看雪3万课程笔记-FRIDA高级API实用方法：Frida Hook Java（二）

原创

kfyzjd2008 于 2022-02-16 10:32:21 发布 97 收藏
分类专栏： 安卓 文章标签： java 安卓逆向 frida 看雪三万 安卓hook

本节接上一节课，APP进入第一关。

jadx点击代码跟进到相应代码处进行分析：

```
        public void onClick(View view) {
            String obj = editText.getText().toString();
            String obj2 = editText2.getText().toString();
            if (TextUtils.isEmpty(obj) || TextUtils.isEmpty(obj2)) {
                Toast.makeText(LoginActivity.this.mContext, "username or password is empty.", 1).show();
            } else if (LoginActivity.a(obj, obj).equals(obj2)) {
                LoginActivity.this.startActivity(new Intent(LoginActivity.this.mContext, FridaActivity1.class));
                LoginActivity.this.finishActivity(0);
            } else {
                Toast.makeText(LoginActivity.this.mContext, "Login failed.", 1).show();
            }
        }
    });
}
```


根据下图可以看到，关键判断点在a函数返回的值是否等于后面的字符串，

破解思路：直接hook a函数让其返回这个字符串。

```java
@Override // com.example.androiddemo.Activity.BaseFridaActivity
public void onCheck() {
    try {
        if (a(b("请输入密码:")).equals("R4jSLLLLLLLLLOrLE7/5B+Z6fsl65yj6BgC6YWz66gO6g2t65Pk6a+P65NK44NNROl0wNOLLLL=")) {
            CheckSuccess();
            startActivity(new Intent(this, FridaActivity2.class));
            finishActivity(0);
            return;
        }
        super.CheckFailed();
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```



```java
public static String a(byte[] bArr) throws Exception {
    StringBuilder sb = new StringBuilder();
    for (int i = 0; i <= bArr.length - 1; i += 3) {
        byte[] bArr2 = new byte[4];
        byte b = 0;
        for (int i2 = 0; i2 <= 2; i2++) {
            int i3 = i + i2;
            if (i3 <= bArr.length - 1) {
                bArr2[i2] = (byte) (b | ((bArr[i3] & 255) >>> ((i2 * 2) + 2)));
                b = (byte) ((((bArr[i3] & 255) << (((2 - i2) * 2) + 2)) & 255) >>> 2);
            } else {
                bArr2[i2] = b;
                b = 64;
            }
        }
        bArr2[3] = b;
        for (int i4 = 0; i4 <= 3; i4++) {
            if (bArr2[i4] <= 63) {
                sb.append(table[bArr2[i4]]);
            } else {
                sb.append('=');
            }
        }
    }
    return sb.toString();
}
```


在第一节hook代码中加入：

```
        var FridaActivity1 = Java.use("com.example.androiddemo.Activity.FridaActivity1");
        FridaActivity1.a.implementation = function(barr){
            console.log("FridaActivity1",barr)
            return "R4jSLLLLLLLLLOrLE7/5B+Z6fsl65yj6BgC6YWz66gO6g2t65Pk6a+P65NK44NNROl0wNOLLLL="
        }
```

这里的a是有参数的，但是却不用写overload，哪位大佬知道为什么请告知。谢谢。