DOI: https://doi.org/10.5281/zenodo.12195516

MOBIL ILOVALARNING ZAIFLIGINI ANIQLASH USUL VA VOSITALARINING TAHLILI

Nuriddin Akbarovich Jabbarov
Renessans ta'lim universiteti, assistent
nuriddinjabbarov2606@gmail.com

Ma'murjon Ma'rupovich Murodov
Toshkent axborot texnologiyalari universiteti, assistent
mamurmurodov9500@gmail.com

ANNOTATSIYA

Mobil ilovalar zamonaviy dunyoda keng tarqalgan bo'lib, ular foydalanuvchilarga ko'plab qulayliklar yaratadi. Biroq, mobil ilovalardagi zaifliklar kiberxavfsizlik tahdidlarini keltirib chiqarishi mumkin. Ushbu maqolada mobil ilovalar zaifliklarining turlari, ularni aniqlash usullari va foydalaniladigan vositalar haqida umumiy ma'lumot beriladi. Shuningdek, zaifliklarni aniqlash usullari – statik tahlil, dinamik tahlil va penetratsion test – haqida batafsil ma'lumot beriladi. Mobil ilovalar zaifliklarini aniqlashda keng qo'llaniladigan vositalar, jumladan OWASP ZAP, MobSF, Burp Suite va Qark haqida ham so'z yuritiladi. Ushbu ishda mobil operatsion tizim ilovalarining zaifliklarini aniqlash usul va vositalari hamda ularning tahlili keltirilgan.

Kalit so'zlar: *mobil OT, OWASP ZAP, Burp Suite, Metasploit, SonarQube, Checkmarx, Fortify, MobSF, QARK (Quick Android Review Kit), Kali Linux.*

ABSTRACT

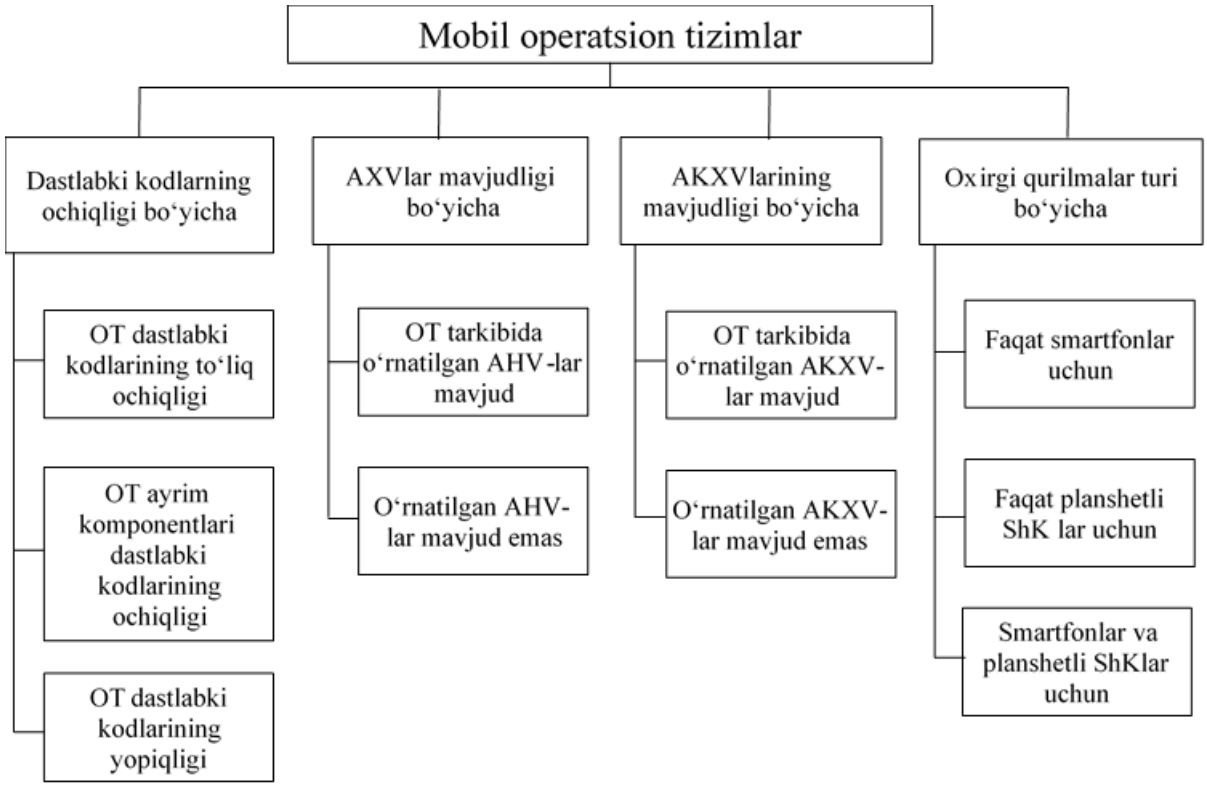
Mobile applications are widespread in the modern world and they provide many conveniences to users. However, vulnerabilities in mobile applications can pose cyber security threats. This article provides an overview of the types of mobile application vulnerabilities, how to detect them, and the tools used. It also provides detailed information on vulnerability detection methods - static analysis, dynamic analysis and penetration testing. Common tools for detecting mobile application vulnerabilities are also covered, including OWASP ZAP, MobSF, Burp Suite, and Qark. In this work, methods and tools for identifying vulnerabilities of mobile operating system applications and their analysis are presented.

