Universidad Nacional de Luján
REPUBLICA ARGENTINA

Nº DISPOSICION:

NOMBRE DE LA ACTIVIDAD: "Taller de Desarrollo Seguro Modelado de amenazas y prevención de vulnerabilidades más frecuentes"

| | |
|---|---|
| Grupo de Trabajo (detalle de antecedentes de los instructores – formación profesional y/o laboral)<br><br>A.S. Mauro A. Meloni – Jefe de División Administración de Seguridad. | Cantidad de Horas: 12 hs.<br><br>Teóricas: 5 hs.<br><br>Prácticas: 7 hs. |
| OBJETIVOS GENERALES:<br><br>Se espera que luego de finalizado el taller, los participantes sean capaces de:<br>• Identificar y ejemplificar las vulnerabilidades consideradas críticas por la industria de desarrollo de aplicaciones web.<br>• Determinar y examinar las amenazas y vulnerabilidades a las que está expuesta cualquier<br>• aplicación.<br>• Reconocer y detectar de manera proactiva las falencias del desarrollo de las aplicaciones.<br>• Diseñar y desarrollar modelos de amenazas para aplicaciones de software.<br>• Aplicar las contramedidas necesarias para aumentar la seguridad de las aplicaciones. | |
| MODALIDAD:<br><br>Presencial | |
| DESTINATARIOS:<br><br>Personal No Docente que desempeñe funciones en la Dirección General de Sistemas | |
| CANTIDAD MÁXIMA DE ALUMNOS:<br><br>30 personas | |
| REQUISITOS PARA EL CURSADO:<br><br>Ninguno | |
| CANTIDAD DE ENCUENTROS:<br><br>4 encuentros | |
| RECURSOS NECESARIOS:<br><br>Materiales requeridos: computadora, proyector, pizarra, marcadores (equipo de capacitación); cuaderno de anotaciones, bolígrafo (participantes). | |

**CONTENIDOS A DESARROLLAR**

**Unidad 1:**

El modelado de amenazas en el ciclo de vida de desarrollo de software

Objetivo: introducir a los asistentes al modelado de amenazas orientado al software como un proceso que permite a los equipos de desarrollo comprender las amenazas de seguridad que pueden afectar a un sistema informático.

Temario:

- El ciclo de Vida de desarrollo de software
- El proceso de modelado de amenazas orientado de software
- Diagramación de arquitectura de aplicaciones
- Enumeración de amenazas
- Mitigación de amenazas

Estrategia didáctica: desarrollo del contenido teórico, exposición de un caso problema, formación de grupos de trabajo para analizar casos particulares, intercambio y discusión de los resultados.

Materiales requeridos: computadora, proyector, pizarra, marcadores (equipo de capacitación); cuaderno de anotaciones, bolígrafo (participantes).

Tiempo estimado: 4 horas.

**Unidad 2**

Vulnerabilidades más comunes en aplicaciones web

Objetivo: acercar a los asistentes las vulnerabilidades de seguridad más importantes en aplicaciones web y sus consecuencias, proveyendo técnicas básicas para proteger de las distintas amenazas en el entorno y promoviendo la incorporación de estas técnicas y otras buenas prácticas en los desarrollos.

Temario:

- Introducción a la última edición del Top 10 del Open Web Application Security Project (OWASP)
- A1 Inyección de código
- A2 Pérdida de autenticación y gestión de sesiones
- A3 Secuencia de comandos en sitios cruzados
- A4 Referencia directa insegura a objetos
- A5 Configuración de seguridad incorrecta
- A6 Exposición de datos sensibles
- A7 Ausencia de control de acceso a funciones
- A8 Falsificación de peticiones en sitios cruzados
- A9 Utilización de componentes con vulnerabilidades conocidas
- A10 Redirecciones y reenvíos no validados

Estrategia didáctica: desarrollado del contenido teórico, discusión de problemáticas particulares y alternativas de mitigación con los participantes.

Tiempo estimado: 3 hs.

**Unidad 3**

Objetivo: analizar las vulnerabilidades vistas en la unidad anterior mediante una serie de escenarios de ataque sobre aplicaciones vulnerables en entornos virtuales de práctica, buscando comprender el origen de las vulnerabilidades y las formas de prevención habituales.
Estrategia didáctica: presentación del entorno virtual de práctica, resolución de ejercicios prácticos entre pares, discusión de los resultados.
Materiales requeridos: computadora, proyector, pizarra, marcadores (equipo de capacitación); computadoras (una por cada dos participantes) conectadas en red, entornos virtuales de práctica (provistos por los el equipo instructor).
Tiempo estimado: 5 hs.

**FORMA DE EVALUACIÓN. (Desarrollo)**

**REQUISITOS DE ASISTENCIA**: Se requiere la asistencia de los participantes al 80% de los encuentros.

La evaluación de los aprendizajes será de proceso: en cada encuentro se propondrá una actividad de análisis grupal y/o global en la que el instructor planteará un interrogante o problema para el análisis y discusión. La participación en estas actividades contribuye al seguimiento de los avances, la orientación y reorientación de los aprendizajes.

**BIBLIOGRAFIA**

De carácter obligatorio:
• "Microsoft Threat Modeling Tool 2014 User Guide". Microsoft Corporation. 2014
http://www.microsoft.com/security/sdl/adopt/starterkit.aspx http://aka.ms/By12as
• "OWASP Top 10 – 2013. Los diez riesgos más críticos en aplicaciones web".
The OWASP Foundation. 2013
https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf
• Material de los encuentros de capacitación sobre Seguridad en el Ciclo de Vida de Desarrollo de Software desarrollados en 2012.
De consulta:
• Shostack, Adam. "Threat Modeling: Designing for Security". John Wiley & Sons. 2014
• Kendall K & Kendall J. "Análisis y diseño de sistemas". 6ta ed. Capítulo 7 "Uso de diagramas de flujo de datos". Pearson Educación. México, 2005
• Gane, C. Sarson, T. "Structured System Analysis: Tools and techniques". IST Databooks. McDonalds Douglas Corporation. 1986.