WIZELINE

Seguridad en Aplicaciones y Mejores Prácticas de Seguridad en Codificación

Documento Informativo

Digital Skills Accelerator-Wizeline

Dirigido al equipo de Desarrollo de Carrix

Etapa: Entrenamiento

CONTENIDO

Bienvenido/a

Te damos la más cordial bienvenida a la etapa de entrenamiento del curso “Seguridad de Aplicaciones y Mejores Prácticas de Seguridad en Codificación". A continuación, encontrarás toda la información necesaria que deberás revisar para prepararte de la mejor forma para esta experiencia.

Objetivo del Entrenamiento

Este entrenamiento tiene como objetivo brindar a los participantes una comprensión integral de las mejores prácticas de codificación segura, permitiéndoles desarrollar software robusto contra amenazas de ciberseguridad.

A través de conocimientos teóricos y ejemplos prácticos, los participantes aprenderán la importancia de la seguridad de las aplicaciones, los principios esenciales de codificación, los principios de codificación segura, la identificación y mitigación de vulnerabilidades y la optimización de los procesos de desarrollo.

Sesión Informativa Pre-Entrenamiento

Previo al arranque del entrenamiento, participarán en una sesión informativa en donde se te compartirá toda la información relacionada con el entrenamiento y en donde podrás resolver cualquier duda que tengas con referencia a esta experiencia.

El día **28 de Septiembre 2023** se habilitarán 2 bloques de sesiones informativas para que puedas elegir la que mejor se acomode a tu carga laboral:

Bloque 1 : 11:00 am a 12:00 pm **Zoom**

Bloque 2 : 5:00 pm a 6:00 pm **Zoom**

Estructura del Entrenamiento

- **Duración:** Cada sesión durará 1 hora y 30 minutos
- **Cadencia:** Las sesiones del entrenamiento se llevarán de forma semanal los días Lunes y Miércoles.
- **Horario:** 5:00 PM a 6:30 PM CST
- **Medio:** Todas las sesiones serán en vivo a través de **Zoom**

Módulos de Entrenamiento

El entrenamiento está dividido en tres módulos que contienen distintos temas centrales para el objetivo del entrenamiento:

MODULO 1	MODULO 2	MODULO 3
Introducción a la seguridad de aplicaciones y mejores prácticas en codificación.	**Técnicas de codificación segura.**	**Evaluación de riesgos y gestión de vulnerabilidades.**
• **Sesión 1 :** Importancia de la seguridad de las aplicaciones • **Sesión 2 :** Mejores prácticas en codificación • **Sesión 3 :** Prácticas de codificación segura • **Sesión 4 :** Mejores prácticas de software	• **Sesión 5 :** Principios de codificación segura • **Sesión 6 :** Validación de entrada • **Sesión 7 :** Autenticacion y autorizacion • **Sesión 8 :** Estándares de protección de datos • **Sesión 9 :** Criptografía	• **Sesión 10 :** Marco de evaluación de riesgos • **Sesión 11 :** Categorización de vulnerabilidad • **Sesión 12 :** Identificación de vulnerabilidades • **Sesión 13 :** Mitigación y remediación de vulnerabilidades

Onboarding GitHub (Modulo Adicional)

Parte integral de la dinámica del entrenamiento será el uso de GitHub. Éste se usa como un repositorio central de información y con el fin de que conozcas su funcionamiento y aplicación, se tendrán tres sesiones de onboarding para conocer esta herramienta. A continuación te mostramos los diferentes horarios en los que se darán las sesiones. Tú podrás elegir la que mejor se acomode a tu carga laboral.

¿Por qué usar GitHub? *GitHub es un servicio basado en la nube que aloja un sistema de control de versiones (VCS) llamado Git. Éste permite a los desarrolladores colaborar y realizar cambios en proyectos compartidos, a la vez que mantienen un seguimiento detallado de su progreso.*

¿Qué es Git? *Es un sistema de control de versiones distribuido diseñado para ayudar a gestionar los cambios del código fuente durante el desarrollo de software. Permite a los desarrolladores realizar un seguimiento de los cambios en su código base, colaborar con otros y mantener múltiples versiones de su trabajo.*

Fechas y Horarios

- **3 de Octubre :** 5:00 - 6:30 PM **Zoom**
- **5 de Octubre :** 5:00 - 6:30 PM **Zoom**
- **6 de Octubre 2023 :** 11:00 - 12:30 PM **Zoom**

Calendario del Entrenamiento

Con el objetivo de facilitar el proceso de aprendizaje, te proponemos el siguiente calendario para que tengas una guía de cómo ir completando los contenidos.

Septiembre 2023

CARRIX SECURITY TRAINING				
SEPTIEMBRE 2023				
LUNES	MARTES	MIERCOLES	JUEVES	VIERNES
9/25/2023	9/26/2023	9/27/2023	9/28/2023	9/29/2023
			Sesión Informativa Pre-Entrenamiento	
			Lecturer: DSA & SMEs	

Octubre 2023

OCTUBRE 2023				
LUNES	**MARTES**	**MIERCOLES**	**JUEVES**	**VIERNES**
10/2/2023	10/3/2023	10/4/2023	10/5/2023	10/6/2023
Sesión 1 : Importancia de la seguridad de las aplicaciones	GitHub Onboarding	Sesión 2 : Mejores prácticas en codificación	GitHub Onboarding	GitHub Onboarding
Lecturer: Mauricio Sotelo		*Lecturer: Mauricio Sotelo*		
SESIONES DE MENTORIA (Mentor : Mauricio Sotelo & Andres Martinez)				
10/9/2023	10/10/2023	10/11/2023	10/12/2023	10/13/2023
Sesión 3 : Prácticas de codificación segura		Sesión 4 : Mejores prácticas de software		
Lecturer: Mauricio Sotelo		*Lecturer: Mauricio Sotelo*		
SESIONES DE MENTORIA (Mentor : Mauricio Sotelo & Andres Martinez)				
10/16/2023	10/17/2023	10/18/2023	10/19/2023	10/20/2023
Sesión 5 : Principios de codificación segura		Sesión 6 : Validación de entrada		1er Entregable Proyecto Final
Lecturer : Miguel Angel Martínez		*Lecturer : Miguel Angel Martínez*		
SESIONES DE MENTORIA (Mentor : Miguel Angel Martinez & Andres Martinez)				
10/23/2023	10/24/2023	10/25/2023	10/26/2023	10/27/2023
Sesión 7 : Autenticacion y autorizacion	Retroalimentación Mitad del Entrenamiento	Sesión 8 : Estándares de protección de datos		
Lecturer : Miguel Angel Martínez		*Lecturer : Miguel Angel Martínez*		
SESIONES DE MENTORIA (Mentor : Miguel Angel Martinez & Andres Martinez)				

Noviembre 2023

NOVIEMBRE 2023				
LUNES	**MARTES**	**MIERCOLES**	**JUEVES**	**VIERNES**
10/30/2023	10/31/2023	11/1/2023	11/2/2023	11/3/2023
Sesión 9 : Criptografía		Sesión 10 : Marco de evaluación de riesgos	Dia Festivo	2ndo Entregable Proyecto Final
Lecturer : Andres Martinez		*Lecturer: Mauricio Sotelo*		
SESIONES DE MENTORIA (Mentor : Miguel Angel Martinez & Andres Martinez)				
11/6/2023	11/7/2023	11/8/2023	11/9/2023	11/10/2023
Sesión 11 : Categorización de vulnerabilidad		Sesión 12 : Identificación de vulnerabilidades		
Lecturer: Mauricio Sotelo		*Lecturer : Guillermo Esguerra*		
SESIONES DE MENTORIA (Mentor : Mauricio Sotelo & Guillermo Esguerra)				
11/13/2023	11/14/2023	11/15/2023	11/16/2023	11/17/2023
Sesión 13 : Mitigación y remediación de vulnerabilidades				3er Entregable Proyecto Final
Lecturer : Guillermo Esguerra				
SESIONES DE MENTORIA (Mentor : Mauricio Sotelo & Guillermo Esguerra)				
11/20/2023	11/21/2023	11/22/2023	11/23/2023	11/24/2023
Dia Festivo	Presentacion Proyecto Final	Retroalimentación Final del Entrenamiento		
	Lecturer: DSA & SMEs			
SESIONES DE MENTORIA (Mentor : Mauricio Sotelo & Guillermo Esguerra)				