Keywords: *mobile OS, OWASP ZAP, Burp Suite, Metasploit, SonarQube, Checkmarx, Fortify, MobSF, QARK (Quick Android Review Kit), Kali Linux.*

KIRISH

Mobil ilovalar zamonaviy texnologiya dunyosida keng tarqalgan va kundalik hayotimizning ajralmas qismiga aylangan. Ular turli xil vazifalarni bajarishda bizga yordam berib, hayotimizni ancha qulay va samarali qiladi. Biroq, bu ilovalar xavfsizlik bilan bog‘liq jiddiy muammolarni ham keltirib chiqarishi mumkin. Mobil ilovalardagi zaifliklar nafaqat foydalanuvchilarning shaxsiy va moliyaviy ma'lumotlarini xavf ostiga qo‘yadi, balki kompaniyalar va tashkilotlarning obro‘siga ham zarar yetkazishi mumkin. Mobil ilovalar zaifliklari ko‘p hollarda dasturiy ta'minotning rivojlanish jarayonidagi kamchiliklar, noto‘g‘ri autentifikatsiya va avtorizatsiya, ma'lumotlarni shifrlashdagi xatolar, hamda yangilanishlarni boshqarishdagi muammolar bilan bog‘liq. Bu zaifliklar tajovuzkorlarga foydalanuvchi ma'lumotlarini o‘g‘irlash, qurilmalarni zararli dasturlar bilan yuqtirish va boshqa zararli faoliyatlarni amalga oshirish imkonini beradi.

Mobil operatsion tizimlarni quyidagi alomatlari bo‘yicha tasniflash mumkin (1-rasm):



1-rasm. Mobil operatsion tizimlarning tasnifi

Zaifliklarni aniqlash va bartaraf etish jarayonida turli usul va vositalardan foydalaniladi. Statik tahlil, dinamik tahlil va penetratsion test kabi usullar yordamida ilovalardagi xavfsizlik teshiklari aniqlanadi va bartaraf etiladi. Ushbu usullar dasturiy

ta'minot kodini tahlil qilish, ilova xatti-harakatlarini kuzatish va hujumlar simulyatsiyasini o‘z ichiga oladi.

Mobil ilovalar zaifliklarini aniqlash uchun turli vositalar, jumladan OWASP ZAP, MobSF, Burp Suite va Qark keng qo‘llaniladi. Bu vositalar dasturchilarga va xavfsizlik mutaxassislariga zaifliklarni tez va samarali aniqlash va tuzatishga yordam beradi.

MUHOKAMA VA NATIJALAR

Mobil ilovalarining xavfsizligi zaifliklarini aniqlash uchun bir qancha usullar mavjud. Bu usullar ilovalarni hujumlar va zararli faoliyatlarga qarshi himoya qilishda juda muhimdir. Quyida mobil ilovalarni tekshirishning asosiy usullari keltirilgan:

Statik kod tahlili (Static Code Analysis). Statik kod tahlili dasturiy ta’minotning kodini ishlatilmasdan oldin tahlil qilishni o‘z ichiga oladi. Bu tahlil usuli ilovadagi potentsial xavfsizlik zaifliklarini, masalan, buffer overflows, XSS (Cross-site Scripting) va SQL injection kabi zaifliklarni aniqlashga qaratilgan. Bu usul shuningdek, kodning sifatini oshirish va dasturlash standartlariga rioya qilinishini ta’minlash uchun ham foydalaniladi. Kodni tahlil qilish uchun turli xil vositalar mavjud, jumladan SonarQube, Fortify va Checkmarx kabi dasturlar keng tarqalgan.

