academia madesyp

AUDITORIA DE APLICACIONES WEB CON METODOLOGIA OWASP 3.0 (20 H.)

⊙ Descripción del Curso

Este Curso de 20 horas permitirá al participante auditar aplicaciones web de modo seguro presentando ejemplos reales de vulnerabilidades en las aplicaciones, el mecanismo de explotación y su correspondiente contramedida.

⊙ Objetivos

Después de completar el curso, el participante será capaz de:

- Hacer una valoración de las amenazas que tienen las aplicaciones
- Identificar las normas o estándares del mercado para comercio electrónico
- Conocer los mecanismos de autenticación y sus problemas asociados
- Identificar los requerimientos necesarios para autenticar las aplicaciones
- Reconocer los principales fallos de seguridad asociados a validación de datos
- Realizar pruebas sobre las aplicaciones para la explotación de vulnerabilidades
- Identificar los requisitos para el control de errores y auditoría

⊙ Perfil

Consultores, Ingenieros de Sistemas, Desarrolladores y todos aquellos que manejen información restringida o confidencial para la empresa

⊙ Prerrequisitos

- Experiencia en desarrollo de aplicaciones web
- Experiencia en Bases de Datos
- Conocimiento de alguno de los lenguajes: PHP, ASP, Java, Perl
- Alto nivel de compresión de lectura en inglés

⊙ Materiales entregados

- Presentaciones, documentos y herramientas relevantes con acceso online
- Guía OWASP impresa
- Certificado de Asistencia (para aquellos que asistan a un mínimo del 80%)

Academia MADESYP
Cl. Tejares, nº 76 – Bajo · 02002 – Albacete · Tlfno. 967-044 939
http://www.madesyp.com madesyp@madesyp.com

academia madesyp

⊙ Programación

MODULO	RESUMEN	CONTENIDO
Modulo I A1 – Injection	Las vulnerabilidades de inyección como SQL, sistema operativo y LDAP, ocurren cuando los datos no son de confianza y son enviados a un intérprete como parte de un comando o consulta. Datos hostiles del atacante podrían engañar al intérprete para que este ejecute comandos no deseados o tener acceso a datos no autorizados.	Tipos y clasificación de inyecciones Riesgos Asociados Mecanismos de Defensa: - Parameterized Queries (Prepared Statements) - Procedimientos Almacenados - Escape de datos de entrada - Privilegio Mínimo - Validación de "Lista Blanca" CWE 77 y 89
Modulo II A2 – Cross-Site Scripting (XSS)	Las fallas de XSS ocurren cuando una aplicación toma datos que no son de confianza y lo envía a un navegador web sin una validación adecuada y control de caracteres de escape. XSS permite a los atacantes ejecutar scripts en el navegador de la víctima que pueden robar sesiones de usuario, desfigurar sitios web, o redirigir al usuario a sitios maliciosos.	Tipos y clasificación de XSS Riesgos Asociados Reglas de prevención en: - HTML - JavaScript - CSS/DHTML - DOM CWE 79
Modulo III A3 – Broken Authentication and Session Management	Funciones relacionadas con la autenticación de aplicaciones y gestión de sesiones a menudo no se aplican correctamente, lo que permite a los atacantes comprometer contraseñas, claves, tokens de sesión, o la explotación de otros defectos de aplicación asumiendo la identidad de otros usuarios.	Técnicas y Principios de Autentificación Gestión de Sesiones Seguras CWE 287
Modulo IV A4 – Insecure Direct Object Referentes	Una referencia de objeto directo se produce cuando un desarrollador expone una referencia a un objeto de implementación interna, tal como un archivo, directorio o base de datos clave. Sin un control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder a datos no autorizados.	Implementación de control de acceso Filtros CWE 22 y 639
Modulo V A5 – Cross-Site Request Forgery (CSRF)	Un ataque CSRF fuerza una sesión en el navegador de la víctima para enviar una petición HTTP falsa, incluida la cookie de sesión de la víctima y cualquier otra información de autenticación incluida automáticamente a una aplicación web vulnerable. Esto permite a un atacante forzar el navegador de una víctima para que genere solicitudes a la aplicación vulnerable de manera que piense que son peticiones legítimas.	Synchronizer Token Pattern CSRFGuard Project CWE 352
Modulo VI A6 – Security Misconfiguration (NEW)	Una buena seguridad requiere tener una configuración segura, definida e implementada para; la aplicación, frameworks, servidor de aplicaciones, servidor web, servidor de base de datos, y la plataforma. Todos estos ajustes deben ser definidos, implementado y mantenido, ya que muchos no se entregan con valores predeterminados seguros. Esto incluye el mantener todo el software al día, incluyendo todas las bibliotecas de código que utiliza la aplicación.	Arquitecturas Seguras Seguridad de Servicios de Infraestructura - Servidores de Aplicaciones - Bases de Datos - Sistemas Operativos - Servicios de Directorio

academia madesyp

MODULO	RESUMEN	CONTENIDO
Modulo VII A7 – Insecure Cryptographic Storage	Muchas aplicaciones web no implementan una adecuada protección de datos sensibles, como tarjetas de crédito, números de Seguro Social y credenciales de autenticación, con un cifrado apropiado o huellas digitales. Los atacantes pueden robar o modificar datos débilmente protegidos para llevar a cabo robo de identidades, fraudes de tarjetas de crédito, y otros delitos.	Uso seguro de librerías criptográficas Integridad y Confidencialidad CWE 310, 312 y 326
Modulo VIII A8 – Failure to Restrict URL Access	Muchas aplicaciones web comprueban los derechos de acceso de una dirección URL antes de desplegar vínculos y botones. Sin embargo, las aplicaciones necesitan controles similares de control de acceso cada vez que se accede a estas páginas, o atacantes serian capaces de falsificar URLs para acceder a páginas ocultas o protegidas.	Autenticación y Autorización Control de Acceso Filtros CWE 285
Modulo IX A9 – Insufficient Transport Layer Protection	Las aplicaciones frecuentemente fallan para autenticar, cifrar y proteger la confidencialidad e integridad del tráfico de red sensible. Cuando lo hacen, usan algoritmos débiles, certificados vencidos o no válidos, o no los usan correctamente.	Criptografía: Algoritmos y Claves Infraestructura de Claves Publicas Certificados Digitales Gestión y Almacén de Claves criptográficas HTTPS/SSL
Modulo X A10 – Unvalidated Redirects and Forwards (NEW)	Las aplicaciones Web frecuentemente redireccionan ó reenvían a los usuarios a otras páginas y sitios web, usando datos no confiables para determinar las páginas de destino. Sin validación adecuada, los atacantes pueden redirigir a las víctimas a sitios phishing o malware, o usar reenvíos para acceder a páginas no autorizadas.	Protocolo http Redirecciones Seguras Técnicas anti-phishing CWE 601

⊙ Modalidad

- Modalidad presencial de Lunes a Jueves.

⊙ Precio

- **Importe total del Curso: 120 Euros** (exento de IVA según Artículo 20, apartado uno, número 9º, de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido)

⊙ Fechas programadas

- Octubre, Noviembre y Diciembre de 2012 en horario de tardes de 20:30 a 22:30 horas. Consultar con el Centro de Formación para más información sobre los grupos.