ИТМО

Безопасность мобильных приложений

Курс: Обеспечение безопасности мобильных устройств

Преподаватель: доцент ФБИТ, к.т.н, Федоров Иван Романович

Основные источники угроз

- Пользователь
- Операционная система
- Сеть
- API-сервер
- Сторонние библиотеки и SDK

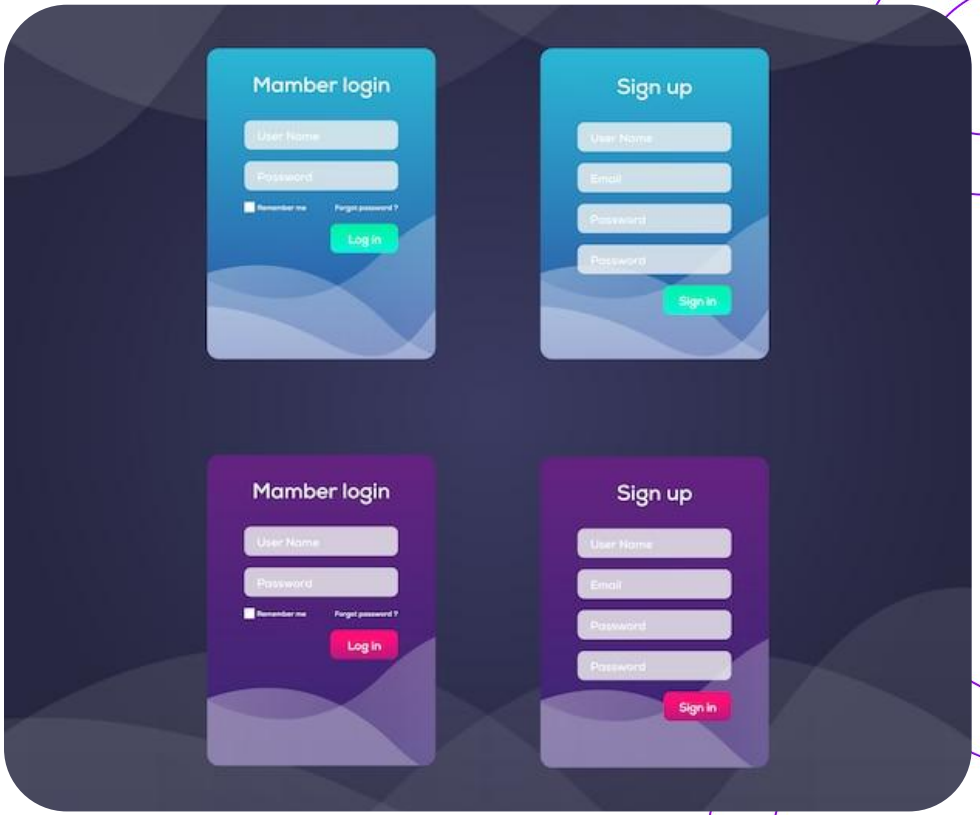
Методология STRIDE

ИТМО

STRIDE THREAT MODEL

	Threat	Property Violated	Threat Definition
S	Spoofing	Authentication	Pretending to be something or someone other than yourself
T	Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere.
R	Repudiation	Non- Repudiation	Claiming that you didn't do something or we're not responsible. Can be honest or false
I	Information Disclosure	Confidentiality	Providing information to someone not authorized to access it.
D	Denial of service	Availability	Exhausting resources needed to provide service.
E	Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do.