Dinamik tahlil (Dynamic Analysis). Dinamik tahlil ilovani ishga tushirish va uni turli scenariylar ostida sinab ko‘rish orqali amalga oshiriladi. Bu jarayonda ilovaning real vaqt rejimida qanday ishlashini kuzatish mumkin, bu esa runtime xatosi, xotira sizib chiqishi va boshqa runtime muammolarini aniqlashga imkon beradi. Bu usul, shuningdek, tarmoq faoliyati va qurilma resurslariga kirish kabi jihatlarni ham kuzatadi. Frida va Charles Proxy kabi vositalar dinamik tahlil uchun keng qo‘llaniladi.

Penetratsion sinov (Penetration Testing). Penetratsion testlar xavfsizlik tizimini sinovdan o‘tkazish uchun hujumlar yordamida amalga oshiriladi. Bu usul ilovaning xavfsizligini sinash va uning turli hujumlarga qarshi qanchalik bardoshli ekanligini baholash imkonini beradi. Penetratsion sinovlar orqali dastur ichida va tashqarisida bo‘lishi mumkin bo‘lgan xavfsizlik zaifliklari aniqlanadi. OWASP ZAP, Burp Suite va Metasploit kabi vositalar bu maqsadlar uchun ishlatiladi.

Foydalanuvchi ro‘yxatdan o‘tish protokollari tahlili (User Credential Analysis). Bu usul foydalanuvchi autentifikatsiyasi va kirish boshqaruv protseduralarini tekshiradi. Bu tahlil orqali ilovaning foydalanuvchi ma’lumotlarini qanday himoya qilishini va hujumlarga qarshi qanchalik mustahkam ekanligini baholash mumkin. Masalan, parol kuchini, autentifikatsiya mehanizmlarini va kirish nazoratini tekshirish kiradi.

Konfiguratsiya va muhandislik tahlili (Configuration and Engineering Analysis). Bu usul ilova va uning muhitining konfiguratsiyasini tekshirishni o‘z ichiga oladi. Bu tahlil orqali server sozlamalari, shifrlash usullari va tarmoq xavfsizligi kabi jihatlarni ko‘rib chiqiladi. Bu usul, shuningdek, dasturiy ta’minot arxitekturasini va muhandislik yechimlarini baholashga yordam beradi.

Foydalanuvchi interfeysi xavfsizligi (UI Security Testing). Bu usul foydalanuvchi interfeysi elementlarini (masalan, kirish maydonchalari va tugmalar) tekshirish orqali ilovaning foydalanuvchi ma’lumotlarini qay darajada himoya qilishini baholaydi.

Har bir usul o‘ziga xos yondashuvlarni taklif qiladi va ilovalarni xavfsizroq qilish uchun bir-biri bilan birlashtirilishi mumkin.

1-jadvalda mobil ilovalarni xavfsizlik zaifliklarini aniqlash usullarini tahlili keltirilgan:

Zaifliklarni aniqlash darajasi: Statik kod tahlili vositalari o‘rtacha 70-85% samaradorlik bilan kodda mavjud bo‘lishi mumkin bo‘lgan zaifliklarni aniqlay oladi. Bu ko‘rsatkichlar dasturiy ta’minotning turi va tahlil qilinayotgan kodning murakkabligiga qarab o‘zgarishi mumkin.

Run-time xatolarni aniqlash. Dinamik tahlil ilovalarni ishlatish jarayonida 50-70% samaradorlik bilan run-time xatolarni va xotira sizib chiqish kabi muammolarni aniqlaydi.

Umumiy aniqlangan zaifliklar: Penetratsion sinovlar, odatda, ilovalarning 90% ga yaqinida kamida bitta xavfsizlik zaifligini aniqlay oladi. Bu yuqori foiz, sinovning chuqur va kompleks tabiati sababli.

Autentifikatsiya va kirish nazorati zaifliklari. Bu tahlil, odatda, ilovalarning 30-50% ida autentifikatsiya yoki kirish nazorati bilan bog‘liq zaifliklarni aniqlaydi.

Konfiguratsiya xatolari. Ilovalarning taxminan 70%da konfiguratsiya yoki muhandislik xatolari aniqlanadi, bu esa umumiy xavfsizlik holatiga salbiy ta’sir qiladi.

