**App Name :** PanCakeswap

**Package Name :** pancakeswap.development.team

**Version Code :** 1

**Version Name :** 1.0

**Compile SDK version :** 31

**Build version code :** 31

**Minimum SDK version :** 21

**Target SDK version :** 31

1. This application is being validated for phishing
2. Let us understand the definition of phishing

Applications which try to impersonate the other applications and steal user sensitive information without user acknowledgement is known as phishing.

1. Permissions responsible for phishing :

android.permission.INTERNET

1. Lets start reversing it.
2. We will check phishing related permission in this app.
3. For that we will check androidmanifest.xml

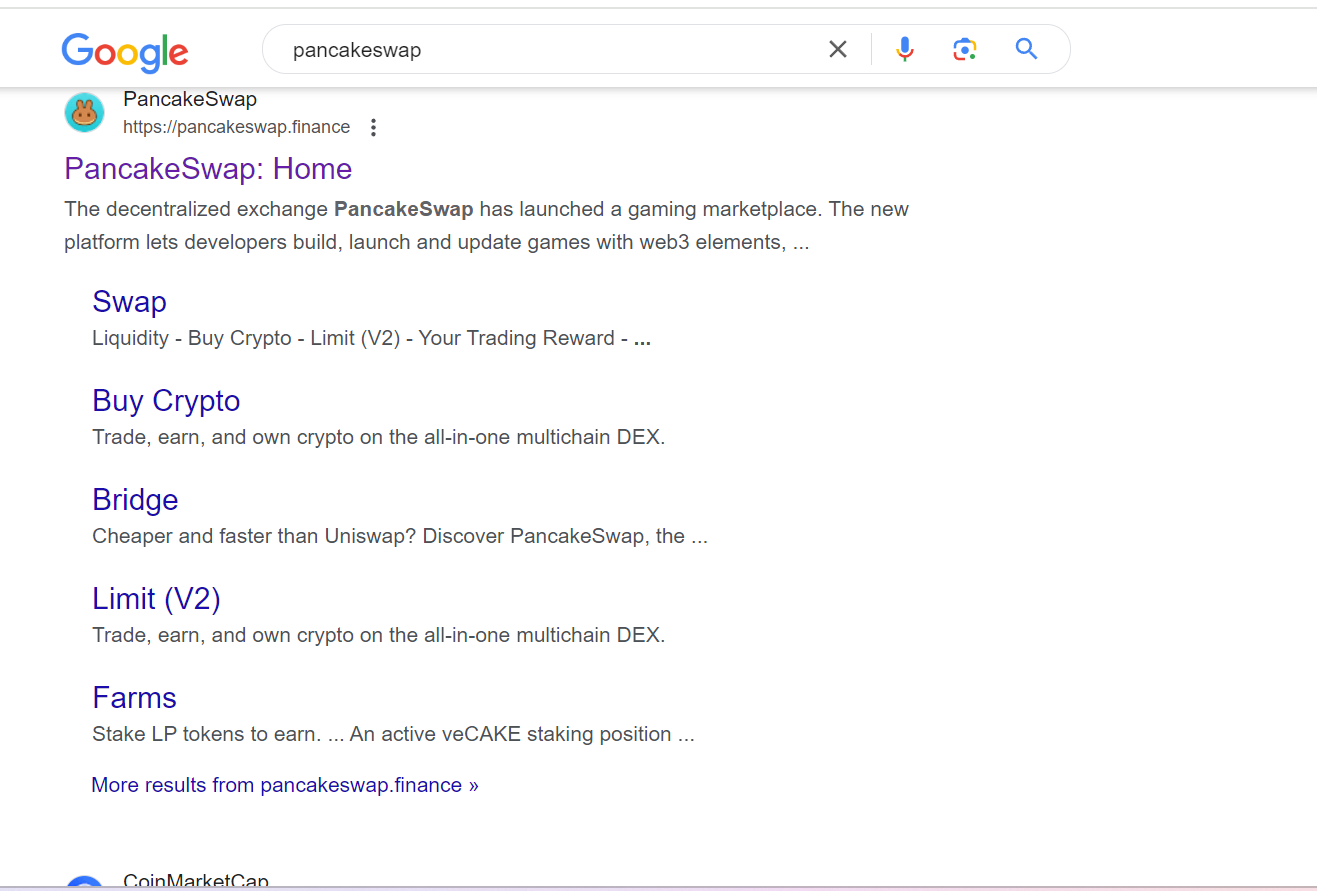
A screenshot of a computer

Description automatically generated

Here we can see that only internet permission is there

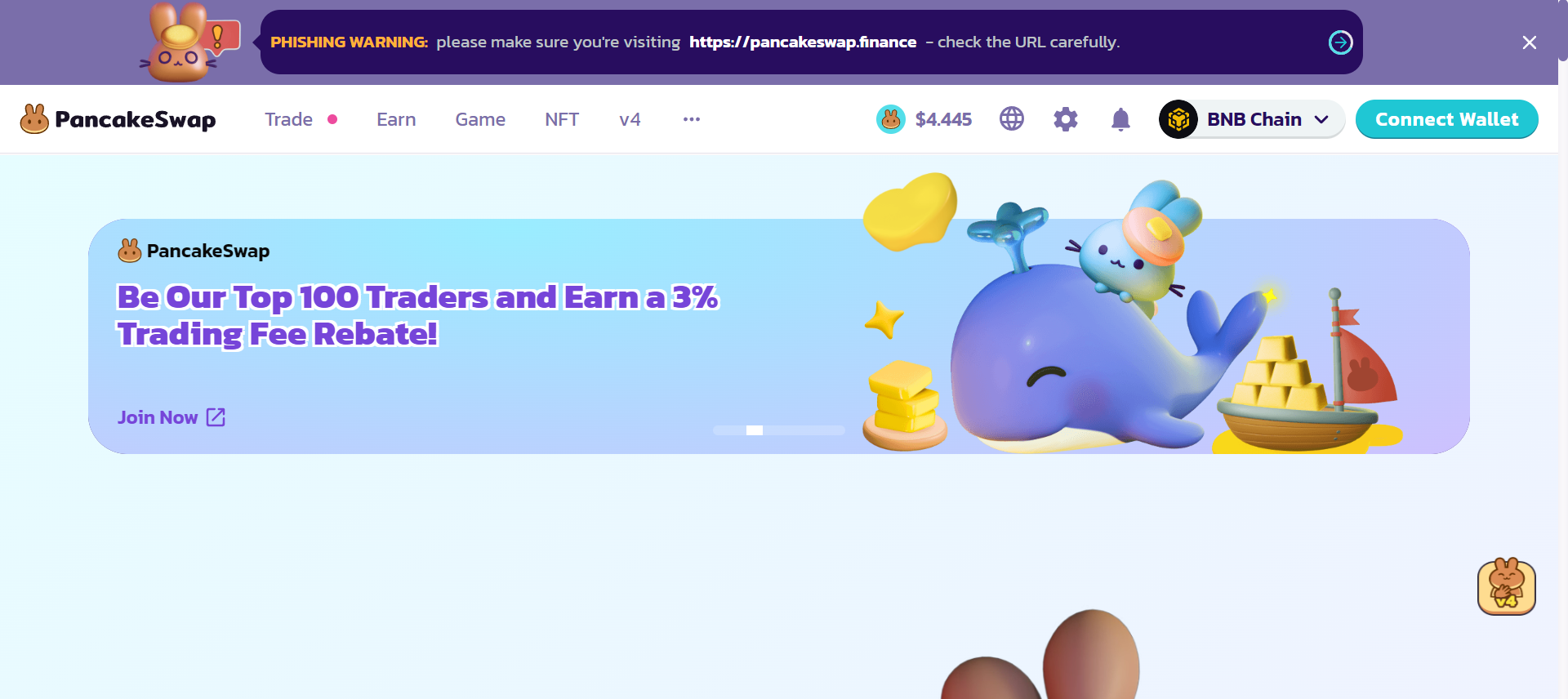
So we will check for phishing

1. First we will do OSINT part and try to find out which type of application it is.
2. We will search pancakeswap on google and find out if there is any google play link is available or not.



On google we see that there is no any link for downloading app from google playstore.

1. Now will check google playstore link on website.



Here on its website we can see that there is no link for downloading app from playstore.

And after exploring the site it seems that this app is crypto wallet app.