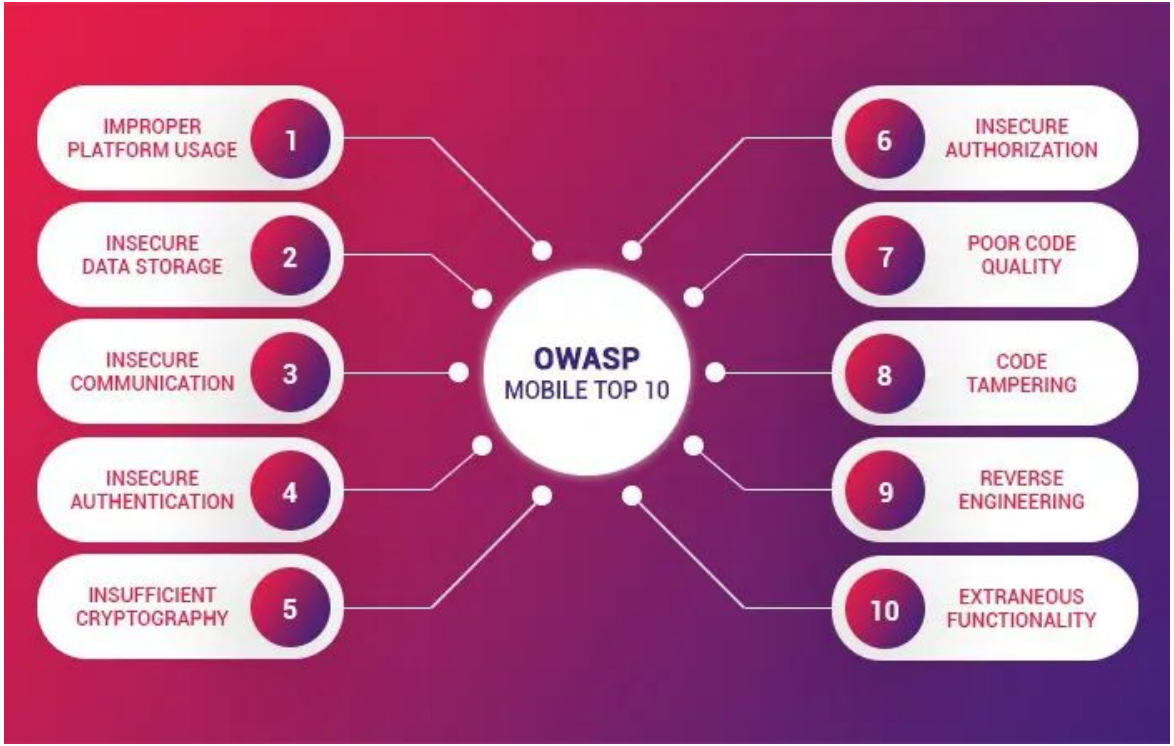
STRIDE-анализ



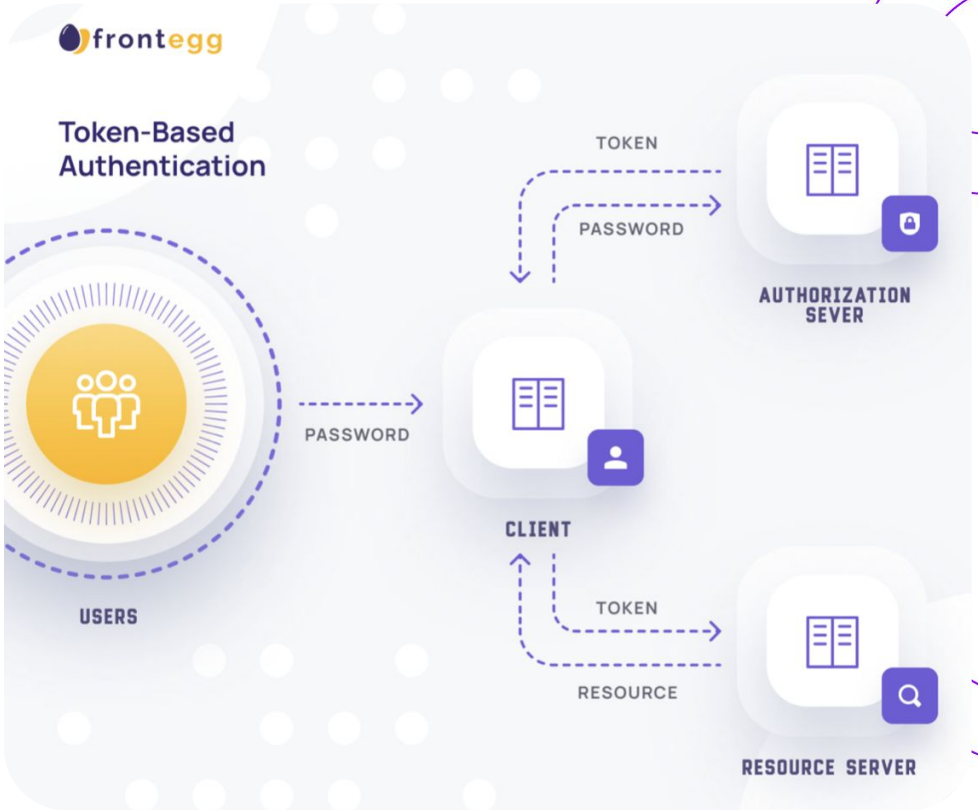
- Может ли кто-то подделать идентичность (S)?
- Может ли кто-то изменить данные (T)?
- Можно ли отрицать действия (R)?
- Может ли произойти утечка информации (I)?
- Можно ли сделать систему недоступной (D)?
- Может ли кто-то получить больше прав, чем положено (E)?

