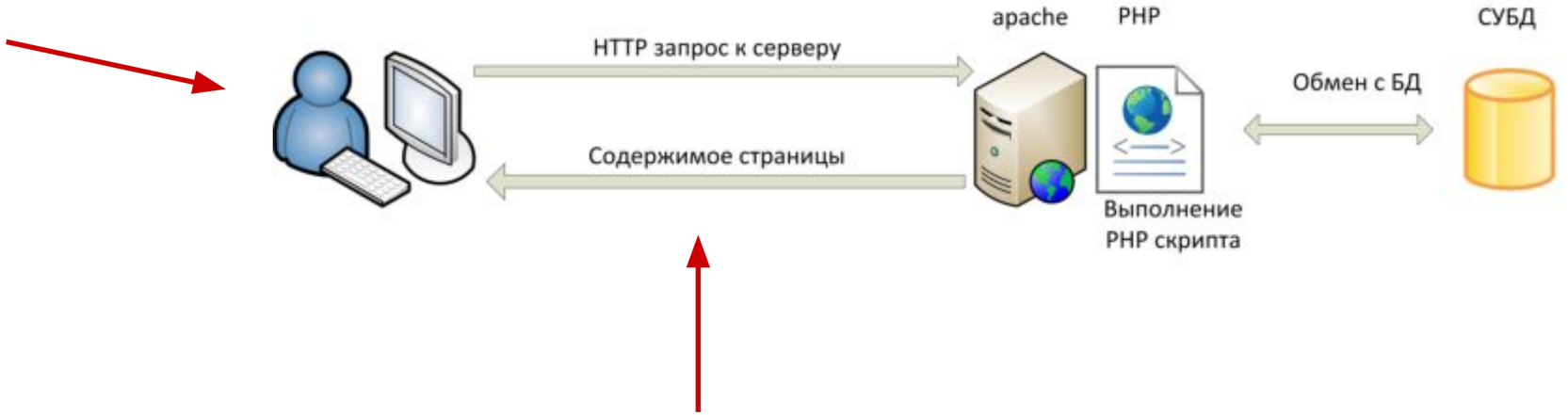
Skillbox

Уязвимости веб-приложений

Что может пойти не так?

бесконечное число попыток авторизации (возможность подобрать пароль)

небезопасное хранение данных в базе



передача данных в открытом виде

Отчет Positive Technologies

Уровень защищенности веб-приложений продолжает постепенно расти, но все еще остается довольно низким.

Про веб-приложения:

