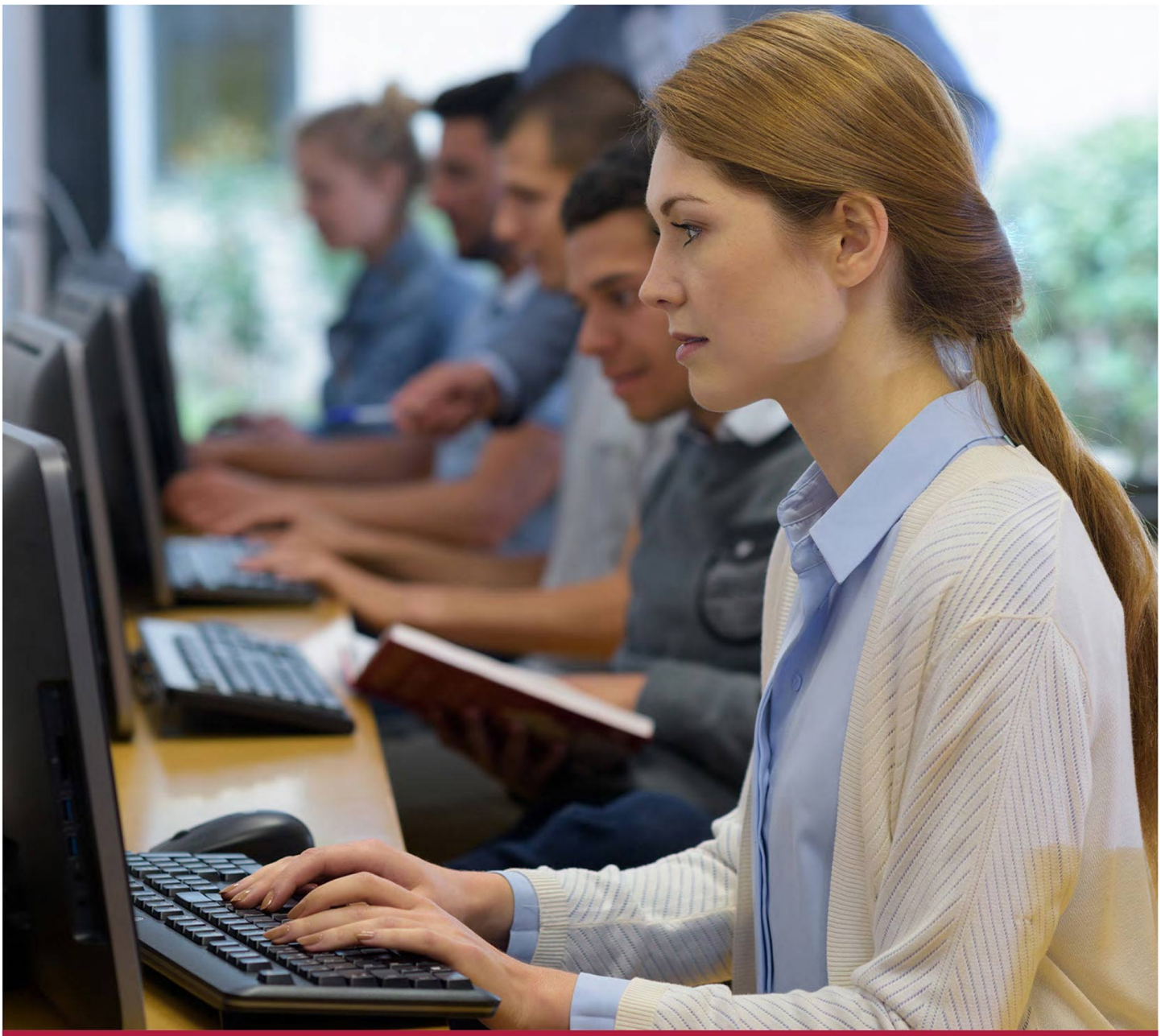
Академия АйТи
a Softline Company



Безопасная web-разработка

Код курса: DSO_web

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Безопасная web-разработка

Код курса: DSO_web

Длительность	40 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Курс предназначен для веб-разработчиков и специалистов по информационной безопасности, желающих углубить свои знания в области защиты веб-приложений. В рамках курса изучаются современные угрозы безопасности и методы их предотвращения, включая OWASP Top Ten и способы защиты от SQL-инъекций и XSS-атак. Слушатели получат практический опыт работы с инструментами для анализа безопасности веб-приложений, научатся внедрять лучшие практики безопасного кодирования и мониторинга. Особое внимание уделяется защите пользовательских данных и обеспечению конфиденциальности, а также интеграции безопасности в процессы CI/CD. Этот курс поможет слушателям повысить уровень защиты их проектов и минимизировать риски кибератак.

Подробная информация

Профиль аудитории:

- Веб-разработчики, стремящиеся улучшить безопасность своих приложений.
- Инженеры по тестированию, желающие внедрить практики безопасного тестирования.
- Руководители проектов, заинтересованные в интеграции безопасности на всех этапах разработки.
- Специалисты по информационной безопасности, стремящиеся обновить свои знания в области веб-безопасности.
- Начинающие специалисты в области кибербезопасности, имеющие базовые технические навыки.

Предварительные требования:

- Знакомство с основами веб-разработки и архитектуры веб-приложений.
- Базовые знания языков программирования, таких как JavaScript, Python или PHP.
- Понимание моделей данных и запросов в базах данных.
- Желательно иметь опыт работы с системами контроля версий, такими как Git.

По окончании курса слушатели смогут:

- Оценивать и внедрять ключевые требования безопасности в своих проектах.
- Моделировать угрозы и разрабатывать стратегии их предотвращения для своих приложений.
- Защищать свои приложения от современных атак, используя знания об актуальных рисках.
- Интегрировать процессы безопасной разработки в жизненный цикл своих проектов.
- Работать с инструментами DevSecOps для обеспечения безопасности на всех этапах разработки.
- Выполнять базовые пентесты и оценивать критичность обнаруженных уязвимостей.
- Управлять и проверять безопасность используемых зависимостей и пакетов в приложениях.

Программа курса

Модуль 1. Архитектура современных веб-приложений

- Основы архитектуры и ключевые компоненты современных веб-приложений.

Модуль 2. Базовые требования безопасности

- Понятие и важность security defaults.
- Практика: Составление перечня требований безопасности для выбранного приложения.

Модуль 3. Моделирование угроз

- Практика: Бизнес-моделирование угроз для реальных сценариев.
- Практика: Разработка продуктовой модели угроз.

Модуль 4. Современные риски для приложений

- Подробный разбор OWASP Top 10 и других актуальных рисков.
- Практика: Защита от SQL Injection, OS Command Injection, XSS и других векторных атак.

Модуль 5. CVSS и оценка критичности

- Понимание CVSS и как правильно оценивать критичность уязвимостей.
- Практика: Оценка критичности на примерах и кейсах.

Модуль 6. Безопасность зависимостей

- Обработка и защита зависимостей через пакетные менеджеры, container registry, artifact registry.
- Типы атак на зависимости и как им противодействовать.
- Практика: Ревью и подготовка собственного манифеста безопасности.
- Практика: Сборка образов и артефактов, подпись и проверка подписи.

Модуль 7. SSDLC и практики

- Жизненный цикл безопасной разработки и интеграция практик.
- Практика: Внедрение методов SSDLC в существующий процесс разработки.

Модуль 8. DevSecOps, AppSec и Pentest

- Вехи развития и объединение DevOps с безопасностью.
- Практика: Проведение пентестов на примере приложения.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru