Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління_____
(повна назва)

Кафедра _____Безпеки інформаційних технологій_____
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

Дослідження вразливостей мобільних додатків корпоративної мережі
(тема)

Виконав:
студент __2_ курсу, групи БІКСм-20-1_____

_____Слабов Д.В._____
(прізвище, ініціали)

Спеціальність _____125 Кібербезпека _____
(код і повна назва спеціальності)

Освітня програма «Безпека інформаційних і комунікаційних систем_____
(повна назва освітньої програми)

Керівник ____доцент Федюшин О.І._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____Халімов Г.З._____
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління

Кафедра Безпеки інформаційних технологій

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

Студентові Слабову Даніїлу Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження вразливостей мобільних додатків корпоративної мережі

затверджена наказом по університету від «08» листопада 2021 р. № 1685Ст

2. Термін подання студентом роботи до екзаменаційної комісії 16 грудня 2021 р.
3. Вихідні дані до роботи Дослідження технологій статичних та динамічних аналізаторів програм. Дослідження проблематики тестування програмного забезпечення в сучасних методологіях розробки мобільних додатків. Методологія тестування вразливостей OWASP Mobile TOP 10.

4. Перелік питань, що потрібно опрацювати в роботі: Сценарії та ризики використання мобільних пристроїв у корпоративному середовищі; аналіз загроз безпеки мобільних додатків в корпоративній мережі; розробка мобільного додатку; можливість використання сучасних підходів до аналізу програм в комплексі для підвищення ефективності виявлення вразливостей; тестування мобільного додатку за методологією OWASP Mobile TOP 10; розробка рекомендацій щодо використання інструментів аналізу вразливостей та методів блокування потенційних загроз при розробці мобільних додатків для використання в корпоративних мережах .

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) презентаційний матеріал у вигляді слайдів

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Затвердження плану і завдання кваліфікаційної роботи	08.09.2021	Виконано
2	Аналіз літературних джерел за отриманим завданням	09.09.2021 – 16.10.2021	Виконано
3	Вивчення фундаментальних понять про вразливості мобільних додатків	17.10.2021 – 01.11.2021	Виконано
4	Вивчення сучасних підходів до аналізу вразливостей в мобільних додатках	02.11.2021 - 10.11.2021	Виконано
5	Розробка мобільного додатку	10.11.2021 – 20.11.2021	Виконано
6	Створення вимог, завдань та схем тестування вразливостей в мобільному додатку	20.11.2021 – 07.12.2021	Виконано
7	Розробка рекомендацій щодо використання інструментів аналізу вразливостей та методів блокування потенційних загроз	01.12.2021 – 07.12.2021	Виконано
8	Оформлення пояснювальної записки	06.12.2021 – 10.12.2021	Виконано
9	Здача роботи керівнику	12.12.2021	Виконано
10	Підпис кваліфікаційної роботи у керівника	12.12.2021	Виконано
11	Перевірка та підпис кваліфікаційної роботи у нормоконтролера	13.12.2021	Виконано
12	Проходження перевірки на оригінальність кваліфікаційної роботи	13.12.2021	Виконано
13	Допуск завідувачем кафедри до захисту	13.12.2021	Виконано
14	Захист кваліфікаційної роботи	17.12.2021	Виконано

Дата видачі завдання 08 09 2021 р.

Студент _____
(підпис)

Керівник роботи _____ _____ доцент Федюшин О.І.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 71 сторінки, 25 рисунків, 18 таблиць, 1 додатку, 27 джерел за переліком посилань.

ВРАЗЛИВІСТЬ, МОБІЛЬНИЙ ДОДАТОК, КОРПОРАТИВНА МЕРЕЖА, ТЕСТУВАННЯ, OWASP MOBILE TOP 10, IONIC, ІНСТРУМЕНТ АНАЛІЗУ

Об’єкт дослідження – процес пошуку вразливостей в мобільних додатках корпоративної мережі.

Предмет дослідження – технології та інструменти пошуку вразливостей на етапі розробки мобільного додатку.

Метою даної роботи є дослідження та виявлення вразливостей в мобільних додатках корпоративної мережі за допомогою різних програмних інструментів та стандартизованої методології пошуку вразливостей OWASP Mobile Top 10 та розробка рекомендацій з їх усунення.

В роботі розглянуті основні сценарії та ризики використання мобільних пристроїв в корпоративному середовищі, проаналізовані джерела загроз для мобільних додатків та досліджена стандартизована методологія пошуку вразливостей OWASP Mobile Top 10 на прикладі розробленого мобільного додатку. За результатами дослідження розроблені рекомендації:1) щодо організації та проведення процедури безпечного тестування програмних додатків для мобільних пристроїв; 2) щодо методів захисту від виявлених загроз.

ABSTRACT

Explanatory note includes: 78 pages, 25 pictures, 18 tables, 27 sources, 1 application for references.

VULNERABILITY, MOBILE APP, CORPORATE NETWORK, TESTING, OWASP MOBILE TOP 10, IONIC, ANALYSIS TOOL

The object of research is the process of finding vulnerabilities in mobile applications of the corporate network.

The subject of research is technologies and tools for finding vulnerabilities at the stage of mobile application development.

The aim of this work is to study and identify vulnerabilities in mobile applications of the corporate network using various software tools and standardized methodology for finding vulnerabilities OWASP Mobile Top 10 and develop recommendations for their elimination.

The paper considers the main scenarios and risks of using mobile devices in the corporate environment, analyzes the sources of threats to mobile applications and investigates the standardized methodology for finding vulnerabilities OWASP Mobile Top 10 on the example of the developed mobile application. Based on the results of the study, recommendations were developed: 1) on the organization and conduct of the procedure of safe testing of software applications for mobile devices; 2) on methods of protection against identified threats.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

API – Application Programming Interface

ARP – Address Resolution Protocol

BYOD – Bring Your Own Device

COPE – Corporate-Owned, Personally Enabled

CSS – Cascading Style Sheets

CYOD – Choose Your Own Device

EDGE – Enhanced Data Rates for GSM Evolution)

GPS – Global Positioning System

GSM – Global System for Mobile Communications

HTML – HyperText Markup Language

HTTP – HyperText Transfer Protocol

HTTPS – HTTP Secure

IP – Internet Protocol address

IPC – Inter-Process Communication

JSON – JavaScript Object Notation

LTE – Long Term Evolution

MAC – Media Access Control

MD – Mobile Device

NoSQL – Not Only SQL

OAUTH – Open Authorization

OWASP – Open Web Application Security Project

PAN – Personal Area Network

PWA – Progressive Web App

SDK – software Development Kit

SMS – short message service

SSL – Secure Sockets Layer

SSO – Single Sign-On

TLS – Transport Layer Security

ІБ – інформаційна безпека

ОС – операційна система

ІТ – інформаційні технології

ВСТУП

На сучасному етапі йде активний розвиток мобільних технологій, сучасні вимоги бізнесу такі, що доступ до інформації повинен здійснюватися швидко, надійно та з будь-якої точки світу. Мобільна операційна система має свою специфіку, тому в кожній з них можна виявити велику кількість як нових вразливостей, так і добре відомих.

Програми для мобільних пристроїв можна класифікувати за багатьма критеріями, але в контексті безпеки програм нас цікавлять наступні: за місцем розташування програми та за типом використовуваної технології передачі даних.

За місцем розташування програми:

– SIM-додатки – програма на SIM-карті, написана відповідно до стандарту SIM Application Toolkit (STK);

– Web-додатки – спеціальна версія web-сайту;

– Мобільні додатки – програма, розроблена для певної мобільної ОС з використанням спеціалізованого API, що встановлюється у смартфон.

За типом використовуваної технології взаємодії з сервером:

– Мережні додатки – використовують власний протокол спілкування поверх TCP/IP, наприклад HTTP;

– SMS-додатки – програма на основі SMS (Short Messaging Service). Програма обмінюється із сервером інформацією за допомогою коротких текстових повідомлень;

– USSD-додатки – програма на основі USSD (Unstructured Supplementary Service Data). Сервіс ґрунтується на передачі коротких повідомлень, схожих на SMS, але має ряд відмінностей;

– IVR-додатки — програма, що базується на технології IVR (Interactive Voice Response). Система базується на заздалегідь записаних голосових повідомленнях та тональному наборі.

Саме програми, розроблені для певної мобільної ОС з використанням спеціалізованого API, що встановлюються в смартфон зараз найбільш поширені, тому що повністю використовують можливості мобільного апарату і мають найбільш дружній інтерфейс користувача. Їх ми й розглядаємо у цьому дослідженні.

Під час аналізу захищеності мобільного додатка проводиться оцінка захищеності трьох основних компонентів: серверної частини, клієнтської частини та каналу зв'язку.

Як методи оцінки безпеки клієнтського додатку на практиці найчастіше застосовуються методи динамічного та статичного аналізу.

Динамічний аналіз: налагодження запущеної програми (на емуляторі або пристрої); фазинг; аналіз мережного трафіку; аналіз взаємодії із файловою системою; аналіз пам'яті програми.

Статичний аналіз: аналіз вихідного коду (якщо є); зворотне проектування (Reverse Engineering): дизасемблювання; декомпіляція; аналіз отриманого представлення на наявність слабких ділянок коду.

Цілісний підхід до безпеки необхідно забезпечувати на всіх стадіях проекту від проектування та розробки до розгортання та на всіх рівнях інформаційної системи: у мережі, на сервері та в самому додатку.

Для кожного додатка застосовуються ті чи інші етапи тестування, серед яких: сканування портів, піддоменів та контенту; перевірка контролю доступу; тестування функцій та параметрів; перевірка правильності виконання команд; тестування логіки роботи веб-програми; перевірка серверного оточення.

В рамках даного дослідження пропонується використовувати для виявлення уразливостей методи як статичного, так і динамічного аналізу коду клієнтської частини (мобільного додатку) комбінуючи методи чорної та білої скриньки.

Щоб тестування програми було ефективним, ми застосовуємо систематизований підхід на основі стандартизованої методики OWASP Mobile Top 10.

Виконуючи розгорнуте тестування програми, можна послідовно досліджувати його компоненти та виявити можливі вразливості.

У процесі дослідження буде здійснюватися пошук вразливостей і недоліків, пов'язаних з параметрами компіляції програми, використанням небезпечного API, відсутністю механізмів безпеки. За результатами дослідження будуть розроблені рекомендації щодо ефективності інструментів тестування, а також запропоновані заходи щодо захисту від виявлених уразливостей.

1. СЦЕНАРІЇ ТА РИЗИКИ ВИКОРИСТАННЯ МОБІЛЬНИХ ПРИСТРОЇВ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

За даними Help Net Security (2020)[1], лише 41% компаній мають повний контроль над файлами, якими обмінюються користувачі в різних програмах, а підключені хмарні програми на пристроях користувачів контролюють лише 37% компаній.

30% підприємств взагалі не можуть контролювати навіть корпоративні програми. Тільки 9% здатні виявляти шкідливе програмне забезпечення в корпоративних додатках для обміну повідомленнями. Захист кінцевих точок від шкідливих програм можуть забезпечити лише 42% компаній (Bitglass, 2020)[2]. У зв'язку з цим компанії модернізуються під впливом «мобільної революції» і замислюються про регламенти та безпеку використання мобільного пристрою (MD) у робочих цілях.

1.1 Вплив мобільних пристроїв на бізнес-процеси

Проникнувши в бізнес-середовище, мобільні технології змінили як поведінку співробітників, так і підхід до побудови бізнес-процесів.

Основна перевага, яку дає MD, це мобільність співробітників та можливість їх віддаленої роботи. Таким чином, компанія може оптимізувати витрати за рахунок скорочення орендованих площ, витрат на утримання офісу (електроенергія, канцелярія та ін), зниження фонду оплати праці, при цьому не втрачаючи у продуктивності та зберігаючи якість послуг, що надаються. Крім того, віддалена робота відкриває можливість залучати фахівців з інших країн без їхньої фізичної присутності, що, по-перше, теж економічно вигідно, а подруге, підвищує інтелектуальний капітал організації. Загалом, компанія та її бізнес-процеси стають гнучкими.

У той же час, «мобільна революція» бізнесу має і зворотний бік. Діджиталізація підвищує навантаження на IT-відділи. Вони повинні підтримувати коректну роботу систем у режимі 24x7, а будь-який збій має для компанії критично важливе значення. Також потрібні інвестиції у закупівлю корпоративних мобільних девайсів (Choose Your Own Device, CYOD) та/або у розробку та підтримання стандартів безпеки для моделі BYOD (Bring Your Own Device).

1.2 Вплив мобільних пристроїв на корпоративну культуру

Для співробітників робота з дому зручна тим, що економить час на дорогу до офісу та підвищує їхню продуктивність. MD не прив'язують їх до робочого комп'ютера. У цьому співробітники може бути «на зв'язку» постійно, миттєво обмінюватися файлами, працювати у хмарних сервісах над спільними документами, організовувати онлайн-наради тощо.

1.3 Види ризиків використання мобільних пристроїв у корпоративному середовищі

Використання мобільних пристроїв для робочих процесів неминуче знижує рівень захищеності ділової конфіденційної інформації. Якщо стаціонарні комп'ютери знаходяться в межах одного приміщення та підключені до захищеної корпоративної мережі, то MD більшу частину часу проводять за периметром компанії.

Можна виділити кілька груп ризику, пов'язаних із використанням мобільних пристроїв у корпоративному середовищі: фізичні, організаційні, технічні ризики.

Таблиця 1.1 - Види ризиків використання мобільних пристроїв у корпоративному середовищі

Види ризиків	Приклади
Фізичний ризик	– втрата пристрою (втрата, крадіжка, пошкодження тощо).
Організаційний ризик	– низька компетенція співробітників у функціях смартфона, синхронізація додатків; – зміна поколінь MD, технологій та додатків; – привілейований доступ до баз даних на MD; – нецільове використання співробітником MD .
Технічний ризик	– витік конфіденційної інформації через шкідливе ПЗ, програми-шпигуни; – відстеження поведінки користувача.

1.3.1 Фізичний ризик використання мобільних пристроїв у корпоративному середовищі

Істотним фізичним ризиком для мобільного пристрою є його втрата та, як наслідок, крадіжка даних. Якщо на девайс не встановлено пароль, то важлива інформація стане доступна будь-якому перехожому. Навіть якщо пароль встановлений, то, маючи певні компетенції, його можна зламати. Як правило, операційні системи смартфонів прив'язуються до облікового запису. При маніпуляції з нею дані можуть бути безповоротно втрачені.

