1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad en Aplicaciones Web
Clave de la asignatura:	DSB-2305
SATCA[1]:	1-4-5
Carrera:	Ingeniería Informática

2. Presentación

Caracterización de la asignatura

La asignatura de Seguridad Web aporta al perfil del egreso, los conocimientos, habilidades y metodologías para garantizar la seguridad de las aplicaciones Web. Esta asignatura toma una importancia trascendental debido que la información es un recurso elemental para la toma de decisiones de cualquier organización y garantizar la seguridad e integridad es una meta que debe ser atendida.

La asignatura de Seguridad Web se encuentra estructurada de tal manera que el aprendizaje sea evolutivo en el conocimiento adquirido iniciando con los conceptos legales de seguridad y las principales amenazas a lo que se encuentra expuesta nuestra información en la web.

Es sumamente importante porque las habilidades que propicia en el estudiante permiten que se involucre en áreas tales como configuración, administración, análisis, auditoria, base de datos y desarrollo web, mismas que hoy en día son imprescindibles para toda empresa a nivel mundial.

Se sugiere que esta asignatura se aborde en forma teórico-práctico, es necesario que el personal docente explique y demuestre con ejemplos los posibles ataques a las aplicaciones web, así como su prevención.

Intención didáctica

Hacer uso de herramientas automatizadas para evaluar la vulnerabilidad de las aplicaciones web y tomar las medidas pertinentes para paliar las debilidades.
En la primera unidad se identifican los elementos de seguridad y los aspectos legales que lo rigen en relación al uso y protección de datos en la Internet

1 Sistema de Asignación y Transferencia de Créditos Académicos

En la segunda unidad se revisan las técnicas de la ingeniería social cuyo fin es la obtención de datos de forma engañosa así mismo se revisan los mecanismos de cómo evitarlo. En la tercera se implementan las medidas pertinentes para asegurar que las aplicaciones web tengan un alto grado de seguridad. En la cuarta se aborda los temas sobre la autenticación para comprender como funcionan los protocolos y mecanismos que utilizan las aplicaciones web modernas para poder iniciar sesión con API'S de terceros y seguir manteniendo la integridad de la información que se comparte al momento de autorizar acceso a sistemas de información.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico del Valle de Oaxaca, 16 de octubre de 2019.	Academia de Ingeniería Informática e Ingeniería en Tecnologías de la Información y Comunicaciones del ITVO	Taller para generar la especialidad de la Ingeniería Informática.

4. Competencia(s) a desarrollar

Competencia específica de la asignatura
Identifica los aspectos legales que rigen la seguridad en Internet para hacer conciencia acerca de las implicaciones legales de acceder a datos no autorizados, así como las posibles vulnerabilidades de este tipo de sistemas con el objetivo de conocer posibles puntos de acceso no autorizados y corregirlos

5. Competencias previas

Desarrolla aplicaciones mediante el paradigma MVC para mejorar el diseño y funcionalidad de las mismas. Desarrolla aplicaciones usando diferentes lenguajes de programación Web (HTML, CSS, Javascript, PHP, etc.) para crear aplicaciones dinámicas con herramientas diversas. Administra de base de datos relacionales a través de distintos motores.

6. Temario

No.	Temas	Subtemas
1	Introducción a la Seguridad	1.1 Los principios de seguridad 1.2 Estados de los datos 1.3 Seguridad en Internet. 1.4 Legislación informática en México. 1.4.1 Comercio electrónico 1.4.2 Firma electrónica
2	Amenazas y vulnerabilidades	2.1 Tipos de ciberataques 2.2 Ingeniería social 2.2.1 Técnicas de Ingeniería social 2.2.2 Técnicas de Protección 2.3 Phising 2.4 Malware 2.5 Ransomware
3	Vulnerabilidad de las aplicaciones web.	3.1 Ataques de inyección de scripts. 3.1.1 XSS (Cross-Site Scripting). 3.1.1.1 XSS Reflejado 3.1.1.2 XSS Almacenado 3.1.1.3 XSS Basado en DOM 3.1.2 CSRF (Cross-Site Request Forgery). 3.1.3 Clickjacking. 3.2 Ataques de inyección de código. 3.2.1 SQL (Inyeccion SQL). 3.2.1.1 Serialized SQL Injection. 3.2.1.2 Inyecciones SQL y NoSQL 3.2.1.3 Blind SQL Injection. 3.2.1.6 RFD (Remote File Downloading). 3.2.2 Ataques a archivos. 3.2.2.1 Ataques de inyección de archivos. 3.2.2.2 LFI(Local File Inclusion). 3.2.2.3 RFI(Remote File Inclusion). 3.4 Denegación de Servicio (DoS).
4	Autenticación de Aplicaciones Web	4.1 Introducción a la Autenticación. 4.2 Autorización. 4.3 JSON Web Tokens. 4.3.1 Autenticación. 4.3.2 JWT. 4.4 OAuth 2.0. 4.4.1 OpenID Connect. 4.5 Middleware.