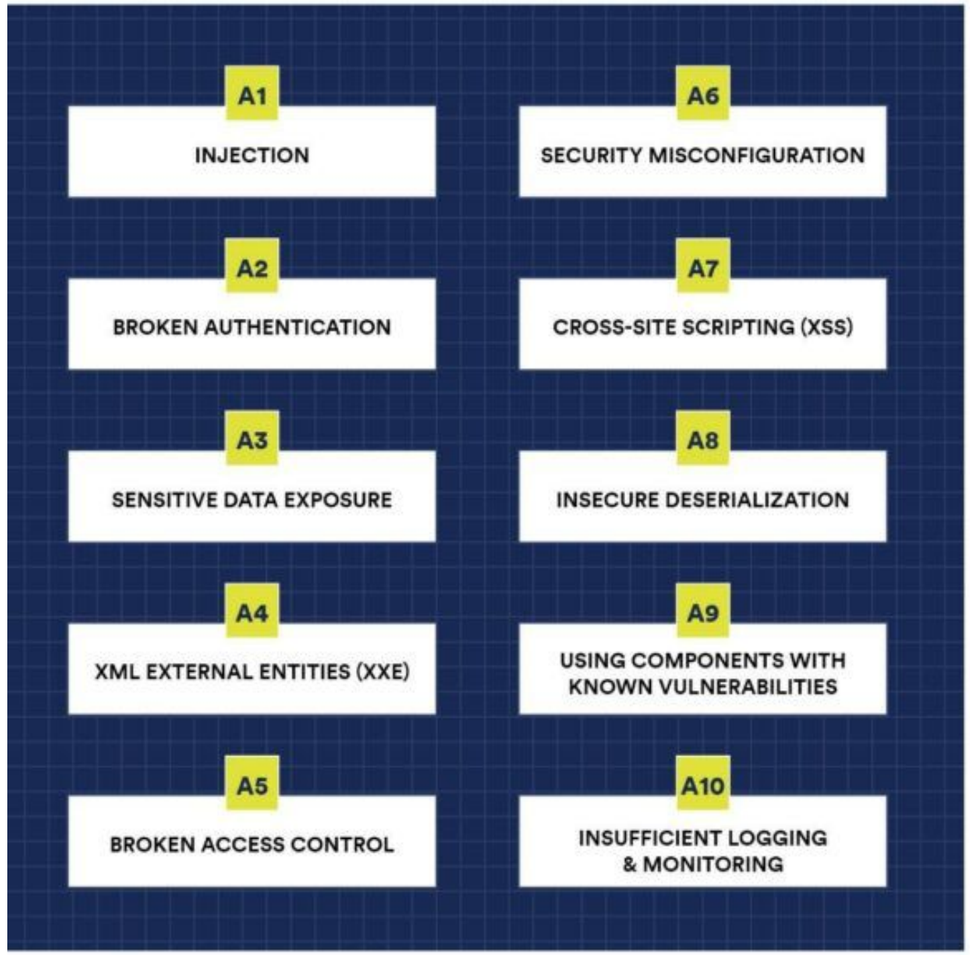
- **В 9 из 10 веб-приложений преступники могут проводить атаки на пользователей.** В том числе — перенаправлять клиентов на подконтрольный им ресурс, похищать учетные данные с помощью фишинговых атак, заражать компьютер вредоносным ПО.
- **Несанкционированный доступ к приложению возможен на 39% сайтов.** Кроме того, в 2019 году полный контроль над системой был получен в 16% веб-приложений, а в 8% систем полный контроль над сервером веб-приложения позволял проводить атаки на локальную сеть организации.
- **Угроза утечки важных данных присутствует в 68% веб-приложений.** Среди «утекших» данных на первом месте персональные (47% утечек), а на втором — учетные (31%).

Про уязвимости:

- **82% уязвимостей содержались в коде приложения.**
- **Число уязвимостей, которое в среднем приходится на одно веб-приложение, снизилось по сравнению с 2018 годом в полтора раза.** В среднем на одну систему приходятся 22 уязвимости, четыре из которых имеют высокий уровень риска.
- **Каждая пятая уязвимость — высокого уровня риска.**

