

Forum:[Hack Forums](#)

Thread: [Frida mobile app exploitation cheat sheet](#)

Clumsy - June 20, 2024, 5:16 am

Setup

Code # Install Frida

```
pip install frida-tools
```

Download Frida server for your device from <https://github.com/frida/frida/releases>

```
adb push frida-server /data/local/tmp/
```

```
adb shell "chmod 755 /data/local/tmp/frida-server"
```

Start Frida server on the device

```
adb shell "/data/local/tmp/frida-server &"
```

Basic Commands

Code # List connected devices

```
frida-ls-devices
```

List running applications on the device

```
frida-ps -U
```

Attach to a running application

```
frida -U -n <app_name>
```

Spawn and attach to an application

```
frida -U -f <app_id> --no-pause
```

Information Gathering

Code # List application information

```
frida-ps -Uai
```

Dump memory

```
frida-dump -U -n <app_name>
```

Enumerate loaded modules

```
frida --no-pause -U -n <app_name> -l list_modules.js
```

List exported functions

```
frida -U -n <app_name> -l list_exports.js
```

JavaScript Injection

Code # Inject a JavaScript file

```
frida -U -n <app_name> -l script.js
```

Run a script directly

```
frida -U -f <app_id> -l script.js --no-pause
```

Example Scripts

Code # Intercept method calls

```
Interceptor.attach(Module.getExportByName(null, 'open'), {  
  onEnter: function(args) {  
    send('open() called');
```

```
}  
});
```

```
# Bypass SSL pinning
```

```
Java.perform(function() {  
    var SSLContext = Java.use('javax.net.ssl.SSLContext');  
    SSLContext.init.overload('[Ljava.net.ssl.KeyManager;', '[Ljava.net.ssl.TrustManager;',  
'java.security.SecureRandom').implementation = function(a, b, c) {  
        send('Bypassing SSL pinning');  
        this.init(a, b, c);  
    };  
});
```

```
# Modify function return value
```

```
Java.perform(function() {  
    var MainActivity = Java.use('com.example.app.MainActivity');  
    MainActivity.isRooted.implementation = function() {  
        return false;  
    };  
});
```

```
Memory Operations
```

```
Code # Read memory
```

```
var memory = Process.getModuleByName('<module_name>').base.add(<offset>);  
var buffer = Memory.readByteArray(memory, <length>);
```

```
# Write memory
```

```
Memory.writeByteArray(memory, [0x90, 0x90, 0x90, 0x90]);
```

```
File Operations
```

```
Code # List files in a directory
```

```
var files = new File('<path>').list();
```

```
# Read a file
```

```
var file = new File('<path>', 'r');  
var content = file.read(file.size());
```

```
# Write to a file
```

```
var file = new File('<path>', 'w');  
file.write('Hello, Frida!');
```

```
Network Analysis
```

```
Code # Intercept network requests
```

```
var URLConnection = Java.use('java.net.URLConnection');  
URLConnection.getInputStream.implementation = function() {  
    send('Request URL: ' + this.getURL());  
    return this.getInputStream();  
};
```

```
# Capture network traffic
```

```
var httpClient = Java.use('org.apache.http.impl.client.DefaultHttpClient');  
httpClient.execute.overload('org.apache.http.client.methods.HttpUriRequest').implementation =  
function(request) {  
    send('HTTP Request: ' + request.getURI().toString());  
    return this.execute(request);  
};
```

Logcat Commands

Code # Start logcat

```
adb logcat
```

Filter logcat output

```
adb logcat -s <tag_name>
```

Miscellaneous

Code # Restart Frida server on the device

```
adb shell su -c "/data/local/tmp/frida-server &"
```

Update Frida to the latest version

```
pip install --upgrade frida-tools
```

Display help for a command

```
frida --help
```

mrshlash - *August 17, 2024, 11:11 am*

Interesting topic thank you