Щоб мінімізувати ризики від втрати або крадіжки mobile device, можна попередньо вжити додаткових заходів захисту, серед яких:

1) Встановити послуги геолокаційного відстеження місцезнаходження пристрою.

2) Налаштувати функції дистанційного блокування. Ця можливість передбачена більшістю сучасних смартфонів. Якщо задати в настойках потрібні параметри, можна впливати на пристрій з іншого девайса.

3) Налаштувати можливість блокування SIM-картки.

4) Використовувати надійні паролі, регулярно оновлювати програми.

І все ж найкращим захистом залишається ретельний нагляд за мобільним пристроєм і запобігання його попаданню в руки зловмисників, т.к. завжди є можливість обійти обмеження операційної системи через баги в програмному забезпеченні та помилки інтерфейсу.

1.3.2 Організаційний ризик використання мобільних пристроїв у корпоративному середовищі

Один з організаційних ризиків пов'язаний із мобільною гігієною співробітника. Для корпоративного використання MD недостатньо компетенції користувача. У сучасних смартфонах багатофункціональне меню налаштувань. Далеко не кожен розуміється на всіх його пунктах і усвідомлено розуміє, до чого веде «галочка» навпроти тієї чи іншої функції. Кожна встановлена програма має свою політику, а користувачі, приймаючи угоду при завантаженні, читають її у виняткових випадках. В результаті часто зустрічаються помилки в конфігурації і, наприклад, синхронізація робочої та особистої електронної пошти, відкриття доступу підозрілим додаткам, синхронізація файлів з хмарними сервісами та ін.

Серйозною проблемою використання MD у робочому середовищі є їхнє моральне зношування. Для корпоративних цілей важлива потужність пристрою та коректна робота. Покоління девайсів та технологій змінюються регулярно, вимагаючи періодичних вкладень у технічний парк. Цикл використання корпоративного MD у великих компаніях становить близько двох років. Оновити або замінювати програми потрібно ще частіше. Разом з

цим необхідно навчати персонал новим інтерфейсам та технічним можливостям.

1.3.3 Технічний ризик використання мобільних пристроїв у корпоративному середовищі

Технічні ризики є найбільшою групою ризиків з погляду наявності лазівок для нецільового використання інформації. Ряд програм, шкідливе програмне забезпечення або програми-шпигуни можуть довго залишатися непоміченими, відстежувати активність користувача та перехоплювати інформацію. Для управління зараженим MD зловмиснику потрібен канал передачі, тобто несанкціоноване підключення до мережі. Зараження також може статися через отримані електронною поштою файли або підключення до громадського Wi-Fi.

Джерело атаки на MD криється навіть у веб-інтерфейсі та мобільній версії сайтів. Незважаючи на те, що більшість мобільних пристроїв підтримують всі протоколи мережі, для зручнішого перегляду сторінки з невеликого екрана пропонується мобільна версія. Перехід на мобільну версію може бути атакою, особливо поширеною на сайтах та програмах, призначених для фінансових операцій. Наприклад, користувач може перейти не на офіційну мобільну версію сайту, а на легітимну сторінку, яка передає введені дані третім особам.

Ризик втрати конфіденційних даних компанії з mobile device підвищується тим, що багато файлів дублюються з корпоративної мережі та зберігаються у пам'яті пристрою. У багатьох власників девайсів такі функції передачі даних, як Wi-Fi, Bluetooth, GPS завжди активні, що підвищує ризик несанкціонованого вторгнення в пристрій і збору інформації про користувача. Щоб підвищити рівень захищеності корпоративної інформації на пристроях (наприклад, файлів doc, xls, ppt та ін.), компанії необхідно передбачити політикою безпеки обов'язкове шифрування накопичувачів. Важливо створювати корпоративні файлові сховища, які обслуговуватимуться і захищатимуться місцевим IT-відділом, щоб співробітники не

використовували в робочих цілях загальнодоступні хмарні сервіси, що пропонуються браузерами.

1.4 Сценарії використання мобільних пристроїв у корпоративному середовищі

У зв'язку з розвитком можливостей смартфона, їх ціновою доступністю, диджиталізації оточення та зміцненням позицій MD у житті кожного виробилося кілька сценаріїв використання мобільних пристроїв у корпоративному середовищі. Найпопулярніші стратегії роботи з mobile device - це BYOD (Bring Your Own Device - "принеси свій пристрій", CYOD (Choose Your Own Device - "вибери свій пристрій") та COPE (Corporate-Owned, Personally Enabled - "корпоративні пристрої, налаштування") та обслуговуванням яких співробітник займається самостійно»). Наприклад, простежується закономірність, що чим більша компанія, тим частіше вона самостійно закуповує корпоративні девайси, контролює їх налаштування та інформаційну безпеку. Але яке б рішення не було обрано, важливо визначити правила їх використання.

Концепція BYOD передбачає, що співробітник використовує особистий пристрій у робочих цілях, як в офісі, так і за його межами, самостійно його набуває та обслуговує. Можливий варіант, що компанія оплачує мобільний зв'язок. В рамках CYOD компанія набуває корпоративних пристроїв самостійно. Сценарій COPE є менш популярним. Він передбачає, що сам пристрій купує та видає компанія, але його налаштуванням та обслуговуванням займається співробітник. Тому може використовувати паралельно в особистих та робочих цілях. Такий підхід виправдовує себе, якщо штат має достатні технічні знання.

Будь-який сценарій вимагає для реалізації три компоненти: Web, бездротовий зв'язок та мобільний пристрій. Web – це платформа для різноманітних сервісів та програм у віртуальному середовищі. Бездротовий

зв'язок робить життя повністю мобільним, надаючи доступ до робочого середовища з будь-якого місця, де є зв'язок. Мобільний пристрій – це інструмент для використання Web-сервісів через бездротову мережу.

Якщо компанія вирішила освоювати мобільні пристрої для робочих цілей, необхідно акуратно підходити до правової сторони питання. Важливо заздалегідь обумовити, хто несе майнову відповідальність за девайс, які обмеження компанія може накладати на права користувача в рамках BYOD, наслідки для співробітника у разі витоку інформації та ін. Дані моменти краще заздалегідь документально оформити.

Таблиця 1.2 – Переваги та недоліки різних сценаріїв використання мобільних пристроїв у корпоративному середовищі

	BYOD	CYOD	COPE
Переваги	– зниження витрат компанії на придбання mobile device; – співробітники користуються зручними для них самими пристроями; – особисті MD, як правило, більш сучасні та продуктивні.	– цільове використання MD; – немає прив'язки до робочого місця та меж робочого дня; – вищий рівень захисту корпоративної інформації; – єдність політик безпеки та ОС; – оновлення програм.	– часткова персоналізація пристрою; – зменшення витрат на технічне обслуговування MD.

	Мобільність працівників, немає прив'язки до робочого місця та меж робочого дня		
Недоліки	– низька компетенція користувачів при виборі настройок; – відсутність технічної підтримки пристрою; – низький рівень захисту корпоративної інформації; – ризик крадіжки інформації співробітником, що звільнився; – змішані цілі використання MD; – різноманітність пристроїв та ОС.	– витрати на придбання мобільних пристроїв, їх заміну, ремонт.	– високі вимоги до технічних знань користувача.
	Розмиття кордонів між приватним життям та роботою, співробітник завжди «на зв'язку»		

2. АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ МОБІЛЬНИХ ДОДАТКІВ В КОРПОРАТИВНІЙ МЕРЕЖІ

Мобільні додатки почали впроваджуватися організаціями для підвищення продуктивності та обміну інформацією. У середовищі громадської безпеки програми повинні будуть забезпечувати розширені можливості місії, щоб допомогти користувачам громадської безпеки виконувати свої обов'язки. Однак мобільні програми потенційно можуть спричинити серйозні ризики для безпеки. Програми можуть містити вразливості, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до ресурсів пристрою, включаючи конфіденційну інформацію, що знаходиться на мобільному пристрої. Таким чином, мобільні додатки є критичним компонентом мобільної екосистеми, що потребує подальшого дослідження з метою розробки рекомендацій, стандартів та засобів контролю безпеки, необхідних для зменшення ризиків, пов’язаних із мобільними додатками.

2.1 Програмні загрози

Функціонал мобільних пристроїв забезпечується системним програмним забезпеченням та його розширеннями, а також програмами, які користувач завантажує та встановл.є. Однак деякі з таких додатків та розширень можуть бути спочатку зловмисними. Ці загрози мають високий рівень ризику та аналогічні для стаціонарних комп'ютерів.

2.2 Використання вразливих мобільних ОС та додатків

Вразливості в мобільних ОС та додатках аналогічні таким же вразливим для стаціонарних комп'ютерів. Такі вразливості, як у стаціонарних, так і в

мобільних ОС та додатках виявляються регулярно. Вразливості ОС становлять більшу загрозу, оскільки процеси ОС виконуються з більш високим пріоритетом, ніж програми. Мобільні програми, як і програми для інших пристроїв, також можуть бути безграмотно складені та вразливі для атак та використання «дір». Багато програм вразливі через помилки розробки або програмування, або ж некоректно налаштовані або конфігуровані з точки зору безпеки.

Одна з найраніших і найнебезпечніших атак полягає у відключенні зловмисниками вбудованих засобів захисту (процес, відомий як «jailbreaking» для Apple iOS або "rooting" для Google Android). Вимкнення вбудованих засобів захисту ОС дозволяє користувачам встановлювати програми та системні розширення, які заборонені політикою безпеки. Такі установки можуть призвести до навмисного або випадкового запровадження шкідливого коду. Як правило, процес обходу (зламування) засобів захисту ОС та додатків займає дні або навіть години після виходу нової версії з виправленими помилками попередньої. Такі небезпеки мають високий рівень ризику.

2.3 Web-загрози

Все більше пристроїв мають доступ до Інтернету і, відповідно, зростає кількість та витонченість Web-загроз. При цьому цілями, у тому числі, є смартфони, планшети та спеціалізовані пристрої та сервіси (наприклад, Інтернет, телебачення, радіо та ін).

2.3.1 Мобільний код

Це активний контент, що отримується через мережу і який виконується на мобільному пристрої. Мобільний код доставляється за допомогою HTML5, JavaScript, Adobe Flash та інші додатки, що підтримують інтерпретовані мови.

2.3.2 Завантаження «на льоту»

Ця загроза полягає в автоматичному отриманні шкідливого коду результатом відвідування користувачем інфікованого веб-сайту. Багато

легальних сайти можуть містити шкідливий код, оскільки були інфіковані раніше. Завантаження «на льоту» надзвичайно небезпечна, оскільки мета атаки (користувач) не була вразлива до відвідування такого сайту.

2.4 Мережеві загрози

Мережеві загрози безпеці - це загрози, де потенційним джерелом є використання вразливостей через мережу оператора зв'язку на прикладному рівні або всередині додатків, файлів або даних, як і в плані контролю, відповідального за конфігурацію та керування пристроєм. Мережеві загрози безпеці здійснюються через мережу оператора зв'язку або мережеві протоколи, а також пристрої, додатки та дані, що постійно використовують мережу. Пристрої, що використовують для зв'язку мережі Wi-Fi і мобільної, доступніші і вразливіші, ніж пристрої, що використовують тільки провідні мережі. Ці загрози мають високий рівень ризику та специфічні виключно для мобільних пристроїв.

2.4.1 Знімання голосу/даних «по повітрю»

Мобільні пристрої для взаємодії використовують різні бездротові протоколи, в яких дані можуть бути перехоплені або скомпрометовані. Більшість пристроїв підтримують мобільні протоколи, а також Wi-Fi та Bluetooth. Загрози цього класу відносяться до впливів каналу зв'язку від користувача мобільного пристрою до базової станції оператора зв'язку.

1) Wi-Fi.

Мобільні пристрої використовують, зокрема, Wi-Fi – бездротовий спосіб взаємодії на основі сімейства стандартів IEEE 802.11a/b/g/n. Такі пристрої можуть підключатися до будь-якої мобільної, персональної чи корпоративної точки доступу або іншого подібного пристрою для взаємодії "точка - точка". Пристрої, що використовують Wi-Fi, уразливі для перехоплення іншим Wi-Fi-пристроєм, бездротовим програмним інструментарієм, а також

аналізатором сигналів. Неконтрольовані точки доступу (несанкціонована точка всередині адміністративно контрольованого домену).

2) Мобільний зв'язок

Мобільні пристрої можуть взаємодіяти з використанням мобільних мереж різних технологій (GSM, EDGE, LTE та ін.). Деякі оператори зв'язку можуть надавати криптографічні засоби захисту. Дані та голос в мережах мобільного зв'язку можуть бути перехоплені, а також конфігурація та ключові компоненти пристрою можуть бути скомпрометовані каналами управління.

3) Bluetooth

Bluetooth – це малопотужна бездротова технологія ближньої дії, що забезпечує взаємодію мобільних пристроїв за стандартним протоколом. Bluetooth використовується для передачі даних між пристроями всередині персональної мережі (PAN), а також для передачі команд та голосової взаємодії між пристроєм та гарнітурою. Bluetooth має вбудовані механізми шифрування та аутентифікації, однак відомі вразливості та «дірки» цієї технології, такі як перехоплення ключів при ініціалізації сеансу.

2.4.2 З’єднання з недовіреним сервісом

Користувачі мобільних пристроїв, які використовують той чи інший мережевий сервіс, можуть ненавмисно звернутися до не довіреного сервісу. При цьому легальний сервіс міг бути раніше скомпрометовано. Або користувач навмисне звернувся до сервісу, до якого не звертався раніше, і надійність якого не підтверджена. В результаті, критична інформація може бути розкрита або скомпрометована. Також існує ризик порушення цілісності чи доступності даних.

2.4.3 Затор (Jamming)

Jamming - це загроза, яка заважає отриманню або передачі бездротового з'єднання. Інакше кажучи, затор – це постановка чи використання перешкод. Будь-який бездротовий протокол, що використовується мобільним пристроєм, схильний до перешкод, включаючи мобільне з'єднання, GPS, Wi-Fi та Bluetooth.

