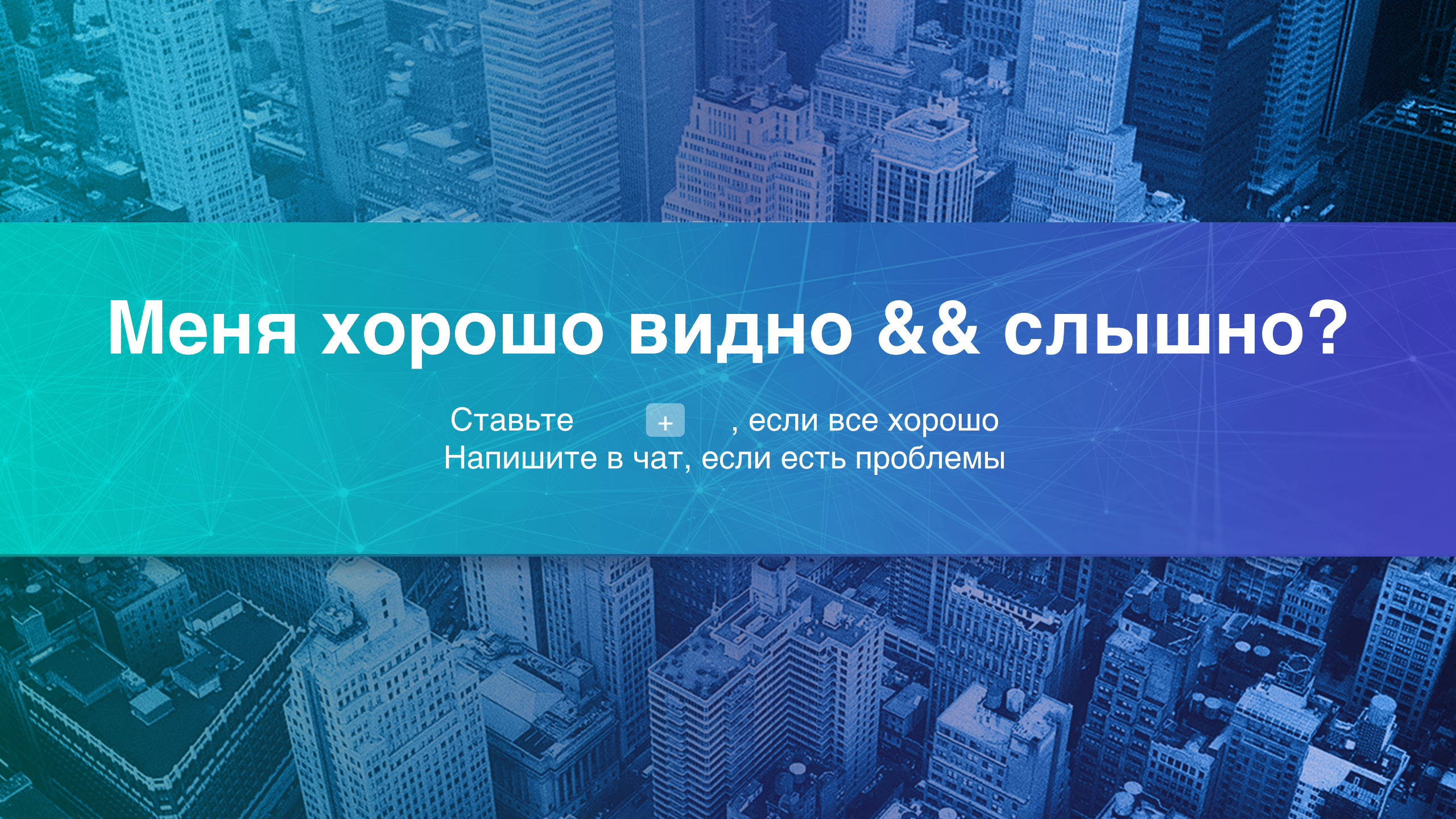
OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Проверить, идет ли запись!



Меня хорошо видно && слышно?