Owasp mobile top 10

ИТМО



Безопасная аутентификация



- Пароли + Хэширование
- Аутентификация через токены
- Биометрическая аутентификация
- Многофакторная аутентификация (MFA)

Хранение паролей и токенов

ИТМО

- Никогда не хранить пароли в открытом виде
- Использование безопасного хранилища
- Локальное шифрование чувствительных данных
- Удаление данных при выходе пользователя

Распространенные ошибки

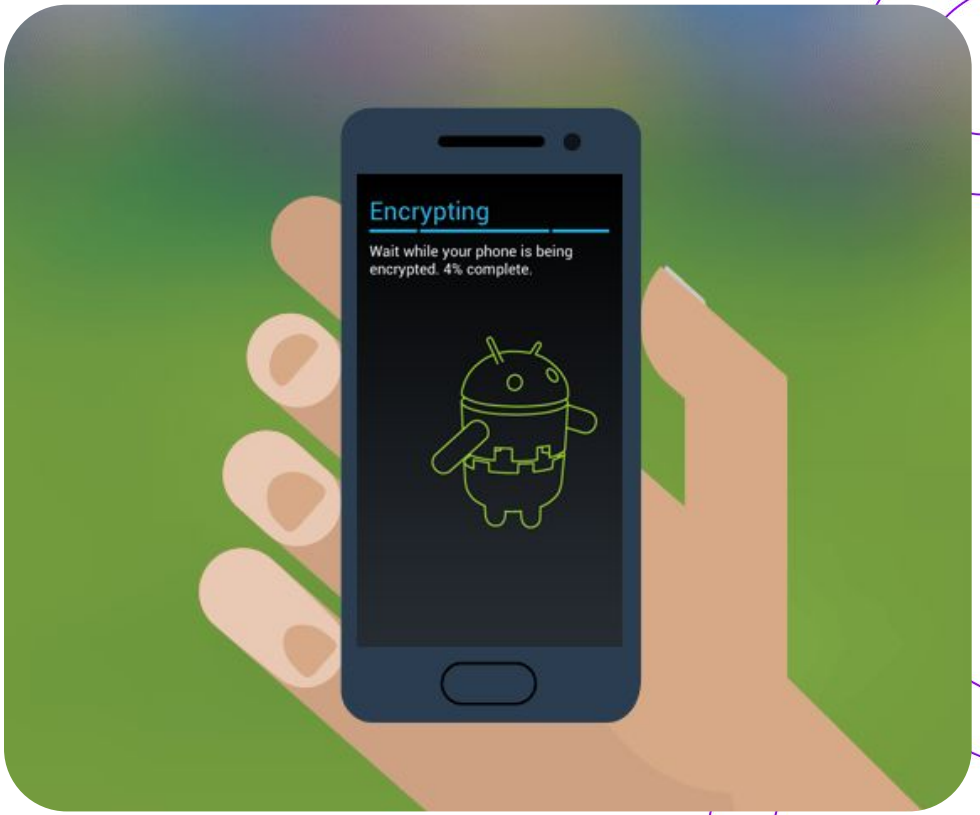
ИТМО

- Хранение токена в SharedPreferences без шифрования
- Отправка пароля по HTTP
- Отсутствие ограничения попыток входа
- Использование устаревших хэш-функций (MD5, SHA1)
- Логирование токенов или паролей