2.4.4 Затоплення (Flooding)

Атака Flooding переповнює систему даними, обсяг яких більший, ніж система може обробити. Будь-який бездротовий протокол, який використовується мобільним пристроєм, схильний до затоплення, включаючи мобільне з'єднання, GPS, Wi-Fi та Bluetooth. Результатом атаки зазвичай відмова в обслуговуванні. Даній загрозі схильні користувачі будь-яких пристроїв, дротових та бездротових.

2.4.5 GPS/Геолокація

Майже всі мобільні пристрої забезпечують для своїх програм той чи інший рівень служби геолокації. Такі програми можуть використовувати цю службу для відображення поточного розташування пристрою на карті, визначати місцезнаходження найближчих ресурсів, здійснювати трасування маршруту користувача та навіть виконувати популярну у користувачів функцію навігації маршруту пересування. Разом з тим ця служба має потенційну можливість розкриття місцезнаходження пристрою або виводити некоректну інформацію про місцезнаходження користувача за рахунок зовнішніх перешкод чи маніпуляцій. Ця загроза характерна виключно для мобільних пристроїв.

2.5 Слабкі елементи керування на стороні сервера

Слабкі елементи керування на стороні сервера включають практично все те, що мобільний додаток може зробити погано, що не відбувається на мобільному пристрої.

Через те, що більшість мобільних додатків також покладаються на з’єднання із сервером, це робить їх порівнянними з традиційними програмами клієнт/сервер. Проблема в тому, що розробники мобільних додатків часто не враховують традиційних проблем безпеки на стороні сервера. Хоча більшість загроз безпеки досить подібні до веб-додатків, здатність зловмисника обробляти мобільний пристрій і отримувати контроль над ним значно

відрізняється від того, що він знаходиться в Інтернеті. Існують різні причини, які призводять до проблем із керуванням на стороні сервера:

- відсутність знань та впровадження безпеки;
- часті оновлення та порив на ринок;
- використання простих у роботі фреймворків, які не мають пріоритету безпеки;
- якщо припустити, що мобільна операційна система несе повну відповідальність за безпеку мобільних програм;
- неефективна кросплатформна інтеграція та розвиток.

2.6 Небезпечне зберігання даних

Для зберігання особистих або конфіденційних даних, таких як номери кредитних карток або паролі, потрібен безпечний механізм. Як правило, розробники використовують файли та бази даних для зберігання даних на стороні клієнта в мобільних додатках, припускаючи, що обмежить доступ користувачів до даних.

Однак останні тенденції показують, що більшість порушень безпеки мобільних додатків були викликані непотрібним або незахищеним зберіганням даних клієнта.

Зловмисники можуть легко отримати root-права або зробити джейлбрейк мобільного пристрою та обійти безпеку мобільних додатків. Інший спосіб зламати мобільний додаток – це якщо зловмисники фізично отримують мобільний пристрій і підключають прийстрій до комп’ютера з доступним програмним забезпеченням.

Ці програми дозволяють зловмиснику бачити всі каталоги програм сторонніх розробників, які часто містять збережені дані, наприклад конфіденційну інформацію організації. Тоді зловмисники можуть змінити мобільний додаток, щоб вкрасти або видалити важливі дані.

Це призводить до кількох проблем бізнесу, таких як:

- крадіжка особистих даних або облікових даних;
- шахрайство;
- пошкодження репутації на ринку;
- погані відносини з клієнтами.

2.7 Ненавмисний витік даних

Розміщення конфіденційний данних в небезпечне місце на мобільному пристрої, призводить до ненавмисного витоку даних. До незахищеного розташування можуть отримати доступ інші мобільні програми, запущені на тому ж пристрої, що робить мобільний пристрій уразливим для атак.

Код мобільного додатка стає вразливим до серйозних атак, оскільки вектори загроз можуть легко використовувати ці вразливості витоку даних. Додавши невеликий фрагмент коду, зловмисник отримує доступ до місця, де зберігаються конфіденційні дані.

2.8 Погана авторизація та аутентифікація

Погані або відсутні схеми аутентифікації дозволяють зловмисникам обійти протоколи аутентифікації та отримати доступ до конфіденційних даних у мобільному додатку. Це відбувається шляхом анонімного виконання функцій на серверному сервері або мобільному додатку.

Багато мобільних додатків використовують 4- або 6-значний PIN-код для аутентифікації. Виконання перевірки на стороні клієнта небезпечно, оскільки для цього потрібно буде зберегти PIN-код на мобільному пристрої, що підвищує ризик його витоку.

Розробники повинні знати, що методи автентифікації можуть створити вразливості безпеки в мобільному додатку. У автономному режимі мобільні

додатки можуть дозволити користувачам з меншими привілеями виконувати дії та отримувати несанкціонований доступ до конфіденційних даних.

Погана аутентифікація та авторизація зазвичай поширені в мобільних додатках і часто залишаються непоміченими, їх технічні та бізнесові наслідки є серйозними.

2.9 Порушена криптографія

Розробники мобільних додатків часто впроваджують шифрування та дешифрування на пристрої за допомогою жорстко закодованого ключа у вихідному коді, що робить безпеку даних і криптографію вразливими для зловмисників, які можуть перепроектувати мобільний додаток.

Програми iOS за замовчуванням захищені від зворотного проектування за допомогою шифрування коду. Модель безпеки iOS вимагає, щоб мобільний додаток був зашифрований і підписаний надійними джерелами для виконання в середовищі без джейлбрейка.

Коли програма запускається, завантажувач iOS розшифровує мобільний додаток у пам’яті та виконує код після перевірки підпису iOS. Теоретично це запобігає зловмисникові від запуску бінарних атак на мобільний додаток.

Зловмисники використовують такі інструменти, як GBD або ClutchMod, щоб завантажити зашифрований додаток на джейлбрейкнутий пристрій і зробити знімок розшифрованого мобільного додатка, коли завантажувач iOS розшифрує його в пам'ять. Це дозволяє зловмиснику використовувати мобільний додаток.

Використання користувацьких алгоритмів шифрування замість сучасних, які вважаються надійними спільнотою безпеки, також є способом неправильного поводження з криптографією.

Багато криптографічних протоколів і алгоритмів виявили значну слабкість або недостатні для захисту мобільних додатків сьогодні. До них належать:

- SHA1;
- RC2;
- MD5;
- MD4.

2.10 Ін'єкція на стороні клієнта

Зловмисники вводять шкідливий код на стороні клієнта, який зазвичай надається у вигляді вхідних даних у мобільний додаток за допомогою різних засобів. Оскільки дані неправильно сформовані, якщо мобільний додаток обробляє їх (як і будь-які інші дані), а базова структура інтерпретує деформовані дані як виконувані, код буде виконуватися мобільним додатком.

Код виконується з привілейованими дозволами з більшим обсягом доступу, що призводить до значного компромісу.

Більше того, інші форми ін’єкції на стороні клієнта передбачають пряме введення двійкового коду через двійкові атаки в мобільний додаток. Така атака з метою виконання шкідливого коду призводить до ще більшої потенційної шкоди, ніж ін'єкції вхідних даних.

2.11 Рішення безпеки через ненадійні вхідні дані

Розробники мобільних додатків використовують приховані значення, файли чи інші приховані функції, щоб відрізнити користувачів високого рівня від користувачів низького рівня.

Якщо зловмисник перехоплює виклики IPC або веб-служби та втрутитися в таку конфіденційну інформацію, зловмисник може отримати несанкціонований доступ до мобільного додатка.

Погана реалізація таких прихованих функцій призводить до неналежної поведінки мобільного додатка, а також надає несанкціонований доступ і надати зловмиснику більш високі привілеї.

Це призводить до обходу механізмів безпеки мобільного додатка, що призведе до втрати цілісності та конфіденційності. У той же час ця вразливість мобільного додатка впливає на репутацію організації.

2.12 Неправильна обробка сеансів

Тривалі або незавершені сеанси користувача роблять мобільний додаток зручним і простим у використанні. Це допомагає скоротити час на покупку та оформлення замовлення, щоб компанія отримала більше доходу.

Мобільні програми використовують маркери OAUTH, служби SSO та файли cookie для керування сеансами. Щоб забезпечити належну обробку сеансів, мобільний додаток повинен аутентифікувати користувача через серверну систему, а потім видати файл cookie сеансу для мобільного додатка.

Неправильна обробка сеансу відбувається, коли зловмисник отримує доступ до маркера сеансу під час транзакції між мобільним додатком і серверними серверами.

2.13 Відсутність бінарного захисту

Відсутність двійкового захисту є серйозною вразливістю мобільного додатка, яка надає зловмисникам конфіденційні дані мобільного додатка, такі як інтелектуальна власність, облікові дані тощо. Використовуючи зворотну інженерію, зловмисники виявляють таку конфіденційну інформацію, як бізнес-логіка, паролі, ключі API тощо.

Зловмисники використовують автоматизовані інструменти для зворотного проектування програми та модифікації її для виконання шкідливих дій.

Розміщення коду мобільного додатка в ненадійному середовищі, наприклад на телефоні зловмисника, є ймовірність, що додаток може бути використано зловмисниками.

2.14 Безпека обміну даними та Людина посередині

Функціональні можливості більшості програм засновані на зв’язку із сервером. Залежно від потреб програма надсилає або отримує різні типи даних: облікові дані для входу, дані сеансу користувача, особисті дані, банківські дані тощо. HTTP є стандартом для зв’язку між клієнтом і сервером. Проте зв’язок потенційно може бути перехоплений, змінений або перенаправлений, оскільки цей протокол не має вбудованих функцій безпеки. Оодна з поширених атак використовує отруєння ARP. Ця техніка дозволяє захопити комунікаційні потоки між програмою та шлюзом: маршрутизатором, коробкою тощо. Коротше кажучи, це атака Man in the Middle, під час якої зловмисник надсилає помилкові повідомлення, щоб отруїти кеш ARP користувача і таким чином зв’язати його MAC-адреса на законну IP-адресу. Роблячи це, вони можуть перехоплювати, змінювати або видаляти будь-яке спілкування, яке проходить між програмою та сервером.

2.15 Вразливі місця в бізнес-логіці

Вразливості бізнес-логіки можуть призвести до того, що користувачі можуть зіткнутися з такими загрозами, як грубий злом кодів підтвердження або паролів, атаки повторного відтворення, велика кількість спам-повідомлень і навіть розкриття конфіденційної інформації (наприклад, паролів або даних кредитних карток).

Розробка мобільних додатків включає в себе багато сторонніх пакетів SDK, включаючи платежі, статистику, рекламу, соціальні мережі, push, карти тощо. Після використання вразливостей SDK зловмисники можуть

використовувати функції самого SDK для запуску шкідливих атак, наприклад, увімкнути камеру, щоб робити знімки, не помічаючи користувача, вкрасти маркери двофакторної аутентифікації шляхом надсилання текстових повідомлень або повернути пристрій. в частину ботнету.

3. РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ

3.1 Типи додатків за технологіями

Кожен, хто планує створити додаток для свого бізнесу, неодмінно повинен відповісти на питання: який тип мобільного додатка ми створюємо?

Схематичне зображення див. на рис.3.1

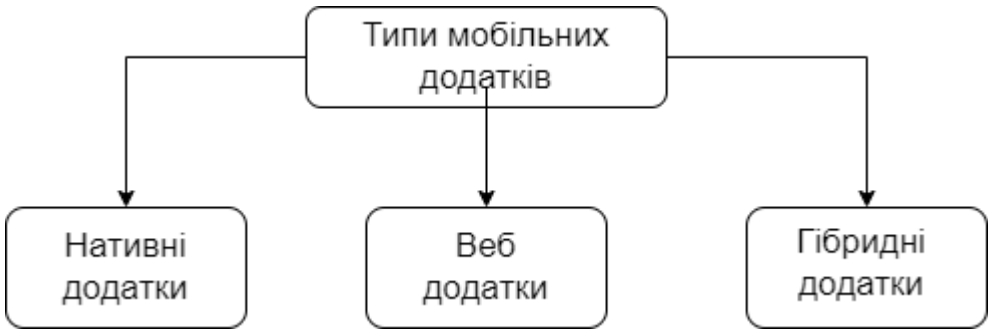


Рисунок 3.1 – Типи мобільних додатків за тезнологіями

3.1.1 Нативні додатки

Нативні програми – це тип мобільних додатків, розроблених для певного мобільного пристрою чи ОС – Android, iOS. Ці типи програм можуть працювати або функціонувати лише на пристроях, для яких вони створені. Широко відомими платформами є Android, iOS.

Нативні мобільні додатки є рідними для певних пристроїв чи операційних систем і добре оптимізовані для певного пристрою чи платформи, завдяки чому такі типи мобільних додатків дають чудову продуктивність.

Технологія, яка використовується для розробки нативних мобільних додатків, є специфічною для платформи, для якої вони створені. Наприклад, мовами програмування для створення додатків iOS є Objective C або Swift, а програми для Android кодуються мовою програмування Java.

Крім того, рідні програми можуть розповсюджуватися лише через магазини додатків відповідних платформ.

Таблиця 3.1 – Переваги та недоліки нативних додатків

Тип	Переваги	Недоліки
Нативні додатки	– вбудовані програми розширюють швидкий і гладкий інтерфейс користувача. Вони надзвичайно надійні та чутливі; – використовує менше апаратних ресурсів, оскільки кодування ефективніше; – отримання доступ до вбудованих функцій пристрою, завдяки чому весь досвід буде чудовим; – можливість працювати в автономному режимі; – використовувати push-сповіщення, для збільшення використання програми та спонукати до бажаної дії.	– обмежено однією платформою і, отже, однією аудиторією; – створення одного додатка для двох різних платформ займає багато часу та дорого; – підтримка й оновлення програми в різних магазинах додатків займає багато часу та вимагає багато часу; – немає переносимості коду.

3.1.2 Веб-додатки

Веб-додатки – це додатки з підтримкою Інтернет-браузера. Ви можете отримати доступ до веб-програм через веб-браузери на своєму мобільному. Їх не потрібно встановлювати або завантажувати на свій мобільний телефон. Завантажити їх, по суті, означає зберегти їх як закладку.

Хороша частина веб-додатків (бізнес-програм) полягає в тому, що вони не займають багато ваших апаратних ресурсів, таких як оперативна пам’ять і сховище. Вони також не мають доступу до функцій пристрою, оскільки працюють через мобільний або веб-браузер.

Веб-програми створюються з використанням таких веб-технологій, як HTML, CSS, та JavaScript тощо. Вони розповсюджуються лише через Інтернет і пропонують багатоплатформенну підтримку.

