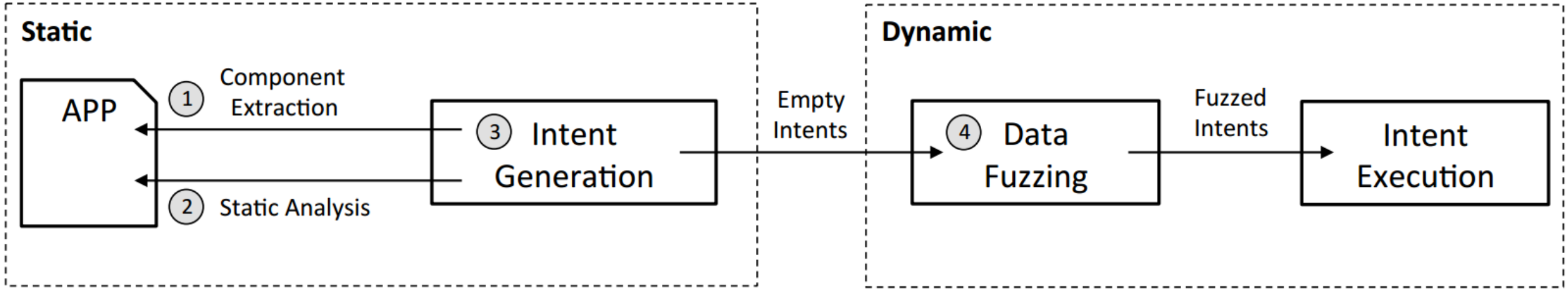
Android Intent Fuzzing Module for Drozer

