MobileApp-Pentest-шпаргалка

Публичный

танпратан Обновление README.md

2cfe8bf · 3 года назад 105 Коммитов

MobileApp_Check...	Обновленный контрол...	8 лет назад
Mobile_App_Secu...	Новый контрольный с...	4 года назад
README.md	Обновление README.md	3 года назад

Шпаргалка по тестированию на проникновение мобильных приложений была создана с целью предоставления краткого сборника ценной информации по конкретным темам тестирования на проникновение мобильных приложений.

#статический анализ #мобильное приложение #android-приложение #ios-приложение #динамический анализ #пентестинг #реверс-инженеры #сетевой анализ #анализ времени выполнения

Прочти меня

Активность

4,8 тыс. звезд

221 смотрят

Памятка по тестированию на проникновение мобильных приложений

Шпаргалка по тестированию на проникновение мобильных приложений была создана для предоставления краткого сборника ценной информации по конкретным темам тестирования на проникновение мобильных приложений, а также контрольного списка, который сопоставлен с OWASP Mobile Risk Top 10 для проведения тестирования на проникновение.

- Лицензия

Дистрибутивы для тестирования безопасности мобильных приложений

- Appie — портативный программный пакет для пентестинга Android и великолепная альтернатива существующим виртуальным машинам.
- Android Tamer — Android Tamer — это виртуальная/живая платформа для профессионалов в области безопасности Android.
- Androl4b — виртуальная машина для оценки приложений Android, обратного проектирования и анализа вредоносного ПО
- Проект Vezir — среда для пентестинга мобильных приложений и анализа вредоносного ПО.
- Mobexler — Mobexler — это настраиваемая виртуальная машина, разработанная для помощи в тестировании на проникновение приложений Android и iOS.

Универсальные фреймворки мобильной безопасности

- Mobile Security Framework - MobSF - Mobile Security Framework - это интеллектуальная, комплексная автоматизированная среда для тестирования на проникновение для мобильных приложений с открытым исходным кодом (Android/iOS), способная выполнять статический и динамический анализ.
  - `python manage.py runserver 127.0.0.1:1337`
- Needle — Needle — это модульная структура с открытым исходным кодом, которая упрощает процесс проведения оценок безопасности приложений iOS, включая двоичный анализ, статический анализ кода,

манипуляции во время выполнения с использованием Cycript и перехвата Frida и т. д.

- Objection - Objection - это набор инструментов для исследования мобильных приложений во время выполнения, работающий на базе Frida. Он был создан с целью помочь оценить мобильные приложения и их состояние безопасности без необходимости взломанного или рутированного мобильного устройства.
- RMS-Runtime-Mobile-Security - Runtime Mobile Security (RMS) на базе FRIDA — это мощный веб-интерфейс, который помогает вам управлять приложениями Android и iOS во время выполнения.

Тестирование на проникновение приложений Android

Обратный инжиниринг и статический анализ

- APKTool - Инструмент для обратного проектирования сторонних, закрытых, бинарных приложений Android. Он может декодировать ресурсы в почти исходную форму и восстанавливать их после внесения некоторых изменений.
  - Разборка файла Android apk
    - `apktool d <apk file>`
  - Восстановление декодированных ресурсов обратно в двоичный APK/JAR с подписью сертификата
    - `apktool b <modified folder>`
    - `keytool -genkey -v -keystore keys/test.keystore -alias Test -keyalg RSA -keysize 1024 -sigalg SHA1withRSA -validity 10000`
    - `jarsigner -keystore keys/test.keystore dist/test.apk -sigalg SHA1withRSA -digestalg SHA1 Test`

- Bytecode Viewer - Bytecode Viewer - это расширенный облегченный просмотрщик байт-кода Java, он полностью написан на Java и имеет открытый исходный код.
- Jadx — декомпилятор Dex в Java: инструменты командной строки и графического интерфейса для создания исходного кода Java из файлов Android Dex и Apk.
- APK Studio — кроссплатформенная IDE на базе Qt с открытым исходным кодом для обратного проектирования пакетов приложений Android.
- Oat2dex — инструмент для преобразования файлов .oat в файлы .dex.
  - Деоптимизировать классы загрузки (выходные данные будут находиться в папках «odex» и «dex»)
    - `java -jar oat2dex.jar boot <boot.oat file>`
  - Деоптимизировать приложение
    - `java -jar oat2dex.jar <app.odex> <boot-class-folder output from above>`
  - Получить одекс из овса
    - `java -jar oat2dex.jar odex <oat file>`
  - Получить odex smali (с оптимизированным кодом операции) из oat/odex
    - `java -jar oat2dex.jar smali <oat/odex file>`
- Spotbugs - SpotBugs - преемник FindBugs. Инструмент статического анализа для поиска ошибок в коде Java.
- Qark — этот инструмент предназначен для поиска уязвимостей безопасности приложений Android, как в исходном коде, так и в упакованных APK-файлах.
- SUPER - SUPER - это приложение командной строки, которое можно использовать в Windows, MacOS X и Linux, которое анализирует файлы