Таблиця 3.2 – Переваги та недоліки веб додатків

Тип	Переваги	Недоліки
Нативні додатки	– швидкі та доступні витрати на розробку, оскільки налаштовування під конкретну платформу не потрібно; – розгортання та розповсюдження веб-програм легше. Оновлення миттєві і не вимагають оновлення у відповідних магазинах додатків; – підтримка кількох платформ і не потребує окремої бази коду для кожної платформи; – не потребує схвалення від магазинів додатків для уповільнення/запобігання запуску.	– недоступний через магазин додатків. І не може отримати доступ до можливостей пристрою; – повільніша швидкість. – менш інтерактивний інтерфейс користувача. – Обов’язкове підключення до інтернету; – не працює добре на старих пристроях і веб-браузерах; – можливість виявлення програми залежить від охоплення веб-сайту.

3.1.3 Гібридні додатки

Як випливає з назви, гібридні мобільні додатки є сумішшю як нативних, так і мобільних додатків. Гібридні програми іноді називають кросплатформними мобільними додатками. Єдина подібність між гібридним мобільним додатком і кросплатформним додатком — це «спільне використання коду». Тут ми зосередимося на гібридному мобільному додатку, оскільки вони набагато кращі.

З одного боку, вони схожі на рідні програми, оскільки ви можете легко завантажити їх із магазинів додатків, і вони з’являються на головному екрані.

З іншого боку, вони використовують браузер, вбудований у саму програму, для відтворення даних.

Навіть ви будете здивовані, дізнавшись, що деякі відомі програми є гібридними мобільними додатками, такими як Instagram, Twitter, а одним із прикладів програм для підвищення продуктивності є Evernote.

Гібридні програми використовують цілий набір різних технологій веб-розробки та рідних API. Вони закодовані в Objective C, Swift, HTML5, React-Native, Ionic.

Таблиця 3.3 – Переваги та недоліки веб додатків

Тип	Переваги	Недоліки
Нативні додатки	– можливість отримати доступ до рідних функцій пристрою; – швидко розвивається. Тому що вони використовують технології стандартної мережі; – побудовані на єдиній базі коду, що економить час і ресурси; – підтримка кількох платформ; – легко розгортати оновлення; – можливість змусити працювати без підключення до Інтернету, якщо підтримка бази даних не потрібна; – поширення через магазини додатків.	– порівняно з нативними програмами продуктивність дещо погіршена; – деякі функції можуть бути відсутні на певних пристроях; – високі витрати через більше налаштувань; – важко отримати досвід, подібний до нативних програм. Оскільки гібридні додатки розробляються для двох платформ і повинні адаптуватися до обох одночасно; – не працює добре на старих пристроях і браузерах; – можливі проблеми дизайну, які не підтримують обидва пристрої.

3.2 Опис проекту

В ході виконання даної дипломної роботи для практичного дослідження та тестування вразливостей був розроблений мобільний додаток. Мобільний додаток являє собою рішення для організації для комунікації, створення новин, питанньь та відповідей до них.

При виборі технології та інструментів розробки враховувались наступні фактори:

– низька вартість та простота розробки;
– доступ до нативних функцій;
– продуктивність;
– привабливий дизайн;
– підтримка кількох платформ, в цілях економії часу для розробки.

Враховуючи зазначені фактори, а також власні знання та навички у розробці web додатків, технології Angular, було прийнято рішення розробити гібридний мобільний додаток на базі Ionic.

Ionic[15] – це технологія, що дозволяє розробляти повноцінні програми для iOS та Android. Для розробці яких, не потрібно мати глибокі знання у кожній із платформ.

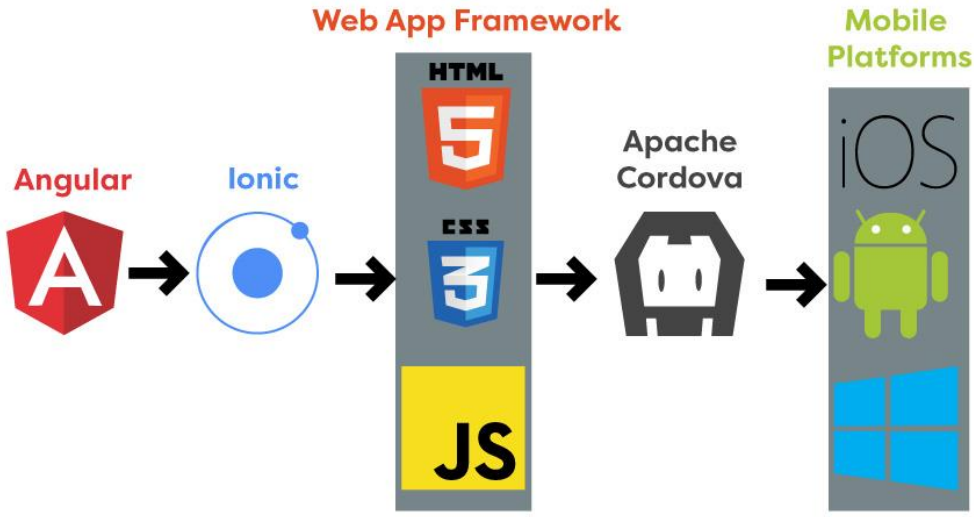


Рисунок 3.2 – Схема роботи додатку на ionic

Ionic має вбудовану бібліотеку стандартних елементів, які можна використовувати аналогічно елементам Bootstrap: картки, кнопки, перемикачі, сегменти, попапи, поля введення, списки, сітка з рядків та колонок тощо. За замовчуванням ці елементи змінюються так, щоб виглядати як нативні на iOS та Android, але їхній вигляд можна змінити і при необхідності. Також для платформи Ionic є безліч плагінів, які дозволяють використовувати залізо смартфона (Ionic Native/Cordova).

Для швидкої реалізації зберігання та обробки даних була вибрана база даних Firebase Realtime – це хмарна NoSQL база даних компанії Firebase. База даних Firebase Realtime - це база даних, розміщена у хмарі. Дані зберігаються у форматі JSON та синхронізуються в реальному часі з кожним підключеним клієнтом. Коли ви створюєте кросплатформні програми за допомогою наших платформ Apple, Android та SDK для JavaScript, всі ваші клієнти використовують один екземпляр бази даних у реальному часі та автоматично отримують оновлення з новітніми даними.

Всі послуги Firebase (крім App розподілу та Firebase App Indexing) успішно завершили ISO 27001 та SOC 1, SOC 2 та SOC 3 процесу оцінки, а деякі з них також завершили ISO 27017 та ISO 27018 процес сертифікації[20].

Таблиця 3.3 – Стандарти безпеки для послуг Firebase

Наіменування послуг	ISO 27001	ISO 27017	ISO 27018	SOC 1	SOC 2	SOC 3
База даних Firebase у реальному часі	✓			✓	✓	✓
Динамічні посилання Firebase	✓			✓	✓	✓
Лаборатория тестирования Firebase	✓	✓	✓	✓	✓	✓

Наіменування послуг	ISO 27001	ISO 27017	ISO 27018	SOC 1	SOC 2	SOC 3
Моніторинг продуктивності Firebase	✓			✓	✓	✓
Хмарне сховище для Firebase	✓	✓	✓	✓	✓	✓
Хмарні функції для Firebase	✓	✓	✓	✓	✓	✓
Обмін повідомленнями Firebase у програмі	✓			✓	✓	✓
Обмін повідомленнями Firebase Cloud	✓			✓	✓	✓
Платформа Firebase	✓			✓	✓	✓
Перевірка автентичності Firebase	✓	✓	✓	✓	✓	✓
Прогнози Firebase	✓			✓	✓	✓
Тестування Firebase A/B	✓			✓	✓	✓
Віддалена конфігурація Firebase	✓			✓	✓	✓
Хостинг Firebase	✓			✓	✓	✓
Cloud Firestore	✓	✓	✓	✓	✓	✓
Firebase Crashlytics	✓			✓	✓	✓
Firebase ML	✓			✓	✓	✓
Google Analytics для Firebase	✓					

3.3 Функціональні компоненти

У цій главі було розглянуто, та продемонстровані функціональні компоненти створеного додатка. Додаток був зібран та запущений на емуляторі Android під версією ОС Android 11.0.

Нижче можна побачити функціональні схеми роботи мобільного додатку:

1) Блок-схема 1 описує запуск програми та перевірку авторизації користувача.
2) Блок-схема 2 описує роботу компоненту реєстрації.
3) Блок-схема 3 описує роботу компоненту авторизації.
4) Блок-схема 4 описує можливості та функціональність компонентів.

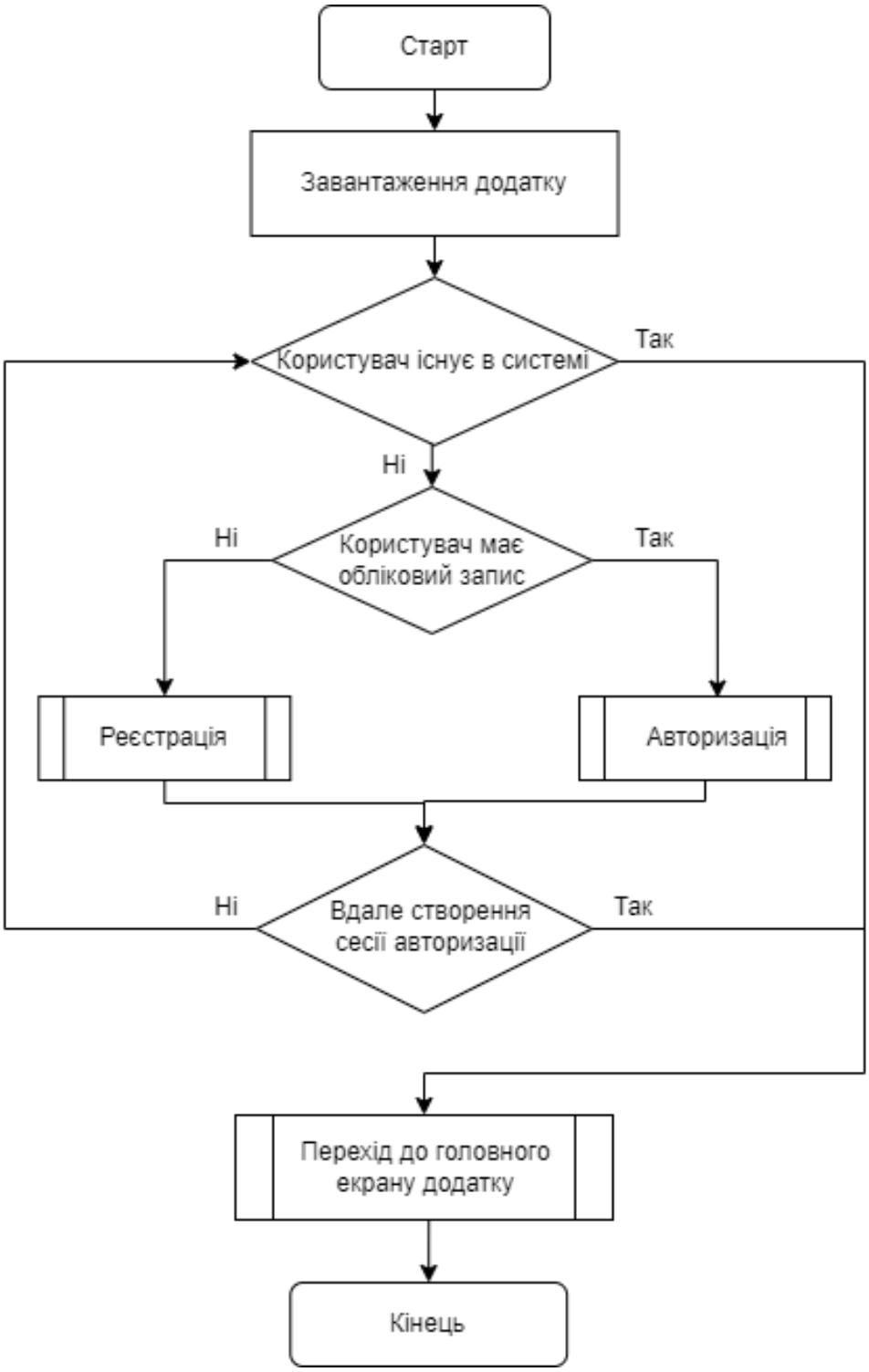


Рисунок 3.3 –Блок-схема роботи додатку

Рисунок 3.4 –Блок-схема роботи екрану реєстрації додатку

Рисунок 3.5 –Блок-схема роботи екрану авторизації додатку

Рисунок 3.6 –Блок-схема роботи головного екерану додатку

3.2.1 Функціональний компонент авторизіція

Firebase пропонує службу для керування автентифікацією користувачів, використовуючи різні парадигми. Окрім парадигми Email-Password, автентифікація Firebase надає можливість безпосередньо аутентифікувати користувача за допомогою його/її профілів Google, Twitter, Facebook або GitHub тощо. Тим не менш, для додатку була обрана лише парадигма Email-Password, оскільки, додаток має корпоративне призначення, було прийнято рішення не пов’язувати його з соціальними профілями.

Firebase також керує випадками, коли користувач намагається створити різні облікові записи, використовуючи ту саму адресу електронної пошти з різними постачальниками аутентифікації. Програма може вибрати, дозволити чи уникнути цього. Крім того, він автоматично обмежує кількість нових анонімних або електронних реєстрацій, які надходять з тієї самої IP-адреси, щоб уникнути можливих порушень.

Служба аутентифікації також надає деякі моделі для створення електронної пошти та SMS для спілкування з користувачами. Наприклад, модель для перевірки електронної пошти, використаної для створення облікового запису, або для зміни пароля користувача, якщо він його забуде.

Після створення кожен користувач автоматично отримує Uid, унікальний ідентифікатор, не пов’язаний з інформацією користувача або постачальником аутентифікації. Цей ідентифікатор буде використовуватися в базі даних з двох основних причин: по-перше, правила бази даних можуть керувати UID, щоб дозволити доступ до певної гілки лише користувачеві, якому вона належить, по-друге, щоб зробити базу даних анонімною.

Результат роботи екрану авторизації та реєстрації користувача можна побачити на малюнку 3.7 та малюнку 3.8.

