objection 框架	__EMPTY
objection -g cn.com.ccccaa.ui explore	objection注入指定应用
android sslpinning disable	过ssl证书认证
android root disable	
android hooking list activities	查找所有可用activities
android intent launch_activity 类名	启动指定的类
android intent launch_service 类名	启动指定服务
android hooking generate simple 类名	查指定类下面有哪些方法
android hooking list class_methods 类	列出类的所有方法
android hooking watch class 类名	监视进行某个操作的时候调用了哪些方法（hook类的所有方法）
objection -g com.hd.zhibo explore --startup-command "android hooking watch class_method android.app.AlertDialog.onCreate --dump-args --dump-backtrace --dump-return"	hook方法的参数、返回值和调用栈，这种实现方式是启动的时候就hook
android hooking watch class_method android.app.AlertDialog.onCreate --dump-args --dump-return --dump-backtrace	具体方法调用之前hook
env	应用环境信息
ls	
jobs list	创建的Hooks列表
jobs kill id	
memory list modules	查看内存中加载的库
memory list exports libssl.so	查看库的导出函数
memory dump all from_base	提取整个(或部分)内存
memory dump from_base 0xc935628c 100 memory.dex	
memory search "64 65 78 0a 30 33 35 00"	暴力搜内存
memory search "aiyou,bucuoo" --string	搜索整个内存
memory search "aiyou,bucuoo" --string --offsets-only	仅看偏移地址

