Mobile Hacking (Android & iOS)

UMA INTRODUÇÃO AO TEMA

Conteúdo

- Desmestificando o ambiente para mobile hacking
- Proteções comuns em ambos ambientes
  - Evasão pública
  - Evasão manual
- Análise SAST vs Análise DAST
- WebView – What hell is it?
- App nativo vs App híbrido
- Flutter - O temido =)
- Show me the code
  - Entendendo um script frida para bypass simples

whoami

- Filipe Cordeiro
- Offensive Security Consultant
- Mobile XP 3+ (apenas um newbie buscando o seu lugar ao sol)
- @unl0g1c - Telegram
- Um baiano em sergipe xD

Desmestificando o ambiente para mobile hacking

1. Device vs Emulador – Android;
2. Device vs Emulador – iOS;
3. MobSF;
4. Jadx-GUI;
5. Disassembler (Hopper, Ghidra);
6. Frida vs Objection;
7. Proxy (Burp, mitmproxy, caido etc).

Obs: posso ter esquecido de algum rs.

Algumas proteções comuns em ambos ambientes

1. Root detection;
2. Jailbreak;
3. SSL Pinning;
4. Código ofuscado;
5. Anti debugger;
6. Anti frida;
7. Body encrypted.

1. Evasão pública:
   a. Script frida compartilhado na internet;
2. Evasão manual:
   a. Criar o script com base na implementação.

Análise SAST vs Análise DAST

1. Análise SAST: Static Application Security Testing
    a. MobSF
    b. Jadx-GUI
    c. Disassembler (iOS, Flutter app)
    d. Horusec

1. Análise DAST: Dynamic Application Security Testing
    a. Dispositivo ou Emulador
    b. Frida
    c. Proxy
    d. Adb toolkit (shell, logcat etc)
    e. SSH (iOS)

WebView – The good way to the RCE

O **WebView** do Android é um componente do sistema do Google que vem pré-instalado e permite que apps Android mostrem conteúdo da Web.

Ways to exploit them:

1. setJavaScriptEnabled(true);
2. setAllowUniversalAccessFromFileURLs(true);
3. setWebContentsDebuggingEnabled(true).

Caso de RCE em webview: App do tiktok (desfrutem =))

App nativo vs App híbrido (What's the difference?)

App nativo: Aplicativos desenvolvidos somente para uma plataforma.
App híbrido: Aplicativos desenvolvidos para mais de uma plataforma.

Ways to exploit:
App nativo: decompila *e/ou* recupera o bytecode e explora
App híbrido: Extração do código Javascript no arquivo android.bundle em caso de ReactNative .

Flutter - O temido =)

libapp.so – Código DART do aplicativo;
libflutter.so – Implementações do aplicativo.

Ways to exploit:
libapp.so – Doldrums para a extração do código DART;
libflutter.so – Disassembler.

O frida

- Frida
- Frida-trace
- Codeshare
- Frida API (Javascript, typescript, objective-C)

Show me the code

Steps:

1. Executar o aplicativo para ver a detecção;
2. Ler o código da implementação;
3. Criar um script do frida explicando cada ponto
4. Executar o script do frida
5. Bypass do rootbeer <3

VALEU RAPAZIADA!

Leiam a PHRACK Magazine!

Keep hacking