OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Меня хорошо видно && слышно?

Ставьте  , если все хорошо

Напишите в чат, если есть проблемы

Проверить, идет ли запись!

Утилиты для статического и динамического анализа защищенности Fuzzing

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

Fuzzing

Fuzzing приложений

Fuzzing Web

Практика

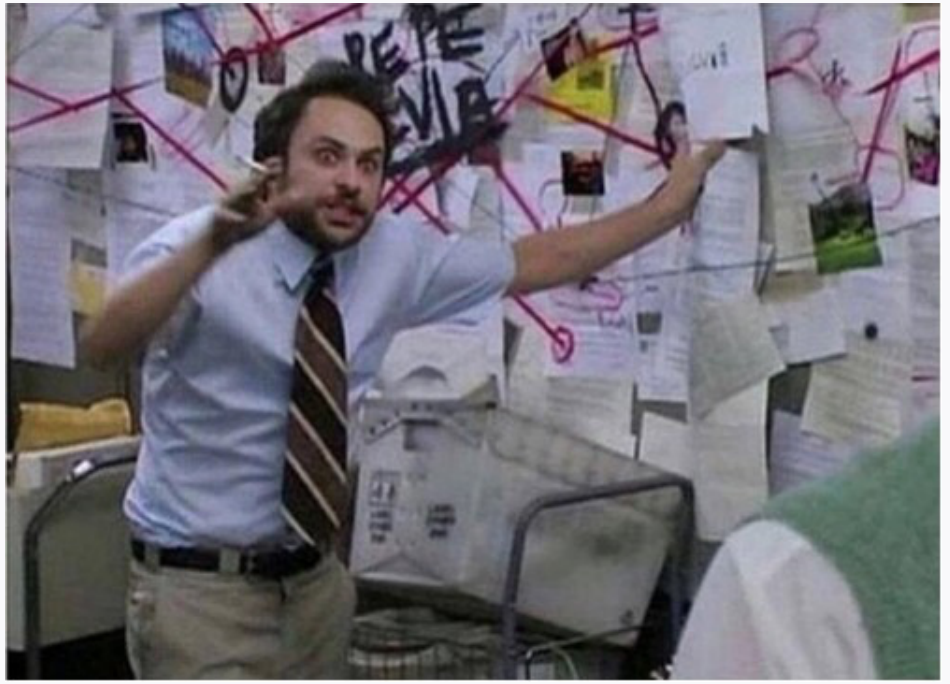
Цели

1. Разобрать основные типы приложений для поиска уязвимостей
2. Познакомиться с особенностями и ограничениями
3. Провести тесты


Что такое Fuzzing?

Теория

- **Основные понятия:**
  - **Fuzzing** - процесс тестирования приложения путем передачи ему автоматически сгенерированных входных данных