Foydalanuvchi ma’lumotlari himoyasizligi. Foydalanuvchi interfeysi xavfsizligi bo‘yicha tahlillar, odatda, ilovalarning 40-60%ida foydalanuvchi ma’lumotlarini himoya qilishda kamchiliklar borligini ko‘rsatadi.

Endi mobil ilovalarning xavfsizlik zaifliklarini aniqlash uchun ishlatiladigan vositalarni kengroq tushunish uchun ularning har birining afzalliklari va qo‘llanilishini tahlil qilamiz.

1. Statik kod tahlili vositalari (SAST)

SonarQube. Bu yirik loyihalarni tahlil qilish uchun mo‘ljallangan keng ko‘lamli vosita bo‘lib, xavfsizlik zaifliklarini, kodning sifati va ishlashini yaxshilash bo‘yicha tavsiyalar beradi.

1-jadval
Mobil ilovalarni xavfsizlik zaifliklarini aniqlash usullari tahlili

Usul nomi	Ta’rif	Aniqlangan zaifliklar foizda	Aniqlanadigan zaiflik turlari	Foydalaniladigan vositalar	Afzalliklari
Statik kod tahlili	Dasturiy ta’minot kodini ishlatishdan oldin tahlil qilish	70-85%	Kod zaifliklari (masalan, XSS, SQL injection)	SonarQube, Fortify, Checkmarx	Tez va ommabop, kodni ishga tushirishdan oldin tahlil qiladi
Dinamik tahlil	Ilovani real vaqt rejimida ishlatish orqali xavfsizlik zaifliklarini aniqlash	50-70%	Run-time xatolari, xotira sizib chiqishlari	Frida, Charles Proxy	Real vaqt rejimida ishlaydigan ilovalar uchun ideal
Penetratsion sinov	Maxsus tayyorlangan hujumlar yordamida ilovaning xavfsizlik tizimini sinovdan o‘tkazish	~90%	Turli xil xavfsizlik zaifliklari	OWASP ZAP, Burp Suite, Metasploit	Chuqur va kompleks, real dunyo hujumlarini simulyatsiya qiladi
Foydalanuvchi ro‘yxatdan o‘tish protokollari tahlili	Foydalanuvchi autentifikatsiyasi va kirish boshqaruv protseduralarini tekshirish	30-50%	Autentifikatsiya va kirish nazorati zaifliklari	-	Foydalanuvchi ma’lumotlarining xavfsizligini ta’minlaydi
Konfiguratsiya va muhandislik tahlili	Ilova va uning muhitining konfiguratsiyasini va muhandislik yechimlarini tekshirish	~70%	Konfiguratsiya va muhandislik xatolari	-	Tizim va server sozlamalarini optimallashtirish imkoniyati
Foydalanuvchi interfeysi xavfsizligi	Ilovaning foydalanuvchi interfeysi elementlarini tekshirish	40-60%	Foydalanuvchi ma’lumotlari himoyasizligi	-	Foydalanuvchi interfeysi orqali ma’lumot oqishining oldini oladi

Ishlatilishi. SonarQube, manba kodining xavfsizlik, sifat va texnik qarzdorlik (technical debt) jihatlarini tahlil qiladi. Misol uchun, Android ilovasining Java kodida xavfsiz bo‘lmagan API chaqiruvlarini yoki SQL injektsiyasiga yo‘l qo‘yadigan kod qismlarini aniqlaydi.

Afzalliklari. SonarQube turli tillar uchun qo‘llab-quvvatlash beradi va jamoatchilik tomonidan yaxshi qabul qilingan ko‘plab plaginlarni taklif etadi.

Checkmarx. Checkmarx, kodni tahlil qilish jarayonini avtomatlashtirishga qaratilgan, katta korporativ miqyosda ishlatiladigan vositadir. Ushbu platforma tez-tez yangilanib turadigan zaifliklar bazasi bilan integratsiyalangan.

Ishlatilishi. Checkmarx, kod bazasi bo‘ylab murakkab xavfsizlik muammolarini topish uchun ishlatiladi, masalan, qayta yo‘naltirish hujumlari (redirect attacks) yoki fayl yuklash bo‘yicha zaifliklar.

Afzalliklari. U integratsiyalangan rivojlanish muhiti (IDE) bilan yaxshi integratsiyalanadi va dasturchilarga kodni yozish jarayonida xavfsizlikni yaxshilash bo‘yicha bevosita maslahatlar beradi.

