ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2022-23

MÁSTER EN INGENIERÍA INFORMÁTICA (PLAN 2018)

DATOS DE LA ASIGNATURA

Nombre:
SEGURIDAD WEB
Denominación en Inglés:
Web Security

Código:	**Tipo Docencia:**	**Carácter:**
1180423	Semipresencial	Optativa

Horas:

	Totales	**Presenciales**	**No Presenciales**
Trabajo Estimado	75	15	60

Créditos:

Grupos Grandes	**Grupos Reducidos**			
	Aula estándar	**Laboratorio**	**Prácticas de campo**	**Aula de informática**
1.5	0	1.5	0	0

Departamentos:	**Áreas de Conocimiento:**
TECNOLOGIAS DE LA INFORMACION	LENGUAJES Y SISTEMA INFORMATICOS
Curso:	**Cuatrimestre**
1º - Primero	Segundo cuatrimestre

DATOS DEL PROFESORADO (*Profesorado coordinador de la asignatura)

Nombre:	E-mail:	Teléfono:
* Inaki Josep Fernandez De Viana Gonzalez	i.fviana@dti.uhu.es	959 217 378
Docente por contratar (Departamento_TECNOLOGIAS DE LA	Docente_T135@uhu.es	

Datos adicionales del profesorado (Tutorías, Horarios, Despachos, etc...)

Horarios de Tutorías		
Profesor	**Direccción**	**Tutorías**
Fernandez De Viana Gonzalez, Iñaki Josep	Despacho 128, Escuela Técnica Superior de Ingeniería.	Consultar

Otros datos de interés	
Horarios de clases	Consultar
Aula virtual	Acceder

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):

- 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.
- NoSQL injection.

2. Situación de la asignatura:

2.1 Contexto dentro de la titulación:

La asignatura se imparte en el segundo cuatrimestre del Máster en Ingeniería Informática y tiene un carácter optativo. Se complementa con el resto de asignaturas del máster que abordan 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 resultado 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.

Competencias específicas:
· Capacidad para modelar, diseñar y desarrollar Aplicaciones Web.
· Capacidad para desarrollar y consumir servicios web de terceras partes

4. Competencias a adquirir por los estudiantes

4.1 Competencias específicas:

-

4.2 Competencias básicas, generales o transversales:

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.

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

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.

CT5: Utilizar de manera avanzada las tecnologías de la información y la comunicación, desarrollando, al nivel requerido, las Competencias Informáticas e Informacionales (CI2).

CT3: Desarrollar una actitud y una aptitud de búsqueda permanente de la excelencia en el quehacer académico y en el ejercicio profesional futuro.

5. Actividades Formativas y Metodologías Docentes

5.1 Actividades formativas:

- Sesiones de teoría/problemas/casos prácticos 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

- 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, ...)

5.2 Metodologías Docentes:

- Clase magistral participativa

- Desarrollo de prácticas en laboratorios especializados o en 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

- 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

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 los 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; aun 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 la Seguridad Web**
  - Introducción
  - Concepto de aplicación Web
  - Conceptos básicos sobre servidores web
  - Conceptos básicos sobre el protocolo HTTP
  - Conceptos básico sobre hacking de aplicaciones 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**
    - Introducción
    - 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**
    - Introducción
    - 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:

- González, P., 2017. *Hacking web technologies*. 2nd ed. OxWord.
- Rando González, E., 2017. *Hacking web applications : client-side attacks*. 1st ed. 0XWord.
- Rando González, E., Alonso, C. and González, P., 2016. *Hacking de aplicaciones web : SQL Injection*. 3rd ed. OxWord.
- Pauli, J. and White, S., 2014. *The basics of web hacking*. 1st ed. Syngress.

7.2 Bibliografía complementaria:

- MackliN, D., 2017. *Unix and linux system administration handbook*. 5th ed. Prentice Hall.
- Kane, S. and Matthias, K., 2018. *Docker: Up & Running: Shipping Reliable Containers in Production*. 2nd ed. O'Reilly Media.
- **VirtualBox Documentation**. Oracle. https://www.virtualbox.org/wiki/Documentation.

