

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Сигурност на мобилни приложения

Ръчно тестване на мобилни приложения, оценено спрямо OWASP Mobile Application Security Verification Standard: какво издава двоичният файл, какво приложението оставя на устройството, как се държи под инструментация и дали сървърът зад него се доверява на клиента.

ПОДХОДЯЩО ЗА	Потребителски и корпоративни приложения; преглед преди пускане и преди сертификация; финансови и здравни приложения с регулирани данни
ПОЛУЧАВАТЕ	Констатации, съотнесени към MASVS, доказателства от изпълнението, приоритизирани корекции, писмо за повторен тест
ОБХВАЩА	iOS, Android, OWASP MASVS

Клиентът е в ръцете на нападателя, не във вашите

Всяка друга цел е ваша. Мобилното приложение го раздавате: пакетът стига до всеки, който има достъп до магазина, и от този момент двоичният файл, локалното хранилище и изпълнението са на нападателя, за да ги разглобява на спокойствие. Започваме оттам, откъдето започва и той — разопаковаме публикувания артефакт и го четем — защото вграденото в него не може да бъде отменено с промяна на сървъра. При един ангажимент това беше достатъчно, за да се възстановят идентификационни данни, даващи активна, удостоверена сесия към вътрешен API за данни; цялата верига е публикувана.

Втората половина от работата е частта, до която скенерите никога не стигат: закачане към работещото приложение, за да се види срещу какво защитите му наистина устояват. Откриването на root и jailbreak, фиксирането на сертификати (certificate pinning) и защитата от подправяне са контроли, които очакваме да можем да преодолеем; въпросът, на който отговаряме, е какво пази всяка от тях и какво остава, когато я няма. Тестваме приложението и API, с който то общува, като една система, защото контрол от страна на клиента е контрол само ако сървърът не приема думата на клиента за чиста монета.

Какво тестваме

- Публикуваният двоичен файл: тайни, ключове, крайни точки и логика, възстановени чрез обратно инженерство
- Данни в покой: локални бази, използване на keychain и keystore, кешове, резервни копия и журнали
- Криптография и извеждане на ключове, включително ключове, извличими от самото устройство
- Транспорт: валидиране на TLS, фиксиране на сертификати (certificate pinning) и конфигурацията, която го изключва
- Платформена повърхност: deep links, IPC, експортирани компоненти, WebView и вградени локални сървъри
- Устойчивост: откриване на root и jailbreak, защита от дебъгване и подправяне, закачане по време на изпълнение
- Удостоверяване, управление на сесиите и биометрично заключване
- API на сървъра, с който приложението общува, тестван като част от същата система

Как протича

- Обхват и компилации — Платформите, артефактите на компилациите, тестовите акаунти и достъпът до устройства или емулатори се договарят предварително.

- Статичен анализ — Разопаковаме и подлагаме на обратно инженерство публикувания пакет: тайните, крайните точки, ключовия материал и логиката, които издава.
- Динамичен анализ и изпълнение — Инструментирано тестване на устройство — закачане, прихващане, проверка на хранилището и заобикаляне на контроли — продължено към API зад приложението.
- Доклад и повторен тест — Констатации, съотнесени към контролните групи на MASVS, приоритизирани, след което проверени и потвърдени писмено.

Какво получавате

- Резюме за ръководството — Бизнес рискът, представен ясно за ръководството и управителния съвет.
- Доклад, съотнесен към MASVS — Всяка констатация със степен на критичност, доказателства, стъпки за възпроизвеждане и контролната група по MASVS, към която принадлежи — заедно с възстановените артефакти и прихванатия трафик зад нея.
- Приоритизирани корекции — Конкретни стъпки за отстраняване, съобразени с платформата и рамката, които използвате.
- Писмо за повторен тест — Проверяваме вашите корекции и потвърждаваме писмено закриването им.

Методологии и стандарти, на които се опираме

OWASP MASVS (Mobile Application Security Verification Standard) · OWASP MASTG (Mobile Application Security Testing Guide) · OWASP Mobile Top 10 · OWASP API Security Top 10 · NIST SP 800-163 (проверка на мобилни приложения) · CWE · CVSS и EPSS за контекст на критичността

Старши тестери. Доказателства за всяка констатация. Включен повторен тест. Минимум пет дни тестване. Обхват и примерни доклади — pxlsec.com/bg/services/mobile-application-security.