看雪3万课程笔记-FRIDA高级API实用方法：Frida Hook Java（一）

原创

kfyzjd2008 于 2022-02-10 17:17:34 发布 1242 收藏
分类专栏： 安卓 文章标签： java android 逆向 frida

一、环境：

1、安装frida的已root手机

2、课程配套的apk文件

二、需具备的知识点：

1、在命令行执行frida的hook脚本

```
frida -U {APP包名} -l {脚本文件}
```

2、命令行像文本框输入文本

```
adb shell
input test "文本内容"
#手机文本框获取焦点后运行
```

三、课程内容

1、通过提示字符串在jadx中找到对应的判断位置

2、找到判断的代码

```java
public class LoginActivity extends AppCompatActivity {
    private Context mContext;

    @Override // androidx.activity.ComponentActivity, androidx.core.app.ComponentActivity, androidx.appcompat.app.AppCompatAc
    public void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        this.mContext = this;
        setContentView(R.layout.activity_login);
        final EditText editText = (EditText) findViewById(R.id.username);
        final EditText editText2 = (EditText) findViewById(R.id.password);
        ((Button) findViewById(R.id.login)).setOnClickListener(new View.OnClickListener() {
            /* class com.example.androiddemo.Activity.LoginActivity.AnonymousClass1 */

            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();
                }
            }
        });
    }

    private static String a(byte[] bArr) {
```

判断点

3、找到调用的函数

```java
    /* access modifiers changed from: private */
    public static String a(String str, String str2) {
        try {
            SecretKeySpec secretKeySpec = new SecretKeySpec(str2.getBytes(), "HmacSHA256");
            Mac instance = Mac.getInstance("HmacSHA256");
            instance.init(secretKeySpec);
            return a(instance.doFinal(str.getBytes()));
        } catch (Exception e) {
            e.printStackTrace();
            return BuildConfig.FLAVOR;
        }
    }
```


4、编写hook代码

```
function hook_java(){
    Java.perform(function(){
        var LoginActivity = Java.use("com.example.androiddemo.Activity.LoginActivity");
        LoginActivity.a.overload('java.lang.String', 'java.lang.String').implementation = function(str,str2
            var result = this.a(str,str2);
            console.log("LoginActivity.a:",str,str2,result);
            return result;
        }
        console.log("hook_java");
    });
}

function main() {
        hook_java();
}

setImmediate(main);
```

点击登录后将输出的result值填入密码框即可启动下一关