l春秋 Reverse Smali题 150pt

原创

勇敢的鑫9 于 2018-01-10 19:51:16 发布 447 收藏

分类专栏： CrackMe 文章标签： reverse PCTF i春秋Smali

本文链接：https://blog.csdn.net/hujiuding/article/details/79027604


CrackMe 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

l春秋 Reverse

1. Smali 150pt

   先用工具Smali2JavaUI将

```
public class Crackme {
    private String str2 = "cGhyYWNrICBjdGYgMjAxNg==";

    public Crackme() {
        GetFlag("sSNnx1UKbYrA1+MOrdtDTA==");
    }

    private String GetFlag(String p1) {
        byte[] "content" = Base64.decode(p1.getBytes(), 0x0);
        String "kk" = new String(Base64.decode(str2.getBytes(), 0x0));
        System.out.println(decrypt("content", "kk"));
        return null;
    }

    private String decrypt(byte[] p1, String p2) {
        String "m" = 0x0;
        try {
            byte[] "keyStr" = p2.getBytes();
            SecretKeySpec "key" = new SecretKeySpec("keyStr", "AES");
            Cipher "cipher" = Cipher.getInstance("AES/ECB/NoPadding");
            "cipher".init(0x2, "key");
            byte[] "result" = "cipher".doFinal(p1);
            return "m";
        } catch(NoSuchPaddingException "e") {
            "e".printStackTrace();
        }
        return "m";
    }
}
```

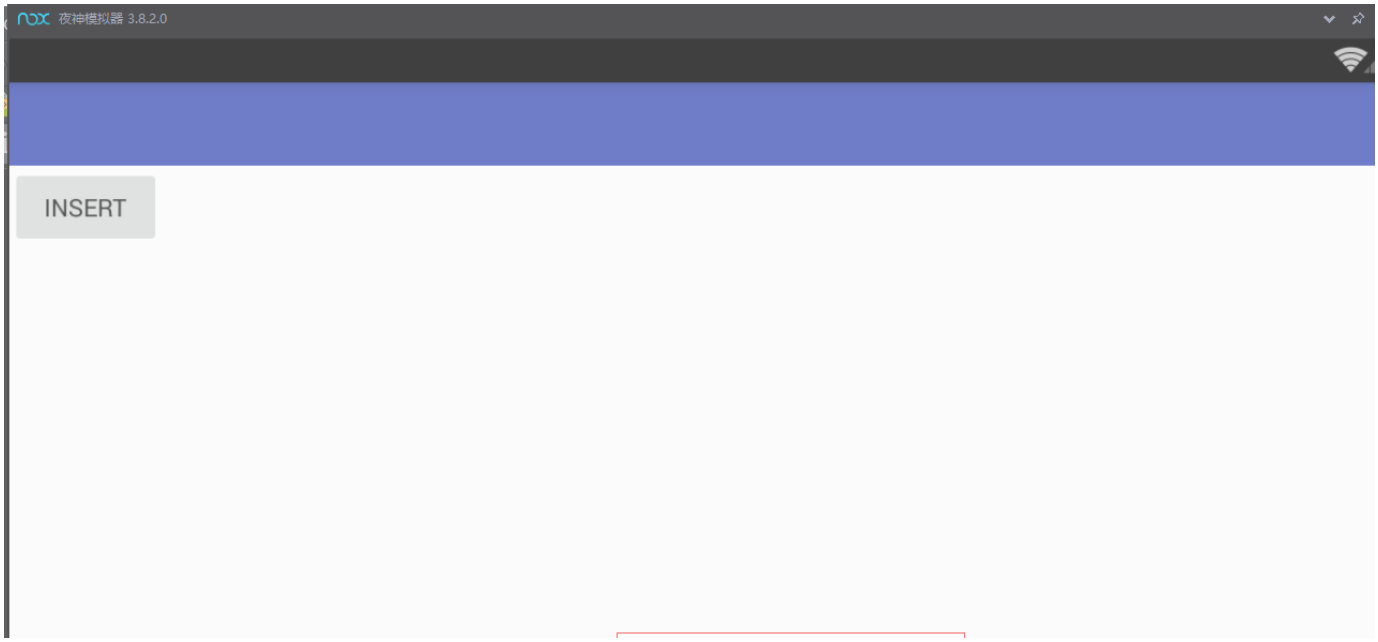

   smali文件转为java

```
public class crackme {
    private String str2 = "cGhyYWNrICBjdGYgMjAxNg==";

    public byte[]  GetFlag() throws Exception{
        String p1="sSNnx1UKbYrA1+MOrdtDTA==";
        byte[] content = Base64.decode(p1.getBytes(), flags: 0x0);
        String kk;
        kk = new String(Base64.decode(str2.getBytes(), flags: 0x0));
        //System.out.println(decrypt(content, kk));
        return decrypt(content, kk);
    }

    private byte[]  decrypt(byte[] p1, String p2) throws Exception {
        byte[] m = {0x00};;
        try {
            byte[] keyStr = p2.getBytes();
            SecretKeySpec key = new SecretKeySpec(keyStr, algorithm: "AES");
            Cipher cipher = Cipher.getInstance("AES/ECB/NoPadding");
            cipher.init(0x2, key);
            byte[] result= cipher.doFinal(p1);
            return result;
        } catch(NoSuchPaddingException e) {
```


修改部分有问题代码，这是修改以后的

```
//点击事件
OnClickListener listener= new OnClickListener(){
   public void onClick(View v){
       //ContentValues对象
       crackme t=new crackme();
       try {
           byte[] s;
           s = t.GetFlag();
           String res = new String(s);
           Toast.makeText(getApplicationContext(), res, Toast.LENGTH_SHORT).show();
       }catch(Exception e) {
           e.printStackTrace();
       }
```


我将其添加到我原来的android项目中，调用此类，Toast显示算出的结果，



添加异常。运行结果如第一个图。
PCTF{Sm4liRiver}