Основные уязвимости в безопасности веб-приложений

Код: SECR-005

Длительность: 16 ч.

Описание:

Курс нацелен на разработчиков, тестировщиков, архитекторов, бизнес-аналитиков и аналитиков по безопасности и является описанием десяти наиболее важных и серьезных уязвимостей в ПО по версии проекта OWASP.В ходе курса описываются теоретические детали каждой уязвимости, демонстрируется каждая из них на реальных примерах (именно то, что видит рядовой пользователь), рассматриваются проблемы и ошибки в исходном коде приложения, описываются пути тестирования и защиты. Каждая уязвимость показывается с точки зрения бизнеса – какой ущерб для компании способна нанести та или иная проблема.

Цели:

Демонстрация основных уязвимостей в веб-приложениях, проблем и ошибок в исходном коде приложения, путей тестирования и нахождения в приложениях.

Разбираемые темы:

Список 10-ти наиболее серьезных уязвимостей по версии проекта OWASP:
1. Внедрение кода (Injections);
2. Межсайтовый скриптинг (Cross-Site Scripting);
3. Ошибки в механизме аутентификации и управлении сеансами (Broken Authentication and Session Management);
4. Небезопасные прямые ссылки на объекты (Insecure Direct Object References);
5. Подделка межсайтовых запросов (Cross-Site Request Forgery);
6. Небезопасная конфигурация окружения (Security Misconfiguration);
7. Небезопасное хранение важных данных (Insecure Cryptographic Storage);
8. Несанкционированный доступ к ресурсам по URL (Failure to Restrict URL Access);
9. Недостаточная защищенность транспортного протокола (Insufficient Transport Layer Protection);
10. Непроверенные редиректы (Unvalidated Redirects and Forwards).

Целевая аудитория:

Разработчики, тестировщики, архитекторы, бизнес-аналитики.

Предварительная подготовка – общее:

- От слушателей необходимы понимание основ веб и начальные знания в разработке и/или тестировании веб-приложений.
- Базовые знания английского языка.

Рекомендуемые дополнительные материалы, источники:

www.owasp.org

Примечание:

Материалы курса представлены на английском языке.