Fechas Importantes

Sesión Informativa Pre-Entrenamiento : Jueves 28 de Septiembre 2023

Inicio del Entrenamiento : Lunes 2 de Octubre 2023

Retroalimentación a Mitad del Entrenamiento : Martes 24 de Octubre 2023

1er Entregable Proyecto Final : Viernes 20 de Octubre 2023

2ndo Entregable Proyecto Final : Viernes 3 de Noviembre 2023

Fin del Entrenamiento : Lunes 13 de Noviembre 2023

3er Entregable Proyecto Final : Viernes 17 de Noviembre 2023

Presentacion Proyecto Final : Martes 21 de Noviembre 2023

Retroalimentación Final del Entrenamiento : Miércoles 22 de Noviembre 2023

Sesion Inicial (Kick Off)
Sesión Inaugural / Introducción
Instructor: Personal de DSA Fecha: miércoles Sep 28, 2023

Programa del Entrenamiento

El periodo del entrenamiento será del día **2 de Octubre de 2023** al día **13 de Noviembre 2023.**

Los 3 módulos y 13 sesiones del entrenamiento se desglosan en los siguientes temas:

Módulo 1 : Introducción a la seguridad de aplicaciones y mejores prácticas en codificación

Semana 1
Sesión 1 : Importancia de la seguridad de las aplicaciones
Instructor: Mauricio Sotelo Morales Fecha: lunes Oct 2, 2023
Sesión 2 : Mejores prácticas en codificación
Instructor: Mauricio Sotelo Morales Fecha: miércoles Oct 4, 2023

Semana 2
Sesión 3 : Prácticas de codificación segura
Instructor: Mauricio Sotelo Morales Fecha: lunes Oct 9, 2023
Sesión 4 : Mejores prácticas de software
Instructor: Mauricio Sotelo Morales Fecha: miércoles Oct 11, 2023

Módulo 2 : Técnicas de codificación segura

Semana 3
Sesión 5 : Principios de codificación segura
Instructor: Miguel Angel Martínez Reyes Fecha: lunes Oct 16, 2023
Sesión 6 : Validación de entrada
Instructor: Miguel Angel Martínez Reyes Fecha: miércoles Oct 18, 2023

Semana 4
Sesión 7 : Autenticacion y autorizacion
Instructor: Miguel Angel Martínez Reyes Fecha: lunes Oct 23, 2023
Sesión 8 : Estándares de protección de datos
Instructor: Miguel Angel Martínez Reyes Fecha: miércoles Oct 25, 2023

Semana 5
Sesión 9 : Criptografía
Instructor: Arturo Garcia Martin del Campo Fecha: lunes Oct 30, 2023

Módulo 3 : Evaluación de riesgos y gestión de vulnerabilidades

Semana 5
Sesión 10 : Marco de evaluación de riesgos
Instructor: Mauricio Sotelo Morales Fecha: miércoles Nov 1, 2023

Semana 6
Sesión 11 : Categorización de vulnerabilidad
Instructor: Mauricio Sotelo Morales Fecha: lunes Nov 6, 2023
Sesión 12 : Identificación de vulnerabilidades
Instructor: Guillermo Esguerra Bautista Fecha: miércoles Nov 8, 2023

Semana 7
Sesión 13 : Mitigación y remediación de vulnerabilidades
Instructor: Guillermo Esguerra Bautista Fecha: lunes Nov 13, 2023

Retroalimentación de la Sesión

La retroalimentación posterior a cada sesión tiene como finalidad atender sus comentarios y opiniones acerca del entrenamiento de manera eficaz y atender sus dudas y comentarios de manera ágil.

