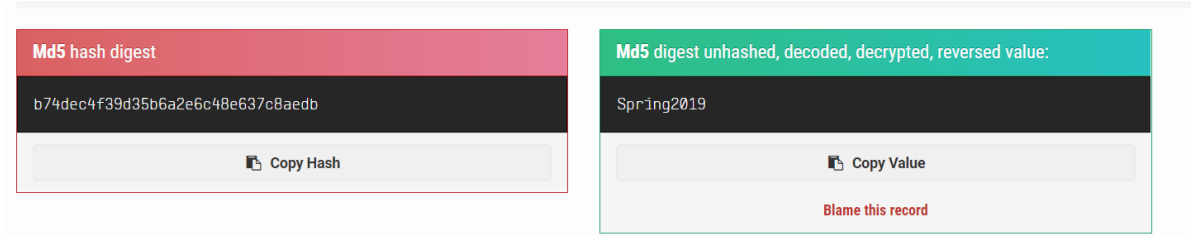
Q1.

First use jadx to disassemble the apk file and search for the flag.


```
14 public class MainActivity extends AppCompatActivity {
       /* access modifiers changed from: protected */
       @Override // androidx.core.app.ComponentActivity, androidx.appcompat.app.AppCompatActivity, androidx.fragment.app.FragmentActivity
15     public void onCreate(Bundle bundle) {
16         super.onCreate(bundle);
17         setContentView(R.layout.activity_main);
       }

20     public void submitPassword(View view) {
21         EditText editText = (EditText) findViewById(R.id.editText2);
25         if (DigestUtils.md5Hex(editText.getText().toString()).equalsIgnoreCase("b74dec4f39d35b6a2e6c48e637c8aedb")) {
27             ((TextView) findViewById(R.id.textView)).setText("Success! CTFlearn{" + editText.getText().toString() + "_is_not_secure!}");
           }
       }
   }
```

Then I decrype the string "b74de...." and get the result:



So the flag is:

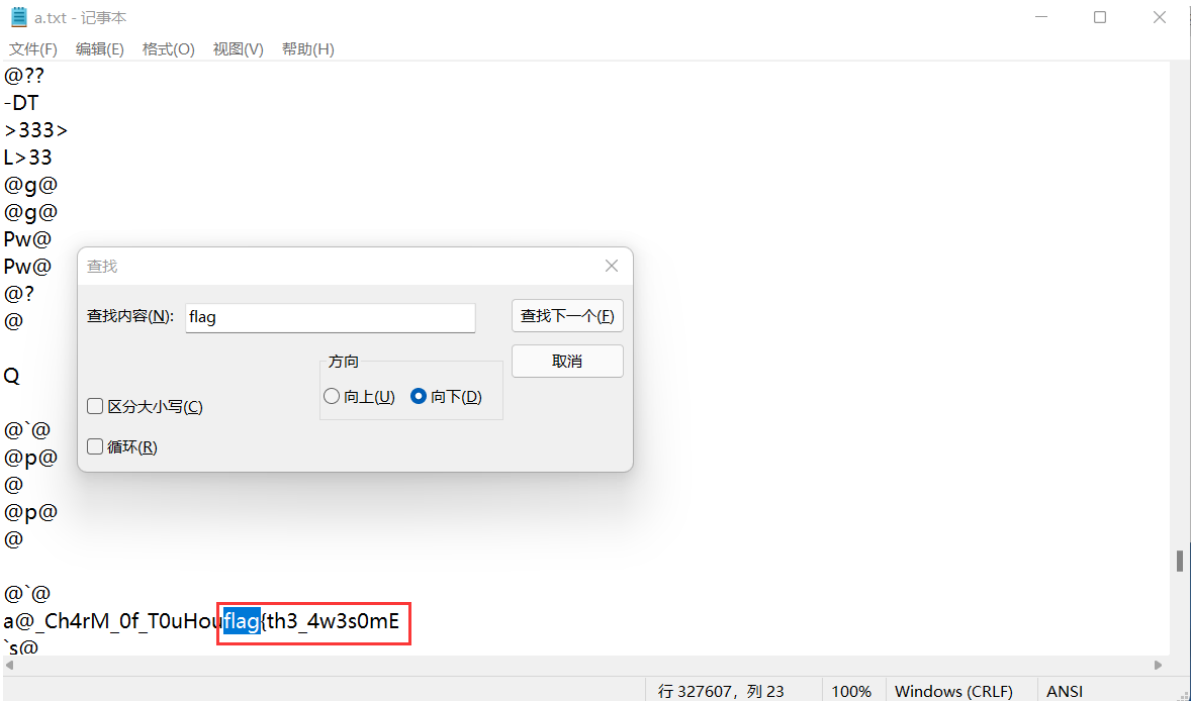
```
CTFlearn{Spring2019_is_not_secure!}
```

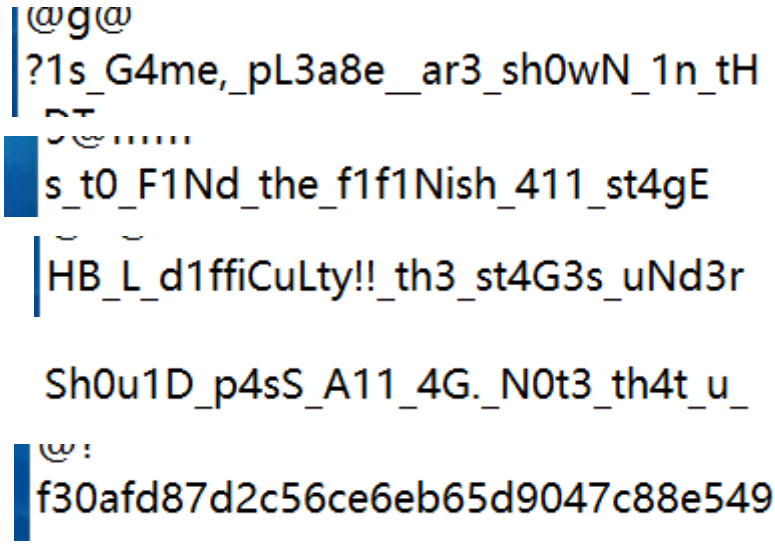
Q2

use strings tools to print all the strings in the exe file and write to a txt file.

```
strings C:\Users\联想\Desktop\week6-2\Taisei-1.3.108-windows-x86_64\taisei.exe
>a.txt
```

and try to find te flag:






```
_Ch4rM_0f_T0uHouflag{th3_4w3s0mE

1s_G4me,_pL3a8e__ar3_sh0wN_1n_tH

s_t0_F1Nd_the_f1f1Nish_411_st4gE

Sh0u1D_p4sS_A11_4G._N0t3_th4t_u_

_L_d1ffiCuLty!!_th3_st4G3s_uNd3r

f30afd87d2c56ce6eb65d9047c88e549

but since the flag is 32 chars long each, but the strings tools read 16 each
time, so the right half and left half is reversed!
After reverse it , I get the final flag.
```

```
flag{th3_4w3s0mE_Ch4rM_0f_T0uHou_ar3_sh0wN_1n_tH1s_G4me,_pL3a8e_f1Nish_411_st4gE
s_t0_F1Nd_the_f14G._N0t3_th4t_u_Sh0u1D_p4sS_A11_th3_st4G3s_uNd3r_L_d1ffiCuLty!!_
eb65d9047c88e549f30afd87d2c56ce6}
```