OWASP TOP 10

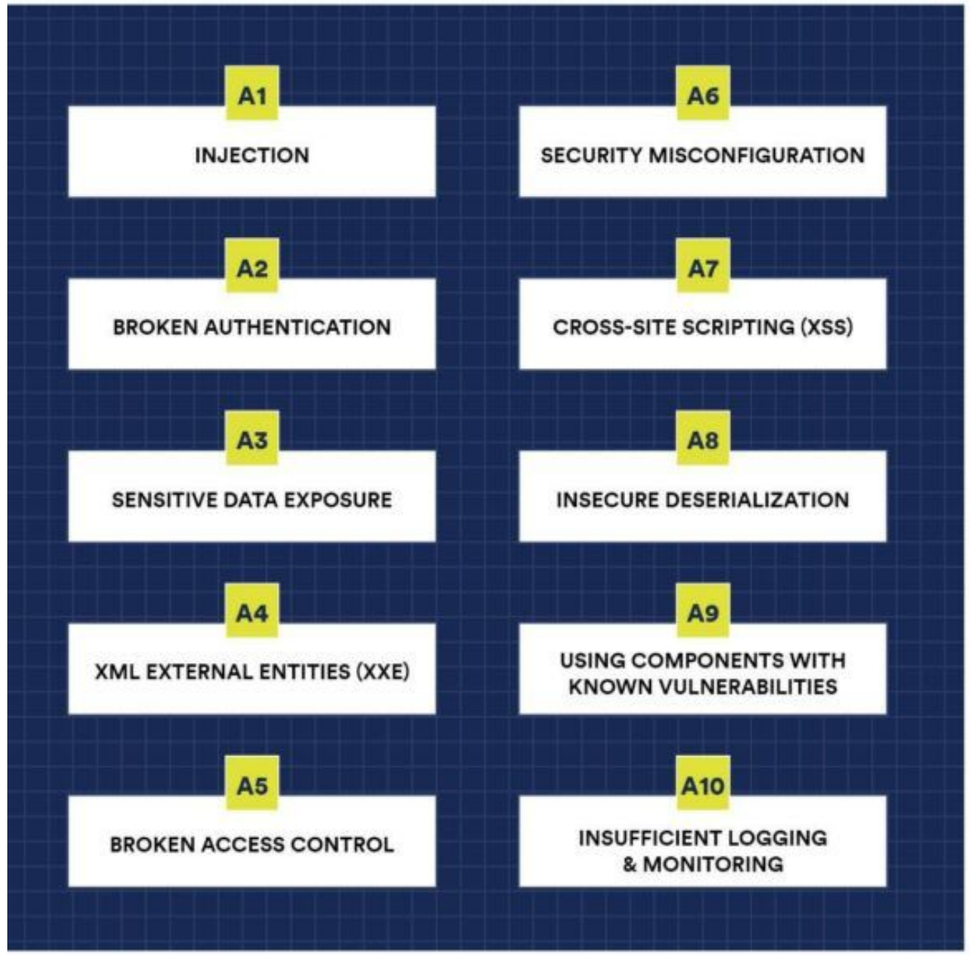
OWASP TOP 10 — это рейтинг 10 самых актуальных уязвимостей веб-приложений, который составляется сообществом OWASP. Наличие в веб-приложении уязвимости из этого списка представляет серьёзную угрозу как для безопасности информации самого веб-приложения, так и для безопасности пользователей этого приложения



OWASP TOP 10

OWASP TOP 10 — это рейтинг 10 самых актуальных уязвимостей веб-приложений, который составляется сообществом OWASP. Наличие в веб-приложении уязвимости из этого списка представляет серьёзную угрозу как для безопасности информации самого веб-приложения, так и для безопасности пользователей этого приложения

OWASP Security Testing Guide — методология тестирования безопасности веб-приложений. Содержит лучшие практические рекомендации для проведения тестирования на проникновение, а также низкоуровневое руководство, которое описывает техники тестирования для наиболее распространенных уязвимостей в веб-приложениях и веб-сервисах.



Методологии тестирования безопасности веб-приложений

- OSSTMM — методология тестирования систем безопасности с открытым исходным кодом
- NIST Special Publications 800-115 — техническое руководство, которое можно применять для проверки уровня информационной безопасности организаций из различных сфер, в том числе финансовых и ИТ-компаний
- ISSAF — фреймворк оценки безопасности информационной системы
- PTES — предлагает рекомендации для проведения базового пентеста, а также несколько расширенных вариантов тестирования, для организаций с повышенными требованиями к информационной безопасности

Общие этапы тестирования безопасности веб-приложений

- Исследование — сбор общей информации об архитектуре приложения, инфраструктуре и других сведений от разработчика и из общедоступных источников
- Моделирование угроз — определение уязвимых мест и векторов атаки, учитывая бизнес процессы и критически важные элементы инфраструктуры
- Анализ и эксплуатация уязвимостей — выявление уязвимостей и оценка потенциальных рисков, а также попытка проведения атак с использованием найденных уязвимостей
- Составление отчета — пентестер составляет итоговый документ, где указывает все найденные уязвимости с оцененной степенью риска и рекомендации по их устранению