

3、drozer

一、安装

二、使用

Android应用程序安全评估的开源安全测试工具。它旨在帮助安全专业人员评估Android应用程序 的安全性，发现潜在的漏洞和弱点。

Drozer提供了一套功能强大的模块，可以用于执行各种安全测试任务，包括但不限于：

▼

Python |

1

1. 应用程序分析： 可以获取应用程序的信息，包括权限、组件、服务等。

2

2. 漏洞利用： Drozer允许安全专业人员检测应用程序中的漏洞，以模拟攻击并找到潜在的弱点。

3

3. SSL验证和劫持： 可以检查应用程序的SSL实现，查找潜在的安全问题。

4

4. 数据存储安全： 可以评估应用程序中的数据存储安全性，包括数据库、共享首选项等。

5

5. 攻击模拟： Drozer允许模拟各种攻击，以测试应用程序的抵抗力。

一、安装

1、PC控制台安装

先决条件

1. Python 2.7

注：在Windows上，请确保将Python安装的路径和Python安装下的安装文件夹添加到PATH环境变量中。















2、drozer安装

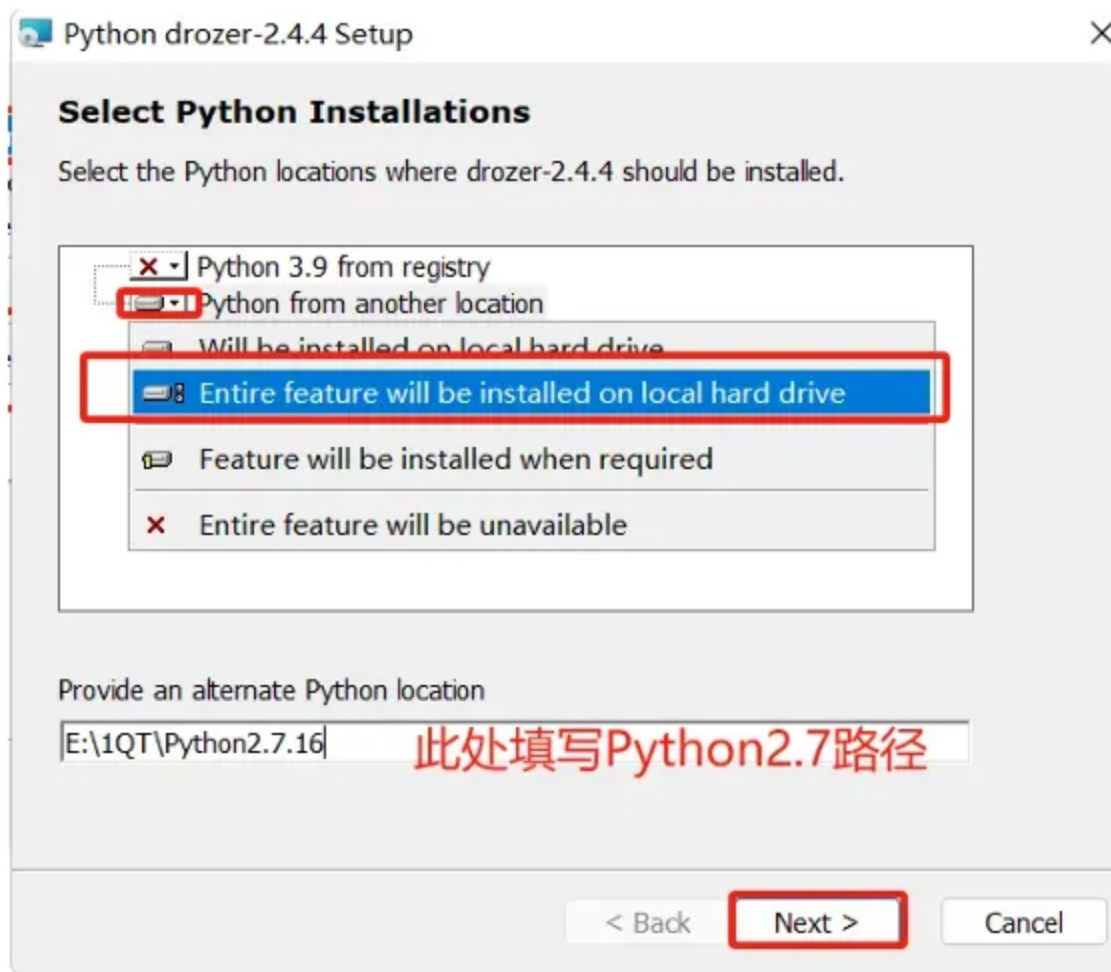
下载位置：<https://github.com/WithSecureLabs/drozer>