Fortify. HP tomonidan ishlab chiqilgan bu vosita, keng qamrovli xavfsizlik tahlilini taqdim etadi va ko‘plab dasturlash tillarini qo‘llab-quvvatlaydi.

Ishlatilishi. Fortify, korporativ darajadagi ilovalar uchun ishlatiladi, bu ilovalar ko‘pincha murakkab va ko‘p qatlamli arxitekturaga ega. Misol uchun, iOS ilovasining Objective-C yoki Swift kodini tahlil qilib, xavfsizlik bo‘yicha tavsiyalar beradi.

Afzalliklari. U katta hajmdagi kod bazalarini samarali tahlil qilish qobiliyatiga ega va turli xil dasturlash tillarini qo‘llab-quvvatlaydi.

2. Dinamik kod tahlili vositalari (DAST)

OWASP ZAP. Bu ochiq manba kodli, ko‘p funktsiyali DAST vositasi bo‘lib, veb-ilovalar uchun xavfsizlik tahlilini osonlashtiradi va ko‘p qirrali hujum senariylarini sinab ko‘rish imkoniyatini beradi.

Ishlatilishi. ZAP asosan veb-ilovalar uchun mo‘ljallangan bo‘lsa-da, u mobil API’lar uchun ham testlar o‘tkazishi mumkin. Masalan, REST yoki SOAP interfeyslari orqali mobil ilovalarning backendiga hujum qilish senariylarini tekshirish.

Afzalliklari. Bu vosita bepul va ochiq manba kodli bo‘lib, kengaytirish uchun ko‘plab plaginlarni taqdim etadi.

Burp Suite. Bu eng mashhur penetratsiya testlash vositalaridan biri bo‘lib, foydalanuvchiga trafikni ushlash, so‘rovlar tahrirlash va avtomatlashtirilgan skriptlar yordamida xavfsizlikni tekshirish imkonini beradi.

Ishlatilishi. Burp Suite, HTTP/HTTPS trafikni ushlash va tahlil qilish orqali mobil ilovalarni sinovdan o‘tkazishda foydalaniladi. Misol uchun, ilova server bilan ma’lumot almashinuvini qanday amalga oshirishini kuzatib, potentsial xavfsizlik bo‘shliqlarini aniqlash mumkin.

Afzalliklari. Bu vosita turli xil testlash usullarini qo‘llab-quvvatlaydi va foydalanuvchiga keng qamrovli xavfsizlik tahlilini taqdim etadi.

3. Mobil ilovalar uchun maxsus tahlil vositalari

MobSF (Mobile Security Framework). Android, iOS va Windows platformalarida ishlaydigan ilovalar uchun to‘liq tahlil vositasi. Bu APK, IPA va APPX fayllarini tahlil qiladi va tezkor xavfsizlik tahlilini taqdim etadi.

Ishlatilishi. MobSF, APK, IPA va APPX fayllarni yuklab olib, ularni avtomatik ravishda tahlil qiladi. Misol uchun, Android APK faylini yuklab olib, ilovada ma’lumotlarni oshkor qiluvchi yoki ruxsatsiz foydalanuvchi ma’lumotlariga kirish mumkin bo‘lgan kod qismlarini aniqlaydi.

Afzalliklari. Bu vosita tezkor va aniq tahlil taqdim etadi, shuningdek, turli xil xavfsizlik hisobotlarini yaratadi.

QARK (Quick Android Review Kit). Android ilovalari uchun ishlab chiqilgan, kodni lokal ravishda tahlil qilib, potentsial zaifliklar va xavfsizlik bo‘yicha tavsiyalar beradi.

Ishlatilishi. QARK asosan Android ilovalarini tahlil qilish uchun ishlatiladi, bu yerda u ilova APKsini lokal tarzda tahlil qiladi va dasturchilarga ilovada topilgan muammolar bo‘yicha aniq maslahatlar beradi.

Afzalliklari. Ushbu vosita tezkor va samarali, shuningdek, foydalanuvchi uchun oson tushunarli hisobotlar yaratish imkoniyatiga ega.

4. Penetratsiya testlash vositalari

Metasploit. Bu keng tarqalgan xavfsizlik vositasi bo‘lib, turli operatsion tizimlar va tarmoqlar uchun zaifliklarni sinash imkonini beradi.

Kali Linux. Bu xavfsizlik mutaxassislari uchun mo‘ljallangan operatsion tizim bo‘lib, o‘rnatilgan ko‘plab penetratsiya testlash vositalarini o‘z ichiga oladi.