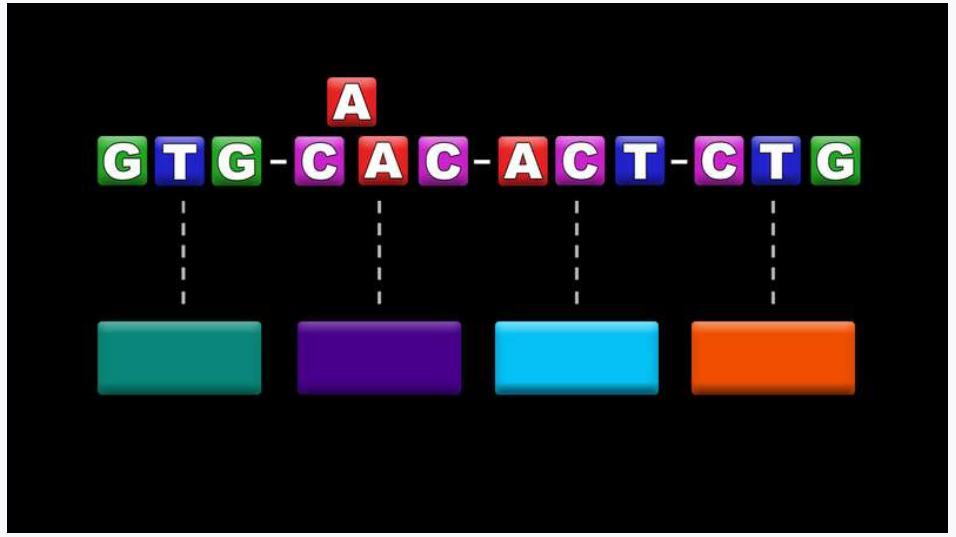


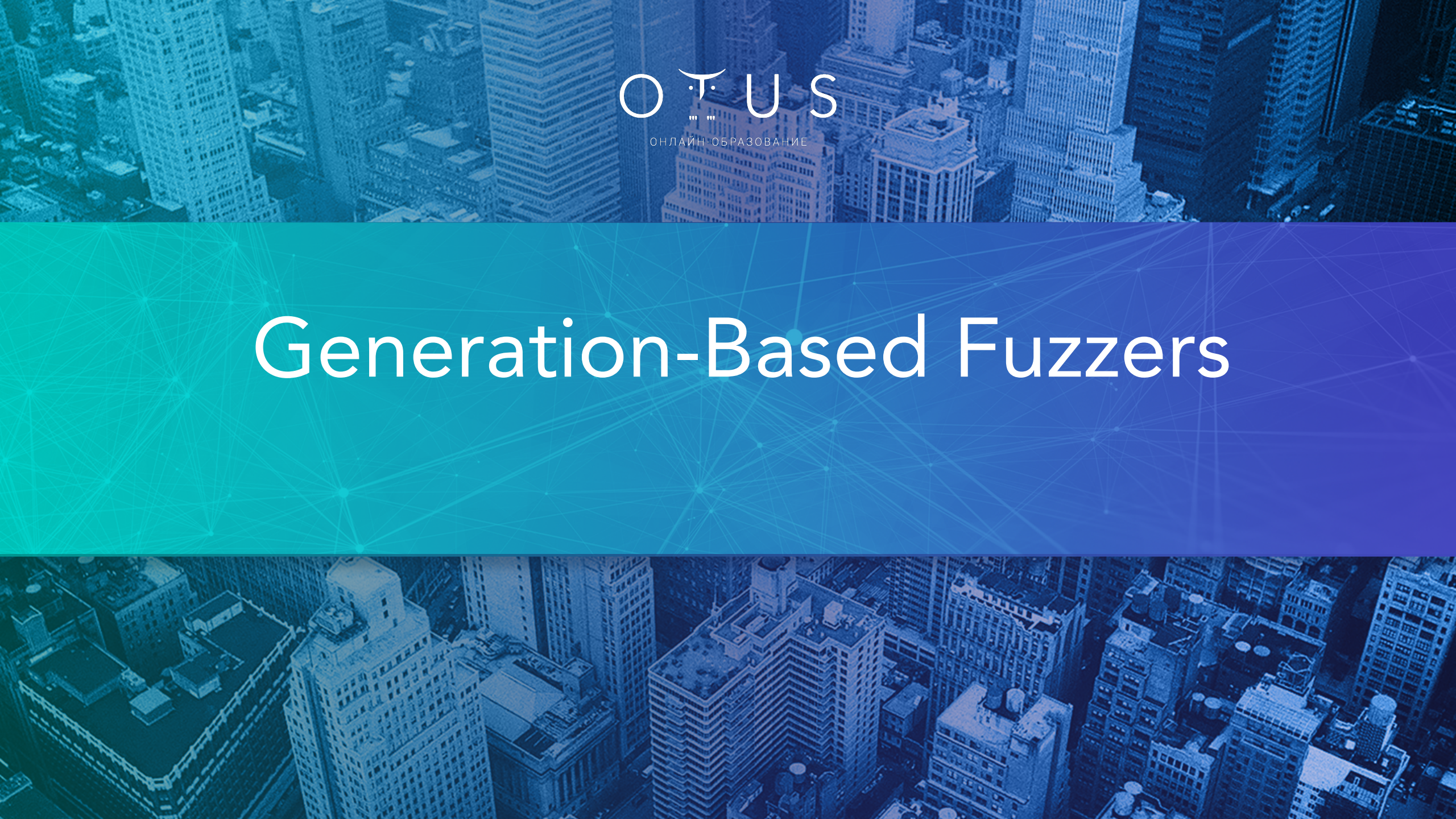
OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ

Mutation-Based Fuzzers

Fuzzing one more time

- **Особенности:**
  - Изменяет данные на основе корректного набора
  - Проводит регистрацию падений
  - Изменение касается каждого байта данных