objection 框架	__EMPTY
android hooking list services	查看可供开启的服务
android intent launch_service [完整Service名]	直接启动指定service
android hooking list classes	列出内存中所有的类
android hooking search classes [display]	在内存中所有已加载的类中搜索包含特定关键词的类
android hooking search methods [display]	在内存中所有已加载的类的方法中搜索包含特定关键词的类
cat .objection/objection.log	日志查看
cat objection.log ｜grep -i http	日志筛选
objection -g com.android.settings explore -c "2.txt"	运行批量hook
Wallbreaker	
objection -g com.android.phone explore -P ~/.objection/plugins	使用Wallbreaker
plugin wallbreaker classsearch	搜索类，根据给的 pattern 对所有类名进行匹配，列出匹配到的所有类名
plugin wallbreaker objectsearch	搜索对象，根据类名搜索内存中已经被创建的实例，列出 handle 和 toString() 的结果。
plugin wallbreaker classdump [--fullname]	ClassDump，输出类的结构， 若加了 --fullname 参数，打印的数据中类名会带着完整的包名。
plugin wallbreaker objectdump [--fullname]	ObjectDump，在 ClassDump 的基础上，输出指定对象中的每个字段的数据。

```
cr[redacted]: on (google: 9) [usb] # plugin wallbreaker classsearch Encrypt
a[redacted]keystore.KeyProperties$EncryptionPadding
i[redacted]plugin.sm2Encrypt.SM2.Util
i[redacted]plugin.sm2Encrypt.SM2.SM2Utils
i[redacted]plugin.sm2Encrypt.pluginEncryptUtil
i[redacted]plugin.sm2Encrypt.SM2.SM2
i[redacted]plugin.sm2Encrypt.SM2.SM3
i[redacted]plugin.sm2Encrypt.SM2.SM3Digest
i[redacted].plugin.sm2Encrypt.SM2.Cipher
```

```
[redacted]on (google: 9) [usb] # plugin wallbreaker classdump --fullname [redacted]in.sm
[redacted]

package [redacted].sm2Encrypt

class pluginEncryptUtil {

        /* static fields */
        static java.lang.String iv; => PffA
        static java.lang.String key; => hpm8
        static java.lang.String privateKey; => 5E9FF2B62D627680C817BEAD30C817AF90ED166B354B46FFE302859C5EADF7C8
        static java.lang.String publicKey; => 0437ADE7B1731DE6CF95529A0325F4F4062A149ADF9BF7A42DB48ADED96161754EFE627DE3BA24736E7A
1962A98F5A863ED9465F12B6C497AEBF2B3FBCFAA4C7A7

        /* instance fields */

        /* constructor methods */
        [redacted]t.pluginEncryptUtil();

        /* static methods */

        /* instance methods */
        java.lang.String getCryptIvp[redacted].DHInterface.IWebview, org.json.JSONArray);
        java.lang.String getCryptKey([redacted].DHInterface.IWebview, org.json.JSONArray);
        java.lang.String getSm2DecryptString([redacted].DHInterface.IWebview, org.json.JSONArray);
        java.lang.String getSm2EncryptString([redacted].DHInterface.IWebview, org.json.JSONArray);

}
```

```
        /* instance methods */
        B[] __4c09dd(int, java.lang.String, B[]);
        B[] __7ef60a(int, java.lang.String, B[]);
        java.lang.String __828031(java.lang.String);
        B[] __834c10(int, java.lang.String, B[]);
        B[] __a79626(int, java.lang.String, B[]);
        int __bb9c88(int, java.lang.String, java.lang.String);
        java.lang.String __c32395(int, int, java.lang.String);
        int __ffc939(java.lang.String);
        boolean a();
        B[] a(B[]);
        B[] b(B[]);
        java.io.InputStream decryptResponseBody(java.io.InputStream);
        B[] decryptResponseBody(B[]);
        java.io.OutputStream encryptRequestBody(java.io.OutputStream);
        B[] encryptRequestBody(B[]);
        java.lang.String getHeaderKey();
        java.lang.String getRequestHeader();
        java.lang.String getRequestHeader(int);
        int onResponseHeader(java.lang.String);
```

```
        static int MSEC_FLAG_ENCRYPTED; => 2
        static int MSEC_FLAG_LOCAL_WEBVIEW; => 8
        static int MSEC_FLAG_NATIVE; => 0
        static int MSEC_FLAG_URL; => 32
        static int MSEC_FLAG_WEBVIEW; => 1
        static int MSEC_USE_NET_LIB_ALL; => 65531
        static int MSEC_USE_NET_LIB_ANDROID_ASYNC; => 128
        static int MSEC_USE_NET_LIB_ASYNC_HTTP_CLIENT; => 8
        static int MSEC_USE_NET_LIB_DCLOUD_OK_HTTP3; => 256
        static int MSEC_USE_NET_LIB_DEFAULT_HTTP_CLIENT; => 16
        static int MSEC_USE_NET_LIB_MS; => 64
        static int MSEC_USE_NET_LIB_OK_HTTP3; => 4
        static int MSEC_USE_NET_LIB_REACT_NATIVE; => 32
        static int MSEC_USE_NET_LIB_URL_OPEN_CONNECTION; => 2
        static int MSEC_USE_NET_LIB_WEB_VIEW; => 1
        static android.content.Context __56444b => [illegible]in.MyApplication@2768f40
__56444b; => [0x30912]: [illegible]ution@2768f40
        static int __65d297; => 100
        static int __9de558; => 2
        static int __a320cc; => 2
        static java.lang.String __ec9984; => [illegible]
        static java.lang.String d; => /data/user/0[illegible]/
        static com.msec.b e => com.msec.b@97c76b6
e; => [0x308da]: com.msec.b@97c76b6
        static boolean f; => false
        static java.lang.String g; => ryau2rcb
        static boolean h; => false
        static boolean i; => false
        static boolean j; => false
        static java.io.FileOutputStream k => java.io.FileOutputStream@cee2fb7
k; => [0x308aa]: java.io.FileOutputStream@cee2fb7

        /* instance fields */
        java.lang.String a;
        int b;
        boolean c;

        /* constructor methods */
        com.msec.MSecClient(java.lang.String);

        /* static methods */
        static java.lang.String __0be676();
        static void __0f2d8f(java.lang.String);
        static boolean __132b10();
        static java.lang.reflect.Field __24ea15(java.lang.Class, java.lang.String);
        static void __30211c(java.lang.String);
        static void __3fdba0(java.lang.Object, boolean);
        static void __421c77(java.lang.String);
        static boolean __4c6c7e(java.lang.String);
```

知识星球

优惠券

Andy

送你一张星球优惠券

移动安全

74 元立减金

限前 10 名加入星球使用

2022/04/13 12:00 至 2022/04/20 12:00

长按扫码领取优惠

加入星球立减