2.4.4

- [Build Process] AppVeyor updated to deploy Windows installer
- [Build Process] Fixed versioning of whl, deb and rpm packages
- [Bug Fixes] Several bug fixes

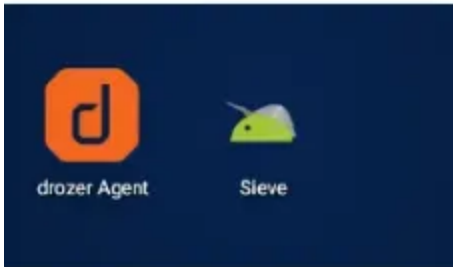
▼ Assets 7

 drozer-2.4.4-1.noarch.rpm	27 MB	Nov 9, 2017	 下载
 drozer-2.4.4-py2-none-any.whl	27.1 MB	Nov 9, 2017	 下载
 drozer-2.4.4.tar.gz	27 MB	Nov 9, 2017	 下载
 drozer-2.4.4.win32.msi	27.7 MB	Nov 9, 2017	 下载
 drozer_2.4.4.deb	25.4 MB	Nov 9, 2017	 下载
 Source code (zip)		Nov 9, 2017	 下载
 Source code (tar.gz)		Nov 9, 2017	 下载



3、agent代理安装

直接将apk拖动到模拟器



sieve(管理密码的APP)端设置密码和pin

二、使用

1.adb连接模拟器

确定模拟器的IP与端口

连接逍遥模拟器，ip:port



Python |

```
1  adb connect 127.0.0.1:62001
```

2、PC端运行drozer



Python |

```
1  adb forward tcp:31415 tcp:31415 (就是将PC端31415收到的数据转发给终端的agent默认监听的31415端口)
2  drozer.bat console connect (连接终端agent)
```

开启模拟器端的drozer

5:12

drozer Server

Enabled



Server Details

SSL Enabled
 Password Protected
 Enabled
 Connected
 Active Sessions

Messages

| Starting Server...
 | Attempting to bind to port 31415...
 | Waiting for connections...
 | Accepted connection...
 | Starting drozer thread...

```

# drozer.bat console connect
D:\Base\apps\python27\current\lib\site-packages\OpenSSL\crypto.py:14: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography import utils, x509
:0: UserWarning: You do not have a working installation of the service_identity module: 'No module named service_identity'. Please install it from <https://pypi.python.org/pypi/service_identity> and make sure all of its dependencies are satisfied. Without the service_identity module, Twisted can perform only rudimentary TLS client hostname verification. Many valid certificate/hostname mappings may be rejected.
Selecting a1c22531430530f2 (Asus ASUS_I003DD 9)

..                               ...
..0..                             r..
..a.. . . . . . . . . . . . . . .nd
  ro..idsnemesisisand..pr
  .otectorandroidsneme.
  .,sisandprotectorandroids+.
  ..nemesisisandprotectorandroidsn:.
  .emesisisandprotectorandroidsnemes..
  ..isandp,..,rotectorandro,..,idsnem.
  .isisandp..rotectorandroid..snemisis.
  ,andprotectorandroidsnemesisisandprotec.
  .torandroidsnemesisisandprotectorandroid.
  .snemesisisandprotectorandroidsnemesisan:
  .dprotectorandroidsnemesisisandprotector.

drozer Console (v2.4.4)
dz>
  
```

如果出现 unknown module: 'aap.package.list'

- 1 解决:
- 2 出现unknownmodule, 这个时候在dz>中输入list, 返回结果也是空白。解决方法是在cmd中将当前目录切换到drozer的安装路径下, 如d:\drozer, 然后再输入"`drozerconsole connect`"启动drozer。
- 3
- 4 <https://blog.csdn.net/bbdog86/article/details/50622963>