Перекличка

ITMO more than a UNIVERSITY

Шифрование данных



Что шифровать:

- Локальные файлы
- SharedPreferences / UserDefaults
- Базы данных (SQLite/Realm)
- Кэш
- Токены и ключи (auth, refresh, API)
- Передача данных (по сети)

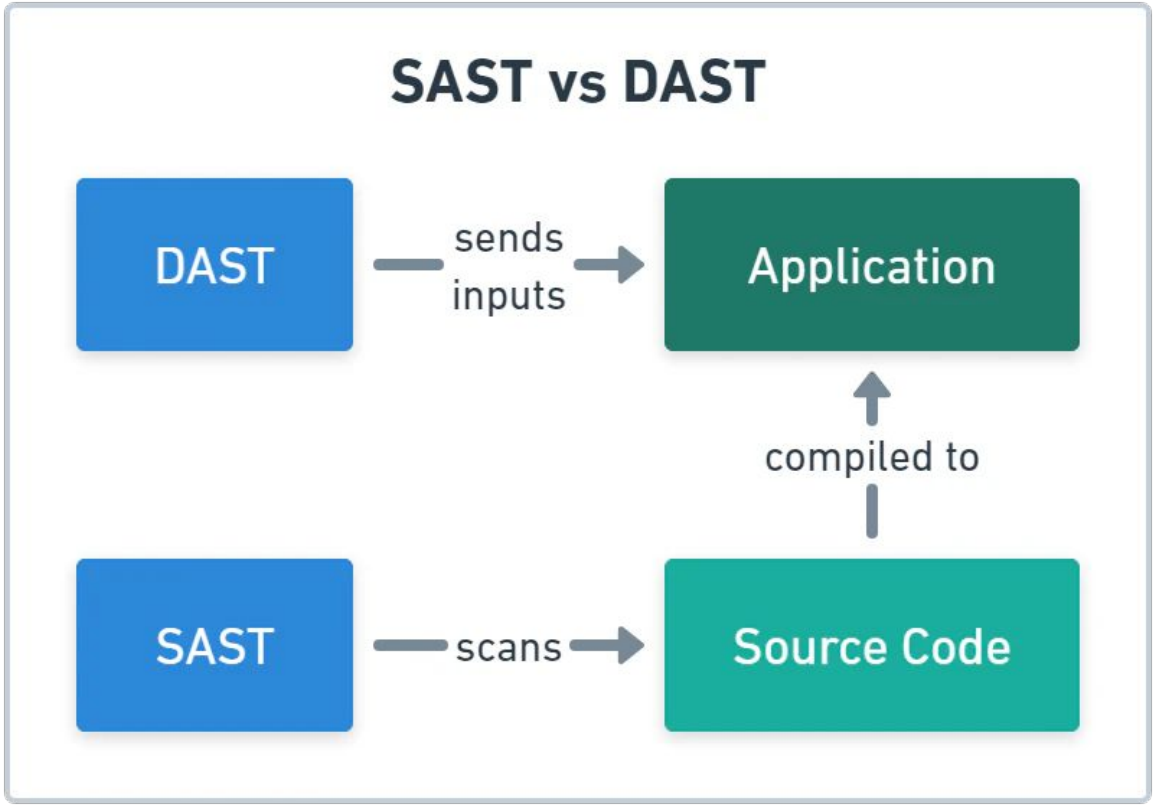
Анализ безопасности: подходы

ИТМО

- Статический анализ (SAST — Static Application Security Testing)
- Динамический анализ (DAST — Dynamic Application Security Testing)
- Анализ сетевого трафика
- Reverse engineering
- Анализ безопасности хранилищ
- Обход защиты