- Al término de cada sesión, se reservarán 5 minutos para poder completar esta **encuesta de retroalimentación de la sesión**. Todas las respuestas requeridas son de opción múltiple para su comodidad, y cuenta con un apartado para poder incluir comentarios adicionales.

Repositorio Central en GitHub

El repositorio central de GitHub será utilizado para diversas actividades durante el entrenamiento. Toda la información relacionada al entrenamiento está disponible en el repositorio de **GitHub** :

- Calendario, horarios, programa del entrenamiento y material adicional de auto-aprendizaje.
- Publicaremos el contenido impartido después de cada sesión así como la liga a el video de la sesión para poder visualizarlo posteriormente.
- Información sobre el proyecto final y sus lineamientos.
- Solicitar mentorías con los expertos de Wizeline en la fecha y horario que más te convenga.
- Aquí también podrás agregar tu perfil de GitHub como “fork” y hacer “push” para que puedas recibir notificaciones en tiempo real de las actividades que se realicen dentro del repositorio central.

Mentorias

Las mentorías son un espacio de **1 hora** donde podrás resolver y despejar dudas sobre temas cubiertos en cualquiera de las sesiones impartidas. Podrás programar las mentorías con base en la disponibilidad de los mentores de Wizeline.

Cada semana, los mentores estarán actualizando sus espacios de tiempo de acuerdo a su disponibilidad y los temas que se abordarán en la semana de entrenamiento.

Criterios de las Mentorías

- Podrás agendar las sesiones de mentoría requeridas mediante el repositorio de GitHub en el apartado de **"Agenda tu Mentoría"**
- Es necesario que al agendar tu sesión de mentoría se incluya el tema y/o dudas que se tratarán durante la sesión. Esto con la intención de preparar mejor los temas en que necesitas ayuda.
- Al agendar la sesión recibirás toda la información necesaria vía email para poder unirse a la sesión de mentoría.
- Si llegas tarde a tu sesión (10 minutos o más) será necesario reagendar enviando un mensaje en **Slack** para informar al mentor y al equipo de DSA.
- Si tienes dudas o dificultades para conectarse a la sesión de mentoría, envía un mensaje por **Slack** al equipo de DSA y/o un correo electrónico a **dsa-carrix@wizeline.com** para poder ayudarte a resolverlo.
- Después de cada sesión de mentoría, deberás contestar la **retroalimentación de la mentoría**.

Proyecto Final (Capstone Project)

Este proyecto final se centra en la exploración integral del desarrollo de software seguro. Dividido en tres secciones, abarca la configuración de un entorno de desarrollo seguro, la creación de una aplicación segura y la realización de una evaluación de riesgos.

Entregable 1

- Escanea el código https://github.com/TsuyoshiUshio/VulnerableApp con SonarQube
- Analizar a detalle los hallazgos de SonarQube, utiliza las secciones What is the risk, Are you at risk? y How can you fix it para desarrollar un reporte con la siguiente información:
- Descripción de las 3 vulnerabilidades que consideres más importantes.
- Líneas de código afectadas por las vulnerabilidades afectadas
- Propuesta de remediación
- Justificación de 3 falsos positivos (Hallazgos que en realidad son falsos positivos)
- Instalar y configurar correctamente Sonarlint en un entorno de Visual Studio
- Automatiza el análisis en el repositorio que utilizarás para el proyecto final con SonarQube utilizando GitHub Actions
- Habilita Dependabot en tu repositorio de GitHub
- Automatiza el análisis en el repositorio que utilizarás para el proyecto final con SonarQube utilizando GitHub Actions

