Tópicos de Seguridad Web

1. Datos Generales de la asignatura

Nombre de la asignatura:	**Tópicos de Seguridad Web**
Clave de la asignatura:	*AWB-1804*
SATCA[1]:	1-4-5
Carrera:	Ingeniería en Sistemas Computacionales

2. Presentación

Caracterización de la asignatura
La seguridad informática es una característica esencial en los actuales contextos computacionales, en donde el recurso de la información puede verse altamente comprometido sino se toman las medidas adecuadas de protección y preservación de datos. Hoy en día existe la necesidad de desarrollar sistemas en la web, y el tema de seguridad es sin duda un punto muy importante. Esta materia aporta al perfil del Ingeniero en Sistemas Computacionales, los conocimientos, habilidades, y metodologías para implementar seguridad informática bajo políticas internas de las organizaciones y estándares aceptados, que permitan plantear soluciones y protección de datos en el desarrollo de aplicaciones web haciendo uso de herramientas de software y hardware adecuadas. La materia se encuentra dividida en cuatro temas, en el primer tema se da una introducción a los conceptos y principios de la seguridad informática. En el segundo tema se estudian aspectos relacionados a la seguridad en infraestructura de aplicaciones. En el tercer tema se exponen los

[1] Sistema de Asignación y Transferencia de Créditos Académicos

mecanismos de autenticación que generalmente se implementan en los desarrollos Web. Por último, se aborda el desarrollo de perfiles, aspecto importante en la validación de usuarios que acceden a información confidencial a través de los desarrollos Web.

La asignatura se relaciona con las materias de programación Web, bases de datos, redes de computadoras, sistemas operativos y desarrollo de sistemas.

Para cursar esta materia se requiere tener las competencias previas de programación Web, Bases de Datos y Redes de Computadoras.

Las competencias adquiridas le permitirán al estudiante cursar materias relacionadas con el Desarrollo de Sistemas y realizar proyectos integradores.

Intención didáctica

El docente debe enfatizar la realidad existente, relacionada con el contexto en el que se ejecutan las aplicaciones web en donde la seguridad es un aspecto fundamental a considerar. Así mismo, se debe concientizar al estudiante que las transacciones realizadas sobre las aplicaciones en internet requieren un soporte tecnológico que garantice su legalidad.

Se recomienda que el enfoque de este curso sea fundamentalmente práctico tocando aspectos teóricos que faciliten la comprensión formal de los temas a tratar. El primer tema, Introducción de Seguridad, le permitirá al estudiante conceptualizar aspectos fundamentales de seguridad de cómputo, abordando políticas y procedimientos de seguridad, así como mecanismos de encriptación. En el segundo tema, Seguridad en Infraestructura Web, se aborda la seguridad en la capa de transporte, tratando principalmente los protocolos de tunelización SSL/TLS, ubicándolos adecuadamente dentro del modelo de protocolos TCP/IP. Además el estudiante aplicará el concepto de Infraestructura de Clave Pública (PKI) y sus componentes, con el fin de mostrar su utilidad en la generación de certificados digitales, también se aborda la seguridad en servidores que tiene como intención el estudio de la seguridad del lado del servidor, incluyendo temas que ilustran la operación de servidores con servicios configurados de forma segura. También se incluyen conceptos de seguridad perimetral como el uso de cortafuegos, sistemas de detección de intrusos y canales seguros con VPNs. El tercer tema estudia un requisito esencial de la seguridad como es la autenticación, indispensable en el desarrollo de aplicaciones Web que soliciten acceso a usuarios, creación y seguimiento de sesiones, etc. En el cuarto tema se trata el manejo de perfiles exponiendo mecanismos genéricos que controlen el correcto y eficiente acceso a módulos de una aplicación dependiendo de las características y derechos de los usuarios, bajo la premisa de que no todos los usuarios pueden acceder a los mismos módulos ni tampoco con los mismos permisos.