5. Shaxsiy ma’lumotlarni himoya qilish vositalari

Google’s Data Safety form. Android ilovalari uchun Google Play do‘konida ilova ma’lumotlarini qanday to‘playotgani va ulardan qanday foydalanayotgani haqida ochiq ma’lumot berishni talab qiladi.

Apple’s privacy labels. iOS ilovalari uchun App Store’da ilovalar tomonidan yig‘iladigan ma’lumot turlarini va ularning foydalanishini ko‘rsatuvchi yorliqlar taqdim etiladi.

2-jadvalda mobil ilovalar zaifliklarini aniqlash vositalarining solishtirma tahlili keltirilgan.

2-jadval

Mobil ilovalar zaifliklarini aniqlash vositalarining solishtirma tahlili

Vosita	Platformalar	Qo‘llab-quvvatlanadigan kod turlari	Narxi	Integratsiya	Xavfsizlikni aniqlash samaradorligi
SonarQube	Hamma	Java, C#, Python, PHP, JS	Bepul, to‘lovli rejalar	Jenkins, Azure	85%
Checkmarx	Hamma	Java, C#, Python, Swift, JS, Scala	Yuqori	GitHub, GitLab, Bitbucket	90%
Fortify	Hamma	Java, C#, VB.NET, JS, Python, PHP	Yuqori	Jenkins, Azure DevOps, JIRA	88%
OWASP ZAP	Veb va mobil API	Veb kodlari va APIlar	Bepul	CLI, API	70%
Burp Suite	Veb va mobil API	HTTP/HTTPS trafik	To‘lovli	CLI	75%
MobSF	Android, iOS, Windows	APK, IPA, APPX	Bepul	Server	80%
QARK	Android	Java, Kotlin	Bepul	CLI, GUI	70%

XULOSA

Mobil ilovalarning zaifliklarini aniqlash uchun turli usullar va vositalardan foydalanish zarur. Har bir usul va vosita o‘ziga xos afzalliklarga ega bo‘lib, ularning kombinatsiyasi ilovalarning xavfsizligini yanada mustahkamlashga yordam beradi. Ilovalar xavfsizligini ta’minlash, foydalanuvchilarning ma’lumotlarini himoya qilish va hujumlardan himoyalanish uchun muntazam ravishda zaiflik tahlilini o‘tkazish lozim. Bu jarayonni yaxshi tashkil etish orqali mobil ilovalarning xavfsizligi ta’minlanadi va foydalanuvchilar ishonchini oshirishga xizmat qiladi.

Mobil ilovalar xavfsizligini ta’minlash uchun zaifliklarni aniqlash usullari va vositalarini to‘g‘ri qo‘llash lozim. Statik, dinamik va qo‘lda tahlil usullarini birgalikda qo‘llash ilovalarning zaifliklarini samarali aniqlashga yordam beradi. Zamonaviy vositalardan foydalanish, xavfsizlik testlarini avtomatlashtirish va mutaxassislarni o‘qitish orqali mobil ilovalarning xavfsizligini ta’minlash mumkin. Bu jarayonni yaxshi tashkil etish orqali foydalanuvchilar ishonchini oshirish va ma’lumotlarning himoyasini ta’minlash mumkin bo‘ladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. OWASP Mobile Security Testing Guide (MSTG). OWASP Foundation. OWASP MSTG.
2. Murphy, J., & Beyer, A. (2018). "Android Security Internals: An In-Depth Guide to Android’s Security Architecture." No Starch Press.
3. Enck, W., Ongtang, M., & McDaniel, P. (2009). "On lightweight mobile phone application certification." Proceedings of the 16th ACM conference on Computer and communications security.
4. Grace, M. C., Zhou, Y., Wang, Z., & Jiang, X. (2012). "Systematic detection of capability leaks in stock Android smartphones." Proceedings of the 19th Network and Distributed System Security Symposium.
5. MobSF (Mobile Security Framework). MobSF.
6. Burp Suite. PortSwigger. Burp Suite.
7. OWASP. (2023). "OWASP Mobile Top Ten." OWASP Mobile Top Ten CWE (Common Weakness Enumeration). "CWE List." CWE List.
8. Veracode. (2023). "State of Software Security (SoSS) Report." Veracode SoSS Report.
9. Google Android Security. "Android Security & Privacy Year in Review." Google Android Security.