



Curso
Desarrollo Seguro
Ante Ciberataques

4ª Edición

24 Horas

22, 23, 24, 25, 29, 30, 31 de Mayo y 1
de Junio de 2023

www.vitaedigital.com



Vitae

INTRODUCCIÓN

Se trata de un curso completamente práctico en el que los alumnos podrán aprender, mediante ejercicios y ejemplos, cómo se producen las vulnerabilidades en aplicaciones desarrolladas en diversos lenguajes de programación. A lo largo de los módulos que componen la formación, se explicará en detalle cada uno de los puntos, todo ello con ejemplos fáciles de seguir y probar por medio del uso de máquinas virtuales.

Dirigido a:

La formación está orientada a profesionales que tengan conocimientos previos sobre desarrollo de software, sin importar el lenguaje o la plataforma, ya que tanto las vulnerabilidades como las técnicas de detección y explotación que se enseñan, tienen aplicabilidad en cualquier tipo aplicación web sin importar el lenguaje utilizado para su construcción.

TEMARIO

Módulo 1

Módulo de introducción, en donde se explican las técnicas que hacen parte del SSDLC (Secure Software Development LifeCycle) y los beneficios que aporta a la seguridad. Se hablará de la cultura DevOps y cómo la seguridad irrumpe en este modelo de trabajo para formar lo que hoy en día se conoce como DevSecOps. El alumno tendrá la posibilidad de entender los esquemas STRIDE y DREAD para el modelado de amenazas y los principales patrones y metodologías orientadas al S-SDLC

- Principios y beneficios del DevOps
- ¿Por qué DevSecOps?
- Integración & Entrega Continua Segura
- SDLC en integración y entrega continua
- Modelado de amenazas STRIDE y DREAD
- Patrones de diseño orientados al S-SDLC

Módulo 2

Una de las premisas del DevOps, consiste en automatizar todo lo posible y en la entrega y despliegue de aplicaciones ágiles. En este sentido, es importante conocer las tecnologías basadas en contenedores, las cuales permiten conseguir estos objetivos. Por otro lado, en este módulo el alumno aprenderá a usar soluciones de integración y despliegue continuo, las cuales son fundamentales en DevOps.




- Arquitectura de contenedores
- Ciclo de vida de los contenedores y despliegue de aplicaciones
- Seguridad en contenedores y e imágenes
- Seguridad en el servicio de DockerD
- Soluciones de integración y despliegue continuo

Módulo 3

En este módulo se enseñan las buenas prácticas de desarrollo aplicadas a diferentes plataformas y lenguajes de programación. Entre otras cosas, el alumno aprenderá a detectar vulnerabilidades en su código mediante el uso de aplicaciones web vulnerables por diseño. Para finalizar, Se enseña el uso de herramientas SAST y DAST para el análisis de proyectos de desarrollo.

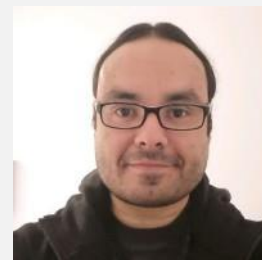
- Introducción a los proyectos OWASP (Open Web Application Security Project)
- Entorno de prácticas TOP 10 para desarrollo seguro - Attack&Defense
- Buenas prácticas de desarrollo en lenguajes de programación modernos
- Frameworks y herramientas enfocadas a la seguridad.
- Análisis estático avanzado (SAST)
- Análisis dinámico avanzado (DAST)

INFORMACIÓN DEL CURSO

 Duración	24 Horas en 8 sesiones de 3 horas
 Lugar	Aula Virtual con clases en directo
 Fechas	22, 23, 24, 25, 29, 30, 31 de Mayo y 1 de Junio de 2023
 Horario	De lunes a jueves de 16:30 a 19:30 h

FORMADOR

Daniel Echeverri





Ingeniero de Sistemas y master en Software Libre Formador e investigador de seguridad informática y hacking.

Conocido por el nick de "Adastra" y sus intervenciones como ponente en múltiples eventos en España y otros países de América Latina.

Autor del blog thehackerway.com y de los libros "Python para Pentesters", "Hacking con Python" y "Deep web - Privacidad y anonimato en TOR, I2P y Freenet" publicados por la editorial OxWORD, así como el libro "25 Técnicas aplicadas a campañas de Red Team y Hacking" de edición propia.

En su trayectoria profesional ha desempeñado desde hace más de 18 años hasta la fecha, actividades de desarrollo y arquitectura de software, administración de servidores, pentesting, hardening de sistemas y formaciones tanto para organizaciones públicas como privadas como Accenture, Ibermática, Plexus, BBVA, Policía nacional, Ejercito de Tierra, Renta4, Mutua Madrileña, Ineco etc...

CONDICIONES ECONÓMICAS

 Tarifa por Asistente	290 €
 Tarifa por asistente a partir de dos personas de la misma empresa u organización	260 €

Forma de Pago:

Por transferencia al finalizar el curso a la recepción de la factura

Se añadirá el 21% de IVA

Inscripción:

Doris Verdes

Doris.verdes@vitaedigital.com

vitae@vitaedigital.com

Tlf : 986 47 21 01

635 559 285

Plazas limitadas, reserva de plazas por riguroso orden de inscripción