.apk в поисках уязвимостей. Оно делает это путем распаковки APK и применения ряда правил для обнаружения этих уязвимостей.

- AndroBugs - AndroBugs Framework - эффективный сканер уязвимостей Android, который помогает разработчикам или хакерам находить потенциальные уязвимости безопасности в приложениях Android. Не требует установки на Windows.
- Simplify — инструмент для деобфускации пакета Android в Classes.dex, который можно использовать для извлечения содержимого файла dex с помощью Dex2jar и JD-GUI.
  - `simplify.jar -i "input smali files or folder" -o <output dex file>`
- ClassNameDeobfuscator — простой скрипт для анализа файлов .smali, созданных apktool, и извлечения строк аннотаций .source.
- Android backup extractor - Утилита для извлечения и повторной упаковки резервных копий Android, созданных с помощью adb backup (ICS+). Во многом основана на BackupManagerService.java из AOSP. Совет!! Команда "adb backup" также может использоваться для извлечения пакета приложения с помощью следующей команды:
  - `adb backup <package name>`
  - `dd if=backup.ab bs=1 skip=24 | python -c "import zlib,sys;sys.stdout.write(zlib.decompress(sys.stdin.read()))" > backup.tar`
- GDA (GJoy Dex Analysizer) - GDA, новый декомпилятор байт-кода Dalvik, реализованный на C++, который обладает преимуществами более быстрого анализа и меньшего потребления памяти и диска, а также более высокой способностью декомпиляции файлов APK, DEX, ODEX, OAT (поддерживает файлы JAR, CLASS и AAR с версии 3.79)

Динамический и динамический анализ

- Cydia Substrate — Cydia Substrate для Android позволяет разработчикам вносить изменения в существующее программное обеспечение с помощью расширений Substrate, которые внедряются в память целевого процесса.
- Xposed Framework — Xposed Framework позволяет изменять аспекты и поведение системы или приложения во время выполнения, без изменения какого-либо пакета приложений Android (APK) или перепрошивки.
- PID Cat — обновление превосходного цветового скрипта logcat Джеффа Шарки, который показывает записи журнала только для процессов из определенного пакета приложений.
- Inspeckage - Inspeckage - это инструмент, разработанный для динамического анализа приложений Android. Применяя хуки к функциям API Android, Inspeckage поможет вам понять, что делает приложение Android во время выполнения.
- Frida — набор инструментов работает по модели клиент-сервер и позволяет внедряться в запущенные процессы не только на Android, но и на iOS, Windows и Mac.
- Diff-GUI — веб-фреймворк для начала работы с доступными модулями, подключающий нативный JavaScript с использованием Frida.
- Fridump - Fridump использует фреймворк Frida для дампа доступных адресов памяти с любой поддерживаемой платформы. Его можно использовать в системах Windows, Linux или Mac OS X для дампа памяти приложения iOS, Android или Windows.
- House — набор инструментов для анализа мобильных приложений во время выполнения с веб-интерфейсом, работающий на базе Frida, предназначен для оценки мобильных приложений путем реализации

динамического подключения и перехвата функций и призван максимально упростить написание скриптов Frida.

- AndBug - AndBug — отладчик, ориентированный на виртуальную машину Dalvik платформы Android, предназначенный для реверс-инженеров и разработчиков.
  - Идентификация процесса приложения с помощью оболочки adb
    - `adb shell ps | grep -i "App keyword"`
  - Доступ к приложению с помощью AndBug для определения загруженных классов
    - `andbug shell -p <process number>`
  - Отслеживание определенного класса
    - `ct <package name>`
  - Отладка с помощью jdb
    - `adb forward tcp:<port> jdwp:<port>`
    - `jdb -attach localhost:<port>`
- Cydia Substrate: Introspy-Android — инструмент Blackbox, помогающий понять, что делает приложение Android во время выполнения, и помочь в выявлении потенциальных проблем безопасности.
- Drozer — Drozer позволяет вам искать уязвимости безопасности в приложениях и устройствах, принимая на себя роль приложения и взаимодействуя с виртуальной машиной Dalvik, конечными точками IPC других приложений и базовой ОС.
  - Начало сеанса
    - `adb forward tcp:31415 tcp:31415`
    - `drozer console connect`
  - Получение информации о пакете
    - `run app.package.list -f <app name>`

