Challenge: Pinned

# Challenge Description:

This app has stored my credentials and I can only login automatically. I tried to intercept the login request and restore my password, but this seems to be a secure connection. Can you help bypass this security restriction and intercept the password in plaintext?

# Context:

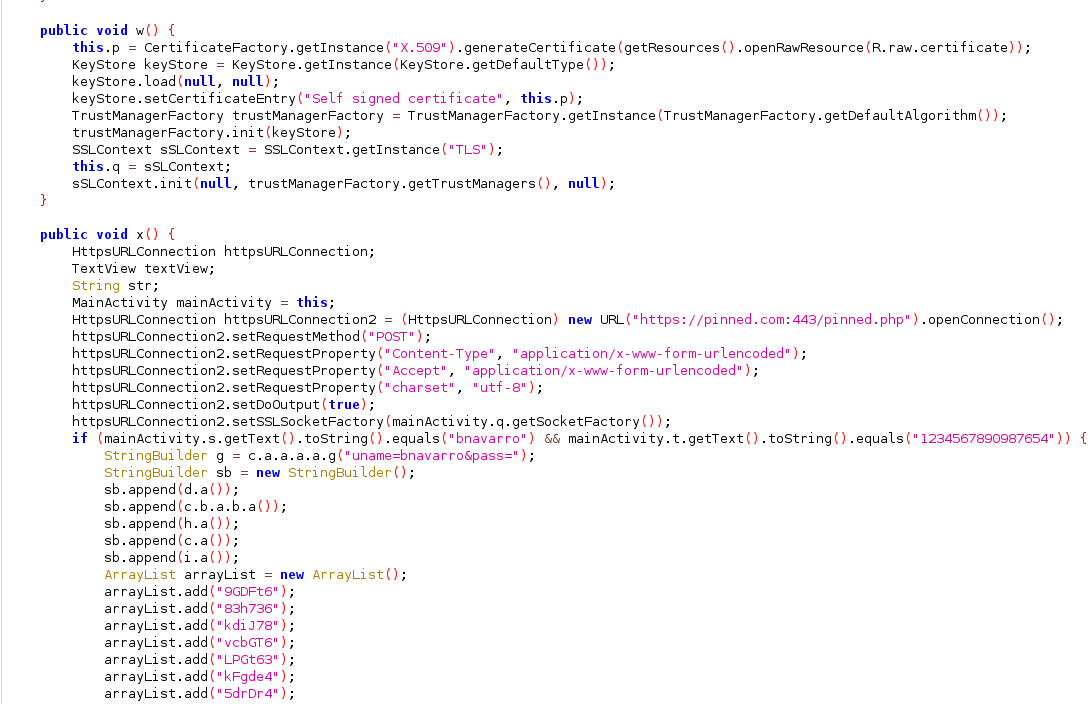
## You can either use jadx-gui for the unpacking of the apk file

## Or you can use MobSF, to run ,scan and monitor the apk file.

# Challenge:

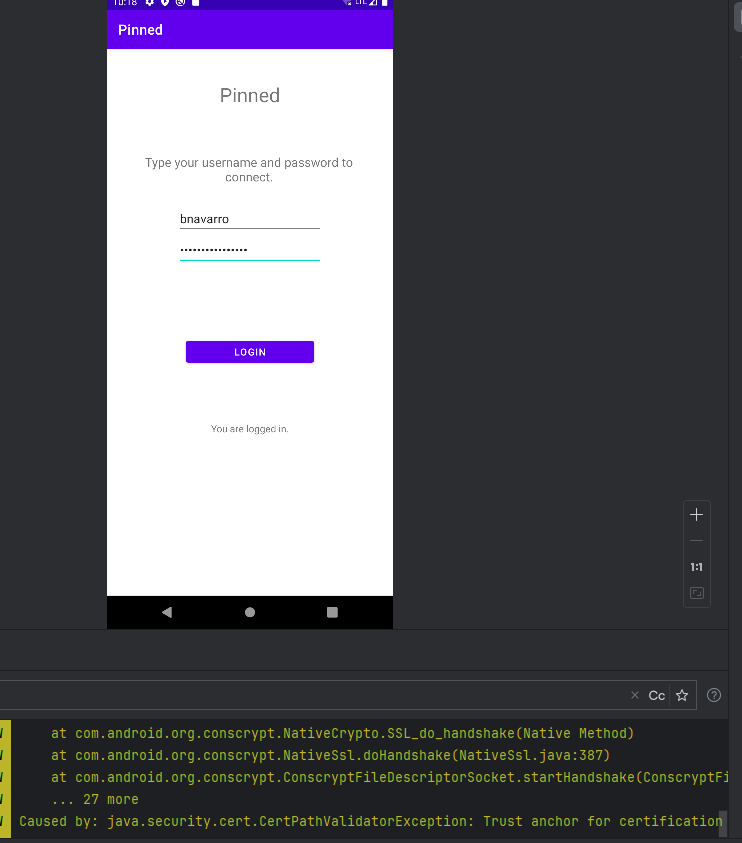
* For the use of jadx-gui after selecting the Pinned.apk file after extraction.

With jadx-gui i look around the unpacked files and i find the username and password needed to login into the actual apk,



Credentials are: bnavarro:1234567890987654

* I Ran the apk with Android Studio, it works but when i try to login i keep getting a certificate error.