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

Основы технологий, необходимые для понимания уязвимостей. Классификация OWASP top 10

Пархомец Павел

Penetration tester

Awillix LLC

тг: gremlin_97

Павел Пархомец

- Yandex hall of fame
- Awillix LLC (Специалист по тестированию на проникновение)
- Победитель международных конкурсов HITB AI Challenge и Kaspersky SecurIT Cup’19
- Разрабатываю курс по информационной безопасности для лицеистов при НИЯУ МИФИ
- Тренер команд по наступательной безопасности
- Специализируюсь на эксплуатации уязвимостей веб-приложений
- CTF игрок (Sploit00n, Eun014)
- eJPT, OSCP, eWPT

Правила вебинара

Активно участвуем

Задаем вопрос в чат или голосом

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

Вопросы вижу в чате, могу ответить не сразу

План вебинара

1)Уязвимости и причины возникновения

2)OWASP Top 10

3)Поиск уязвимостей

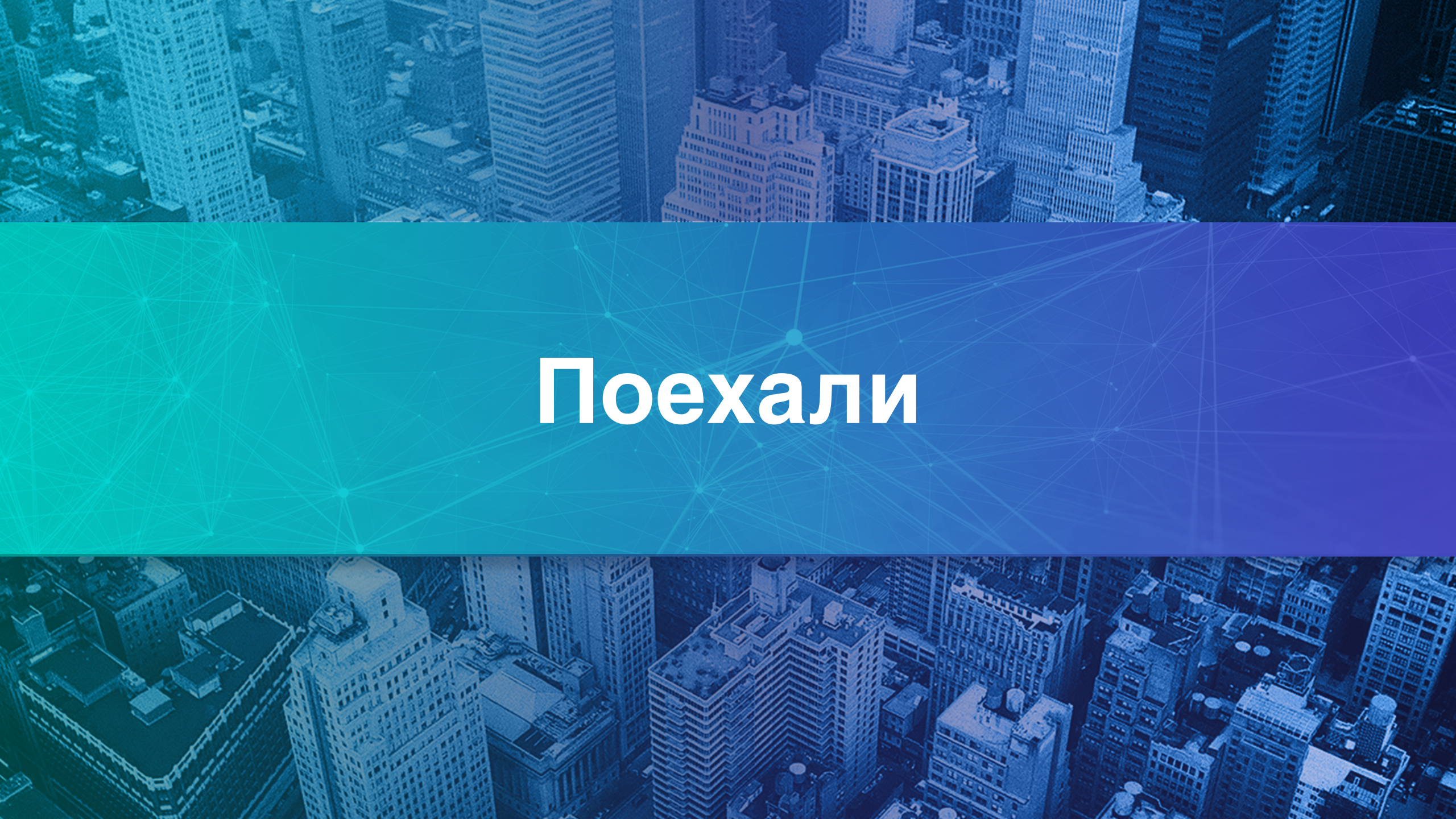
Цели вебинара

1. Познакомиться с уязвимостями веб-приложений
2. Познакомиться с классификацией OWASP Top 10
3. Узнать принципы поиска уязвимостей

