Networking with URLSession

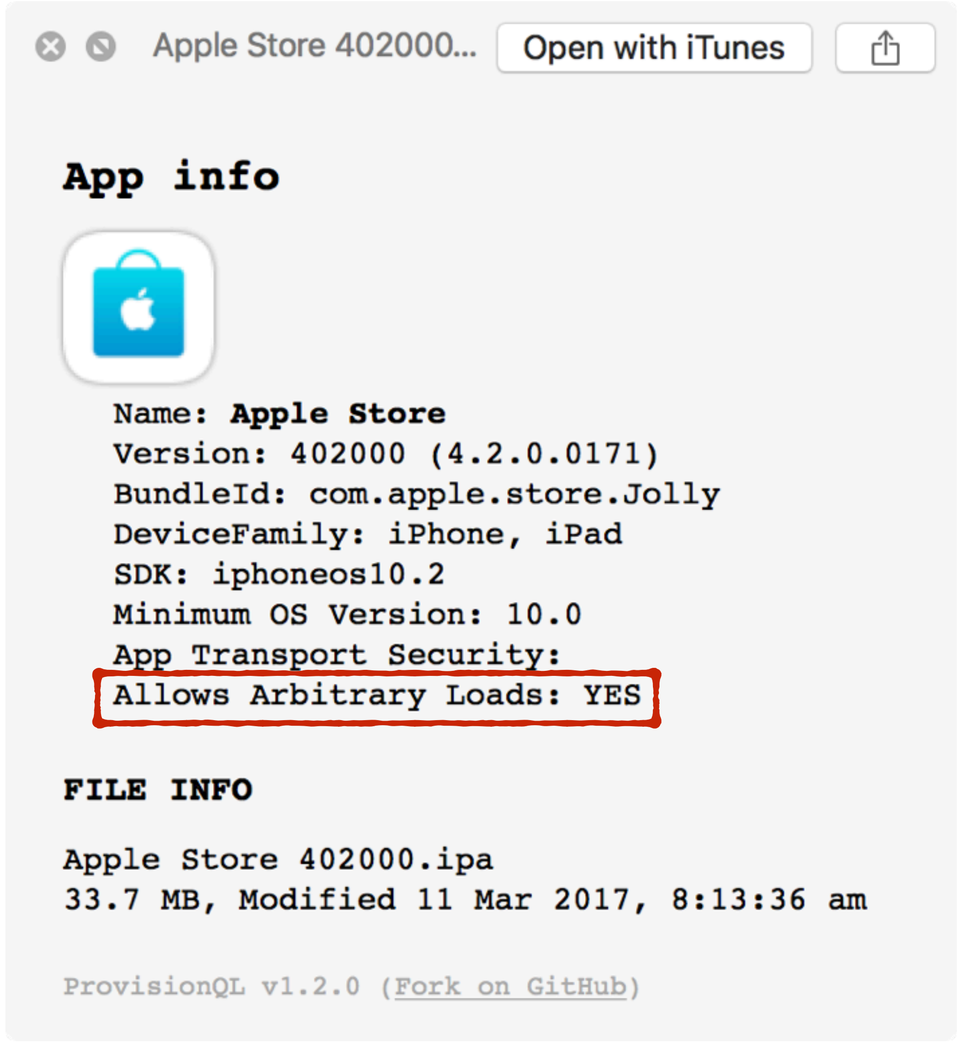
Part 9: ATS

ProvisionQL ATS inspector

RemoveATSExceptions.sh

SSL Server Test

nscurl —ats-diagnostics



App Transport Security

- Since iOS 9 and El Capitan
- Enforces best practices for secure network connections
- Implemented below URLSession and NSURLConnection

ATS Server Requirements

- Server uses HTTPS
- X.509 server cert issued by certificate authority
- TLS 1.2 with Perfect Forward Secrecy
  - ECDHE/AES list
- Leaf server certificate signed with RSA or ECC key, with minimum SHA-256 hashing algorithm

Public Key Pinning

- Defends against Man-In-The-Middle attack
- AKA certificate pinning or SSL pinning
- Server sends client a list of pinned public keys
- Client checks server’s public key against this list

Useful ATS Keys

- NSAllowsArbitraryLoadsInWebContent
- NSAllowsArbitraryLoadsForMedia
- NSAllowsLocalNetworking
- NSAllowsArbitraryLoads

ATS Exception Keys

- NSExceptionDomains
- NSIncludesSubdomains
- NSExceptionRequiresForwardSecrecy
- NSExceptionAllowsInsecureHTTPLoads
- NSExceptionMinimumTLSVersion

Use Cases

- App’s own back-end server
- Some specific server
- An unknown server
- Your app supports iOS9 and iOS10
- Multiple ad, mail, calendar servers
- Protect your domain

Demo

Challenge Time!

▼ App Transport Security Settings	Dictionary	(2 items)
Allow Arbitrary Loads	Boolean	YES
▼ Exception Domains	Dictionary	(1 item)
▼ qualitycoding.org	Dictionary	(2 items)
NSExceptionAllowsInsecureHTTPLoads	Boolean	NO
NSIncludesSubdomains	Boolean	YES