría/problemas
- Defensa de Prácticas
- Defensa de Trabajos e Informes Escritos
- Seguimiento Individual del Estudiante
- Examen de prácticas

8.2. Criterios de evaluación y calificación:

Los principios de evaluación de la asignatura siguen unos criterios de **evaluación preferentemente continua**, entendiendo por tal la evaluación diversificada que se lleva a cabo en distintos momentos del curso académico en curso. Esta evaluación diversificada se realiza, **para todas las convocatorias ordinarias (I, II y III)**, mediante los siguientes sistemas de evaluación presenciales y ponderaciones:

- **Examen de teoría/problemas (ET)** (20%): Examen de preguntas tipo test, tiene un carácter individual y su duración máxima se notificará con antelación suficiente. La materia objeto de examen será toda la tratada en la asignatura. No se podrá utilizar ningún tipo de recurso didáctico o documentación además de la proporcionada por el equipo docente el día del examen. Gracias a este sistema de evaluación, el alumno adquiere las competencias CG2, CG9, CG10, CB7, CB9, CT1, CT5, CETI3, CETI4.
- **Defensa de Prácticas (DP)** (40%): Resolución de los problemas de prácticas propuestos para cada uno de los bloques temáticos.Tienen un carácter individual. Se podrá utilizar cualquier material que se considere siempre que se referencie adecuadamente. Gracias a este sistema de evaluación, el alumno adquiere las competencias CG2, CG9, CB7, CB8, CB10, CT1, CT3, CETI3, CETI4
- **Defensa de Trabajos e Informes Escritos (DT)** (20%): El equipo docente indicará la temática de un trabajo que el alumno deberá desarrollar durante el curso. Tiene un carácter individual. Se podrá utilizar cualquier material que se considere siempre que se referencie adecuadamente. Gracias a este sistema de evaluación el alumno adquiere las competencias CG2, CB8, CB10, CT5, CETI3, CETI4.

y los sistemas de evaluación no presenciales:

- **Pruebas de evaluación mediante plataformas de enseñanza virtual (PE)** (10%): Exámenes de preguntas tipo test, tiene un carácter individual y su duración máxima se notificará con antelación suficiente. Se podrá realizar un máximo de un test por tema cuyas preguntas estarán relacionadas con los contenidos tratados en el tema. No se podrá utilizar ningún tipo de documentación además de la proporcionada por el equipo docente el día del examen. Gracias a este sistema de evaluación el alumno adquiere las competencias CG2, CB8, CB10, CT1, CT3, CETI3, CETI4
- **Participación en las actividades propuestas (PA)** (10%): Preguntas breves de opinión sobre los contenidos de cada uno de los temas impartidos. Además de la documentación proporcionada por el equipo docente para la realización de la prueba, el alumno podrá usar cualquier otro tipo de documento siempre que se referencie adecuadamente. Tienen un carácter individual. Gracias a este sistema de evaluación, el alumno adquiere las competencias CG8, CB9, CB10, CT1, CT5, CETI3, CETI4

Las actividades correspondientes a los sistemas de evaluación ET se realizarán/presentarán en las fechas publicadas por el centro para las convocatorias ordinarias. El resto de sistema de evaluación se realizarán en las fechas establecidas por el equipo docente. La **calificación final** de la asignatura para una convocatoria ordinaria se obtendrá sumando las calificaciones parciales obtenidas en cada uno de los sistemas de evaluación de la convocatoria en curso, ponderadas por los porcentajes arriba indicados, siempre y cuando se supere en un 40% o más el "Examen teórico/problemas".
Aquellos estudiantes que así lo consideren pueden optar por la realización de una **evaluación única final**. En este caso deberá presentar una solicitud en el REGISTRO GENERAL de la Universidad, en cualquiera de sus REGISTROS AUXILIARES o en el REGISTRO TELEMÁTICO, dirigida a la dirección del departamento y al coordinador de la asignatura.
La evaluación única final consistirá en un solo acto académico que, para todas las convocatorias (ordinarias I, II y II y la excepcional), estará formado por las siguientes pruebas:

- **Bloque de teoría (60%):** Cubre los sistemas de evaluación ET (40%), PE (10%) y PA (10%) y consistirá en un examen de preguntas tipo test, tiene un carácter presencial e individual y su duración máxima se notificará con antelación suficiente. La materia objeto de examen será toda la tratada a lo largo de la asignatura. Solo se podrá utilizar la documentación proporcionada por el equipo docente el día de la prueba.En la medida de los posible, se realizará en un aula de informática.
- **Bloque de prácticas (40%):** Cubre los sistemas de evaluación DP. Examen en el que se presentará un enunciado eminentemente práctico similar a los contenidos de los enunciados de prácticas propuestos durante el curso. Este enunciado podrá hacer referencia a más de un bloque temático. Tienen un carácter presencial e individual y su duración máxima se notificará con antelación suficiente. Solo se podrá utilizar la documentación proporcionada por el equipo docente el día de la prueba. En la medida de los posible, se realizará en un aula de informática.

La calificación final de la asignatura para la evaluación única final se obtendrá sumando las calificaciones parciales obtenidas en cada una de las pruebas, ponderadas por los porcentajes arriba indicados, siempre y cuando se alcance, al menos, el 40% de la nota máxima del bloque de teoría
En el caso de haber más candidatos que posibilidades de **Matrículas de Honor** por número de estudiantes en la asignatura, y con el objetivo de discriminar situaciones de equidad en la calificación final, se seguirán los siguientes criterios: primará la regularidad obtenida en todos los sistemas de evaluación propuestos y, si el empate persistiera, se convocaría a los alumnos implicados a una nueva prueba de evaluación.
Para todos los materiales entregados por parte de los estudiantes se asume de forma implícita la declaración de originalidad de los mismos, entendida en el sentido de que no ha utilizado fuentes sin citarlas debidamente. La detección de **plagio** en cualquiera de estos materiales, y en aplicación del artículo 15 del Reglamento de evaluación para las titulaciones de grado y máster oficial de la Universidad de Huelva, conllevará la calificación numérica de cero en la asignatura, independientemente del resto de calificaciones que los alumnos hubieran obtenido. Además, se iniciará el procedimiento disciplinario oportuno ante la Comisión de Docencia del Departamento.

9. Organización docente semanal orientativa:

Semanas	Grupos Grandes	Grupos Reducidos Aula Estándar	Grupos Reducidos Aula de Informática	Grupos Reducidos Laboratorio	Grupos Reducidos prácticas de campo	Pruebas y/o actividades evaluables	Contenido desarrollado
#1	2	0	2	0	0		Tema 1
#2	2	0	2	0	0		
#3	2	0	2	0	0		Tema 2
#4	2	0	2	0	0		
#5	2	0	2	0	0		Tema 3
#6	2	0	2	0	0		
#7	2	0	2	0	0		Tema 4
#8	1	0	1	0	0		
#9	0	0	0	0	0		
#10	0	0	0	0	0		
#11	0	0	0	0	0		
#12	0	0	0	0	0		
#13	0	0	0	0	0		
#14	0	0	0	0	0		
#15	0	0	0	0	0		
	15	0	15	0	0		