

Drozer - Drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

Starting a session

```
adb forward tcp:31415 tcp:31415
```

```
drozer console connect
```

ls – lists all available options

Modules:

module repository enable <path-to-repo>

module search -d – lists all modules with detailed info

module search <keyword> - search for modules with specific keyword

module install <module-name> - installs a module

help <module-name> - information about module

Usage:

Retrieving package information

```
run app.package.list -f <app name>
```

```
run app.package.info -a <package name>
```

Identifying the attack surface

```
run app.package.attacksurface <package name>
```

Exploiting Activities

```
run app.activity.info -a <package name> -u
```

```
run app.activity.start --component <package name> <component name>
```

Exploiting Content Provider

```
run app.provider.info -a <package name>
```

```
run scanner.provider.finduris -a <package name>
```

```
run app.provider.query <uri>
```

```
run app.provider.update <uri> --selection <conditions> <selection arg> <column> <data>
```

```
run scanner.provider.sqltables -a <package name>
```

```
run scanner.provider.injection -a <package name>
```

```
run scanner.provider.traversal -a <package name>
```

Exploiting Broadcast Receivers

```
run app.broadcast.info -a <package name>
```

```
run app.broadcast.send --component <package name> <component name> --extra <type>  
<key> <value>
```

```
run app.broadcast.sniff --action <action>
```

Exploiting Service

```
run app.service.info -a <package name>
```

```
run app.service.start --action <action> --component <package name> <component name>
```

```
run app.service.send <package name> <component name> --msg <what> <arg1> <arg2> --extra  
<type> <key> <value> --bundle-as-obj
```

```
run app.package.launch intent <package name>
```