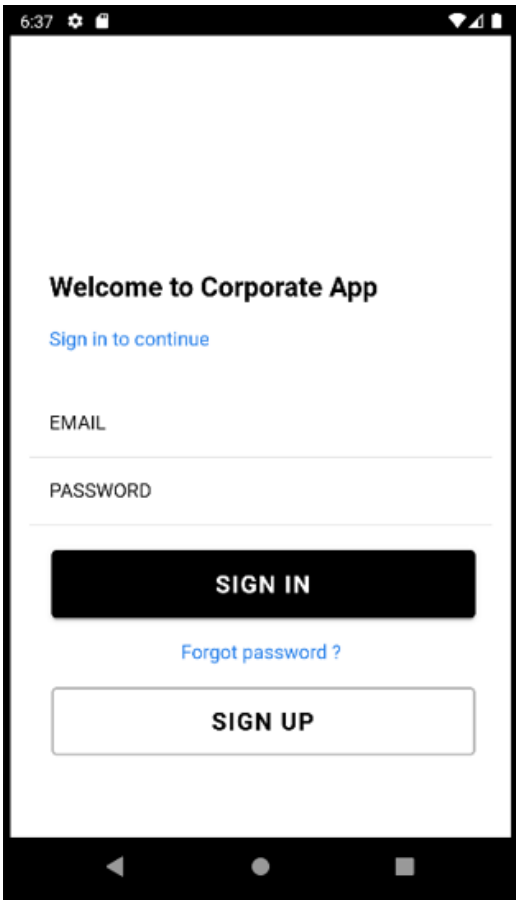


Рисунок 3.7 – Результат роботи функціонального компоненту авторизації

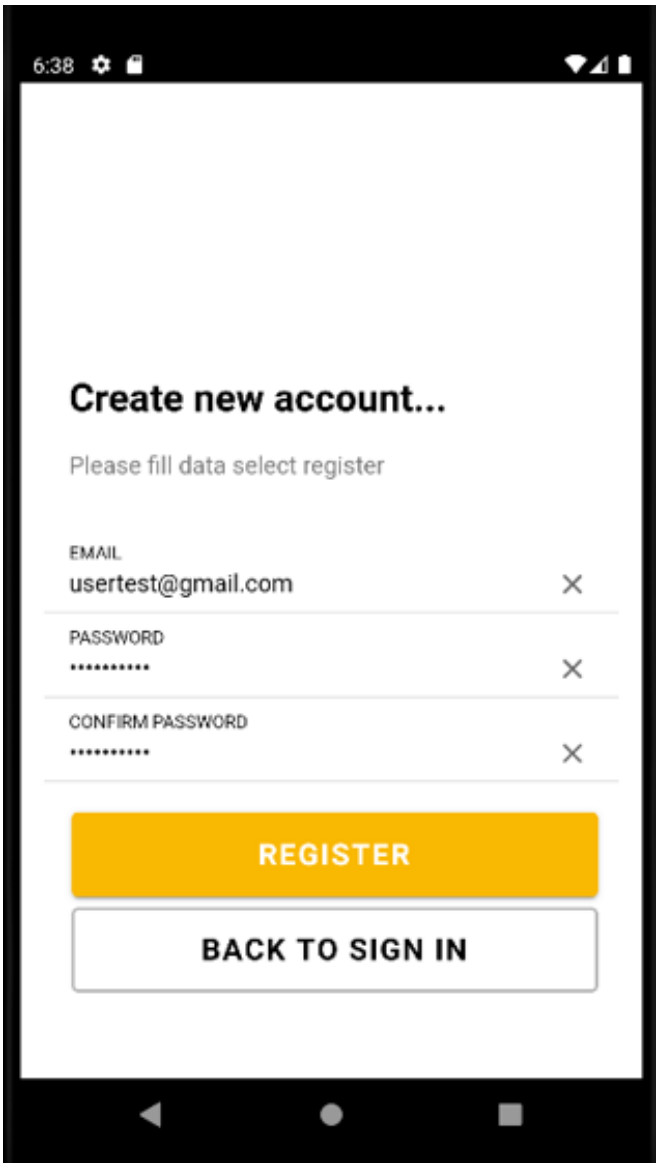


Рисунок 3.8 – Результат роботи функціонального компоненту реєстрації

3.2.2 Функціональний компонент Feed

Функціональний компонент Feed був створений з метою дозволити співробітникам організації ставити запитання (створювати новини) та залишати відповіді чи коментарі до них.

Результат роботи відображення компоненту Feed можна побачити на малюнку 3.9

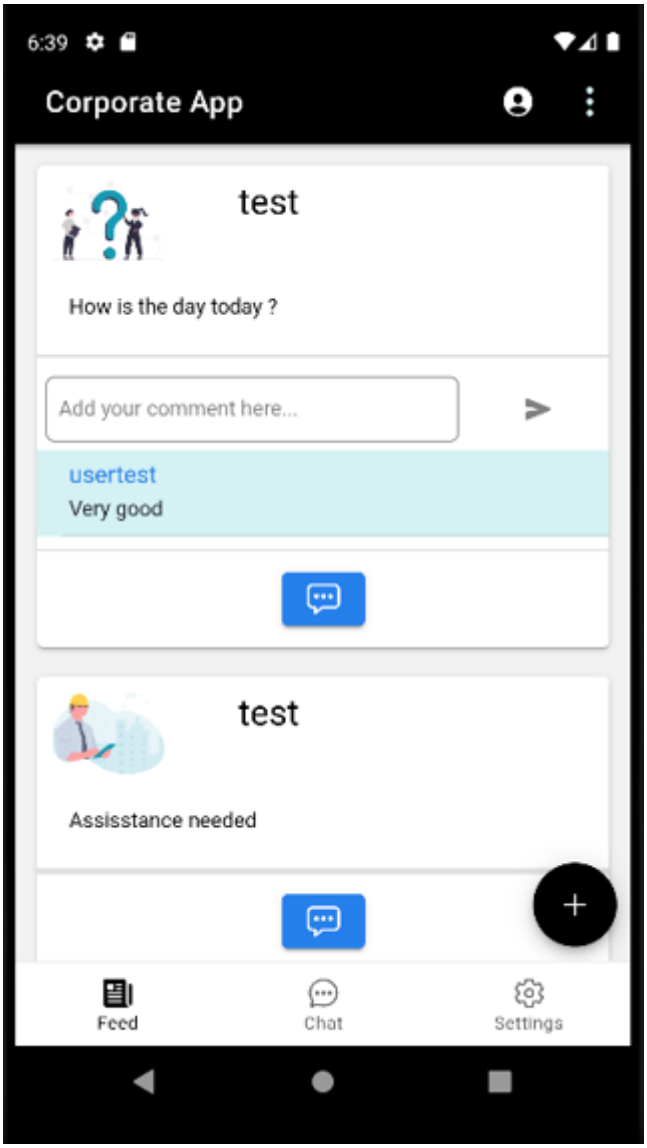


Рисунок 3.9 – Результат роботи функціонального компоненту Feed

Для додавання нових постів внизу екрана була додана кнопка, при натисканні на яку відбувається подія для відкриття вікна з формою для створення посту. Результат роботи форми додавання поста можна побачити на малюнку 3.10.

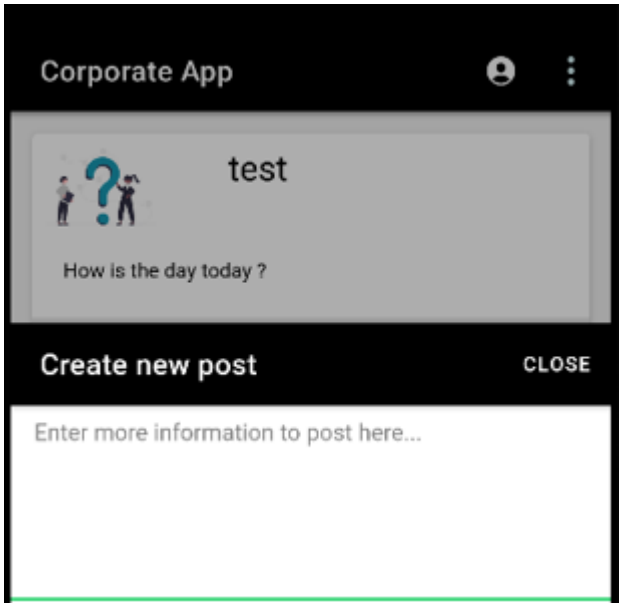


Рисунок 3.10 – Результат роботи форми для створення нового поста

Форма додавання коментаря до посту, знаходиться прямо під повідомленням посту, після заповнення якої та натискання на кнопку відправити, відбувається подія збереження коментаря в базі даних та оновлення відображення постів. Форму додавання коментаря можна побачити на малюнку 3.11.

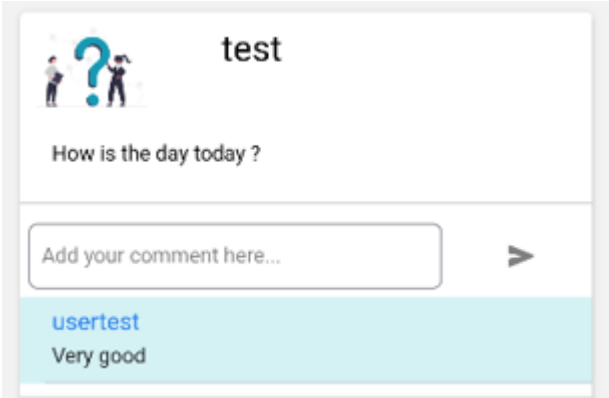


Рисунок 3.10 –Приклад форми додавання коментаря для поста

3.2.3 Функціональний компонент Settings

Функціональний компонент Settings відповідає за обліковий запис користувача. За допомогою даного екрана користувачеві надається

можливість здійснити базові зміни профілю. Результат роботи екрана налаштувань можна побачити на малюнку 3.12.

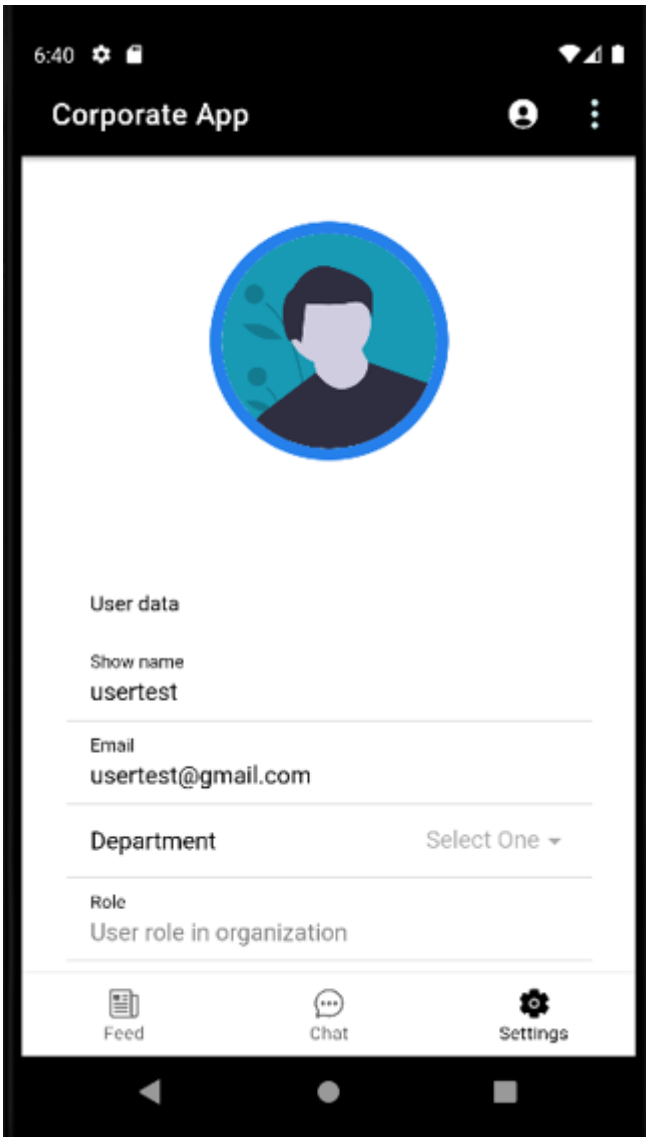


Рисунок 3.12 – Результат роботи функціонального компоненту Settings

3.2.4 Функціональний компонент Chat

Функціональний компонент Chat відображає текстовий чат для співробітників організації. Для того, щоб надіслати повідомлення, потрібно заповнити форму введення повідомлення та натиснути надіслати. Результат роботи чату з прикладами надісланих повідомлень можна побачити на малюнку 3.13.

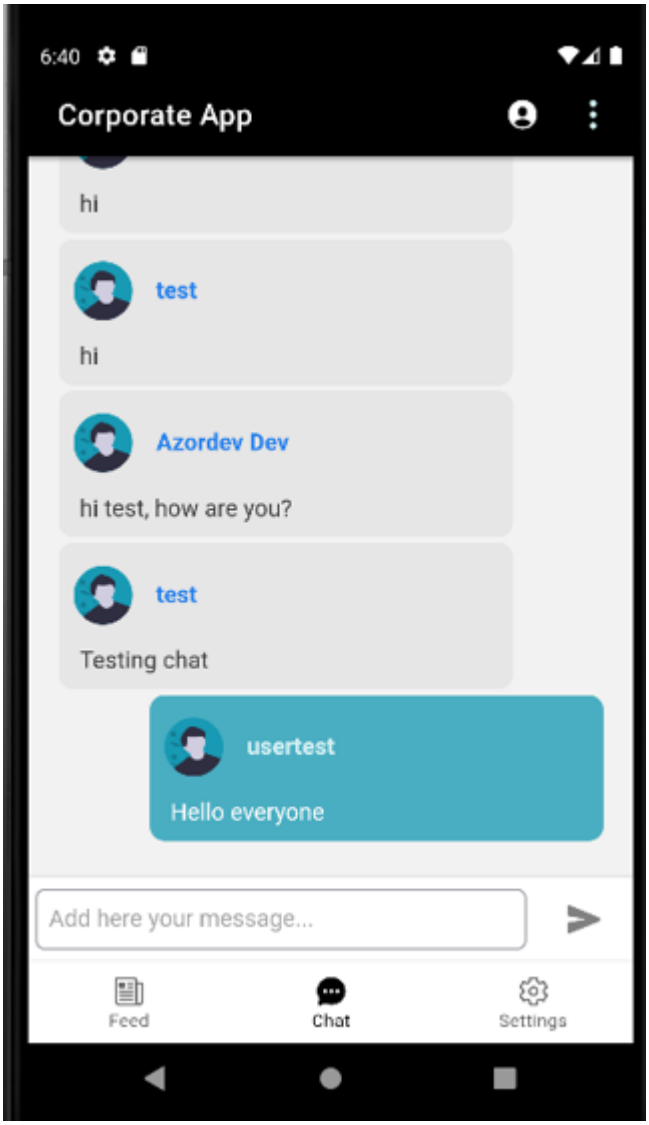


Рисунок 3.13 – Результат роботи функціонального компоненту Chat

4. МОДЕЛЬ ЗАГРОЗ ТА ТЕСТУВАННЯ

Тести, проведені на мобільних додатках з 2012 року, виявили кілька загальних категорій з боку клієнта, які викликають слабкі місця в мобільних додатках, ці слабкі сторони включають небезпечне зберігання даних з відсотком 63%, небезпечну передачу даних з відсотком 57%, відсутність двійкових захист з відсотком 92%, ін'єкція на стороні клієнта з відсотком 40%, жорстко закодований пароль/ключі з відсотком 23%, і витік конфіденційних даних з відсотком 69%.