- run app.package.info -a <package name>
- Определение поверхности атаки
  - run app.package.attacksurface <package name>
- Эксплуатационная деятельность
  - run app.activity.info -a <package name> -u
  - run app.activity.start --component <package name> <component name>
- Использование поставщика контента
  - run app.provider.info -a <package name>
  - run scanner.provider.finduris -a <package name>
  - run app.provider.query <uri>
  - run app.provider.update <uri> --selection <conditions> <selection arg> <column> <data>
  - run scanner.provider.sqltables -a <package name>
  - run scanner.provider.injection -a <package name>
  - run scanner.provider.traversal -a <package name>
- Использование вещательных приемников
  - run app.broadcast.info -a <package name>
  - run app.broadcast.send --component <package name> <component name> --extra <type> <key> <value>
  - run app.broadcast.sniff --action <action>
- Эксплуатация службы
  - run app.service.info -a <package name>
  - run app.service.start --action <action> --component <package name> <component name>

- `run app.service.send <package name> <component name> --msg <what> <arg1> <arg2> --extra <type> <key> <value> --bundle-as-obj`

Сетевой анализ и тестирование на стороне сервера

- Tcpdump — утилита захвата пакетов из командной строки.
- Wireshark — анализатор пакетов с открытым исходным кодом.
  - Захват пакетов в реальном времени
    - `adb shell "tcpdump -s 0 -w - | nc -l -p 4444"`
    - `adb forward tcp:4444 tcp:4444`
    - `nc localhost 4444 | sudo wireshark -k -S -i –`
- Mallory — инструмент «человек посередине» (MiTM), который используется для мониторинга и управления трафиком на мобильных устройствах и в приложениях.
- Burp Suite — Burp Suite — это интегрированная платформа для проведения тестирования безопасности приложений.
  - Установка доверенного центра сертификации на уровне ОС Android (устройство с правами root/эмулятор) для Android N+ выполняется следующим образом:
    - `openssl x509 -inform PEM -subject_hash -in BurpCA.pem | head -1`
    - `cat BurpCA.pem > 9a5ba580.0`
    - `openssl x509 -inform PEM -text -in BurpCA.pem -out /dev/null >> 9a5ba580.0`
    - `adb root`
    - `abd remount`

    - `adb push 9a5ba580.0 /system/etc/security/cacerts/`
    - `adb shell “chmod 644 /system/etc/security/cacerts/9a5ba580.0”`
    - `adb shell “reboot”`
    - Проверьте Настройки > Безопасность > Доверенные учетные данные > СИСТЕМА, чтобы убедиться, что ваш недавно добавленный ЦС указан в списке.
- Мобильный помощник Burp Suite — мобильный помощник Burp Suite — это инструмент для упрощения тестирования приложений iOS с помощью Burp Suite. Он может изменять общесистемные настройки прокси-сервера устройств iOS, чтобы трафик HTTP(S) можно было легко перенаправить на работающий экземпляр Burp. Он может попытаться обойти закрепление сертификата SSL в выбранных приложениях, что позволяет Burp Suite разрывать их соединения HTTPS и перехватывать, проверять и изменять весь трафик.
- OWASP ZAP - OWASP Zed Attack Proxy Project - это сканер безопасности веб-приложений с открытым исходным кодом. Он предназначен как для новичков в области безопасности приложений, так и для профессиональных тестировщиков на проникновение.
- Proxydroid — глобальное прокси-приложение для системы Android.
- mitmproxy — интерактивный прокси-сервер с поддержкой SSL/TLS и консольным интерфейсом для HTTP/1, HTTP/2 и WebSockets.

Обход обнаружения root и SSL-закрепления

- Magisk — комплекты Magisk предоставляют root-доступ к вашему устройству, возможность изменять разделы, доступные только для чтения, путем установки модулей и скрывать Magisk от обнаружения root-доступа/проверок целостности системы.

