2014

Code Engn SmartApp 1

4.Z320

elttzero@gmail.com

Challenges : SmartApp 01

Author : 보안프로젝트 / Link

Korean :
키값을 찾으시오!

English :
Find a key

Download

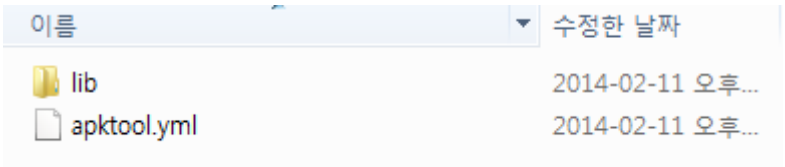
키값을 찾으라는 문제입니다.

1번 문제이기는 하나 2번문제를 바탕으로 작성하였습니다.

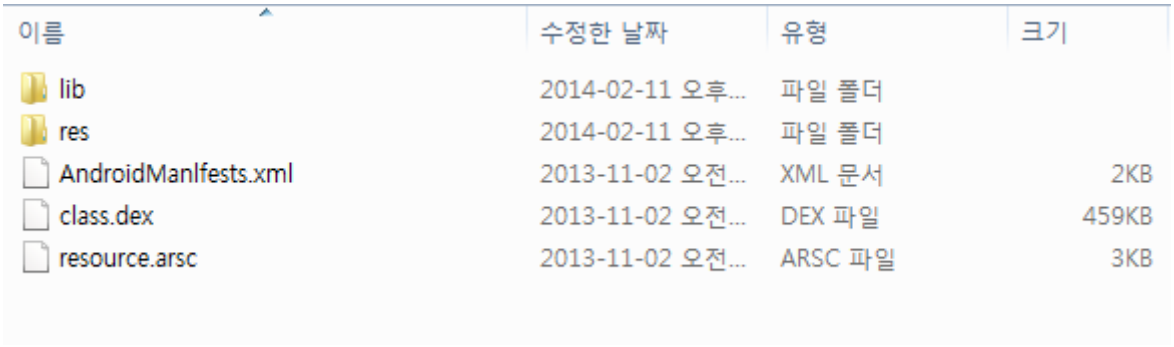
```
D:₩prv_rsrch₩android₩challenges₩01>adb install "SmartApp L01.apk"
file 'SmartApp L01.apk' does not contain AndroidManifest.xml
rm failed for /data/local/tmp/SmartApp L01.apk, No such file or directory

D:₩prv_rsrch₩android₩challenges₩01>
```

AVD에 apk파일을 설치하려고 하면 AndroidManifest.sml파일이 없다며 설치가 되지 않습니다.

실제 핸드폰에 설치하려고 해도 설치가 되지 않으며 비슷한 이유라고 판단하고 있습니다.



apktool을 이용하여 디코딩을 하면 lib와 apktool에 대한 정보만 있는 것을 확인할 수 있습니다

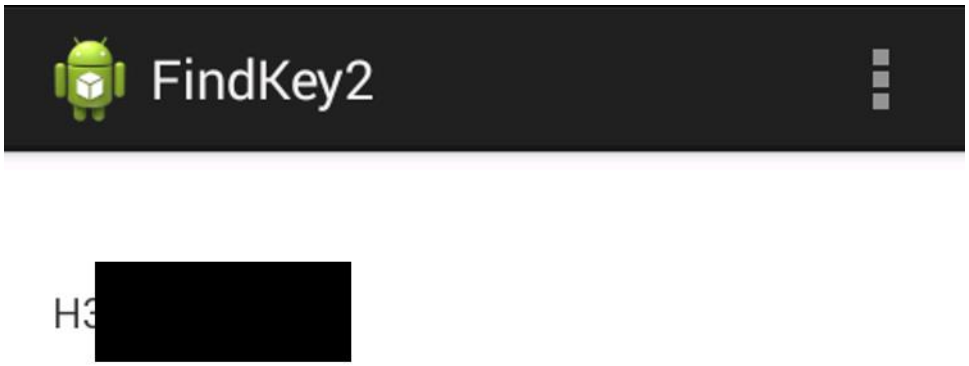


하지만 압축프로그램으로 언팩을 할 경우엔 파일이 몇 개 더 나오며 그중에 dex파일이 있는 것을 확인할 수 있습니다.

dex2jar를 이용해 jar파일로 만든 뒤 디코딩을 하게 되면 소스코드를 확인할 수 있습니다.

```
public void addListenerOnButton()
{
  this.button = ((Button)findViewById(2131230720));
  this.button.setOnClickListener(new View.OnClickListener()
  {
    public void onClick(View paramAnonymousView)
    {
      AlertDialog.Builder localBuilder = new AlertDialog.Builder(MainActivity.this);
      localBuilder.setPositiveButton("close", new DialogInterface.OnClickListener()
      {
        public void onClick(DialogInterface paramAnonymous2DialogInterface, int paramAnonymous2Int)
        {
          paramAnonymous2DialogInterface.dismiss();
        }
      });
      localBuilder.setTitle("Key");
      localBuilder.setMessage(Security.DecryptStr("-1aaa755a1e60915baff1d4cb64cb221a00000000000000000000000000000000"));
      localBuilder.show();
    }
  });
}
```

2번문제와 동일하게 Security.DecryptStr을 사용하여 복호화를 하는 것을 알 수 있으며 이를 2번문제의 문자열과 치환할 경우 키값이 나오리라 예상할 수 있습니다. 이에 2번 문제의 smali를 수정한 뒤 재빌드하여 설치한 뒤 실행하게 되면



2 번문제의 키값과는 다른 값이 나오게 됩니다.