Penetration Testing Report

For

“Native-or-Naive”

S.NO.	Title	#
1.	Challenge Category	Android Pentesting
2.	Challenge Related Files	N/A
3.	File Link / Target IP	N/A

PROCEDURE

1. **Apk file is given**
2. **Test a little bit (after installing click once but it will give you the fake text)**
3. **Time for static analysis decompile apk using apktool or jadx whatever suits you.**
4. **So mainly there are 3 things to know getkey() , final_flag() and encryption function**
5. **They are processed but not shown in app**
6. **Checking helper.java gives hint that its using "AES/ECB/PKCS5Padding"**
7. **final_flag() fetch something from Java native library as well.**
8. **In JNI we get there there are**
    a. **HE{FAKE_PLACEHOLDER_FLAG_which_you_probably_got_using_strings}**
    b. **HAlsTYlQkfdNT1heeufZVMEs4qdIcP9ryR9QQXcrNSS/rMYV5rHJG/dEXiaht1pUK2wzh5qnj7u4iNcKekMG1Q==**
9. **And one char array in main.java file**
10. **Use these 3 as given order decrypt (flag,a+get_key()) toi get the final flag**

Flags:

S.No.	Flag - No.	Flag
1.	Flag 1	HE{Not_always_apk_Serctes_Are_in_java_files_or_maybe_they_are}