8. Sistemas y criterios de evaluación

8.1 Sistemas de evaluación:

- Examen de teoría/problemas

- Defensa de prácticas

- Examen de prácticas

- Defensa de trabajos e informes escritos

- Pruebas de evaluación mediante plataformas de enseñanza virtual

- Participación en las actividades propuestas

8.2 Criterios de evaluación relativos a cada convocatoria:

8.2.1 Convocatoria I:

Los sistemas de evaluación empleados, sus porcentajes y las competencias adquiridas con cada uno de ellos son:

Sistema de evaluación	Porcentaje	Competencias adquiridas
Examen de teoría/problemas (ET)	20	CG2, CG9, CG10, CB7, CB9, CT1, CT5, CETI3, CETI4
Defensa de Prácticas (DP)	40	CG2, CG9, CB7, CB8, CB10, CT1, CT3, CETI3, CETI4
Defensa de Trabajos e Informes Escritos (DT)	20	CG2, CB8, CB10, CT5, CETI3, CETI4
Examen de Prácticas (EP)	0	
Pruebas de evaluación mediante plataformas de enseñanza virtual	10	CG2, CB8, CB10, CT1, CT3, CETI3, CETI4
Participación en las actividades propuestas	10	CG8, CB9, CB10, CT1, CT5, CETI3, CETI4

La **calificación final de la asignatura** para esta convocatoria 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 ET.

Las condiciones específicas en las que se realizarán cada uno de los sistemas de calificación son las siguientes:

- **Examen de teoría/problemas**: Examen de preguntas tipo test, tiene un carácter individual y su duración máxima se notificará con antelación suficiente. Solo se podrán utilizar los recursos didácticos proporcionados por el equipo docente el día del examen.
- **Defensa de Prácticas**: Resolución de los problemas de prácticas propuestos para cada uno de los bloques temáticos. Tienen un carácter individual. Se podrá emplear cualquier material que se considere siempre que se referencie adecuadamente.
- **Defensa de Trabajos e Informes Escritos**: El equipo docente indicará la temática de un trabajo que el alumno deberá desarrollar durante el curso. Tiene un carácter individual. Se

podrá usar cualquier material que se considere siempre que se referencie adecuadamente.
- **Pruebas de evaluación mediante plataformas de enseñanza virtual (PE)**: Exámenes de preguntas tipo test. Se podrá realizar un máximo de un test por tema. Solo se podrán emplear los recursos didácticos proporcionados por el equipo docente el día del examen.
- **Participación en las actividades propuestas (PA)**: Preguntas breves de opinión sobre los contenidos de algunos 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.

Las actividades correspondientes a los sistemas de evaluación ET se celebrarán en las fechas publicadas por el centro para las convocatorias oficiales. El resto de sistemas de evaluación se entregarán en las fechas establecidas por el equipo docente.

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.

8.2.2 Convocatoria II:

Se siguen los mismos criterios indicados para la evaluación continua en la convocatoria ordinaria I.

8.2.3 Convocatoria III:

Se siguen los mismos criterios indicados para la evaluación continua en la convocatoria ordinaria I.

8.2.4 Convocatoria extraordinaria:

Se siguen los mismos criterios indicados para la evaluación continua en la convocatoria ordinaria I.

8.3 Evaluación única final:

8.3.1 Convocatoria I:

La evaluación única final consistirá en un solo acto académico que 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 lo 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 emplear la documentación proporcionada por el equipo docente el día de la prueba. En la medida de lo posible, se celebrará 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.

8.3.2 Convocatoria II:

Se siguen los mismos criterios indicados para la evaluación única en la convocatoria ordinaria I.

8.3.3 Convocatoria III:

Se siguen los mismos criterios indicados para la evaluación única en la convocatoria ordinaria I.

8.3.4 Convocatoria Extraordinaria:

Se siguen los mismos criterios indicados para la evaluación única en la convocatoria ordinaria I.

9. Organización docente semanal orientativa:							
Fecha	Grupos Grandes	G. Reducidos				Pruebas y/o act. evaluables	Contenido desarrollado
		Aul. Est.	Lab.	P. Camp	Aul. Inf.		
20-02-2023	0	0	2	0	0		Tema 1
27-02-2023	0	0	2	0	0	Test y preguntas de opinión Tema 1	Tema 1
06-03-2023	0	0	2	0	0		Tema 2
13-03-2023	0	0	2	0	0	Test y preguntas de opinión Tema 2	Tema 2
20-03-2023	0	0	2	0	0		Tema 3
27-03-2023	0	0	2	0	0	Test y preguntas de opinión Tema 3	Tema 3
10-04-2023	0	0	2	0	0		Tema 4
17-04-2023	0	0	1	0	0	Test y preguntas de opinión Tema 4	Tema 4
24-04-2023	0	0	0	0	0		
01-05-2023	0	0	0	0	0		
08-05-2023	0	0	0	0	0		
15-05-2023	0	0	0	0	0		
22-05-2023	0	0	0	0	0		
05-06-2023	0	0	0	0	0		
12-06-2023	0	0	0	0	0		
TOTAL	**0**	**0**	**15**	**0**	**0**		