OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Меня хорошо видно && слышно?

Ставьте  , если все хорошо

Напишите в чат, если есть проблемы

Проверить, идет ли запись!

Методологии анализа защищенности OWASP

Колесников Александр

Правила вебинара

Активно участвуем

Задаем вопросы в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара

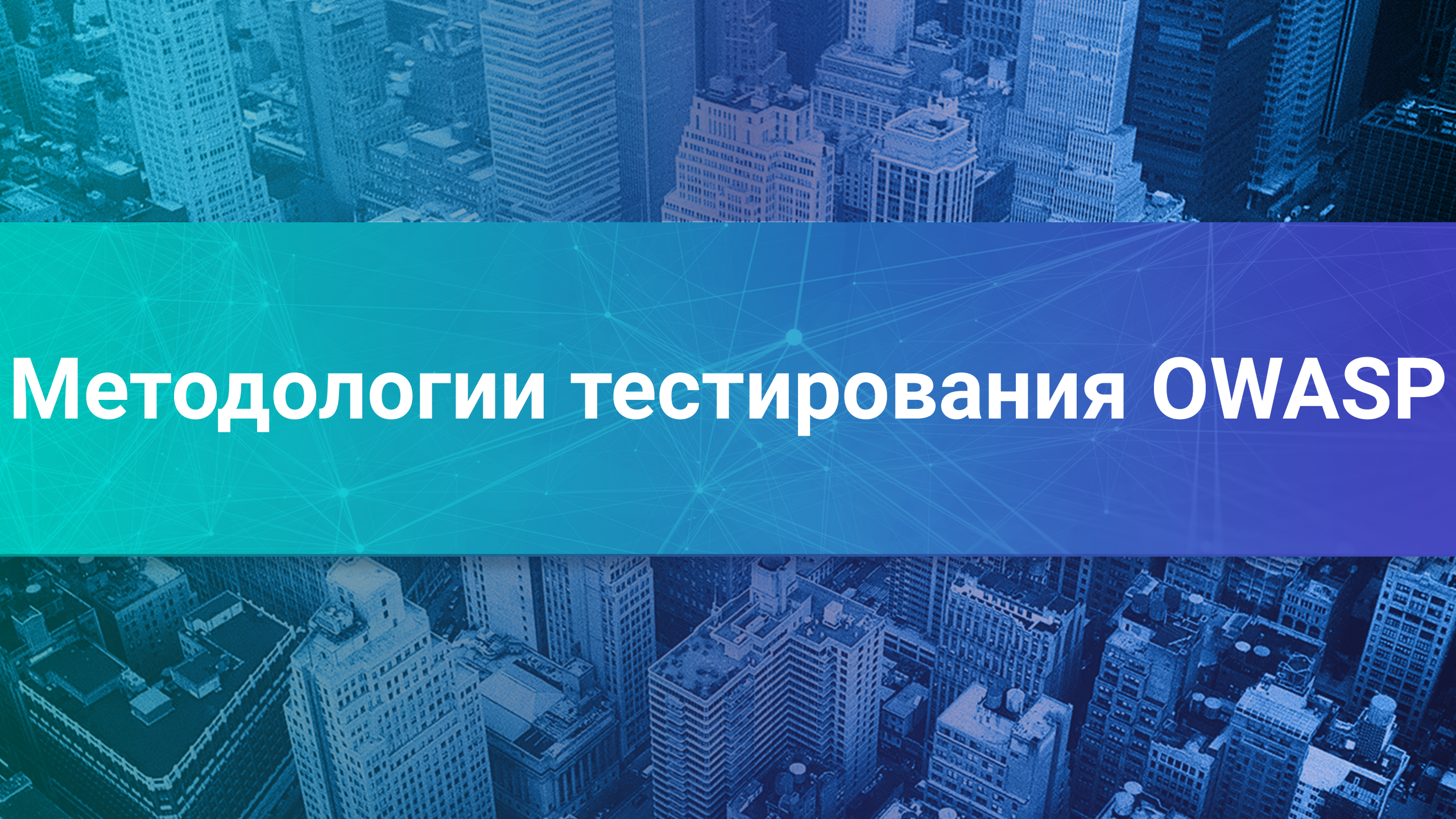
Методологии

Ресурсы и инструменты

Тестирование приложения

Цели

1. Познакомиться с методологиями тестирования
2. Рассмотреть методологии для разных платформ
3. Рассмотреть пример тестирования



Методологии тестирования OWASP

Основные понятия

- **OWASP Testing Guide** - набор методов и техник для тестирования приложения
- **Особенности тестирования:**
  - Есть специальная нотация для проверок - WSTG-<версия><категория>-<номер>

Основные разделы тестирования

- **Introduction and Objectives**
- **Information Gathering**
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management
- Input Validation Testing
- Testing Error Handling
- Testing Weak Cryptography
- Business Logic Testing
- Client Side Testing

Этапы тестирования


OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Passive Testing

Introduction and Objectives

- Общая информация о процессе тестирования
- Перечисление целей тестирования
- Описание основных понятий и используемых терминах

Information Gathering

- Информация о тестируемой системе.
- Google dorks
- Сбор данных по открытым источникам
- Scraping Tools:
  - FOCA
  - Spiderfoot


OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Active Testing

Configuration and Deployment Management Testing

- Раздел для тестирования конфигурации инфраструктуры
- Какие данные не должны присутствовать: WSTG-CONF-02
  - Поиск sensitive информации
  - Как собираются логи?
  - Какой период времени хранятся логи?
  - Как бэкапы хранятся? Есть ли к ним доступ?

Identity Management Testing

- Раздел для тестирования разграничения доступа.

  - Проверка списка ролей
  - Проверка регистрации пользователей
  - Проверка простоты сгенерированных идентификаторов(поиск пользователей)

Authentication Testing

- Раздел тестирования механизмов авторизации
  - Тестирование протокола используемого для шифрования взаимодействия
  - Тестирование механизмов авторизации
  - Проверка стандартных логинов и паролей
  - Проверка поллитик паролей

Authorization Testing

- Тестирование авторизации
  - Тестирование уязвимостей path traversal
  - Обход механизма авторизации
  - Тестирование на эскалацию привилегий
  - Тестирование прямого доступа

Input validation Testing

- Тестирование, данных, которые отправляет в приложение пользователь:
  - Все уязвимости, которые можно найти в OWASP TOP 10.
  - Легко автоматизируемый процесс

Testing Error Handling

- Тестирование полноты данных, которые можно получить из ошибок приложения.

- Тестирование правильности использования кодов возврата
- Тестирование на утечку данных, которые могут скомпрометировать приложение

Testing Weak Cryptography

- Тестирование недостаточных
- Тестирование на типичные атаки:
  - Padding Oracle
  - Тестирование на отправление учетных данных пользователя без шифрования
  - Тестирование на использование слабых алгоритмов шифрования

Business Logic Testing

- Тестирование логики работы приложения
  - Проверка функционала
  - Проверка возможности создания Forge запроса
  - Существует ли ограничение на использование функций
  - Обход механизмов фильтрации для загрузки файлов

Client Side Testing

- Тестирование фронтэнда
  - Тестирование на инжект JavaScript
  - Тестирование на инжект HTML
  - Тестирование на добавление контента

Спасибо за внимание!
Приходите на следующие вебинары

Колесников Александр