Generation-Based Fuzzers

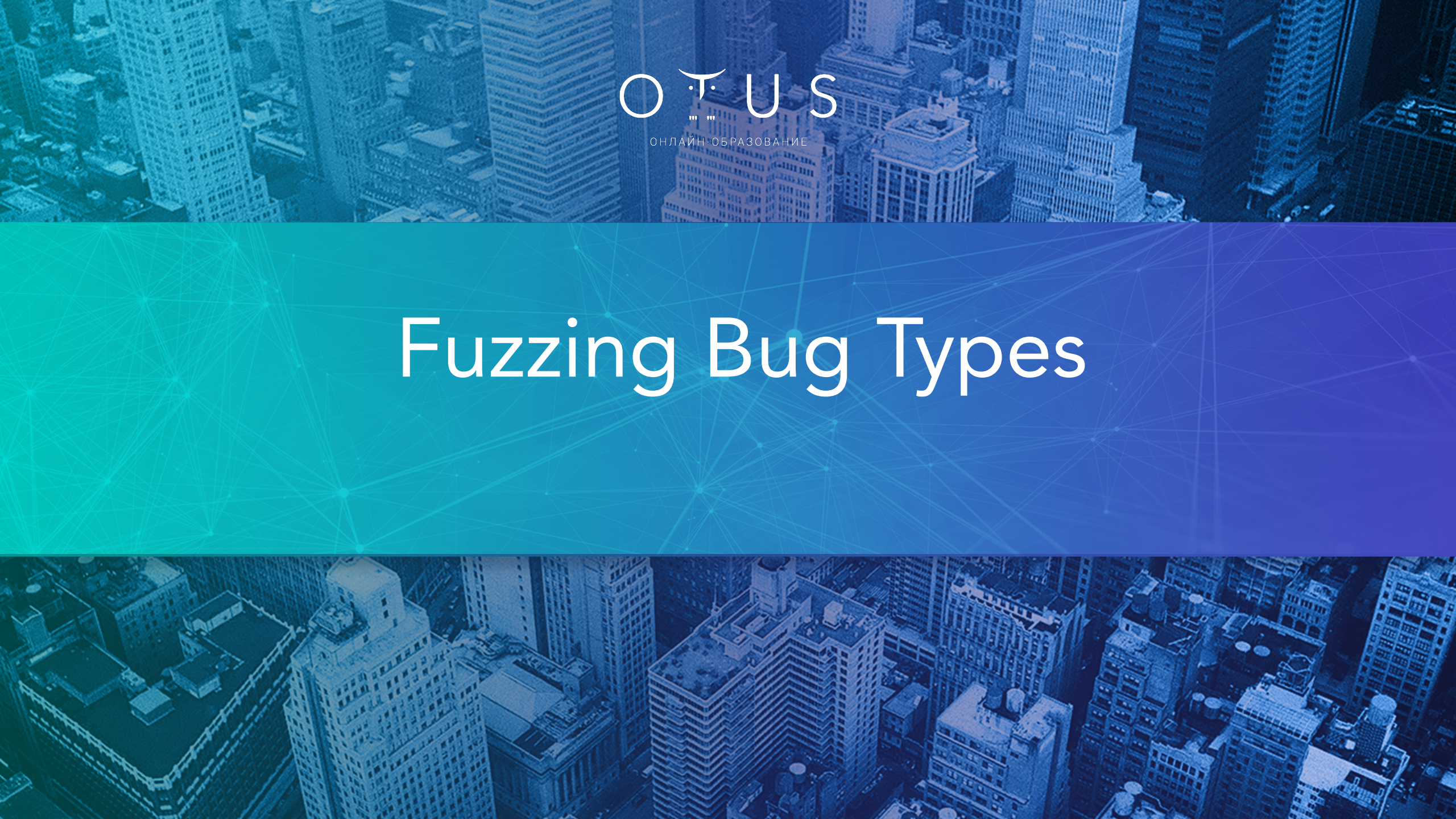
Fuzzing one more time

- **Особенности:**
  - Создает новые данные на основании указанной спецификации
  - Большая вероятность формирования невалидного типа данных

PROTOCOL based Fuzzers

Fuzzing one more time one more time

- **Особенности:**
  - Создает новые данные на основании спецификаций протоколов
  - Пытается генерировать валидные и незавидные последовательности
  - Работает за счёт грамматики



Fuzzing Bug Types

Что можно найти?

- **Assert and memory leaks -** актуальные уязвимости для комплексного программного обеспечения
- **Invalid input -** поиск неверных данных для приложений
- **Correctness** - тестирование для обнаружения правильного функционирования приложения.

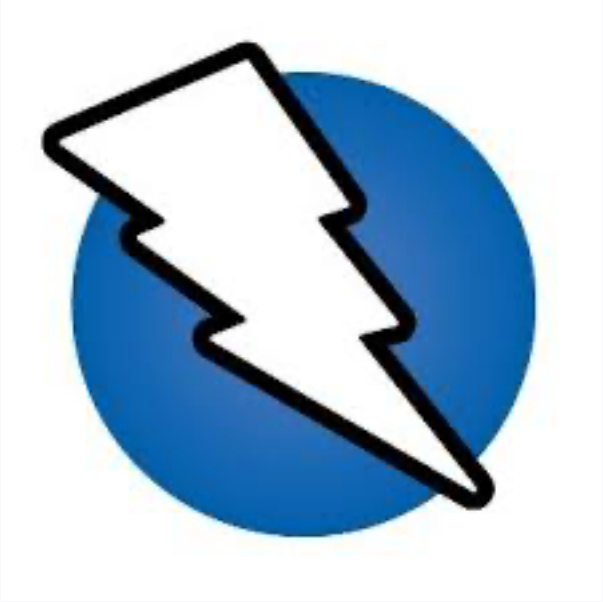
Testing programs

Burp Suite

- Приложение для тестирований web приложений
- Предоставляет возможность конфигурации приложений
- Проверка без исходного кода

OWASP ZAP

- Автоматический сканер
- Ориентирован на web приложения
- Проводит тестирование для заданного набора входных параметров



wFuzz

- Framework для автоматического тестирования:
  - Cookie
  - Path
  - HTTP Requests

Practice

Спасибо за внимание!
Приходите на следующие вебинары

Колесников Александр