4.1 Рейтинг OWASP

OWASP означає Open Web Application Security Project — це неприбуткова організація, розташована в Сполучених Штатах та була заснована 21 квітня 2004 року. Сам фонд OWASP був онлайн 1 грудня 2001 року та став міжнародною організацією та підтримує всі OWASP діяльності у світі. OWASP – це відкрита спільнота, яка зосереджується на розумінні, розвитку, отриманні, експлуатація та обслуговування програм, яким можна довіряти.

Таблиця 4.1 - OWASP Топ-10 уразливостей мобільних додатків

№	Вразливості
1	Неправильне використання платформи
2	Небезпечне зберігання даних
3	Небезпечне спілкування
4	Небезпечна аутентифікація
5	Недостатня криптографія
6	Небезпечна авторизація
7	Якість клієнтського коду
8	Підробка коду
9	Зворотне інжиніринг
10	Сторонній функціонал

4.2 Тестування мобільного додатку на проникнення

Тестування на проникнення є дуже корисним інструментом для пошуку слабких місць у мережевій інфраструктурі, що показує, наскільки вразлива мережа під час атаки. Тестування на проникнення виявилося ефективним у вирішенні проблем безпеки в мережі. Методи тестування на проникнення спрямовані не тільки на програми, але також можуть застосовуватися до мереж та операційних систем, де головна мета полягає в пошуку та спробі використати вразливості, які відомі або виявлені під час попередніх оцінок, що містяться в певних технологіях. Мобільні пристрої, такі як смартфони та планшети, широко використовуються в особистих і ділових цілях. Мобільний пристрій може переносити конфіденційні дані і стає легкою мішенню для кіберзлочинців.

Тестування на проникнення, яке також називають пентестом — це процес, коли компанія наймає фахівців з комп’ютерної безпеки, щоб спробувати проникнути в їх IT-інфраструктуру з наміром знайти найбільші вразливості. По суті, компанія наймає фахівців з безпеки, щоб вони оцінили та зламали їхню мережу, сервери та служби, перш ніж зловмисники зможуть зробити те ж саме. Більшість тестів на проникнення, як правило, зосереджені на експлуатації мереж і вилученні конфіденційних даних, втрата сервісу та нездатність організації використовувати власну бездротову мережу також можуть мати значний вплив на їх продуктивність.

4.3 Методика тестування

Для дослідження вразливостей використовується метод тестування на проникнення внутрішньої мережі. Кроки, які будуть виконуватися в цьому дослідженні, можна побачити на малюнку 4.1.

Рисунок 4.1 – Кроки дослідження

1. Підготовка, яка є етапом, визначає сферу тестування безпеки, що включає визначення використовуваних засобів контролю безпеки, цілей тестування та конфіденційних даних.
2. Збір даних – це етап аналізу обсягу та архітектури програми, щоб отримати загальне уявлення про програму.
3. Відображення програми — це наступний крок для завершення попереднього етапу шляхом автоматичного сканування та вивчення програм вручну. Відображення може надати глибше розуміння програми для тестування, наприклад точки входу, дані та інші потенційні основні недоліки.
4. Експлуатація — це етап, на якому тестувальники безпеки проникають у програму, використовуючи слабкі місця, виявлені під час попереднього процесу. На цьому етапі також визначають реальні слабкі сторони та справжні позитиви.

   На цьому етапі, використовуючи посилання на атаку, знайдене в топ-10 OWASP, можна визначити тип атаки, з якою найчастіше стикаються мобільні програми. На цьому етапі буде здійснено кілька методів атаки, які, ймовірно, будуть здійснені на мобільних додатках.
5. Звіти, важливий етап, тестувальники безпеки надають звіти про слабкі місця знайдених програм і можуть пояснити негативні наслідки слабких місць програми.

4.4 Дослідження та перевірка вразливостей за рейтингом owasp

Дослідження додатку базується на документації та методах, що містяться в OWASP, який складається з 10 проблем безпеки в мобільних додатках, які були досліджені та часто зустрічаються при розробці мобільних додатків.

Таблиця 4.2 – OWASP Mobile Top 10

Код	Вразливості
M1	Неправильне використання платформи
M2	Небезпечне зберігання даних
M3	Небезпечне спілкування
M4	Небезпечна аутентифікація
M5	Недостатня криптографія
M6	Небезпечна авторизація
M7	Якість клієнтського коду
M8	Підробка коду
M9	Зворотне інжиніринг
M10	Сторонній функціонал

4.4.1 Неправильне використання платформи M1

Для перевірки даної вразливості, був використан проект, створений за допомогою зворотньої інженерії.

Під час перевірки файлів проекту, не було знайдено місць, які можна віднести до характеристик даної вразливості.

Рисунок 4.2 – Приклад вразливості M1

В прикладі на малюнку 4.2 можна побачити, що розробник під час дебагінгу використовував logcat, для розуміння помилок виникнувших в даному полі. Але під час компіляції додатку було залишено в проекті. Це може означати, що дії будуть логуватися, якщо там будуть які-небудь помилки або попередження.Тобто, коли користувач заповняє форму, ці дані будуть з’являтися в логах додатку, якщо користувач припуститься помилки при заповнення форми або отримає попередження заповнення.

Підсумок дослідження вразливості наведено в таблиці 6.

Таблиця 4.3 - Результат тестування для M1

Код	M1
Вразливість	Неправильне використання платформи
Рівень ризику	Високий
Вплив	Крадіжка конфіденційної інформації та контроль логіки програми
Рекомендації	Впровадження безпечного кодування та звертання уваги на поради безпеки розробки програми з офіційної документації.

4.4.2 Небезпечне зберігання даних M2

Єдині дані, що зберігаються на стороні мобільного додатка, є інформація за допомогою якої відбувається авторизація користувача з системою.

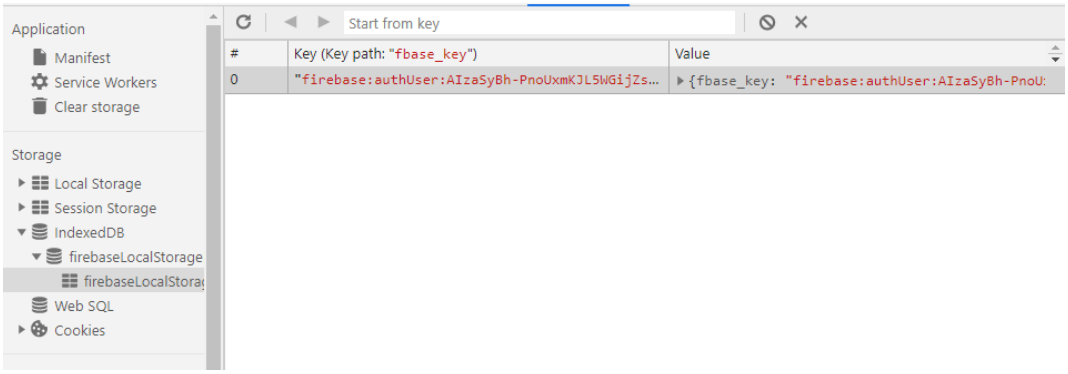


Рисунок 4.3 – Перегляд сховища за домогою інструментів розробки

За замовчуванням дані про корустувача сберігаються в сховищі під назвою IndexedDb.

IndexedDb – це NoSQL база даних, яку можна використовувати на стороні клієнта для зберігання великої кількості даних.

Під час проведення дослідження було виявлено, що IndexedDb вразлива до зловмисного програмного забезпечення та атак фізичного захоплення, що може дозволити зловмисникам викрасти обліковий запис користувача та використовувати його для певних цілей іншими програмами. Підсумок дослідження вразливості наведено в таблиці 4.4

Таблиця 4.4 – Результат тестування для M2

Код	M2
Вразливість	Небезпечне зберігання даних
Рівень ризику	Високий
Вплив	Крадіжка конфіденційної інформації, порушення конфіденційності, шахрайство, псування репутації та порушення зовнішньої політики.
Рекомендації	1. Звертання уваги на дані, що зберігаються. 2. Використовування надійного шифрування для зберігання даних.

4.4.3 Небезпечне спілкування М3

Для вивчення та перевірки вразливості було обрано метод атаки типу «людина посередині».

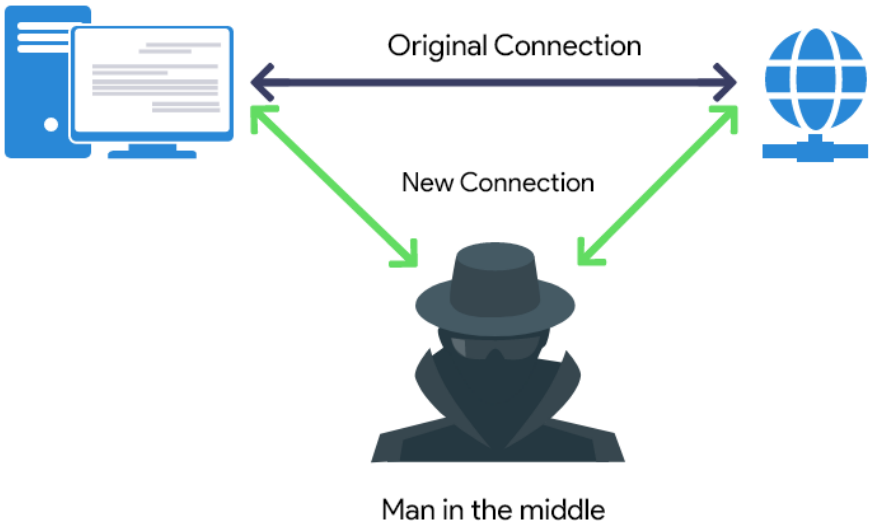


Рисунок 4.4 – Схема атаки типу «людина посередині»

Атаки «людина посередині» - це форма кібератаки, при якій для перехоплення даних використовуються методи, що дозволяють впровадитись у існуюче підключення або процес зв'язку. Зловмисник може бути пасивним слухачем у вашій розмові, який непомітно краде якісь відомості, або активним учасником, змінюючи зміст ваших повідомлень або видаючи себе за іншу людину або систему.

Для того, щоб реалізувати атаку типу «людина посередині» потребується створити проксі-сервер для перехоплення запитів від мобільного додатку до серверу, з цією задачею впорається платформа BurpSuite.

Burp Suite – це інтегрована платформа для виконання тестів безпеки веб-додатків. Планформа включає в себе інструменти, які ефективно працюють разом для підтримки всього процесу тестування, від складання карти сайту та

аналізу поверхні атаки докладання до пошуку та експлуатації вразливостей безпеки.

BurpSuite містить такі ключові компоненти:

– перехоплюючі проксі;
– інструмент repeater;
– інструмент sequencer;
– інструмент intruder;
– розширюваність, що дозволяє вам легко писати ваші власні плагіни.

Перед початком проведення тесту та перехоплення запитів мобільного додатка було проведено налаштування проксі-сервера на платформі BurpSuite, здійснено налаштування проксі на мобільному пристрої. Встановивши програму Burpsuite в режим Intercept, вдалося перехопити запит на автентифікацію.

