Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación
Licenciatura en Computación

Componente Profesional
Opción Aplicaciones en Internet

SEGURIDAD EN LA WEB

UC	HT	HP	HL	Modalidad	Código	Requisito	Ult. Actualización
5	4	2		Optativa / Electiva	6026	Aplicaciones con tecnologías de Internet	Febrero - 2009

Fundamentación:

El amplio uso de tecnologías web para el desarrollo e implantación de aplicaciones tanto para Internet como para las Intranet corporativas ha generado altos riesgos de seguridad, al aumentar las amenazas y al descubrir diariamente vulnerabilidades en las plataformas que soportan estas aplicaciones. Por lo tanto es primordial que los estudiantes de la licenciatura de Computación tengan conocimientos y habilidades para desarrollar e implantar aplicaciones web minimizando los riesgos de seguridad.

Objetivos:

- Conocer los fundamentos de la Seguridad para aplicaciones Web.
- Familiarizar al estudiante con los problemas de seguridad de las aplicaciones Web.
- Identificar las amenazas, vulnerabilidades que pueden afectar la integridad, confidencialidad y disponibilidad de las aplicaciones web.
- Entender y establecer los lineamientos, estándares, mecanismos y medidas de seguridad necesarios para desarrollar e implantar aplicaciones web.
- Establecer las mejores practicas de desarrollo e implantación de aplicaciones Web desde el punto de vista del Cliente, el Servidor y el transito de datos entre ellos.

Contenidos Temáticos

1. Fundamentos de la Seguridad Web.
   Ética profesional de la persona de seguridad informática. Conceptos de la Seguridad Informática. Tecnologías y componentes de la Seguridad Informática. Anatomía de ataques informáticos. Introducción a mecanismos de cifrado simétrico y asimétricos. Protocolo HTTP Seguro, SSL, TLS.

2. Seguridad del lado del Cliente.
   Amenazas, vulnerabilidades y ataques comunes del lado del cliente. Lineamientos, estándares, mecanismos, medidas y mejores practicas a ser tomadas en cuenta para las validaciones de campos de formularios a través de JavaScript, almacenamiento las cookies, uso de los headers HTML y HTTP, uso de los campos ocultos y la subida de archivos, uso de interfaces enriquecidas, uso de Ajax, almacenamiento de datos de los usuarios en los navegadores.

3. Seguridad del lado del Servidor.
   Amenazas, vulnerabilidades y ataques comunes del lado del servidor. Lineamientos, estándares , medidas, mecanismos y mejores practicas a ser tomadas en cuenta cuando se desarrolla del lado del servidor en cuanto al uso de sesiones, la recuperación de password, la validación de datos de entrada, el buffer overflow, los ataques Cross-Site Scripting, los ataques SQL Injection, la

autenticación de usuarios, la autorización de privilegios, el manejo de configuraciones, el control de cambios, el acceso a los datos sensibles almacenados, la codificación de URLs, la sanación de datos de entradas.

4. Seguridad en el transito de datos del cliente al servidor.
   Amenazas, vulnerabilidades y ataques comunes en el transito de datos. Lineamientos, estándares, medidas, mecanismos y mejores practicas a ser tomadas en cuenta cuando se desarrolla del lado del cliente y del servidor en cuanto a cifrado de información sensible del lado del cliente, validación de URLs y su codificación, uso de HTTPS, SSL y TLS.

5. Arquitecturas de seguridad informática.
   Como definir y establecer arquitecturas de seguridad informática, tomando el cuenta los modelos de arquitectura y métodos de desarrollo de aplicaciones web.

Bibliografía:

- Curphey M., Scambray J., Olson E., Howard M. Improving Web Application Security: Threats and Countermeasures. Microsoft Corporation. 2003
- Chaudhry I., Clarke J., Veney,S. Web Application Security Assessment. Microsoft Corporation.
- Neil D., Christoph K., Anita K. Foundations of Security: What Every Programmer Needs to Know (Expert's Voice). Apress. 2007
- Phillip Windley. Digital Identity. O'Reilly. 2005
- Shreeraj Shah. Web 2.0 Security - Defending AJAX, RIA, AND SOA. Thomson. 2008
- Hoffman B., Sullivan B. Ajax Security. Pearson. 2007.
- Dobromir Todorov. Mechanics of User Identification and Authentication: Fundamentals of Identity Management. Auerbach Publications. 2007.
- Stuttard D., Pinto M. The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws. Wiley Publishing. 2008.
- Howard M., Lipner S. The Security Development Lifecycle. Microsoft Corporation. 2006