



UNIVERSIDAD
POLITÉCNICA
DE MADRID

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingeniería de
Sistemas Informáticos

ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

613000100 - Seguridad En Aplicaciones Web

PLAN DE ESTUDIOS

61AF - Master Universitario En Ingeniería Web

CURSO ACADÉMICO Y SEMESTRE

2022/23 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos.....	1
2. Profesorado.....	1
3. Conocimientos previos recomendados.....	2
4. Competencias y resultados de aprendizaje.....	2
5. Descripción de la asignatura y temario.....	3
6. Cronograma.....	6
7. Actividades y criterios de evaluación.....	8
8. Recursos didácticos.....	12
9. Otra información.....	13

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	613000100 - Seguridad en Aplicaciones Web
No de créditos	4 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Primer semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	61AF - Master Universitario en Ingeniería Web
Centro responsable de la titulación	61 - Escuela Técnica Superior De Ingeniería De Sistemas Informáticos
Curso académico	2022-23

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Juan Alberto De Frutos Velasco (Coordinador/a)	1223	juanalberto.defrutos@upm.es	Sin horario.

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

- Back-end Con Tecnologías De Libre Distribución

3.2. Otros conocimientos previos recomendados para cursar la asignatura

El plan de estudios Master Universitario en Ingeniería Web no tiene definidos otros conocimientos previos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. Competencias

CE01 - Requisar, analizar y diseñar en un desarrollo Web bajo las metodologías vigentes en el entorno profesional.

CE02 - Programar y probar en un desarrollo Web con los lenguajes y técnicas vigentes en el entorno profesional.

CE06 - Incorporar seguridad, calidad, usabilidad y persistencia al desarrollo Web vigentes en el entorno profesional.

CE09 - Respetar los marcos legal, social y económico de los desarrollos vigentes en el entorno profesional.

4.2. Resultados del aprendizaje

RA40 - Saber desarrollar software seguro para aplicaciones web usando cualquier plataforma

RA41 - Utilizar herramientas que realicen análisis de vulnerabilidades en las aplicaciones web.

RA36 - Conocer los riesgos de seguridad asociados a las aplicaciones web.

RA39 - Saber identificar vulnerabilidades en las aplicaciones web

RA37 - Configurar un sitio web de forma segura.

RA38 - Utilizar soluciones criptográficas adecuadas para una aplicación web.

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

Análisis de riesgos de seguridad asociados a las aplicaciones web: XSS, robos de sesión, SQL injection, etc.

Identificación de vulnerabilidades en aplicaciones web.

Herramientas de análisis de vulnerabilidades en aplicaciones web.

Desarrollo de aplicaciones web seguras.

Empleo de soluciones criptográficas adecuadas.

Configuración segura de sitios web.

5.2. Temario de la asignatura

1. Tema 1: Conceptos previos
2. Tema 2: El protocolo SSL/TLS
 - 2.1. Comunicación segura entre cliente y servidor web
 - 2.2. Autenticación del servidor web con certificado digital
 - 2.3. Cómo obtener un certificado para un servidor web
 - 2.4. Configurar SSL en el servidor web
 - 2.5. Ataques MITM con SSL
 - 2.6. Autenticación de un cliente con certificado digital
 - 2.7. Cómo obtener un certificado digital de cliente
 - 2.8. Configurar SSL para certificados digitales de cliente
3. Tema 3: Cross Site Scripting (XSS)
 - 3.1. XSS Reflejado
 - 3.2. XSS permanente
4. Tema 4: Robo de Sesión
 - 4.1. Sesiones web
 - 4.2. Robo del identificador de sesión
 - 4.3. Ataques de fijación de sesión (Session Fixation)
 - 4.4. Robo del JWT
5. Tema 5: CSRF y ClickJacking
 - 5.1. CSRF (Cross Site Request Forgery)
 - 5.2. ClickJacking
6. Tema 6: SQL Injection
 - 6.1. Concepto de SQL injection
 - 6.2. Medidas para mitigar SQL injection
 - 6.3. SQL injection a través de metadatos del SGDB
 - 6.4. Blind SQL injection
7. Tema 7: Otros temas de seguridad en las aplicaciones web