- Модуль Xposed: Just Trust Me — модуль Xposed для обхода закрепления SSL-сертификата.
- Модуль Xposed: SSLUnpinning — модуль Android Xposed для обхода проверки SSL-сертификата (закрепление сертификата).
- Модуль Cydia Substrate: Android SSL Trust Killer — инструмент Blackbox для обхода закрепления SSL-сертификатов для большинства приложений, работающих на устройстве.
- Модуль Cydia Substrate: RootCoak Plus — исправление проверки корней на наличие общеизвестных признаков корней.
- Android-ssl-bypass — инструмент отладки Android, который можно использовать для обхода SSL, даже если реализовано закрепление сертификата, а также для других задач отладки. Инструмент работает как интерактивная консоль.
- Apk-mitm — CLI-приложение, которое автоматически подготавливает файлы Android APK для проверки HTTPS.
- Frida CodeShare — проект Frida CodeShare, в котором принимают участие разработчики со всего мира, работающие вместе с одной целью — вывести Frida на новый уровень, используя новые и инновационные способы.
  - Обход обнаружения root-доступа
    - `frida --codeshare dzonerzy/fridantiroot -f YOUR_BINARY`
  - Обход SSL-закрепления
    - `frida --codeshare pcipolloni/universal-android-ssl-pinning-bypass-with-frida -f YOUR_BINARY`

Библиотеки безопасности

- Закрепление открытого ключа — закрепление в Android можно осуществить с помощью специального X509TrustManager.

X509TrustManager должен выполнять обычные проверки X509 в дополнение к настройке закрепления.

- Android Pinning — проект автономной библиотеки для закрепления сертификатов на Android.
- Java AES Crypto — простой класс Android для шифрования и дешифрования строк, призванный избежать классических ошибок, от которых страдает большинство подобных классов.
- Proguard - ProGuard - это бесплатный Java class-сжиматель, оптимизатор, обфускатор и преверификатор. Он обнаруживает и удаляет неиспользуемые классы, поля, методы и атрибуты.
- SQL Cipher — SQLCipher — это расширение SQLite с открытым исходным кодом, которое обеспечивает прозрачное 256-битное AES-шифрование файлов базы данных.
- Secure Preferences — оболочка общих настроек Android, которая шифрует ключи и значения общих настроек.
- Trusted Intents — библиотека для гибкого доверенного взаимодействия между приложениями Android.
- RootBeer — отличная библиотека для проверки root-прав и пример приложения.
- Сквозное шифрование . Capillary — это библиотека, упрощающая отправку сквозных зашифрованных push-сообщений с серверов приложений на базе Java на клиенты Android.

Тестирование на проникновение приложений iOS

Доступ к файловой системе на iDevice

- FileZilla — поддерживает FTP, SFTP и FTPS (FTP через SSL/TLS).

- Cyberduck — свободный браузер FTP, SFTP, WebDAV, S3, Azure и OpenStack Swift для Mac и Windows.
- itunnel — используется для пересылки SSH через USB.
- iProxy — позволяет подключить ноутбук к iPhone для просмотра веб-страниц.
- iFunbox — инструмент управления файлами и приложениями для iPhone, iPad и iPod Touch.

Обратный инжиниринг и статический анализ

- otool — команда otool отображает указанные части объектных файлов или библиотек.
- Clutch — расшифровывает приложение и сохраняет указанный bundleID в двоичном или .ipa-файле.
- Dumpdecrypted - Сбрасывает расшифрованные файлы mach-o из зашифрованных приложений iPhone из памяти на диск. Этот инструмент необходим исследователям безопасности, чтобы иметь возможность заглянуть под капот шифрования.
  - `iPod:~ root# DYLD_INSERT_LIBRARIES=dumpdecrypted.dylib /var/mobile/Applications/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/Scan.app/Scan`
- class-dump — утилита командной строки для изучения информации о времени выполнения Objective-C, хранящейся в файлах Mach-O.
- dsdump — улучшенный дамп классов nm + objc/swift.
- Weak Classdump — скрипт Cycript, который генерирует файл заголовка для класса, переданного в функцию. Наиболее полезен, когда вы не можете classdump или dumpdecrypted, когда двоичные файлы зашифрованы и т. д.