7. Actividades de aprendizaje de los temas

1. Seguridad de la Información y aspectos legales	
Competencias	**Actividades de aprendizaje**
Competencia Específica: Identifica la importancia de la seguridad de la información, así como las implicaciones legales del acceso no autorizado. **Competencias Genéricas:** Comunicación oral y escrita. Capacidad de investigación. Trabajo en equipo. Capacidad de aprender. Desarrolla las actividades con apego a la ética.	Investigación en diversas fuentes bibliográficas y electrónicas sobre aspectos de seguridad de la información y el marco jurídico en materia de seguridad informática. Foro en clase de los diversos delitos informáticos que pueden existir y la forma en que se pueden proteger los programas de cómputo y la información. Debate sobre el tema "el papel del ingeniero en informática en la seguridad de la información"
2. Amenazas y ataques web	
Competencias	**Actividades de aprendizaje**
Competencia Específica: Implementa diversas técnicas para auditar el desarrollo de aplicaciones web y garantizar la seguridad **Competencias Genéricas**: Desarrolla las actividades con apego a la ética. Capacidad de aprender.	Investigación en diversas fuentes el concepto de "Phishing" Reflexión sobre el punto anterior y concluir mediante una lista que muestre las técnicas de ingeniería social más comunes para extraer información Elaboración de un diagrama que represente los principales ataques en la web y sus posibles consecuencias para el usuario Elaboración un cartel tamaño tabloide de forma individual para divulgar dentro del Instituto, las precauciones que se deben seguir para protegerse del phishing.

3. Vulnerabilidad de las aplicaciones web	
Competencias	**Actividades de aprendizaje**
Competencia Específica: Clasifica las distintas amenazas y ataque web, así como técnicas de ingeniería social para la extracción de información de manera ilegal. **Competencias Genéricas:** Capacidad de investigación en diversas fuentes bibliográficas. Trabajo en equipo. Capacidad de aprender.	Investigación de diversas técnicas de ataques a las aplicaciones Web. Implementa técnicas manuales de inyección de SQL. Implementa técnica manuales de inyecciones de XSS. Ejecuta código malicioso con el fin de evaluar las configuraciones realizadas ante ataques de tipo DoS al servidor Web. Usa programas especializados (Herramientas de penetración) para evaluar la seguridad de las aplicaciones web. Elabora reportes técnico y ejecutivo de las pruebas ejecutadas.
4. Autenticación de Aplicaciones Web	
Competencias	**Actividades de aprendizaje**
Competencia Específica: Implementa y entiende conceptos de autenticación en tus aplicaciones Web. **Competencias Genéricas:** Capacidad de investigación en diversas fuentes bibliográficas. Trabajo en equipo. Capacidad de aprender. Desarrolla las actividades con apego a la ética y lo legal. Creatividad (busca nuevas vulnerabilidades en las aplicaciones Web).	Investigación del protocolo para la autorización de APIs Oauth 2.0. Desarrolla una aplicación web que utilice un inicio de sesión consumiendo la API de Google Gmail utilizando el protocolo Oauth 2.0.

