HOZIRGI KUNDA MOBIL ILOVALARDAGI MAVJUD ZAIFLIKLARNI ANIQLASH USUL VA VOSITALARNI TAHLIL QILISH

Jabbarov Nuriddin
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
nuriddinjabbarov2606@gmail.com

Annotatsiya.

Mamlakatimizda sanoatning barcha tarmoqlari raqamli tizimga o‘tishi bilan ularning xavfsizligi, ma’lumotlar xavfsizligi va undan to‘g‘ri foydalanish dolzarb masalalardan biri bo‘ladi. Xususan, bugun biz hayotimizni mobil telefonlar, aqlli soatlar, gadjetlar kabi aqlli qurilmalarsiz tasavvur qila olmaymiz. Afsuski, ulardan foydalanishda ma’lumotlar xavfsizligi kerakli darajada emas. Bu talabni bajarish, axborot almashinuvini takomillashtirish, ularni saqlash vaqtida xavfsizlik choralarini ko‘rish zarur. Mobil ilovalar ilg‘or apparat va dasturiy ta’minotdan, shuningdek, platforma orqali taqdim etilgan mahalliy va joylashtirilgan ma’lumotlardan foydalanib, iste’molchilarga innovatsiya va qulaylik keltirganligi uchun undagi xavfsizlik masalasi juda ham hisoblanadi. Ushbu tadqiqot ishida mavjud xavfsizlik tahdidlari, mobil ilovalarning zaifligini aniqlash usul va vositalarining tahlili kabi masalalar ko‘rib o‘tilgan.

Kalit so'zlar: mobil ilovalar zaifligi, static kod tahlili, dinamik tahlil, penetratsion sinov, SonarQube, Checkmarx, Fortify, OWASP ZAP, BurpSuite, MobSF, QARK.

Аннотация.

Как только все отрасли промышленности нашей страны перейдут на цифровую систему, их безопасность, сохранность данных и их правильное использование станут одним из актуальных вопросов. В частности, сегодня мы не можем представить свою жизнь без умных устройств, таких как мобильные телефоны, умные часы, гаджеты. К сожалению, при их использовании безопасность данных не так хороша, как хотелось бы. Необходимо выполнить это требование, улучшить обмен информацией, принять меры безопасности при ее хранении. Поскольку мобильные приложения приносят потребителям инновации и удобство за счет использования передового аппаратного и программного обеспечения, а также локальных и размещенных данных, предоставляемых через платформу, безопасность является серьезной проблемой. В данной исследовательской работе рассматриваются такие вопросы, как существующие угрозы безопасности, анализ методов и инструментов обнаружения уязвимостей мобильных приложений.

Ключевые слова: уязвимости мобильных приложений, статический анализ кода, динамический анализ, тестирование на проникновение, SonarQube, Checkmarx, Fortify, OWASP ZAP, BurpSuite, MobSF, QARK.

Annotation.

As soon as all branches of industry in our country go to the digital system, their security, data security and its correct use will become one of the urgent issues. In particular, today we cannot imagine our life without smart devices such as mobile phones, smart watches, gadgets. Unfortunately, when using them, data security is not as good as it should be. It is necessary to fulfill this requirement, improve the exchange of information, and take security measures during their storage. As mobile applications bring innovation and convenience to consumers by leveraging advanced hardware and software, as well as local and hosted data provided through the platform, security is a major concern. This research paper deals with issues such as existing security threats, analysis of mobile application vulnerability detection methods and tools.

Keywords: mobile application vulnerability, static code analysis, dynamic analysis, penetration testing, SonarQube, Checkmarx, Fortify, OWASP ZAP, BurpSuite, MobSF, QARK.

Kirish

Mobil operatsion tizimlar shaxsiy kompyuter operatsion tizimining funksionalligini mobil va qo‘lda ishlaydigan qurilmalar: sensorli ekran, uyali, Bluetooth, Wi-Fi, GPS-navigatsiya, kamera, videokamera, nutqni aniqlash, ovoz yozish moslamasi, musiqa pleyeri, NFC va infraqizil masofadan boshqarish moslamalari bilan birlashtiradi. Portativ mobil aloqa vositalari (masalan,

smartfonlar) ikkita operatsion tizimni o‘z ichiga oladi. Foydalanuvchilarning o‘zaro ta’sirlashishining asosiy dasturiy ta’minot platformasi radiotexnikaga xizmat ko‘rsatuvchi ikkinchi darajali, real vaqtda real vaqtda ishlaydigan operatsion tizim bilan to‘ldiriladi. Tadqiqotlar shuni ko‘rsatdiki, bunday past darajadagi operatsion tizimlar mobil qurilmani boshqarishni o‘z zimmalariga olishlari mumkin bo‘lgan zararli baza stantsiyalariga nisbatan zaifdir [4].