    - `iPod:~ root# cycript -p Skype weak_classdump.cy; cycript -p Skype`
    - `#cy weak_classdump_bundle([NSBundle mainBundle],"/tmp/Skype")`
- Fridpa — автоматизированный скрипт-оболочка для исправления приложений iOS (файлов IPA) и работы на устройствах без джейлбрейка.
- Frida-iOS-Dump — извлечение расшифрованного IPA из взломанного устройства.
- bagbak - Еще один расшифрованный дамп iOS на основе Frida, поддерживает расшифровку расширений приложений и не требует SSH.
- bfinject - bfinject загружает произвольные dylib-файлы в работающие приложения App Store. Он имеет встроенную поддержку для расшифровки приложений App Store и поставляется в комплекте с iSpy и Cycript.
    - Простой тест
        - `bash bfinject -P Reddit -L test`
    - Расшифровать приложения App Store
        - `bash bfinject -P Reddit -L decrypt`
    - Кикрипт
        - `bash bfinject -P Reddit -L cycript`
- HopperApp - Hopper — это инструмент обратного инжиниринга для OS X и Linux, который позволяет вам дизассемблировать, декомпилировать и отлаживать исполняемые файлы 32/64-битных Intel Mac, Linux, Windows и iOS.
- hopperscripts — Hopperscripts можно использовать для исправления имени функции Swift в HopperApp.

- Radare2 — это Unix-подобная среда обратной разработки и инструменты командной строки.
- XReSign - XReSign позволяет вам подписывать или переподписывать незашифрованные ipa-файлы с сертификатом, для которого у вас есть соответствующий закрытый ключ. Проверено для разработчиков, ad-hoc и корпоративного распространения.

Динамический и динамический анализ

- cycript — Cycript позволяет разработчикам исследовать и изменять запущенные приложения на iOS или Mac OS X, используя гибрид синтаксиса Objective-C++ и JavaScript через интерактивную консоль с подсветкой синтаксиса и автодополнением по клавише Tab.
  - Показать видимый в данный момент контроллер представления
    - `cy# UIApp.keyWindow.rootViewController.visibleViewController`
  - Показать контроллер представления в верхней части стека навигации
    - `cy# UIApp.keyWindow.rootViewController.topViewController`
  - Получить массив существующих объектов определенного класса
    - `cy# choose(UIViewController)`
  - UI Dump, отсекает множество описаний UIViews
    - `cy# [[UIApp keyWindow] _autolayoutTrace].toString()`
  - Пропустите UIViews и nextResponders, чтобы получить ViewControllers напрямую
    - `cy# [[[UIApp keyWindow] rootViewController] _printHierarchy].toString()`
  - Метод списка во время выполнения

- cy# classname.messages или cy# function printMethods(className, isa) { var count = new new Type("I"); var classObj = (isa != undefined) ? objc_getClass(className)->isa : objc_getClass(className); var methods = class_copyMethodList(classObj, count); var methodsArray = []; for(var i = 0; i < *count; i++) { var method = methods[i]; methodsArray.push({selector:method_getName(method), implementation:method_getImplementation(method)}); } free(methods); return methodsArray; }

ПРОЧИТАЙТЕ МЕНЯ

- cy# a=#0x15d0db80
- cy# *a или
- cy# function tryPrintIvars(a){ var x={}; for(i in *a){ try{ x[i] = (*a)[i]; } catch(e){} } return x; }
- cy# a=#0x15d0db80
- cy# tryPrintIvars(a)

- Манипулирование через собственность
  - cy# [a pinCode]
  - cy# [a setPinCode: @"1234"] или cy# a.setPinCode= @"1234"
- Метод Swizzling для метода Instance
  - cy# [a isValidPin]
  - cy# <classname>.prototype.isValidPin = function(){return 1;}
- Метод Swizzling для метода класса
  - cy# [Pin isValidPin]

    - cy# `Pin.contructor.prototype.['isValidPin'] = function() {return 1;}`

- iNalyzer - AppSec Labs iNalyzer — это фреймворк для манипулирования приложениями iOS, изменения параметров и методов.
- Grapefruit — инструменты выполнения приложений для iOS, ранее Passionfruit.
- Introspy-iOS — инструмент Blackbox, помогающий понять, что делает приложение iOS во время выполнения, и помочь в выявлении потенциальных проблем безопасности.
- Apple configurator 2 — утилита, которую можно использовать для просмотра системного журнала на iDevice.
- keychaindumper — инструмент для проверки того, какие элементы связки ключей доступны злоумышленнику после взлома устройства iOS.
- BinaryCookieReader — инструмент для извлечения всех файлов cookie из двоичного файла Cookies.binarycookies.

Сетевой анализ и тестирование на стороне сервера

- Mallory — инструмент «человек посередине» (MiTM), который используется для мониторинга и управления трафиком на мобильных устройствах и в приложениях.
- Burp Suite — Burp Suite — это интегрированная платформа для проведения тестирования безопасности приложений.
- OWASP ZAP - OWASP Zed Attack Proxy Project - это сканер безопасности веб-приложений с открытым исходным кодом. Он предназначен как для новичков в области безопасности приложений, так и для профессиональных тестировщиков на проникновение.