Todas las actividades de desarrollo deberán ser documentadas por el estudiante de manera que pueda demostrar competencias genéricas como son: Trabajo en equipo, capacidad de aplicar los conocimientos en la práctica, expresión escrita y oral. Se recomienda que todas las actividades realizadas en el curso sean debidamente propuestas y guiadas por el facilitador realizando evaluaciones formativas y sumativas. Las actividades podrán realizarse en equipo donde el alumno podrá demostrar sus competencias genéricas, trabajo colaborativo, participación en equipo, etc. Las competencias específicas que el alumno logrará en la asignatura, deberán ser las suficientes como para lograr que las aplicaciones Web sean funcionales, seguras y de calidad profesional, debidamente validadas y con interfaces agradables.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Zacatepec. Departamento de Sistemas y Computación. Academia de Sistemas y Computación. Reunión para el desarrollo de Especialidades del 22 de Febrero de 2018.	M.C. Humberto Tiburcio Zúñiga, Lic. Venancio Bárcenas Martínez, Ing. Yanet Castrejón Hernández, M.C. Norma J. Ontiveros Hernández, M.T.I. Jesús Ángel Peña Ramírez, Lic. Victor Hernandez Rodriguez, Dra. Ana Celia Campos Hernández, y Dr. Sócrates Espinoza Salgado.	Programa aprobado en el pleno de la Academia de Sistemas y Computación. Esta materia forma parte de la especialidad: **Aplicaciones en entornos Web y Móvil**, para la Carrera Ingeniería en Sistemas Computacionales, Plan de estudios ISIC-2010-224.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Implementa mecanismos de seguridad en infraestructura de software y hardware para el desarrollo de aplicaciones Web.

5. Competencias previas

- Implementa sistemas de infraestructura de software y hardware en redes para dar solución a problemas que impliquen una correcta administración de recursos computacionales.
- Desarrolla programas de cómputo basados en modelado de objetos para resolver problemas reales en diferentes contextos.
- Implementa Sistemas de base de datos basadas en SQL para el almacenamiento estructurado y eficiente acceso de información.

6. Temario

No.	Temas	Subtemas
1	Introducción a la Seguridad	1.1 Requerimientos de seguridad (privacidad, integridad, disponibilidad, autenticación). 1.2 Sistemas criptográficos de clave privada y de clave pública. 1.3 Primitivas criptográficas(firmas digitales, estampas de tiempo, funciones hash, MACs). 1.4 Infraestructura de clave pública.
2	Seguridad en Infraestructura Web	2.1 Seguridad en la capa de transporte (SSL, TLS, DTLS) 2.2 Servidores seguros 2.3 Firewall e IDS 2.4 Protocolos tunelizados y VPN

3	Autenticación	3.1 Mecanismos de autenticación 3.2 Sesiones de trabajo 3.2.1 Creación y seguimiento. 3.2.2 Eliminación 3.2.3 Personalizar 3.3 Control de los datos de autenticación 3.3.1 Bitácoras
4	Desarrollo de Perfiles	4.1 Estructura de perfiles 4.2 Desarrollo e implementación de perfiles 4.3 Definición de usuarios 4.4 Definición de permisos 4.5 Mapeo de programas

7. Actividades de aprendizaje de los temas

Nombre del Tema Introducción a la seguridad	
Competencias	Actividades de aprendizaje
Específica(s): Define los conceptos de seguridad informática para establecer políticas y procedimientos de seguridad y conocer los mecanismos encriptación. Genéricas: - Habilidad para buscar y analizar - Representa e interpreta conceptos en diferentes formas: gráfica, escrita y verbal - Habilidades básicas para elaborar diagramas - Trabajo en equipo - Aplicar conocimientos a la práctica.	• Búsqueda de información en internet. • Realizar lecturas sobre seguridad de cómputo y contestar cuestionarios • Utilizar herramientas (OpenSSL, PGP) disponibles para aplicar mecanismos de encriptación, crear llaves, certificados y firmas.

<table>
<tr><td colspan="2">Nombre del tema
Seguridad en infraestructura Web</td></tr>
<tr><td>Competencias</td><td>Actividades de aprendizaje</td></tr>
<tr><td>Específica(s):

Implementar infraestructura de seguridad en servidores basada en protocolos de seguridad SSL/TLS, para dar soporte al desarrollo y ejecución de aplicaciones Web.

Genéricas:

- Capacidad de análisis y síntesis
- Habilidad para buscar y analizar
- Trabajo en equipo
- Capacidad crítica y autocritica
- Habilidad de investigación
- Capacidad para aprender
- Capacidad de aplicar los conocimientos en la práctica.</td><td>- Búsqueda de información en Internet sobre la seguridad en la capa de transporte y realizar exposiciones.
- Instalar y configurar servidores con seguridad: SSH, HTTPS, etc.,
- Configurar cortafuegos simples que permitan filtrar tráfico de red en base a políticas permisivas y restrictivas.</td></tr>
<tr><td colspan="2">Nombre del Tema
Autenticación</td></tr>
<tr><td>Competencias</td><td>Actividades de aprendizaje</td></tr>
<tr><td>Específica(s):

Desarrolla módulos de autenticación que controlen el acceso seguro a las aplicaciones Web.

Genéricas:

- Trabajo en equipo
- Capacidad crítica y autocritica
- Capacidad para aprender
- Capacidad de aplicar los conocimientos en la práctica.</td><td>• Desarrollar un módulo de autenticación de usuarios con mecanismos de encriptación.
• Desarrollar un esquema de creación, seguimiento y cierre de sesiones de trabajo.</td></tr>
</table>

Nombre del Tema Desarrollo de Perfiles	
Competencias	Actividades de aprendizaje
Específica(s): Desarrolla módulos de seguridad para control de acceso a usuarios basado en perfiles. Genéricas: - Capacidad de análisis y síntesis - Trabajo en equipo - Capacidad crítica y autocritica - Capacidad para aprender - Capacidad de aplicar los conocimientos en la práctica.	• Desarrollar un modelo de base de datos para definir los perfiles. • Desarrollar los módulos que implementen el esquema de perfiles propuesto.

8. Práctica(s)

	Prácticas
1	Aplicar algoritmos de cifrado de información simétricos y asimétricos. Obtener valores Hash de cadenas de información dadas. Cifrar y descifrar archivos con firma digital.
2	Crear un servidor HTTP seguro sobre SSL con un certificado digital autofirmado. Configurar un servidor SSH para realizar conexiones remotas seguras y transferencia de archivos seguros. Instalar, configurar y probar un firewall para permitir o denegar accesos.
3	Crear un usuario que se autentique con una contraseña cifrada con MD5. Desarrollar un módulo que cree, de seguimiento, defina tiempo de vida y cierre una sesión de trabajo a partir de un usuario autenticado.
4	Desarrollar un módulo que permita definir las características del contexto de sesión de un usuario para un perfil determinado.

9. Proyecto de asignatura

Desarrollar una aplicación Web que resuelva un problema del mundo real. La aplicación deberá montarse en un servidor WEB seguro con cifrado SSL, instalando un certificado digital autofirmado.

La aplicación deberá cumplir con las siguientes especificaciones:

1. Debe estar basado en la filosofía de diseño MVC (Modelo Vista Controlador).
2. El sistema deberá implementarse de forma modular. En donde la función de cada módulo este específicamente definida.
3. Deberá contar con un módulo de autenticación, que valide las credenciales del usuario para su acceso al sistema.
4. Deberá contar con un módulo que implemente perfiles, que determinen los permisos de acceso de cada usuario, a los distintos módulos del sistema.
5. El documento del proyecto deberá fundamentarse a partir de los siguientes aspectos:
    - Base teórica
    - Planeación del proyecto
    - Evidencia de la ejecución realizada
    - Conclusiones y recomendaciones

10. Evaluación por competencias

- Realizar evaluación diagnóstica al iniciar el curso y retroalimentar al alumno.
- Motivar y llevar a cabo la evaluación entre pares.
- Realizar evaluaciones mediante: cuestionario teórico, desarrollo de prácticas de laboratorio, tarea y ejercicios.
- Desarrollar proyecto integrador.

11. Fuentes de información

1. Egan, M. (2004).The Executive Guide to Information Security, Estados Unidos: Editorial Addison Wesley.
2. Oppliger, R. (2009). SSL and TLS Theory and Practice, Estados Unidos: Editorial

ArtechHouse.

3. Knudsen, J. (1998). Java Crytography, Estados Unidos: O´Reilly.
4. Hunter, J., Crawford, W. (2001). Java Server Programming, Estados Unidos: O´Reilly.
5. Oaks, S. (1998). Java Security, Estados Unidos: O´Reilly.
6. Murach, J., Urban, M. (2014). Java Servlets and JSP, Estados Unidos: Ray Halliday
7. Kurniawan, B. (2012). Servlet & JSP: A Tutorial, Estados Unidos: BrainySoftware.com