Hozirda mavjud mobil operatsion tizimlar foydalanuvchilarga nafaqat mobil telefonlar uchun odatiy bo‘lgan SMS-xabarlarni jo‘natish va telefon chaqiruvlarini bajarish kabi harakatlarni, balki ma’lumotlarni saqlash, tahrirlash va almashishi bo‘yicha keng imkoniyatlarni taqdim etadi. Ba’zi mobil operatsion tizimlar ma’lumotlarni shifrlab saqlash, hamda mobil qurilmadagi ma’lumotlarni masofadan boshqarish bo‘yicha qo‘shimcha imkoniyatlarga ega.

Mavjud zaifliklarni aniqlash usullarini tahlil qilish

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:

A.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.

B. 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.

C. 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.

D. 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.

E. 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.

F. 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-jadval

Mobil ilovalarning zaifligini 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

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.

Mobil ilovalarning xavfsizlik zaifliklarini aniqlash vositalari tahlili

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

A. 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.

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.

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.

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

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.

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.

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

B. 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.

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.

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.

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.

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

C. 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.

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 rejalari mavjud	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%

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.

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.

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.

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

D. 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.

E. 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.

Kelajakdagi ishlar

Bugungi korxonalar o‘z ilovalarini potentsial kiberhujumlar va ma’lumotlar sizib chiqishidan himoya qilish uchun mustahkam mobil ilovalar xavfsizligini sinovdan o‘tkazish vositalariga muhtoj. Biznesga mobil ilovalar xavfsizligini yaxshilashga yordam beradigan eng yaxshi mobil ilovalar xavfsizligini baholash vositalaridan ba’zilari:

- QARK;
- Ma’lumotlar teoremasi;
- App-Ray;
- Belgilash belgisi;
- NowSecure;
- Appknox;
- Talab bo‘yicha mustahkamlash;

- HCL AppScan;
- AppSweep.

Xulosa

Mazkur tadqiqot ishida mobil operatsion tizimlardagi xavfsizlik muammolarini o‘rganish hamda mobil ilovalardagi zaifliklarni aniqlash usul va vositalari tahlili amalga oshirildi. Va tadqiqot ishi doirasida quyidagilarga erishildi: mobil qurilmalardagi xavfsizlik tahdidlari va ularning ta’siri ko‘rib o‘tildi, mobil ilovalardagi zaifliklar va ularning xavfsizligini baholash jarayoni amalga oshirildi, mobil ilovalar zaifligini aniqlash usul va vositalari qiyosiy tahlil qilindi.

Olingan natijalar asosida esa mobil ilovalar xavfsizligi haqida bilimlarimiz kengaytirildi. Bugungi kunda korxonalar o‘z ilovalarini potensial kiberhujumlar va ma’lumotlar sizib chiqishidan himoya qilish uchun mustahkam mobil ilovalar xavfsizligini sinovdan o‘tkazish vositalariga muhtojdir. Yuqoridagi natijalar korxonalardagi mavjud kamchiliklarni bartaraf etishga yordam beradi.

Foydalanilgan adabiyotlar

1. G‘aniev S. K. , Karimov M. M. , Tashev K. A. “Axborot xavfsizligi”. “Aloqachi” nashriyoti. Toshkent- «fan va tehnologiyalari»-2016.
2. Barry, Burd Android Application Development All-in-One forDummies® / Barry Burd. Moscow: Mechanical engineering, 2011 .--816 p.].
3. Kiberxavfsizlik asoslari. S.K. Ganiyev, A.A. Ganiyev, Z.T. Xudoyqulov 2020 yil 4 iyul – sonli bayonnoma.

A. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. ―A survey of mobile malware in the wild‖, In Proc. of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), (2011), pp. 3-14.

4. Axelle, ―The Evolution of Mobile Malware‖, Computer Fraud & Security vol. 2014, no. 8, pp. 18–20.
5. L. Qing and C. Greg, ―Mobile Security: A Look Ahead‖, IEEE Computer and Reliability Societies, (2013), pp. 78-81.
6. Gao, and J. Liu, ―Modeling and restraining mobile virus propagation‖, IEEE Transactions on Mobile Computing, vol.12, no.3, (2013), pp. 529-541.
7. Mobile Malware Report http://securelist.com/analysis/kaspersky-security-bulletin/58335/ mobile-malware-evolution-2013/, Last accessed 15 March 2015.
8. Sarvar o’g’li, M. S. (2024). MODEL VIEW PRESENTER (MVP) ARXITEKTURASI. Ta'limning zamonaviy transformatsiyasi, 8(4), 186-191.
9. Norqo‘ziyev, Q., Aynakulov, T., Mahkamov, S., & Sodiqov, D. (2024). IMPLEMENTING MOBILE ROBOT WALKING PATH CONTROL AND TRACKING IN C# WINDOWS FORM APPLICATION. International Journal of scientific and Applied Research, 1(3), 95-99.
10. R. P. Weinmann, All Your Baseband Are Belong To Us, hack.lu, 2010, http://2010.hack.lu/archive/2010/Weinmann-All-Your-Baseband-Are-Belong-To-Us-slides.pdf.