Смысл | Зачем вам это уметь

1. Создавать безопасные приложения

2. Помогать создавать безопасные приложения


Поехали

Вебинар

1)Уязвимости и причины возникновения

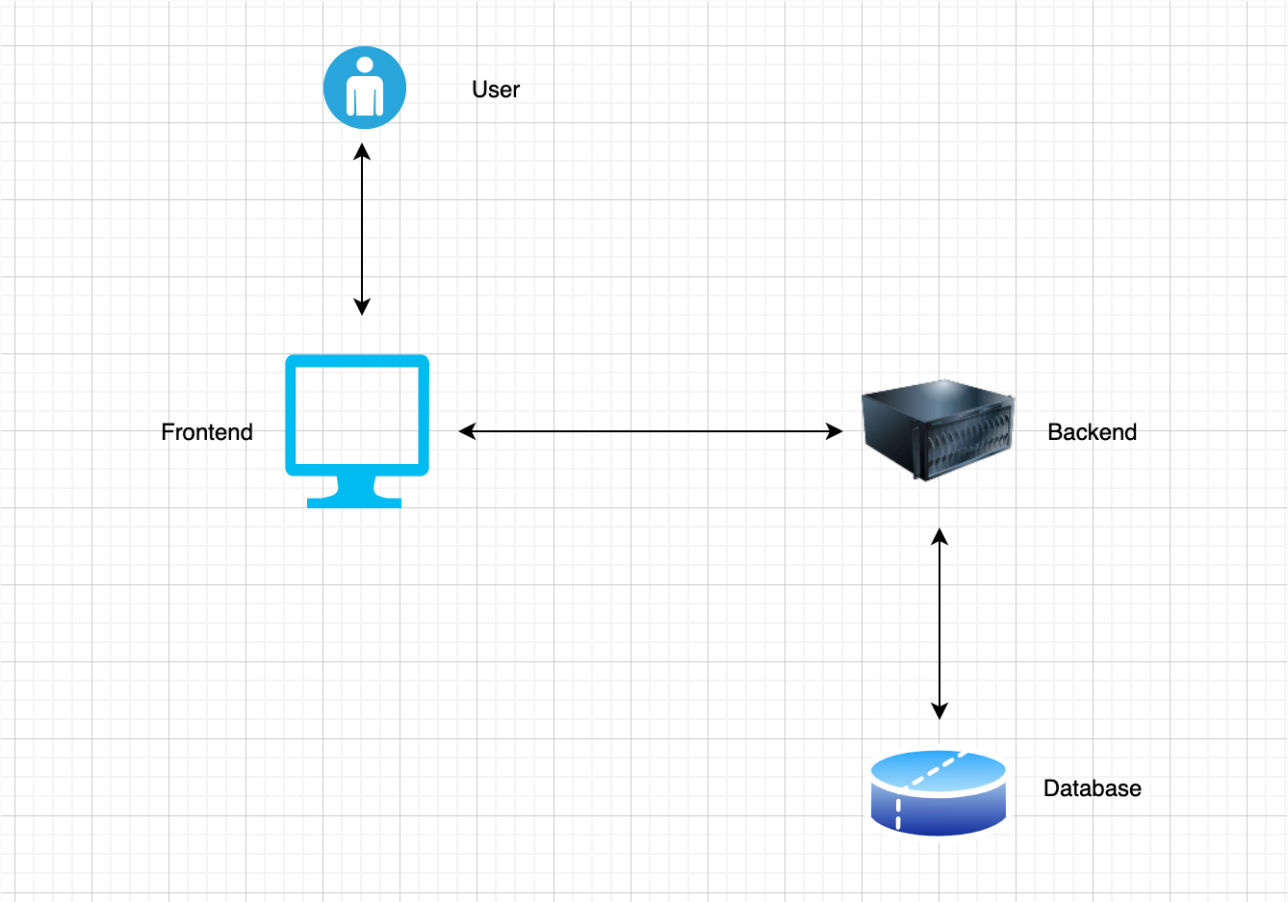
2)OWASP Top 10

3)Поиск уязвимостей

Уязвимость

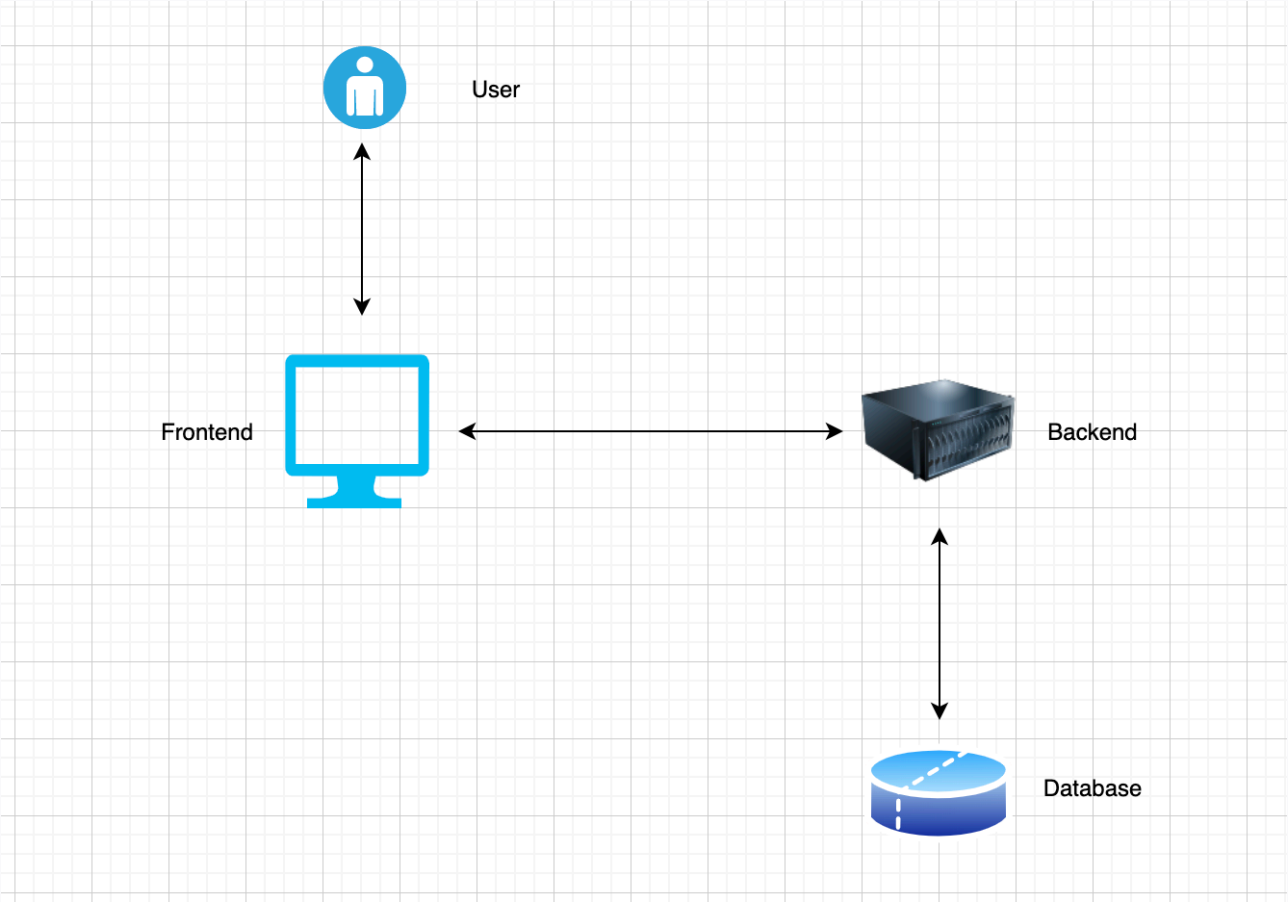
В компьютерной безопасности термин «**уязвимость**» (англ. *vulnerability*) используется для обозначения недостатка в системе, используя который, можно намеренно нарушить её целостность и вызвать неправильную работу. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других вредоносных программ, скриптовых и SQL-инъекций. Некоторые уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты.

Уязвимость | Виды



Уязвимость | Виды

- Атаки на пользователя
- Атаки на сервер



Уязвимость I Причины

- Недостаточная проверка пользовательского ввода
- Ошибки в логике приложения

Уязвимость | Вопросы

- ???

Вебинар

1)Уязвимости и причины возникновения

2)OWASP Top 10

3)Поиск уязвимостей

OWASP Top 10

- Injection
- Broken authentication
- Sensitive data exposure
- XXE
- Broken access control
- Security misconfiguration
- XSS
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient Logging & Monitoring

OWASP Top 10 | Injection

- SQLi
- OS
- Ldap
- NoSQLi

OWASP Top 10 I Injection

Item = mysqli_query(‘SELECT * FROM Items WHERE id=‘ + $_GET[‘id’])

Подаем id = 1, получаем выражение:
SELECT * FROM Items WHERE id=1

Вроде все ок. Давайте попробуем сделать инъекцию.
Подаем id = -1 or 1=1, получаем выражение:
SELECT * FROM Items WHERE id=-1 or 1=1

OWASP Top 10 | Broken Authentication

1) уязвимости JWT
2) Уязвимости сессий
3) Возможность перебора паролей
4) И так далее

OWASP Top 10 | Broken Authentication

Авторизация VS Аутентификация

OWASP Top 10 | Sensitive data exposure

1) Пароли

2) Токены

3) Пользовательские данные

4) И так далее

OWASP Top 10 | Sensitive data exposure

Как хранить пароли?