- 7.1. Validación de los datos no fiables
 - 7.2. Parameter Tampering
 - 7.3. Proteger información sensible
 - 7.4. Ataques de Path Traversal
 - 7.5. Ataques de File Inclusion
 - 7.6. Referencias directas inseguras a objetos
 - 7.7. Carga de ficheros en el servidor (Upload)
 - 7.8. Inyecciones de código del sistema operativo.
8. Tema 8: Herramientas de análisis de vulnerabilidades en aplicaciones web
- 8.1. SAST (Static Analysis Security Testing)
 - 8.2. DAST (Dynamic Analysis Security Testing)
 - 8.2.1. Escaneo pasivo
 - 8.2.2. Escaneo activo
 - 8.3. DevSecOps

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1		Tema 1: Conceptos Previos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio Tema 2: El protocolo SSL/TLS Duración: 06:00 PL: Actividad del tipo Prácticas de Laboratorio Tema 3: Cross Site Scripting Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio		Asistencia y participación en el aula (RA36, RA37, RA38, RA39, RA40, RA41) OT: Otras técnicas evaluativas Evaluación continua Presencial Duración: 00:00 Práctica 1: Autenticación y TLS (RA36, RA37, RA38, RA40) TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final No presencial Duración: 15:00
2		Tema 4: Robo de sesión Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio Tema 5: CSRF y ClickJacking Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio Tema 6 : SQL injection Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio Tema 7: Otros temas de seguridad en las aplicaciones web Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio Tema 8: Herramientas de análisis de vulnerabilidades en aplicaciones web Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio		Asistencia y participación en el aula (RA36, RA37, RA38, RA39, RA40, RA41) OT: Otras técnicas evaluativas Evaluación continua Presencial Duración: 00:00 Práctica 2: XSS y Robo de sesión (RA36, RA39, RA40) TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final No presencial Duración: 15:00 Práctica 3: SQL injection, Path traversal y Pentesting web (RA36, RA39, RA40, RA41) TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final No presencial Duración: 20:00 Evaluación de Test (RA36, RA37, RA38, RA39, RA40, RA41) EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 00:20
3				

4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				Exámen de test (RA36, RA37, RA38, RA39, RA40, RA41) EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 01:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso derivadas de la situación creada por la COVID-19.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Asistencia y participación en el aula (RA36, RA37, RA38, RA39, RA40, RA41)	OT: Otras técnicas evaluativas	Presencial	00:00	5%	5 / 10	CE01 CE02 CE06 CE09
1	Práctica 1: Autenticación y TLS (RA36, RA37, RA38, RA40)	TI: Técnica del tipo Trabajo Individual	No Presencial	15:00	20%	3 / 10	CE01 CE02 CE06 CE09
2	Asistencia y participación en el aula (RA36, RA37, RA38, RA39, RA40, RA41)	OT: Otras técnicas evaluativas	Presencial	00:00	5%	5 / 10	CE01 CE02 CE06 CE09
2	Práctica 2: XSS y Robo de sesión (RA36, RA39, RA40)	TI: Técnica del tipo Trabajo Individual	No Presencial	15:00	22%	3 / 10	CE02 CE06 CE09 CE01
2	Práctica 3: SQL injection, Path traversal y Pentesting web (RA36, RA39, RA40, R41)	TI: Técnica del tipo Trabajo Individual	No Presencial	20:00	33%	3 / 10	CE01 CE02 CE06 CE09
2	Evaluación de Test (RA36, RA37, RA38, RA39, RA40, RA41)	EX: Técnica del tipo Examen Escrito	Presencial	00:20	15%	3 / 10	CE01 CE02 CE06 CE09

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Práctica 1: Autenticación y TLS (RA36, RA37, RA38, RA40)	TI: Técnica del tipo Trabajo Individual	No Presencial	15:00	20%	3 / 10	CE01 CE02 CE06 CE09

