




OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Меня хорошо видно && слышно?

Ставьте  , если все хорошо
Напишите в чат, если есть проблемы

Проверить, идет ли запись!





Анализ защищенности веб-приложения:
ТТР. Часть 1: сбор информации о веб-приложении и его компонентах

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

Этапы тестирования
приложения



Сбор информации



Инструменты и цели



Практика

Цели

- 1 Разобраться с этапами тестирования приложения на уязвимости
- 2 Рассмотреть основные этапы тестирования
- 3 Провести тесты

The image features a central horizontal band with a blue-to-purple gradient background. Overlaid on this band is a white network pattern of interconnected nodes and lines. The text 'Анализ веб-приложения' is centered in white, bold, sans-serif font. The top and bottom portions of the image show an aerial view of a city skyline, rendered in a monochromatic blue color scheme.

Анализ веб-приложения

С чего начать?

- **Виды сбора информации:**
 - **Пассивный** - набор методик по которым нельзя взаимодействовать с системой напрямую. Позволяет собрать информацию о версиях приложения и возможных интерфейсах.
 - **Активный** - набор методик для сбора информации с непосредственным взаимодействием с приложением или его частью



Пример пассивного сбора информации

- **Инструменты для сбора:**

- **Поисковые машины**

- Google
- Shodan
- Censur
- Tineye
- Wayback machine
-

- **Дополнения для браузера:**

- wappalyzer.
- Build with
- whatruns
- shraga



Активный сбор информации

- **Приложения для сбора информации:**
 - theHarvester
 - Osmedeus
 - Burp Suite
 - TIDoS





O T U S
ОНЛАЙН ОБРАЗОВАНИЕ



Practice





Спасибо за внимание!
Приходите на следующие вебинары

Колесников Александр