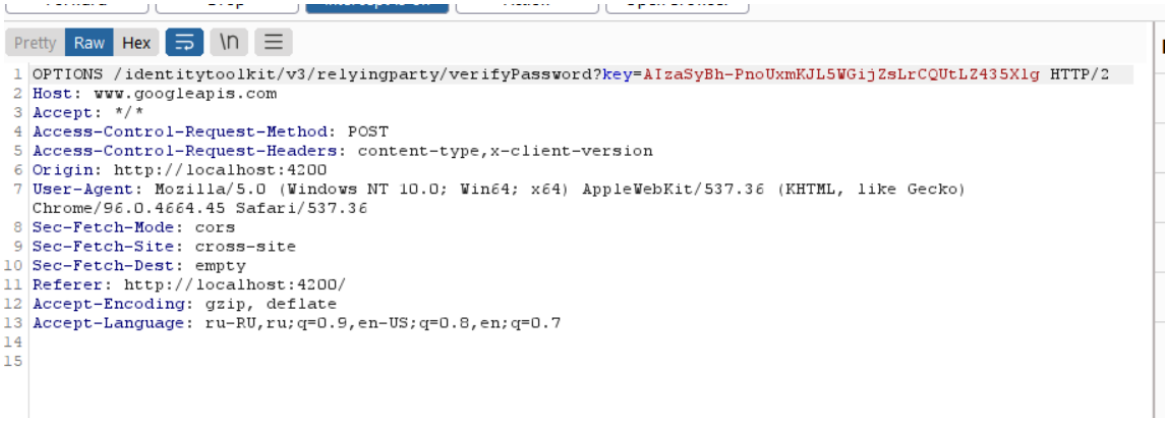


Рисунок 4.5 – Результат перехоплення запиту до серверу

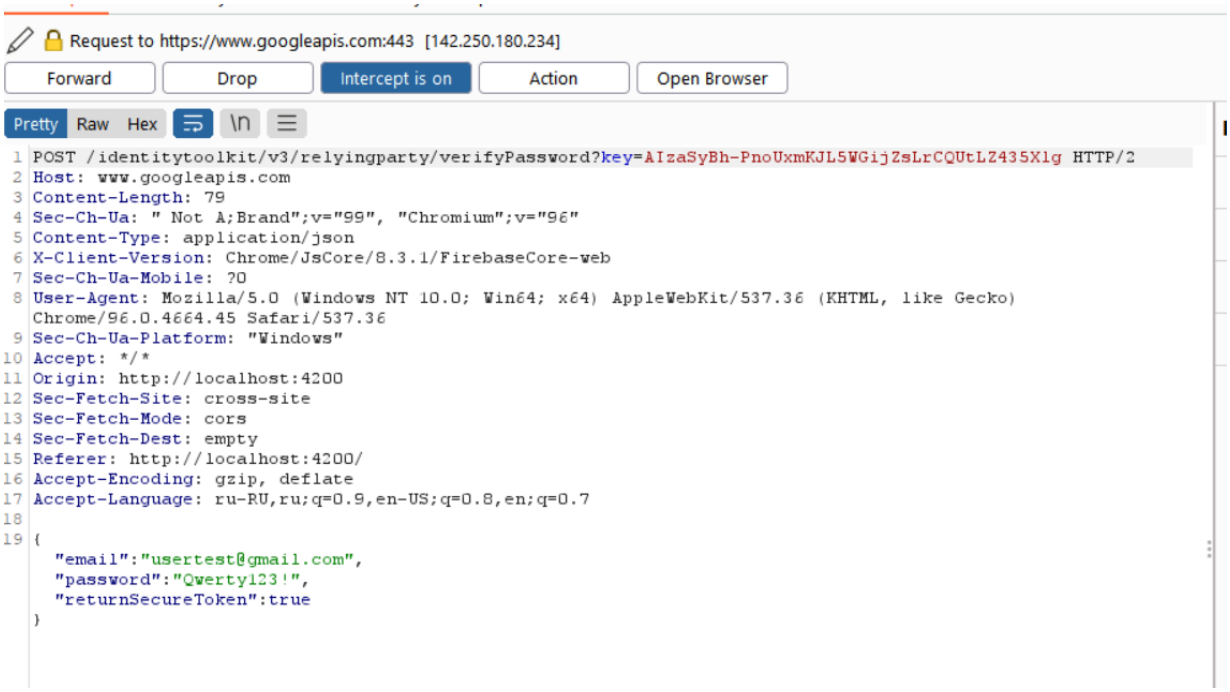


Рисунок 4.6 – Результат перехоплення відповіді від сервера

Результати вищевказаного тесту представлені у вигляді інформації облікового запису для входу, яка надсилається у вигляді оригінального тексту, створює можливість крадіжки даних та завдання шкоди користувачеві. Підсумок дослідження вразливості наведено в таблиці 6

Таблиця 4.5 – Результат дослідження М3

Код	М3
Вразливість	Небезпечне спілкування
Рівень ризику	Високий
Вплив	Крадіжка конфіденційної інформації, порушення конфіденційності, порушення прав користувачів.
Рекомендації	1. Використовування надійного шифрування надісланих даних. 2. Використовування SSL / TLS для зв'язку між сервером і клієнтом.

4.4.4 Небезпечна аутентифікація М4

Небезпечна аутентифікація – це слабкість програми керування користувачами програми. Слабкі сторони, які виникають через користувачів,

які не мають права доступу до функцій програми без проведення аутентифікації. Це можна зробити, минаючи додаток і використання слабких місць у процесі аутентифікації програми.

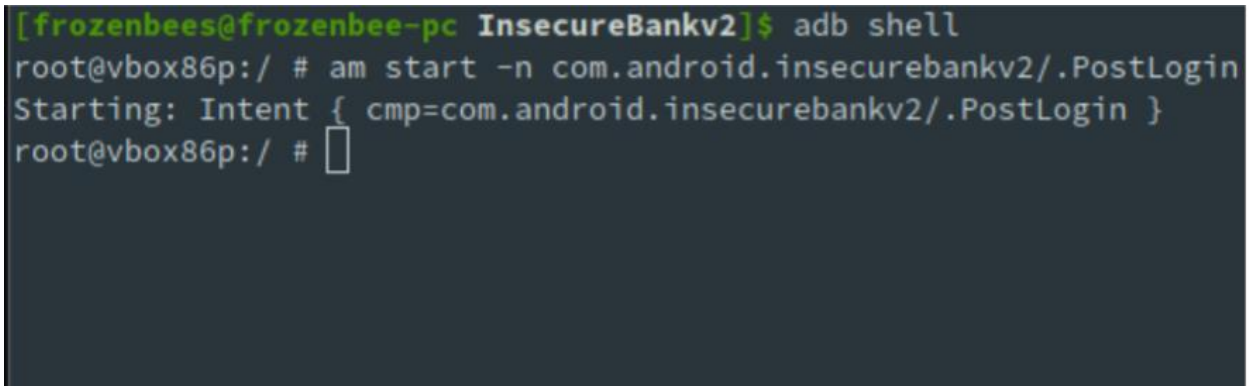


Рисунок 4.7 – Приклад тестування небезпечної аутентифікації

Отримані результати дослідження є обхідними логінами, які можна виконати, щоб користувачі могли перейти на головну сторінку програми без аутентифікації. Підсумок дослідження вразливості наведено в таблиці 6.

Таблиця 4.6 - Результат дослідження M4

Код	M4
Вразливість	Небезпечна аутентифікація
Рівень ризику	Високий
Вплив	Крадіжка особистих даних, порушення прав доступу до даних
Рекомендації	1. Обов'язково використовувати android: exported = true. 2. Переконатися, що вся автентифікація виконується на стороні сервера, а не локально в програмі

4.4.5 Не вистачає криптографії M5

Розглянемо для вивчення даної вразливості приклад файлу на малюнку 4.8, створеного за допомогою методів реверс-інженерії. Файл містить клас, який виконує методи шифрування та розшифрування

```
ublic class FastCrypto

 static
 {
   System.loadLibrary("fastcrypto");
 }

 public static native byte[] decrypt(byte[] paramArrayOfByte1, byte[] paramArrayOfByte2);

 public static native byte[] encrypt(byte[] paramArrayOfByte1, byte[] paramArrayOfByte2);

 public static byte[] jdMethod_void(String paramString)
 {
   try
   {
     paramString = MessageDigest.getInstance("MD5").digest(paramString.getBytes());
     return paramString;
   }
   catch (NoSuchAlgorithmException paramString)
   {
     for (;;)
     {
       paramString.printStackTrace();
       paramString = new byte[0];
     }
   }
 }
```

Рисунок 4.8 – Погана реалізація шифрування

Результати, отримані під час тестування слабких сторін використання криптографії, полягають у поганій криптографічній реалізації, тому її легко розшифрувати. Підсумок дослідження вразливості наведено в таблиці 7.

Таблиця 4.7 - Результат дослідження M5

Код	M5
Вразливість	Не вистачає криптографії
Рівень ризику	Високий
Вплив	Крадіжка особистих даних, порушення прав доступу до даних
Рекомендації	1. Уникання зберігання конфіденційних даних у внутрішній пам’яті. 2. Використовування криптографічних стандартів за останні 10 років. 3. Використовування надійних криптографічних алгоритмів відповідно до рекомендацій NIST.

4.4.6 Небезпечна авторизація M6

Питання авторизації має тісний зв'язок з проблемою аутентифікації і іноді поєднується. Керування неправильною авторизацією може призвести до несанкціонованого використання функції та може спричинити проблеми для інших користувачів.

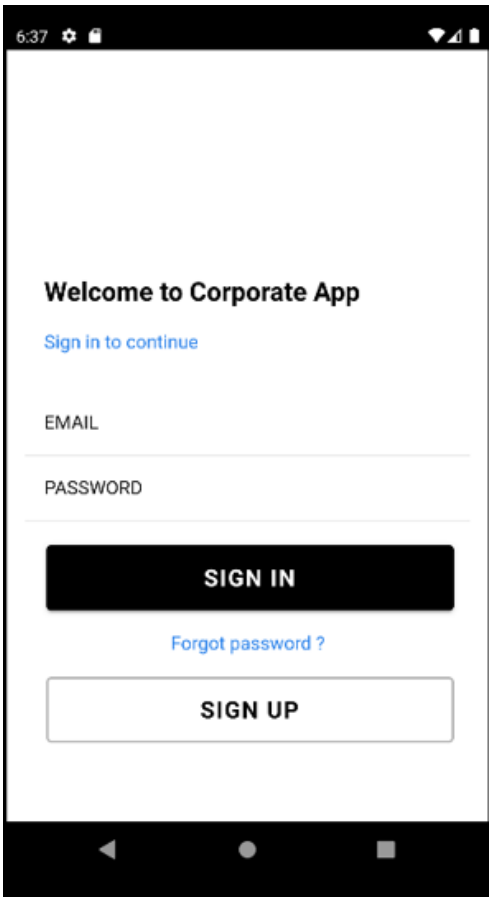


Рисунок 4.9 – Екран авторизації

За результат дослідження не було виявлено неправильної авторизації та отримання несанкціонованого доступу до функцій додатку.

Розглянувши питання проблеми авторизації, можна висунути підсумки, наведені в таблиці 4.8.

Таблиця 4.8 - Результат дослідження М6

Код	М6
Вразливість	Небезпечна авторизація
Рівень ризику	Високий
Вплив	Крадіжка особистих даних, порушення прав доступу до даних
Рекомендації	1. Переконання, що права доступу можна отримати лише з внутрішньої системи. 2. Внутрішня система повинна мати можливість перевіряти кожен запит, що надходить. 3. Не використовувати сховище чи вихідний код для встановлення дозволів.

4.4.7 Погана якість коду М7

Погана якість коду може призвести до помилок у програмі, тому програма не буде працювати, оскільки вона навіть повинна припинити роботу. Програми, які не можуть фільтрувати вхідні дані, можуть змусити безвідповідальні сторони запускати служби без необхідності аутентифікації або авторизації, змінювати робочий процес програми та робити те, що вони хочуть. На рисунку 4.10 можна побачити приклад тестування вразливості М7.

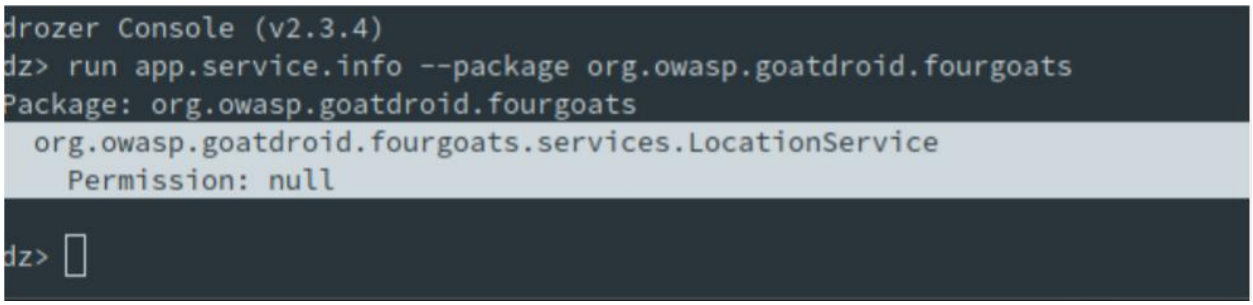


Рисунок 4.10– приклад тестування М7

Результатами дослідження низької якості коду є сервіси програм, які можна запускати через програми чи інші джерела, крім самої програми, не потребують аутентифікації навіть запущених програм. Підсумок дослідження вразливості наведено в таблиці 4.9.

Таблиця 4.9 - Результат тестування M7

Код	M7
Вразливість	Погана якість коду
Рівень ризику	Високий
Вплив	Крадіжка особистих даних, порушення прав доступу до даних
Рекомендації	1. Написання хорошого коду відповідно до документації і простий для розуміння. 2. Використовування фільтрації всіх введених даних у програмі. 3. Звернення уваги на використання дозволів на програму.

4.4.8 Підробка коду M8

Підробка коду – це проблема, яка виникає з програмою через зміну та підробку коду програми іншою стороною. Це може спричинити зміни в логіці та запуску програми, щоб неавторизовані сторони могли отримати вигоду від зміни коду програми. Приклад тестування вразливості M8 можна побачити на рисунку 4.11

Рисунок 4.11 - приклад тестування M8

Результатом дослідження фальсифікації поганого коду є те, що процеси і логіку програми можна змінити за бажанням, щоб програма більше не виявляла корінь пристрою. У таблиці 10 наведено підсумок результатів тестування проблеми підроблення коду.

Таблиця 4.10 - Результат тестування M8

Код	M8
Вразливість	Підробка коду
Рівень ризику	Високий (важкий)
Вплив	Втрата доходу через піратство, псування репутації.
Рекомендації	1. Програма повинна мати можливість перевірити зміни або доповнення до коду в програмі. 2. Використання захисту від несанкціонованого доступу.