- Charles Proxy — HTTP-прокси / HTTP-монитор / обратный прокси-сервер, который позволяет разработчику просматривать весь трафик HTTP и SSL / HTTPS между его компьютером и Интернетом.

Обход обнаружения root и SSL-закрепления

- SSL Kill Switch 2 — инструмент Blackbox для отключения проверки SSL-сертификатов, включая закрепление сертификатов, в приложениях iOS и OS X.
- iOS TrustMe — отключение проверки доверия сертификатов на устройствах iOS.
- tsProtector — еще один инструмент для обхода обнаружения джейлбрейка.
- JailProtect — помимо обхода обнаружения джейлбрейка, он также позволяет легко подделать версию прошивки iOS.
- Shadow — это твик для обхода обнаружения джейлбрейка, который обходит основные методы обнаружения, используемые многими приложениями App Store.
- Frida CodeShare — проект Frida CodeShare, в котором принимают участие разработчики со всего мира, работающие вместе с одной целью — вывести Frida на новый уровень, используя новые и инновационные способы.
  - Обход SSL-закрепления
    - `frida --codeshare lichao890427/ios-ssl-bypass -f YOUR_BINARY`
    - `frida --codeshare dki/ios10-ssl-bypass -f YOUR_BINARY`

Библиотеки безопасности

- PublicKey Pinning — iOS pinning выполняется через NSURLConnectionDelegate. Делегат должен реализовать connection:canAuthenticateAgainstProtectionSpace: и connection:didReceiveAuthenticationChallenge:. В connection:didReceiveAuthenticationChallenge: делегат должен вызвать SecTrustEvaluate для выполнения обычных проверок X509.
- Swiftshield — SwiftShield — это инструмент, который генерирует необратимые зашифрованные имена для объектов вашего проекта iOS (включая модули и раскадровки), чтобы защитить ваше приложение от инструментов, которые выполняют обратную разработку приложений iOS, таких как class-dump и Cycript.
- IOSSecuritySuite - iOS Security Suite - это передовая и простая в использовании библиотека безопасности платформы и защиты от несанкционированного доступа, написанная на чистом Swift! Если вы разрабатываете для iOS и хотите защитить свое приложение в соответствии со стандартом OWASP MASVS, глава v8, то эта библиотека может сэкономить вам много времени.
- OWASP iMAS — iMAS — это совместный исследовательский проект корпорации MITRE, ориентированный на элементы управления безопасностью iOS с открытым исходным кодом.

Лаборатория тестирования на проникновение мобильных устройств

- WaTF Bank - What-a-Terrible-Failure Мобильное банковское приложение (WaTF-Bank), написанное на Java, Swift 4, Objective-C и Python (фреймворк Flask) в качестве внутреннего сервера, предназначено для имитации «реального» мобильного банковского приложения с

поддержкой веб-сервисов, которое содержит более 30 уязвимостей на основе рейтинга OWASP Mobile Top 10 Risks.

- InsecureBankv2 - WЭто уязвимое приложение Android называется "InsecureBankv2" и создано для энтузиастов безопасности и разработчиков, чтобы они могли изучить уязвимости Android, протестировав это уязвимое приложение. Его компонент внутреннего сервера написан на Python.
- DVIA-v2 - Damn Vulnerable iOS App (DVIA) - это приложение iOS, которое чертовски уязвимо. Его главная цель - предоставить платформу энтузиастам/профессионалам мобильной безопасности или студентам для проверки их навыков тестирования на проникновение iOS в юридической среде.
- DIVA Android - DIVA (чертовски небезопасное и уязвимое приложение) — это приложение, намеренно созданное небезопасным. Цель приложения — научить разработчиков/специалистов по контролю качества/безопасности недостаткам, которые обычно присутствуют в приложениях из-за некачественных или небезопасных методов кодирования.
- DVHMA - Damn Vulnerable Hybrid Mobile App (DVHMA) - это гибридное мобильное приложение (для Android), которое намеренно содержит уязвимости. Его цель - дать возможность профессионалам в области безопасности легально тестировать свои инструменты и методы, помочь разработчикам лучше понять распространенные подводные камни при разработке гибридных мобильных приложений безопасно.
- MSTG Hacking Playground - Это коллекция мобильных приложений iOS и Android, которые намеренно созданы небезопасными. Эти