3、查找终端设备所有APK信息

- 1 `run app.package.list`

```
dz> run app.package.list
com.android.cts.priv.ctsshim (com.android.cts.priv.ctsshim)
com.android.internal.display.cutout.emulation.corner (边角显示屏凹口)
com.android.internal.display.cutout.emulation.double (双显示屏凹口)
com.android.providers.telephony (移动网络配置)
com.microvirt.installer (谷歌安装器)
com.android.providers.calendar (日历存储)
com.android.providers.media (媒体存储设备)
org.proxydroid (ProxyDroid)
com.android.wallpapercropper (com.android.wallpapercropper)
com.github.kr328.clash (Clash for Android)
com.android.documentsui (文件)
com.android.externalstorage (外部存储设备)
com.android.htmlviewer (HTML 查看程序)
com.android.companiondevicemanager (Companion Device Manager)
```

4、查看指定apk信息

- 1 `run app.package.info -a com.mwr.example.sieve`

```
dz> run app.package.info -a com.mwr.example.sieve
Package: com.mwr.example.sieve
Application Label: Sieve
Process Name: com.mwr.example.sieve
Version: 1.0
Data Directory: /data/user/0/com.mwr.example.sieve
APK Path: /data/app/com.mwr.example.sieve-KSNBfJ3b9xwwW0euI-r8PA==/base.apk
UID: 10059
GID: [3003]
Shared Libraries: [/system/framework/org.apache.http.legacy.boot.jar]
Shared User ID: null
Uses Permissions:
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.INTERNET
Defines Permissions:
- com.mwr.example.sieve.READ_KEYS
- com.mwr.example.sieve.WRITE_KEYS
```

5、通过关键字过滤来匹配显示

▼ Python |

```
1 run app.package.list -f location
2 含义: -f是过滤的意思, 通过后面的关键字过滤来匹配显示
3 run app.package.info -f location
```

```

drozer Console (v2.4.4)
dz> run app.package.list -f location
com.android.location.fused (涓€浣嶅浣嶇緛淇℃)
dz> run app.package.info -f location
Package: com.android.location.fused
  Application Label: 涓€浣嶅浣嶇緛淇℃
  Process Name: system
  Version: 9
  Data Directory: /data/user_de/0/com.android.location.fused
  APK Path: /system/priv-app/FusedLocation/FusedLocation.apk
  UID: 1000
  GID: [1065, 3002, 1023, 3003, 3001]
  Shared Libraries: [/system/framework/com.android.location.p
  Shared User ID: android.uid.system
  Uses Permissions:
    - android.permission.ACCESS_COARSE_LOCATION
    - android.permission.ACCESS_FINE_LOCATION
    - android.permission.INSTALL_LOCATION_PROVIDER
    - android.permission.INTERACT_ACROSS_USERS_FULL
  Defines Permissions:
    - None

dz> |

```

6、从安卓组件角度出发，查看sieve apk的可攻击点

```

▼ Python |
1  run app.package.attacksurface com.mwr.example.sieve

```



```

dz> run app.package.attacksurface com.mwr.example.sieve
Attack Surface:
  3 activities exported
  0 broadcast receivers exported
  2 content providers exported
  2 services exported
  is debuggable

```

(5) 安卓四大组件

组件	描述
Activity(活动)	在应用中的一个Activity可以用来表示一个界面，意思可以理解为“活动”，即一个活动开始，代表 Activity组件启动，活动结束，代表一个Activity的生命周期结束。一个Android应用必须通过Activity来运行和启动，Activity的生命周期交给系统统一管理。
Service(服务)	Service它可以在后台执行长时间运行操作而没有用户界面的应用组件，不依赖任何用户界面，例如后台播放音乐，后台下载文件等。
Broadcast Receiver(广播接收器)	一个用于接收广播信息，并做出对应处理的组件。比如我们常见的系统广播：通知时区改变、电量低、用户改变了语言选项等。
Content Provider(内容提供者)	作为应用程序之间唯一的共享数据的途径，Content Provider主要的功能就是存储并检索数据以及向其他应用程序提供访问数据的接口。Android内置的许多数据都是使用Content Provider形式，供开发者调用的（如视频，音频，图片，通讯录等）

