OWASP Top 10 Mobile Risks - 2024 (Простое объяснение)

M1: Неправильное использование учётных данных
- Хранение логинов и паролей прямо в коде, в открытом виде или без защиты
- Пример: пароль от сервера внутри приложения — его легко найти.

M2: Недостаточная безопасность цепочки поставок
- Использование сторонних библиотек без проверки их безопасности
- Пример: библиотека для рекламы шпионит за пользователем.

M3: Ненадёжная аутентификация и авторизация
- Плохая реализация входа или проверки прав
- Пример: можно получить чужие данные, просто подставив другой ID.

M4: Недостаточная проверка входных/выходных данных
- Нет фильтрации ввода
- Пример: ввод 'вредного' текста ломает приложение или даёт доступ к базе.

M5: Небезопасная передача данных
- Данные передаются без шифрования
- Пример: логин и пароль через обычный HTTP можно перехватить.

M6: Недостаточная защита личных данных
- Слишком много личной информации хранится без защиты
- Пример: фото и контакты без шифрования.

M7: Недостаточная защита бинарного кода
- Приложение легко взломать
- Пример: хакер может изменить код, декомпилировав APK.

M8: Ошибки в настройке безопасности
- Неправильные настройки
- Пример: открыт отладочный режим или доступ к конфиденциальному API.

M9: Небезопасное хранение данных
- Чувствительные данные хранятся без шифрования
- Пример: токен авторизации в открытом файле.

M10: Недостаточная или неправильная криптография
- Слабое или самодельное шифрование
- Пример: использование устаревшего алгоритма или своего 'шифра'.