2	Práctica 2: XSS y Robo de sesión (RA36, RA39, RA40)	TI: Técnica del tipo Trabajo Individual	No Presencial	15:00	22%	3 / 10	CE02 CE06 CE09 CE01
2	Práctica 3: SQL injection, Path traversal y Pentesting web (RA36, RA39, RA40, R41)	TI: Técnica del tipo Trabajo Individual	No Presencial	20:00	33%	3 / 10	CE01 CE02 CE06 CE09
17	Exámen de test (RA36, RA37, RA38, RA39, RA40, RA41)	EX: Técnica del tipo Examen Escrito	Presencial	01:00	25%	3 / 10	CE01 CE02 CE06 CE09

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Exámen final escrito (RA36, RA37, RA38, RA39, RA40, RA41)	EX: Técnica del tipo Examen Escrito	Presencial	00:00	25%	3 / 10	CE01 CE02 CE06 CE09
Práctica 1: Autenticación y TLS (RA36, RA37, RA38, RA40)	TI: Técnica del tipo Trabajo Individual	Presencial	19:00	20%	3 / 10	CE01 CE02 CE06 CE09
Práctica 2: XSS y Robo de Sesión (RA36, RA39, RA40)	TI: Técnica del tipo Trabajo Individual	Presencial	19:00	22%	3 / 10	CE06 CE09 CE01 CE02
Práctica 3: SQL injection, Path traversal y Pentesting web (RA36, RA39, RA40, RA41)	TI: Técnica del tipo Trabajo Individual	Presencial	26:00	33%	3 / 10	CE01 CE02 CE06 CE09

7.2. Criterios de evaluación

De acuerdo con la normativa reguladora de evaluación del aprendizaje en las titulaciones oficiales de grado y máster universitario de la Universidad Politécnica de Madrid, aprobada por Consejo de Gobierno en su sesión del 26 de mayo de 2022, el sistema de evaluación que contribuye a favorecer el aprendizaje del estudiante y el logro de los resultados de aprendizaje y la adquisición de las competencias correspondientes es el sistema de evaluación progresiva.

SISTEMA DE EVALUACIÓN PROGRESIVA (CONVOCATORIA ORDINARIA)

La calificación de la asignatura se otendrá tomando consideración las siguientes actividades de evaluación:

- Asistencia y participación en el aula (APA)
- Práctica 1 (Pr1)
- Práctica 2 (Pr2)
- Práctica 3 (Pr3)
- Examen de test (Test)

Nota final = 0,1 APA + 0,2 Pr1 + 0,22 Pr2 + 0,33 Pr3 + 0,15 Test

Además de obtener una nota final mayor o igual que 5.0, para superar la asignatura se deberán cumplir los siguientes requisitos:

- Asistir al menos a un 50% de las clases.
- Obtener al menos un 3 en la calificación de cada una de las prácticas y del examen de tipo test: Pr1 \geq 3.0, Pr2 \geq 3.0, Pr3 \geq 3.0 y Test \geq 3.0.

SISTEMA DE EVALUACIÓN GLOBAL (CONVOCATORIA ORDINARIA)

Los alumnos que hubieran obtenido una calificación inferior a 5.0 en alguna/s de las tres prácticas en el sistema de evaluación progresivo, podrán volver a entregarla/s al finalizar el período lectivo para recuperarla/s.

Los alumnos que hubieran obtenido una calificación inferior a 5.0 en el examen de tipo test en el sistema de evaluación progresivo, podrán realizar otro examen de tipo test al finalizar el periodo lectivo para recuperarlo.

Para obtener la calificación final del alumno se aplican dos fórmulas. El resultado mayor de ambas será la nota final:

- La primera fórmula es la misma que en evaluación progresiva: $\text{Nota final} = 0,1 \text{ APA} + 0,2 \text{ Pr1} + 0,22 \text{ Pr2} + 0,33 \text{ Pr3} + 0,15 \text{ Test}$
- La segunda fórmula es: $\text{Nota final} = 0,2 \text{ Pr1} + 0,22 \text{ Pr2} + 0,33 \text{ Pr3} + 0,25 \text{ Test}$

En definitiva, el peso de APA se integra dentro del Test, si eso favorece al alumno. De esta manera, es posible recuperar también la actividad de asistencia y participación en el aula.