OWASP Top 10 | XXE

1) Разглашение информации
2) Сканирование портов
3) Удаленное выполнение кода

OWASP Top 10 | Broken Access Control

1) Доступ к информации других пользователей
2) Изменение информации других пользователей
3) Доступ к конфиденциальным файлам
4) И тд

OWASP Top 10 I Security Misconfiguration

1) Разглашение информации через заголовки
2) Отсутствие заголовков безопасности
3) Неправильные серверные настройки
4) И тд

OWASP Top 10 | Security Misconfiguration

Что такое HSTS?

OWASP Top 10 I XSS

1. Кража Cookie
2. Порча сайта
3. Перенаправление
4. Действие от имени пользователя

OWASP Top 10 I

1. Insecure Deserialization
2. Using Components with Known Vulnerabilities
3. Insufficient Logging & Monitoring

OWASP Top 10 | Вопросы

???

Вебинар

1)Уязвимости и причины возникновения

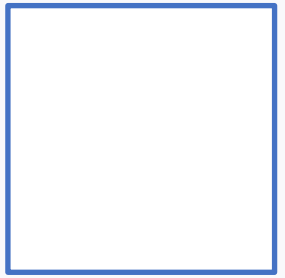
2)OWASP Top 10

3)Поиск уязвимостей

OWASP Top 10 | Поиск уязвимостей

Black box

Grey box



White box

OWASP Top 10 | Black box

1.Понимать, какая уязвимость тут может быть

2.Знать способы детекта той или иной уязвимости

3.Найти все эндпоинты

4.Внедрять пейлоады на эндпоинтах (пофаззить)

OWASP Top 10 | Black box

Инструменты:

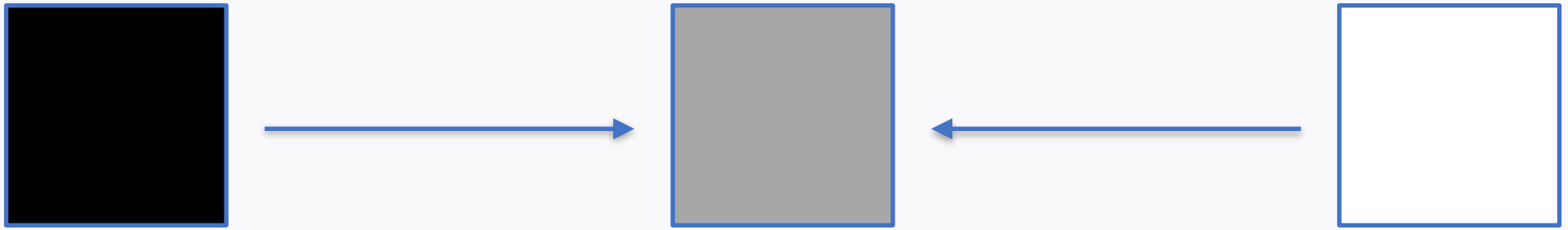
- Dirsearch
- Gobuster
- Dirbuster
- Burp Suit
- webfuzz
- …

OWASP Top 10 | White box

По сути - анализ исходного кода.

- **Ручной анализ**
- **Автоматизированный анализ**

OWASP Top 10 | Grey box



Цели вебинара I Проверка достижения целей

1. Узнали про уязвимости и их классификации

2. Познакомились с основными подходами при Поиске уязвимостей

Рефлексия

С какими основными мыслями и инсайтами уходите с вебинара?

Достигли ли вы цели вебинара?

Следующий вебинар

Тема: Уязвимости класса: Open Redirect, CSRF

12.08

Ссылка на вебинар будет в ЛК за 15 минут

Материалы к занятию в ЛК — можно изучать

Обязательный материал обозначен красной лентой

Список материалов для изучения

1) https://owasp.org/www-project-top-ten/
2) https://ru.wikipedia.org/wiki/Уязвимость_(компьютерная_безопасность)


Заполните, пожалуйста,
опрос о занятии по ссылке в чате

Спасибо за внимание!
Приходите на следующие вебинары

Пархомец Павел

Специалист по тестированию на проникновение

Awillix LLC

tg: @gremlin_97