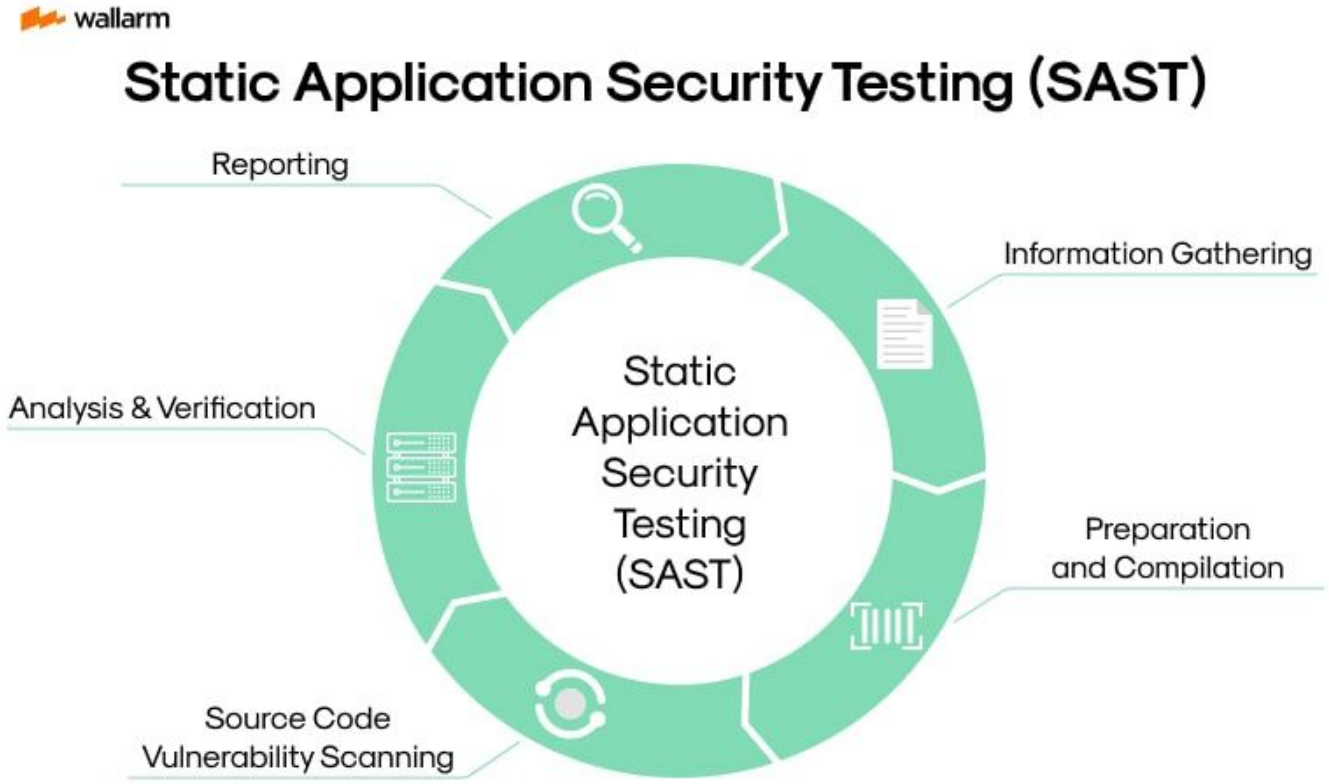
SAST vs DAST

ИТМО



SAST

ИТМО


wallarm
Static Application Security Testing (SAST)
Reporting
Information Gathering
Analysis & Verification
Static Application Security Testing (SAST)
Preparation and Compilation
Source Code Vulnerability Scanning