4.4.9 Зворотна інженерія M9

Зворотна інженерія – це техніка, яка широко використовується для внесення змін до поведінки та аналізу вихідного коду в області розробки додатків. Використовуючи методи зворотного інжинірингу, кожна сторона може отримати важливу інформацію про програму, починаючи з потоку програми, алгоритмів програми, використовуваної криптографії, інформації про серверний сервер та іншу цінну інформацію. Результати тестування на рисунку 4.12 – 4.14

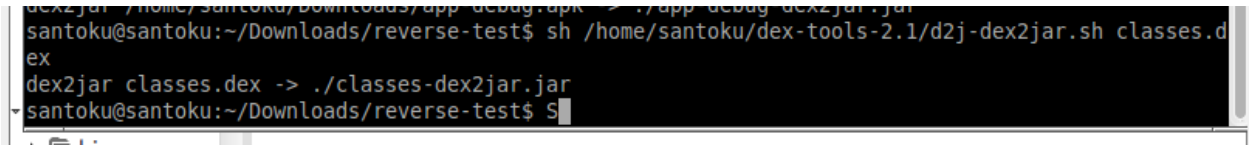


Рисунок 4.12 – Виконання розархівації мобільного додатку

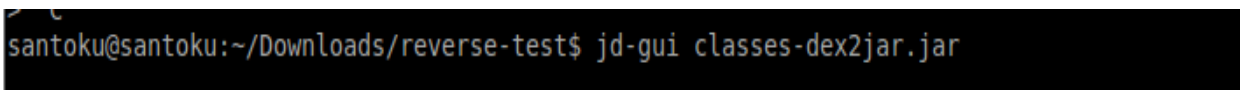


Рисунок 4.13 – Виконання декомпіляції коду

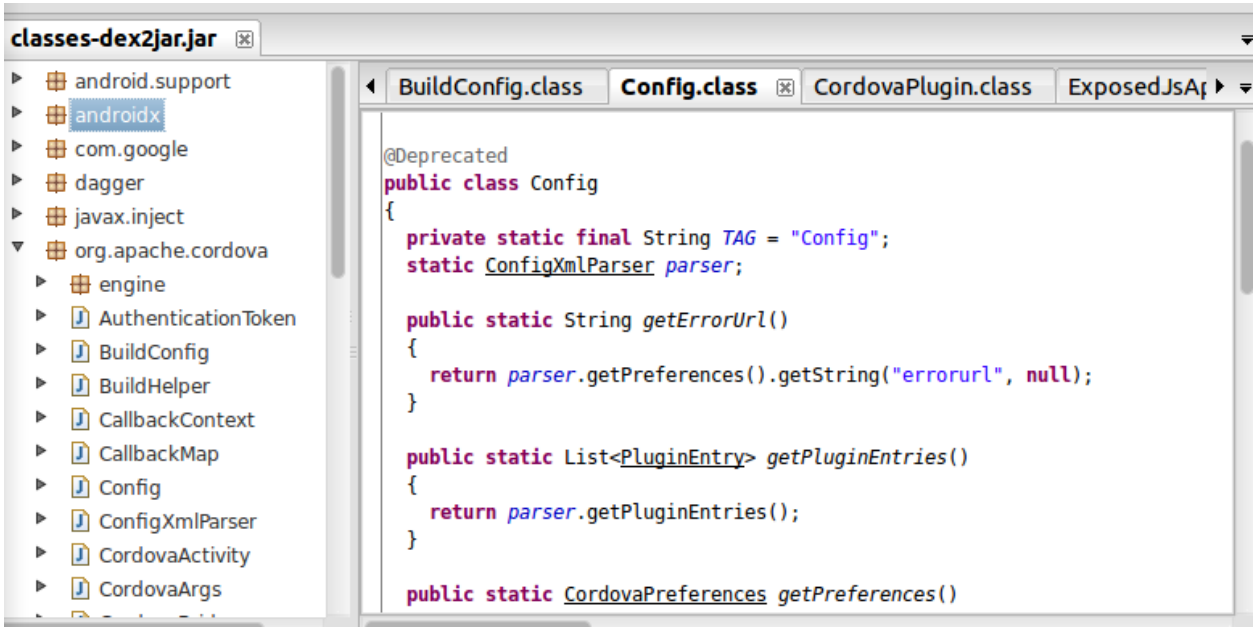


Рисунок 4.14 – Тестування M8

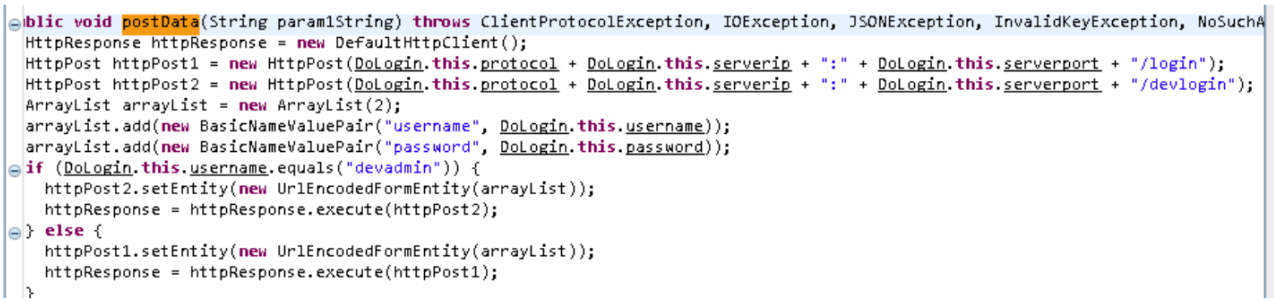
Результатом дослідження зворотного інжинірингу є важливою інформацією з програми, а саме конфігурація та важливі мета дані додатку. Підсумок дослідження вразливості наведено в таблиці 4.11.

Таблиця 4.11 - Результат тестування M9

Код	M9
Вразливість	Зворотне інжиніринг
Рівень ризику	Середній
Вплив	Крадіжка особистих даних, крадіжка інтелектуальної власності та знищення серверної частини.
Рекомендації	за допомогою інструменту обфускації

4.4.10 Зовнішня функціональність M10

Сторонні функції, які зазвичай зустрічаються в програмах, є бекдорами. Цей бекдор, створений розробником у програмі, розроблений, він може бути спрямований на полегшення розробникам покращення програми, коли вона була пошкоджена, але також може використовуватися для проникнення в системи чи програми зі зловмисними цілями. Результати проведення дослідження на рисунку 4.15.



```
blic void postData(String param1String) throws ClientProtocolException, IOException, JSONException, InvalidKeyException, NoSuchA
HttpResponse httpResponse = new DefaultHttpClient();
HttpPost httpPost1 = new HttpPost(DoLogin.this.protocol + DoLogin.this.serverip + ":" + DoLogin.this.serverport + "/login");
HttpPost httpPost2 = new HttpPost(DoLogin.this.protocol + DoLogin.this.serverip + ":" + DoLogin.this.serverport + "/devlogin");
ArrayList arrayList = new ArrayList(2);
arrayList.add(new BasicNameValuePair("username", DoLogin.this.username));
arrayList.add(new BasicNameValuePair("password", DoLogin.this.password));
if (DoLogin.this.username.equals("devadmin")) {
  httpPost2.setEntity(new UrlEncodedFormEntity(arrayList));
  httpResponse = httpResponse.execute(httpPost2);
} else {
  httpPost1.setEntity(new UrlEncodedFormEntity(arrayList));
  httpResponse = httpResponse.execute(httpPost1);
}
```

Рисунок 4.15 – Результат тестування M10

Результатом дослідження зовнішніх функцій представлені у вигляді бекдора в програмі у функції входу в програму, щоб розробник або ті, хто це знає, могли отримати доступ до головної сторінки програми, використовуючи лише ім’я користувача «devadmin», не вимагаючи пароля.

Зведення результатів дослідження питань авторизації пояснюється в таблиці 4.12.

Таблиця 4.12 - Результат тестування M10

Код	M10
Вразливість	Сторонній функціонал
Рівень ризику	High
Вплив	Несанкціонований доступ до конфіденційних функцій та крадіжка інтелектуальної власності
Рекомендації	1. Перевірка конфігурації програми, для знаходження прихованих функції. 2. Не введено пробний код у виробничій програмі. 3. Перевірка журналів програми

ВИСНОВОК

Частка витоків даних через недостатню безпеку додатків істотно зростає, і ця тенденція посилюється. Веб-додатки та мобільні додатки особливо вразливі для атак. До них додаються API-інтерфейси – програмні інтерфейси додатків.

Кіберзлочинці використовують методи для навмисного використання можливих уразливостей у програмному забезпеченні додатків. Класичні системи IT-безпеки, такі як мережні брандмауери або системи запобігання вторгненням, не здатні виявляти такі атаки. Прості мережні брандмауери здатні лише блокувати чи дозволяти певні порти TCP чи UDP.

Атаки на прикладному рівні з використанням протоколу передачі гіпертексту (HTTP/HTTPS) не виявляються і, отже, не можуть бути заблоковані превентивно. Крім того, навіть брандмауерів нового покоління замало. Зазвичай вони не діють як зворотні проксі-сервери і тому не здатні ідентифікувати та запобігати всім атакам, особливо націленим на програми. Вони не здатні аналізувати зашифровані пакети даних та блокувати потенційні загрози.

Сучасні версії мобільних ОС мають різноманітні вбудовані механізми захисту. Так, за замовчуванням усім встановленим програмам дозволено працювати лише з файлами у власних домашніх каталогах, а права користувача неможливо редагувати будь-які системні файли. Незважаючи на це, помилки, допущені розробниками при проектуванні та написанні коду мобільних додатків, призводять до брешів у захисті та відчиняють двері кіберзлочинцям.

Тестування безпеки програм виявляє проломи в безпеці мобільних додатків.

В даній атестаційній роботи були досліджені сценарії та ризики використання мобільних пристроїв у корпоративному середовищі, проведений

аналіз загроз безпеки мобільних додатків в корпоративній мережі та проведено тестування мобільних додатків на предмет виявлення вразливостей за методологією OWASP Mobile Top 10.

OWASP Mobile Top 10 – це рейтинг із десяти найбільш небезпечних ризиків інформаційної безпеки для мобільнихдодатків, складений спільнотою експертів галузі. Для кожного пункту рейтингу ризик розраховується експертами на основі методики OWASP Risk Rating Methodology і включає оцінку за такими критеріями: поширеність відповідних уразливостей у додатках (Weakness Prevalence), складності їх виявлення (Weakness Detectability) та експлуатації (Exploitability), а також а також критичності наслідків їх експлуатації (Technical Impacts).

Керуючись цією методологією та в використанням сучасного програмного інструментарію були проаналізовані підходи до виявлення вразливостей, оцінена їх критичність та запропоновані засоби захисту та пропозиції щодо їх уникнення на стадії розробки.

Оцінка захищеності проводилася методами чорної та білої скриньки з використанням допоміжних автоматизованих засобів. Метод чорного ящика полягає у проведенні робіт з оцінки захищеності інформаційної системи з боку зовнішнього атакуючого без попереднього отримання будь-якої додаткової інформації про неї від власника. При аналізі методом білої скриньки для оцінки захищеності інформаційної системи використовуються всі наявні дані про неї, включаючи вихідний код програм.

Уразливості коду ми розділили на дві групи: вразливості у коді мобільного додатка (помилки, яких припустився програміст при розробці); помилки реалізації механізмів захисту (з'являються у системі ще на етапі проектування).

Рівень ризику вразливостей оцінювався виходячи зі ступеня впливу потенційної атаки на дані користувача і сам додаток, а також з урахуванням складності проведення атаки.

ПЕРЕЛІК ДЖЕРЕЛ ТА ПОСИЛАНЬ

1. BYOD adoption is growing rapidly [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.helpnetsecurity.com/2020/07/09/byod-adoption-is-growing-rapidly-but-security-is-lagging/

2. Bring Your Own Device (BYOD): Bitglass' 2020 Personal Device Report [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.bitglass.com/blog/bitglass-2020-personal-device-report

3. BYOD, CYOD, COPE: What Does It All Mean? [Електронний ресурс] – 2016 – Режим доступу до ресурсу: http://www.business2community.com/mobile-apps/byod-cyod-cope-mean-01025828#KFTYTi88zKb8pP9F.97

4. Does Your Business Need an Enterprise Mobility Strategy? [Електронний ресурс] -2016 – Режим доступу до ресурсу: https://enterprisemobile.com/does-your-business-need-an-enterprise-mobility-strategy/

5. Статистика [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/?sphrase_id=93493#id6.

6. Тестування [Електронний ресурс]. - 2019 Режим доступу до ресурсу: https://www.ptsecurity.com/ww-en/analytics/corp-vulnerabilities-2019/.

7. Аналітика [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.ptsecurity.com/ww-en/analytics/vulnerabilities-corporate-networks-2020/.

8. Перелік загроз [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.vaadata.com/blog/how-to-strengthen-the-security-of-your-mobile-applications-to-counter-the-most-common-attacks/.

9. Перелік загроз [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.vaadata.com/blog/how-to-strengthen-the-security-of-your-mobile-applications-to-counter-the-most-common-attacks/.

10. Безпека корпоративних додатків [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.akkamal.kz/sites/default/files/downloads/enterprise_app_secure.pdf.

11. Перелік загроз [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.cypressdatadefense.com/blog/owasp-mobile-top-10-vulnerabilities/

12. What Are the Different Types of Mobile Apps? And How Do You Choose? [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://clevertap.com/blog/types-of-mobile-apps/

13. Comparing Native and Hybrid Applications with focus on Features', [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.diva-portal.org/smash/get /diva2:944058/FULLTEXT02.

14. Apache Cordova, The Apache Software Foundation [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https: //cordova.apache.org/.

15. Ionic Documentation Overview [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://ionicframework.com/docs/v1/overview

16. Google LLC, "Angular," [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://angular.io/.

17. Comparison of mobile application development technologies', [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.theseus.fi/bitstream/handle/10024/336597/Comparison%20of%20mobile%20application%20development%20technologies.pdf? sequen ce=2

18. Как провести тестирование на безопасность Android-приложения [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://dou.ua/lenta/articles/android-app-secutity-testing/.

19. OWASP Mobile security testing guide (MSTG). [Електронний ресурс]. – 2021 — Режим доступу до ресурсу: https://github.com/ OWASP/owasp-mstg

20. Privacy and Security in Firebase [Електронний ресурс]. – 2021 – Режим доступу до ресурсу: https://firebase.google.com/support/privacy

21. Owasp Mobile Top 10 [Електронний ресурс]. – 2021 – Режим доступу до ресурсу: - https://owasp.org/www-project-mobile-top-10/

22. Vetting the Security of Mobile application. [Електронний ресурс]. – 2019 – Режим доступу до ресурсу: https://doi.org/10.6028/NIST.SP.800- 163r1.

23. Mobile Device Fundamentals, Version 4.0. [Електронний ресурс]. – 2019 – Режим доступу до ресурсу: https://www.niap-ccevs.org/MMO/PP/pp_mdm_v4.0.pdf.

24. Protection Profile for Mobile Device Fundamentals, Version 4.0. [Електронний ресурс]. – 2019 – Режим доступу до ресурсу: https://www.niap-ccevs.org/MMO/PP/pp_mdm_v4.0.pdf..

25. Information technology. Security technique's Application Security, first edition. [Електронний ресурс]. – 2021 – Режим доступу до ресурсу: https://www.iso.org/standard/60804.html.

26. Analysis of testing approaches to Android mobile application vulnerabilities [Електронний ресурс]. – 2019 – Режим доступу до ресурсу: http://ceur-ws.org/Vol-2577/paper22.pdf.

27. Quick heal annual threat report 2019. [Електронний ресурс]. – 2019 – Режим доступу до ресурсу: https://www.google.com/url?sa=t&rct=Annual-Threat-Report-2019.pdf&usg=AOvVaBxp0Txjy0ExKPWN.