Entregable 2

- Desarrolla una página de login, que requiera usuario y contraseña
- Transmite el usuario y la contraseña utilizando AES256
- Se deberán almacenar utilizando el hash SHA256
- Desarrolla funciones que sinteticen el usuario y la contraseña utilizando expresiones regulares.
- Controla los siguientes escenarios:
- Tiempo máximo de sesión
- Tiempo máximo de inactividad
- Permisos del usuario para los elementos que tendrá el sitio web (descritos a continuación)
- Haz una página web tipo foro, donde los visitantes puedan registrar el título de su mensaje y el mensaje
- No deberá poder ser accedido si no hay una sesión activa
- Utiliza sanitización de las entradas
- Asignar un permiso, de tal forma que no todos los usuarios puedan registrar mensajes
- Siguiendo la página web tipo foro, haz una página o sección donde los usuarios puedan ver los mensajes que los demás dejaron
- No deberá poder ser accedido si no hay una sesión activa

- Utilizar sanitización antes de reflejar los textos
- Asignar un permiso, de tal forma que no todos los usuarios puedan registrar mensajes

Entregable 3

- Utiliza Microsoft Threat Modelling Tool para replicar tu arquitectura y detectar riesgos
- Utiliza el navegador MITRE ATT&CK para detectar riesgos de acuerdo a los grupos cibercriminales que pudieran ser de interés para el contexto de tu desarrollo
- Haz un reporte de acuerdo a los hallazgos que hayas tenido con SonarQube, dependabot y Microsoft Threat Modelling Tool:
- Descarta y justifica los falsos positivos
- Documenta el detalle de las vulnerabilidades y riesgos detectados.
- Identifica si alguno de los hallazgos de estas herramientas, está relacionado a alguno de los hallazgos que tuviste con MITRE ATT&CK.
- Haz un plan de remediación, priorizando su riesgo de acuerdo a MITRE ATT&CK y la criticidad que las otras herramientas dieron
- A través de esta práctica, el participante será capaz de comprender las mejores prácticas de codificación segura, desarrollar la capacidad de aprovechar las herramientas de seguridad de forma efectiva, fomentar una comprensión integral de la evaluación de riesgos para el desarrollo de software seguro.

Posterior a cada entregable, se dará un tiempo de 5-7 días (aprox.) para revisar y analizar el entregable para posteriormente recibir la retroalimentación.

Una vez concluída la última entrega, se tendrá un espacio para presentar el proyecto final y demostrar lo aprendido durante el entrenamiento. Toda la información relacionada a este proyecto final se encuentra disponible en el repositorio de **GitHub**

Recomendaciones y consideraciones

- Te recomendamos tener la cámara encendida durante toda la sesión para facilitar la interacción y el aprendizaje.
- En caso de tener dificultades para entrar favor de avisar al equipo de DSA via **Slack** & correo electrónico : **dsa-carrix@wizeline.com**
- En caso de no poder asistir, deberás avisar al equipo de DSA por medio de **Slack** y a tu líder de Carrix con el motivo por el cual no podrás asistir a la sesión. Posteriormente, deberás estar al pendiente de la grabación de la sesión para mantenerte actualizado de los temas cubiertos.
- Cualquier duda que tengas durante la sesión te pedimos que hagas uso de la herramienta de “levantar mano” de Zoom o usa el chat para escribir tu pregunta.
- En dado caso que ingreses tarde a una sesión y ya se hayan cubierto temas, te recomendamos revisar la grabación una vez que esté lista y/o agendar una mentoría para atender cualquier duda que tengas.
- Recuerda que para cumplir con el objetivo del entrenamiento y fortalecer tus capacidades es importante asistir a todas las sesiones del entrenamiento.

Canales de comunicación

Slack

Usaremos Slack como herramienta de comunicación instantánea en la cual podrás contactar con el personal de DSA de manera eficaz y sencilla, así como hacer preguntas, dar seguimiento a algún tema y conversar con el resto del equipo.

Email

Correo institucional de DSA, en el cual puedes realizar consultas sobre el entrenamiento de manera formal, aclarar dudas, enviar preguntas y hacer comentarios en cualquier momento.

Encuestas de Retroalimentación

Los formularios de retroalimentación nos ayudan a captar todos sus comentarios y sugerencias sobre el entrenamiento al término de cada sesión, de esta manera tomamos en consideración su retroalimentación para la aplicación del entrenamiento.