Ademas de obtener una nota final mayor o igual que 5.0, para superar la asignatura se deberán cumplir los siguientes requisitos:

- Obtener al menos un 3 en la calificación de cada una de las prácticas y del examen de tipo test: $\text{Pr1} \geq 3.0$, $\text{Pr2} \geq 3.0$, $\text{Pr3} \geq 3.0$ y $\text{Test} \geq 3.0$.

CONVOCATORIA EXTRAORDINARIA:

La calificación de la asignatura se obtendrá tomando consideración las siguientes actividades de evaluación:

- Práctica 1 (Pr1)
- Práctica 2 (Pr2)
- Práctica 3 (Pr3)
- Examen final escrito (Ex)

Nota final = 0,2 Pr1 + 0,22 Pr2 + 0,33 Pr3 + 0,25 Ex.

Además de obtener una nota final mayor o igual que 5.0, para superar la asignatura se deberán cumplir los siguientes requisitos:

- Obtener al menos un 3 en la calificación de cada una de las prácticas y del examen final escrito. Pr1 \geq 3.0, Pr2 \geq 3.0, Pr3 \geq 3.0 y Ex \geq 3.0.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
https://moodle.upm.es	Recursos web	Plataforma Moodle de la UPM en donde se dispone de todos los recursos utilizados en clase.
http://www.owasp.org	Recursos web	Comunidad abierta y libre, enfocada a facilitar a las organizaciones a desarrollar, adquirir y mantener aplicaciones más seguras.

Web Application Security, Bryan Sullivan, Vincent Luiw, Mc Graw Hill, 2012	Bibliografía	Fundamentos sobre la programación web segura
Pro PHP Security, 2nd Edition, Chris Snider, Thomas Myer, Michale Southwell, Apress, 2010	Bibliografía	Programación web segura con PHP
Essential PHP Security, Chris Shiflett, O'Really, 2005	Bibliografía	Programación web segura con PHP
Bulletproof SSL and TLS, Ivan Ristic, Feisty Duck, 2014	Bibliografía	Protocolo TLS/SSL
Iron-Clad Java: Bulding Secure Web Applications	Bibliografía	Programación web segura con Java

9. Otra información

9.1. Otra información sobre la asignatura

El Máster en Ingeniería Web está disponible en dos modalidades diferentes:

- Modalidad Presencial, con presencialidad de lunes a jueves, en horario de mañana.
- Modalidad Semipresencial, con presencialidad en viernes tarde y sábados mañana.

En ambos casos las actividades formativas llevadas a cabo y las metodologías docentes empleadas permiten evaluar los resultados de aprendizaje descritos en la memoria del programa. La oferta de estas dos modalidades se asienta en tres componentes básicos: las clases presenciales, las tutorías (presenciales, por correo electrónico, foros, chats, videoconferencia, etc.) y los recursos tecnológicos (plataforma virtual Moodle)

Para garantizar la adquisición de las competencias definidas en la memoria del título, se emplea un sistema de evaluación común e independiente de la modalidad de enseñanza elegida.

Las competencias generales se pueden obtener a partir del cuadro adjunto que figura en la memoria de la

titulación:

		Competencias específicas									
			CE1	CE2	CE3	CE4	CE5	CE6	CE7	CE8	CE9
Competiciones Real Decreto	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	CG0	X	X	X	X	X	X	X	X	X
	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	CG1	X	X	X	X	X	X	X	X	X
	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	CG2	X	X	X	X	X	X	X	X	X

	reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios											
	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	CG3										
	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	CG4		X			X					
Competencias de la U.P.M.	Uso de la lengua inglesa	CG5	X	X	X	X						
	Liderazgo de equipos	CG6							X	X	X	
	Creatividad	CG7	X	X	X	X	X	X	X	X	X	
	Organización y planificación	CG8							X	X	X	

	Gestión de la información	CG9	X	X	X	X	X	X	X	X	X	X
	Gestión económica y administrativa	CG10								X	X	X
	Trabajo en contextos internacionales	CG11										