1. Now we will check app icon from mipmap folder as shown below.

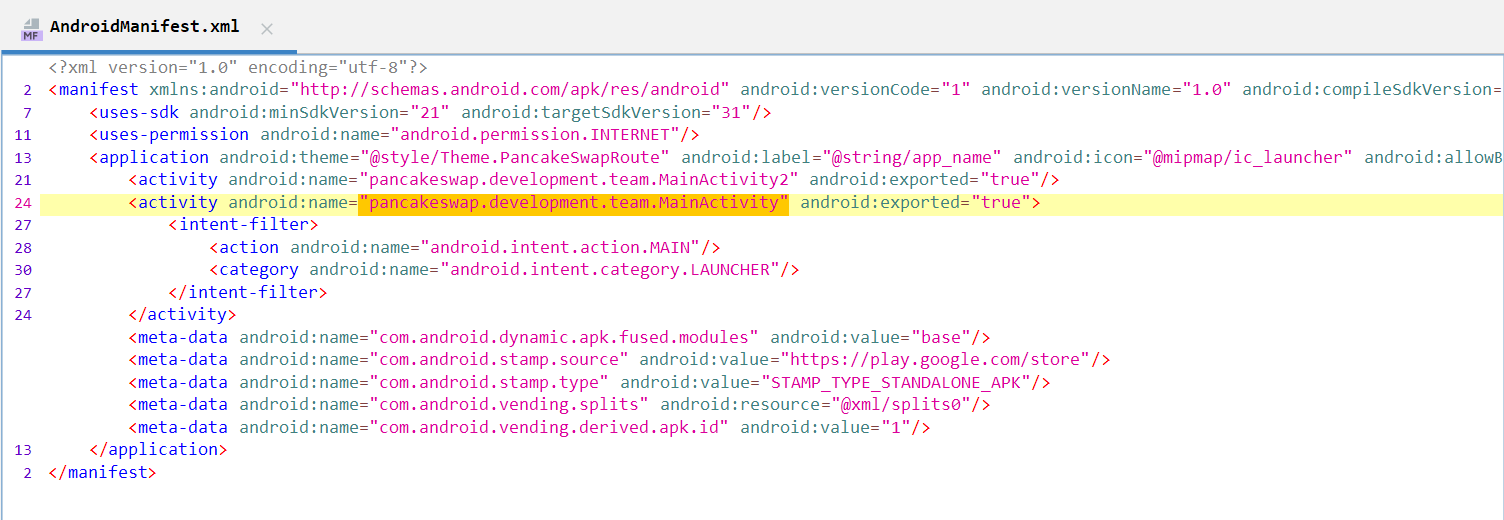
A screenshot of a computer

Description automatically generated

Here we can see that this website has no link for downloading app from playstore and also this app is trying to use website icon as app icon.

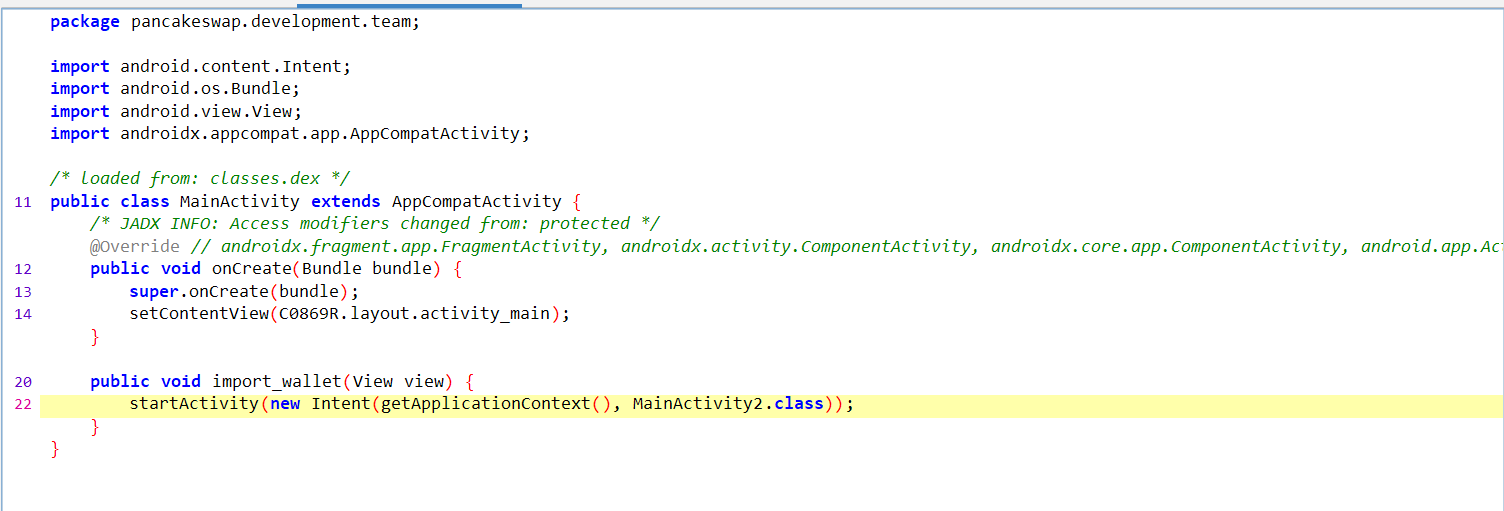
So, there might be chance that this app is doing phishing.

1. Now we will do static part analysis.
2. Since this app is crypto wallet app, so will start from launcher activity.
3. To know which activity is launcher activity, we will check androidmanifest.xml file as shown below.



Here we can see that MainActivity is launcher activity.

1. Now we will check MainActivity



Here we can see that MainActivity2.class is being started by passing intent.

1. Now we will check MainActivity2.class

A screenshot of a computer

Description automatically generated

Here we can see that Volley request is created where data is being sent.

From the above steps, we can conclude that this app is phishing app.