Подходы к тестированию безопасности

Цель данного тренинга – рассказать о подходах к тестированию безопасности, а также обрисовать основные концепции каждого из типов на основании известных открытых методологий (OWASP, Microsoft SDL, PTES). Получить практические навыки выбора и использования инструментария для проведения тестирования безопасности.

Длительность: 16 ч.

В рамках курса рассматриваются следующие вопросы:

- ✓ Терминология, применяемая в сфере тестирования безопасности;
- ✓ Основные методологии, используемые при проведении тестирования безопасности веб-приложений;
- ✓ Разновидности угроз безопасности веб-приложений, методы их обнаружения;
- ✓ Разновидности уязвимостей веб-приложений, отличительные особенности, возможные последствия эксплуатации;

В практической части курса слушатели приобретают навыки:

- ✓ Различать виды тестов безопасности, необходимость и последовательность применения;
- ✓ Определять уровень угрозы, классифицировать в соответствии с методикой OWASP Risk Calculation;
- ✓ Производить поиск и анализ уязвимостей веб-приложений как со стороны серверной, так и клиентской частей;
- ✓ Определять технологический стек (набор технологий) используемый при разработке приложения.

Разбираемые темы:

1. Терминология. *Модель нарушителя. Мобильный код. Уязвимость. Угроза. Эксплуатация уязвимости. Эксплойт. Вектор атаки. Инъекция. Отказ в обслуживании. Доступность. Сниффер. Конфиденциальность данных. Защищенность. Целостность данных. Методология тестирования (OWASP, Microsoft SDL, PTES). Стандарт безопасности. Политика безопасности. Уязвимость нулевого дня. Патч. Заплатка. Сканнер безопасности.*

2. Виды тестов. *Идентификация приложения. Анализ защищенности. Тест на проникновение. Сетевой аудит безопасности. Моделирование угроз. Статический и динамический анализ кода. Социальная инженерия.*

3. Идентификация приложения. *Архитектура веб-приложения (уровень приложения, уровень данных, уровень бизнес-логики). Технологический стек. Spider. Crawler. Fingerprinting. POST и GET запросы. CVE база. Обработчик ошибки. Сканнер портов. Сниффер. Раскрытие данных.*

4. Уязвимости клиента *Валидация данных на стороне клиента. Инъекции кода (SQL, XML, Code, ORM, Javascript, CSS, AD, SMTP). Обход валидации данных. Кросс-сайт скриптинг. DOM атака. Механизм сессий. Аутентификация и авторизация пользователя. Защищенный канал передачи данных.*

5. Уязвимости сервера. *Слабое шифрование (частная реализация криптоалгоритмов, отсутствие SSL). Атаки на отказ в обслуживании (DoS, DDoS). Переполнение буфера. Прямые*

ссылки на объекты. Инъекции команд операционной системы. Раскрытие конфигурационных файлов. Контроль обновления программных продуктов. Атака на консоль администратора.

6. Ошибки реализации бизнес логики. *Защита от средств автоматизации. Условия гонки (race condition). Небезопасное восстановление данных. Горизонтальная и вертикальная эскалация прав пользователя. Противоречивость функциональных требований. Функциональные дефекты.*

7. Средства аудита. Отслеживание изменений. Логгирование действий пользователя. Журналы операционной системы. Контрольная сумма. Хэш-функция. IDS/IPS.

8. Вспомогательный инструментарий. *Выбор инструментария. Kali Linux – дистрибутив инженера по анализу защищенности ПО и сети. Сканнер безопасности. Псевдо-срабатывание. Анализ отчета. Недостатки автоматизированных инструментов.*

9. Оценка риска взлома. Оценка сложности взлома. *OWASP Risk Calculation. Сложность взлома. Критичность уязвимости. Определение значимости взлома. Обзор тенденций. Примеры уязвимостей и успешных атак. Комбинирование уязвимостей при построении атаки.*

10. Внедрение тестирования безопасности в жизненный цикл разработки ПО. *Формирование отчета по тестированию безопасности. Рекомендации по исправлению ошибок кода. Повторный тест безопасности. Тестовая и производственная среды. Миграция ПО в облако (риски). Контроль защищенности ПО на различных стадиях разработки и внедрения. Взаимодействие с разработчиками. Демонстрация уязвимостей. Проект по анализу защищенности веб-приложения*

Рекомендуемые дополнительные материалы, источники:

1. OWASP (Open Web Application Security Project) - https://www.owasp.org/
2. Microsoft SDL (Security Development Lifecycle) - http://www.microsoft.com/en-us/sdl/ .
3. PTES (Penetration Testing Execution Standard) - http://www.pentest-standard.org/ .