8. Práctica(s)

Capturar y analizar una sesión Web completa para determinar las características de tráfico y seguridad de la aplicación.
Desarrollar una Aplicación Web que implemente mecanismos de seguridad.
Someter la Aplicación Web desarrollada a las pruebas de ataque utilizando las diferentes técnicas para ello.
Ejecutar pruebas de vulnerabilidad a sitios Web con el objetivo de probar su seguridad, garantizando de que los efectos negativos sean mínimos y actuando siempre de manera responsable.
Realizar un inicio de sesión que utilice el protocolo Oauth 2.0.

9. Proyecto de asignatura

"Auditorías de seguridad y pruebas de intrusión a las WebApps"

Una auditoría de seguridad informática es el estudio que comprende el análisis y gestión de un Sistema Informático para identificar, enumerar y, posteriormente, escribir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de sus estaciones de trabajo, redes de comunicaciones o servidores y las WebApps.

Fundamentación: Cada vez es mayor la percepción de la importancia de proteger la información en relación a sus tres componentes principales:

• Confidencialidad

• Integridad

• Disponibilidad

La información es uno de los activos de mayor importancia para la organización, por lo que necesita estar bien protegida.

La interacción en línea donde la información está cada vez más expuesta a un mayor número de amenazas y vulnerabilidades incrementa la necesidad de una protección reforzada sobre la misma, y es responsabilidad del encargado de tecnologías de la información proteger estos datos y cumplir las disposiciones legales en materia de protección de datos personales por un lado y por otro lado, muchos de estos datos son privados, de vital importancia para la empresa y probablemente, su capital más preciado. Una falta de seguridad en las TIC nos puede conducir a pérdidas millonarias sufriendo graves prejuicios, tanto a nivel económico

como social, desmejorando la imagen de la empresa y la confianza con la organización, así como una pérdida significativa de los clientes.

Planeación: Para llevar a cabo este proyecto, se forman equipos de 3 a 5 integrantes, se determinan los roles y actividades, el sitio objetivo a evaluar, se asignan las actividades y se elabora un cronograma que sirva de guía para la ejecución del proyecto.

Ejecución: Para lograr el objetivo planeado es importante documentar todos los procesos que se vayan realizando, actuar siempre con responsabilidad y apego con las normas éticas para evitar daños a la organización.

10. Evaluación por competencias

Informe técnico

- Resumen del proceso realizado
- Clasificación de las vulnerabilidades encontradas y su nivel (alto, medio, bajo)
- Propuesta de correcciones y sugerencia de buenas prácticas

Informe ejecutivo.
Reflexión personal sobre las implicaciones en temas de Seguridad Web

Evaluación por competencias:

- Investigación
- Mapas conceptuales
- Bitácora
- Proyecto Uso de listas de cotejo.
- Rúbricas.

11. Fuentes de información

Aceituno Canal (2004). Seguridad de la Información. Madrid. España: Creaciones Cppyright

Dafid Stuttard, Marcus Pinto (2007). The Web Application Hacker's HandBook. Indianapolis, Indiana: Wiley Publishing, Inc.

Enrique Rando y Chema Alonso (2010). Hacking de Aplicaciones Web: SQL Injection. España: OxDWORD

García y Pérez (2011). Hacking y Seguridad en comunicaciones móviles GSM / GPRS / UMTS / LTE. Madrid. España : Ed. Informatica64.

Johnny Long (2008). Google Hacking for Penetration Testers - Volume 2. Syngress: USA: Syngress Media Inc

Moron Lerma, Esther (2005). Aspectos legales de la seguridad informática. Bilboa, España: Planeta UOC.

Mike Shema (2012). Hacking Web Apps: Detecting and Preventing Web Application Security Problems. Syngress. USA: Syngress

Parravicini, Luis (2011). Programación web segura. Hackeando tu aplicación. Argentina: Edición del Autor

Rando, Alonso (2012). Hacking de Aplicaciones Web: SQL Injection: Móstoles, Madrid: Edición del Autor

- http://www.taddong.com/docs/RootedCon2011-AtaquePracticoGPRS.pdf
- http://www.penetration-testing.com/home.html
- http://www.protektnet.com/servicios_ley_proteccion.html
- http://www.protektnet.com/servicios_gestion_seguridad.html