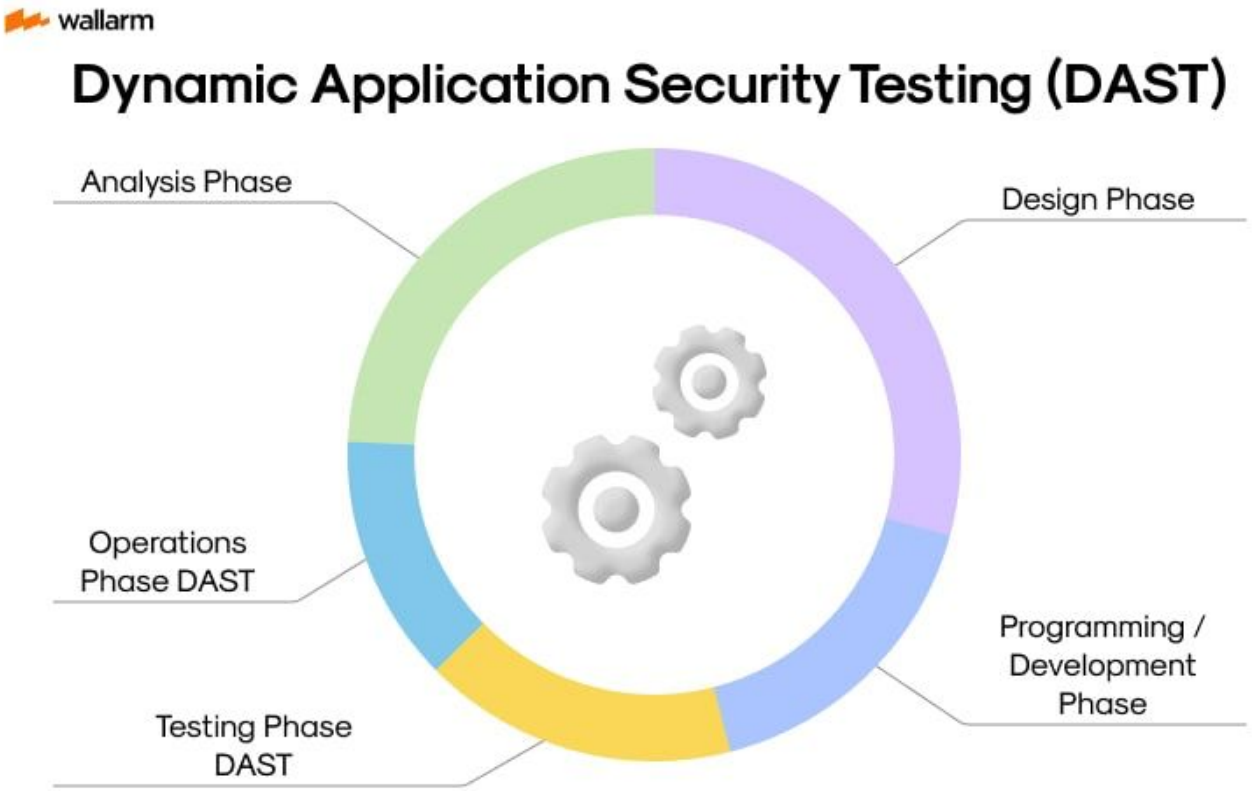
Что можно найти

ИТМО

- Hardcoded API-ключи, токены, пароли
- Использование небезопасных API
- Уязвимости авторизации
- Недостатки конфигурации
- Ошибки шифрования
- Утечки информации

DAST

ИТМО


wallarm
Dynamic Application Security Testing (DAST)
Analysis Phase
Design Phase
Operations Phase DAST
Programming / Development Phase
Testing Phase DAST

Что можно найти

ИТМО

- Токены/пароли в трафике
- Отсутствие SSL-пиннинга
- Утечки в логах (logcat)
- Слишком подробные ошибки от API
- Поведение при MITM (принимает поддельный сертификат?)
- Обход рут-чеков, подмена интентов, чтение приватных файлов

Best practices

ИТМО

- Использовать OWASP Mobile Testing Guide
- Проверять build с помощью MobSF
- Отслеживание ошибок в runtime (например, внедрение Frida в pipeline)
- Хранение чувствительных данных в Keystore/Keychain

Ваши вопросы

ITMO more than a UNIVERSITY

Спасибо
за внимание!

ITMO more than a UNIVERSITY

ivanfedorov@itmo.ru
@VanesFedorov