* One way to bypass this would be to remove the certificate’ [s] that are pinned on the apk.

# Flag:

* Either use Frida to run the application with a Certificate unpinned script

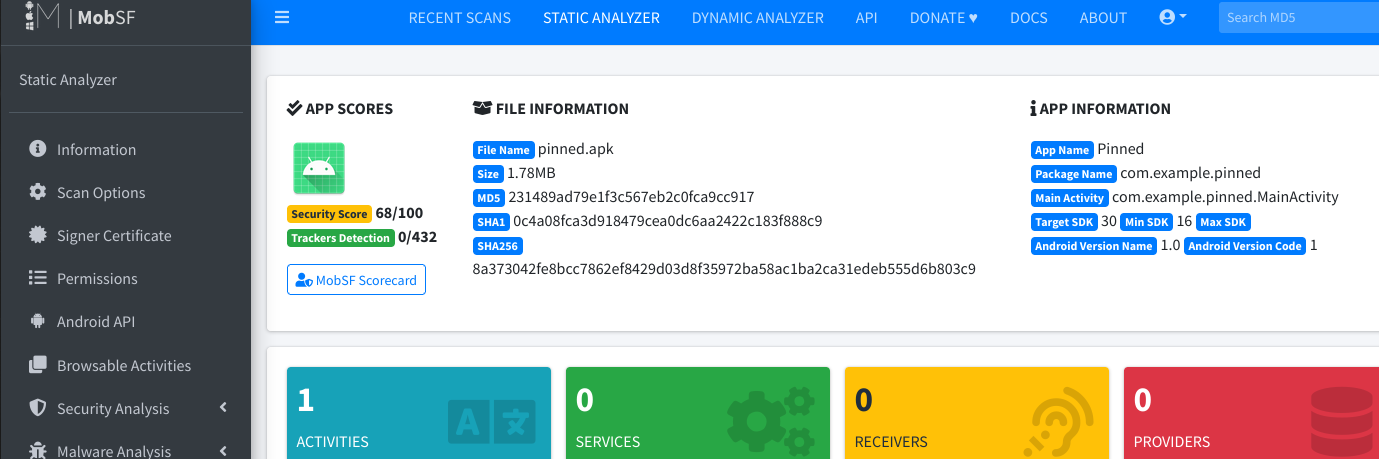
**’**[**https://github.com/httptoolkit/frida-interception-and-unpinning**](https://github.com/httptoolkit/frida-interception-and-unpinning)**’**

**Or**

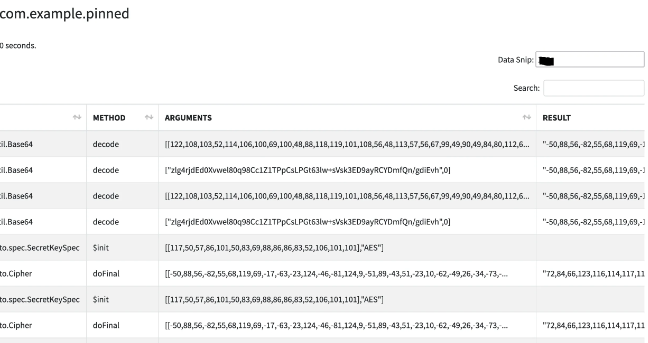
**‘**[**https://codeshare.frida.re/@sowdust/universal-android-ssl-pinning-bypass-2/**](https://codeshare.frida.re/@sowdust/universal-android-ssl-pinning-bypass-2/)**’**

## I Attempted this and it was successful after the correct configuration, you should also get a flag either via burp-suite or a MITM / proxy service you might have set up.

## To use The MobSF, first install and run the setup then, or just Use docker to run it knowing it will work, then place the apk into the upload section.



* In the Second Half we first look at the static analysis results, nothing interesting in the report, we then start with the dynamic analysis and get something interesting in the Live API monitor section.



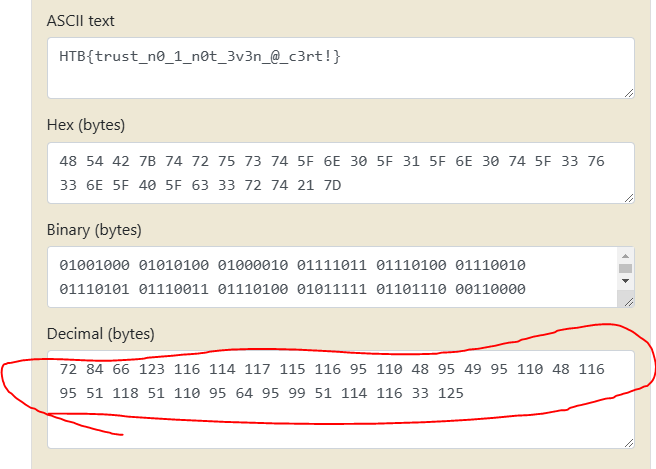
* After looking at the results I try to see if I can get any identification on what it might be. I finally came to the conclusion that it is Decimal (Bytes) that I need to convert to txt.

The evidence for this is that the result of [ 72,84,66,123,116 ] converted into text will be [ HTB{T ],

The full string of this strings is:



Fully Decoded we get :



* We get the flag : HTB{trust\_n0\_1\_n0t\_3v3n\_@\_c3rt!}

From Birdo