7、获取activity信息


```
1 run app.activity.info -a com.mwr.example.sieve
```

```
dz> run app.activity.info -a com.mwr.example.sieve
Package: com.mwr.example.sieve
  com.mwr.example.sieve.FileSelectActivity
    Permission: null
  com.mwr.example.sieve.MainLoginActivity
    Permission: null
  com.mwr.example.sieve.PWList
    Permission: null
```

8、启动activity

```
1 run app.activity.start --component com.mwr.example.sieve com.mwr.example.sieve.FileSelectActivity
```

9、获取Content Provider信息

```
1 run app.provider.info -a com.mwr.example.sieve
```

```
dz> run app.provider.info -a com.mwr.example.sieve
Package: com.mwr.example.sieve
  Authority: com.mwr.example.sieve.DBContentProvider
    Read Permission: null
    Write Permission: null
    Content Provider: com.mwr.example.sieve.DBContentProvider
    Multiprocess Allowed: True
    Grant Uri Permissions: False
    Path Permissions:
      Path: /Keys
      Type: PATTERN_LITERAL
      Read Permission: com.mwr.example.sieve.READ_KEYS
      Write Permission: com.mwr.example.sieve.WRITE_KEYS
  Authority: com.mwr.example.sieve.FileBackupProvider
    Read Permission: null
    Write Permission: null
    Content Provider: com.mwr.example.sieve.FileBackupProvider
    Multiprocess Allowed: True
    Grant Uri Permissions: False
```

10、获取所有可以访问的Uri—— Content Providers（数据泄露）

```
1 run scanner.provider.finduris -a com.mwr.example.sieve
```

```
dz> run scanner.provider.finduris -a com.mwr.example.sieve
Scanning com.mwr.example.sieve...
Unable to Query content://com.mwr.example.sieve.DBContentProvider/
Unable to Query content://com.mwr.example.sieve.FileBackupProvider/
Unable to Query content://com.mwr.example.sieve.DBContentProvider
Able to Query content://com.mwr.example.sieve.DBContentProvider/Password
Able to Query content://com.mwr.example.sieve.DBContentProvider/Keys/
Unable to Query content://com.mwr.example.sieve.FileBackupProvider
Able to Query content://com.mwr.example.sieve.DBContentProvider/Password
Unable to Query content://com.mwr.example.sieve.DBContentProvider/Keys

Accessible content URIs:
content://com.mwr.example.sieve.DBContentProvider/Keys/
content://com.mwr.example.sieve.DBContentProvider/Passwords
content://com.mwr.example.sieve.DBContentProvider/Passwords/
dz>
```

11、检测SQL注入

```
1 run scanner.provider.injection -a com.mwr.example.sieve
```

```
Unable to Query content://com.mwr.example.sieve.DBContentProvider
Able to Query content://com.mwr.example.sieve.DBContentProvider/Passwords/
Able to Query content://com.mwr.example.sieve.DBContentProvider/Keys/
Unable to Query content://com.mwr.example.sieve.FileBackupProvider
Able to Query content://com.mwr.example.sieve.DBContentProvider/Passwords
Unable to Query content://com.mwr.example.sieve.DBContentProvider/Keys
```

Accessible content URIs:

```
content://com.mwr.example.sieve.DBContentProvider/Keys/
content://com.mwr.example.sieve.DBContentProvider/Passwords
content://com.mwr.example.sieve.DBContentProvider/Passwords/
```

```
dz> run scanner.provider.injection -a com.mwr.example.sieve
```

```
Scanning com.mwr.example.sieve...
```

Not Vulnerable:

```
content://com.mwr.example.sieve.DBContentProvider/Keys
content://com.mwr.example.sieve.DBContentProvider/
content://com.mwr.example.sieve.FileBackupProvider/
content://com.mwr.example.sieve.DBContentProvider
content://com.mwr.example.sieve.FileBackupProvider
```

Injection in Projection:

```
content://com.mwr.example.sieve.DBContentProvider/Keys/
content://com.mwr.example.sieve.DBContentProvider/Passwords
content://com.mwr.example.sieve.DBContentProvider/Passwords/
```

Injection in Selection:

```
content://com.mwr.example.sieve.DBContentProvider/Keys/
content://com.mwr.example.sieve.DBContentProvider/Passwords
content://com.mwr.example.sieve.DBContentProvider/Passwords/
```

```
dz>
```