

strange apk

发表于 2021-01-04 分类于 [Challenge](#) , [2019](#) , [SCTF](#) , [Reverse](#)
[Challenge](#) | [2019](#) | [SCTF](#) | [Reverse](#) | [strange apk](#)

[点击此处](#) 获得更好的阅读体验

解题思路

前12个chr

```
1 localObject2 = new StringBuilder();
2 ((StringBuilder) localObject2).append(paramAnonymousView);
3 ((StringBuilder) localObject2).append(str.charAt(i));
4 paramAnonymousView = ((StringBuilder) localObject2).toString();
5 i++;
6 if (((String) localObject2).equals("c2N0ZntXM2xjMG1l"))
```

```
1 >>> base64.b64decode("c2N0ZntXM2xjMG1l")
2 'sctf{W3lc0me'`
```

有个data加密后的，直接虚拟机打开存着解密后的apk，拖下来直接分析。后18个chr：
这里先用intent启动了其他class：

```
1 localObject1 = new Intent();
2 ((Intent) localObject1).putExtra("data_return", paramAnonymousView);
3 s.this.setResult(-1, (Intent) localObject1);
4 s.this.finish();
```

最后一段关键比较：

```
1 if (f.encode(paramIntent.getStringExtra("data_return"), (String) localObject1).equals("~8t808_8A8n848r808i8d8-8w808r8l8d8}8"))
```

这里生成MD5：

```
1 try {
2     Object localObject2 = MessageDigest.getInstance("MD5");
3     ((MessageDigest) localObject2).update("syclover".getBytes());
4     BigInteger localBigInteger = new java/math/BigInteger();
5     localBigInteger.<init>(1, ((MessageDigest) localObject2).digest());
6     localObject2 = localBigInteger.toString(16);
7     localObject1 = localObject2;
8 } catch (Exception localException) {
9     localException.printStackTrace();
10 }
```

照着写了个函数：

```
1 public static void genMd5(){
2     String plaintext = "syclover";
3     try{
4         MessageDigest m = MessageDigest.getInstance("MD5");
5         m.reset();
6         m.update(plaintext.getBytes());
7         byte[] digest = m.digest();
8         BigInteger bigInt = new BigInteger(1,digest);
9         String hashtext = bigInt.toString(16);
10        System.out.print(hashtext);
11    } catch (Exception localException) {
12        localException.printStackTrace();
13    }
14 }
```

得到8bfc8af07bca146c937f283b8ec768d4

那个关键比较有个encode函数：

```
1 public static String encode(String paramString1, String paramString2) {
2     int i = paramString1.length();
3     int j = paramString2.length();
4     StringBuilder localStringBuilder = new StringBuilder();
5     for (int k = 0; k < i; k++)
6     {
7         localStringBuilder.append(paramString1.charAt(k));
8         localStringBuilder.append(paramString2.charAt(k / j));
9     }
10    return localStringBuilder.toString();
11 }
```

出题人好像把取整跟取余搞混了。应该是 $k \% j$ ，这样的话，直接在flag里插入8得到字符串：~8t808_8A8n848r808i8d8-8w808r8l8d8}8所以后半段flag：~t0_An4r0id-w0rld}

FLAG

```
1 sctf{W3lc0me~t0_An4r0id-w0rld}
```

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2019/SCTF/Reverse/kKLC14droh5TtTcuZS5mgt.html>
- 版权声明： 本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

[#Challenge](#) [#Reverse](#) [#2019](#) [#SCTF](#)
[music](#)
[Who is he](#)