Razvan Ionescu && Stefania Popescu

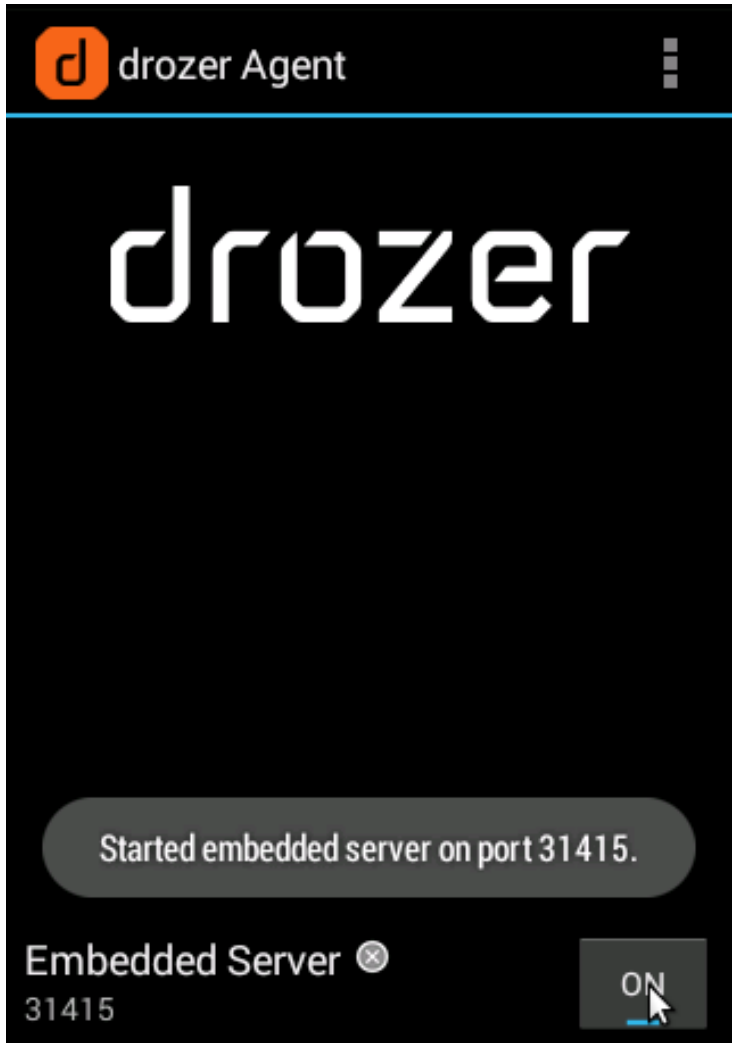
Intel OTC Romania

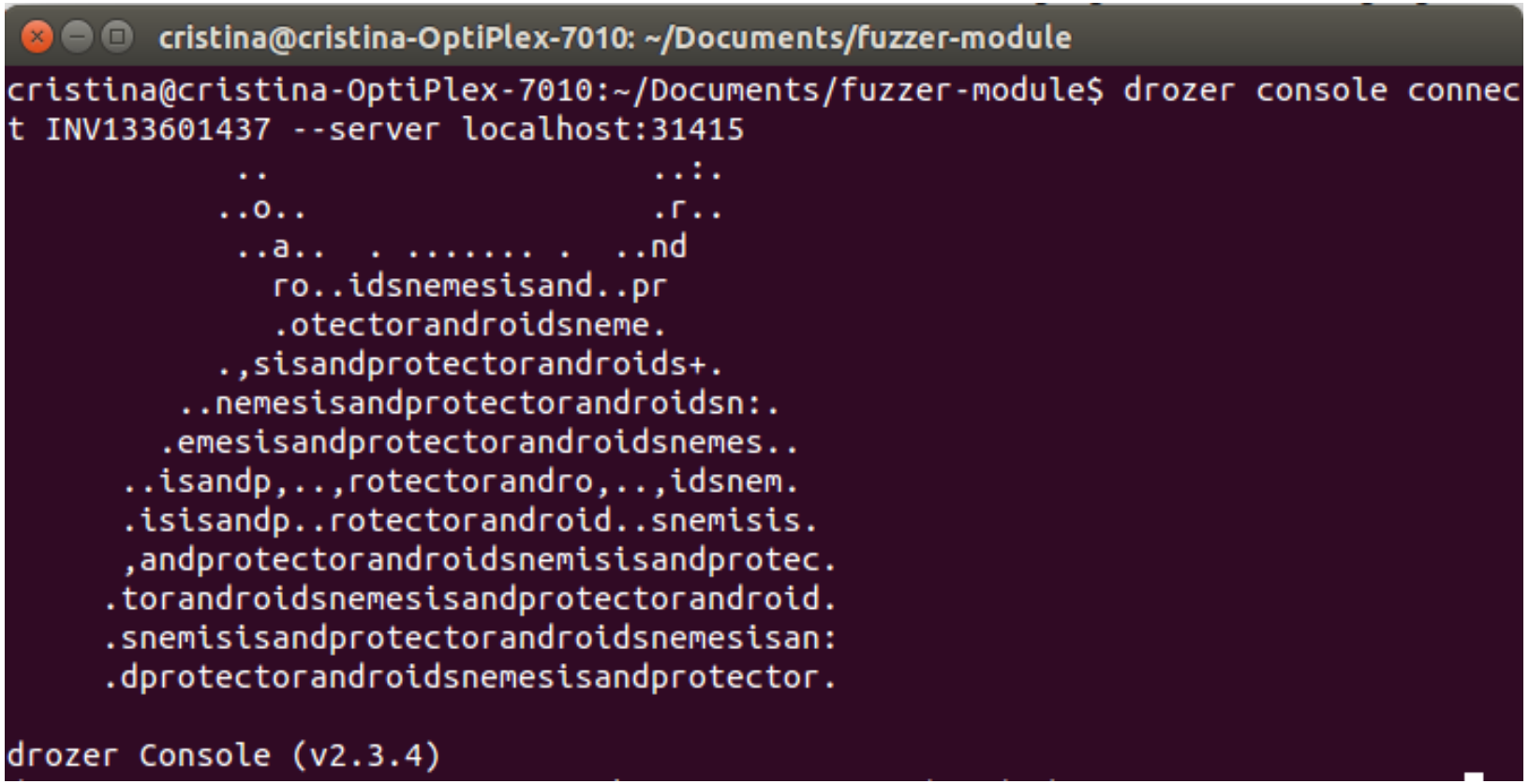
Intro



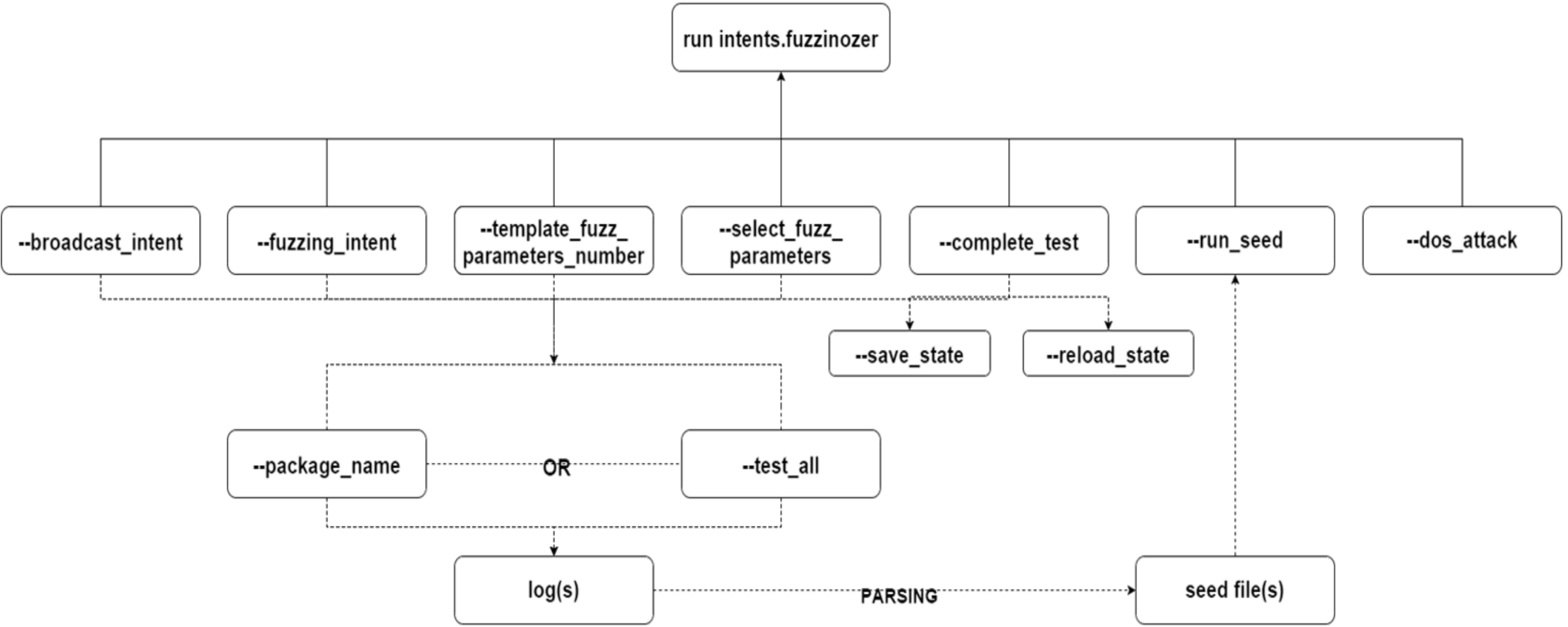

```
Intent intent = new Intent(Intent.ACTION_SEND);
intent.setType("text/plain");
intent.putExtra(android.content.Intent.EXTRA_TEXT, "Hello!");
startActivity(intent);
```

drozer


drozer Agent
drozer
Started embedded server on port 31415.
Embedded Server
31415
ON


cristina@cristina-OptiPlex-7010: ~/Documents/fuzzer-module
cristina@cristina-OptiPlex-7010:~/Documents/fuzzer-module$ drozer console connec
t INV133601437 --server localhost:31415
..   ..:.
..o..   .r..
..a.. . ...nd
ro..idsnemesisand..pr
.otectorandroidsneme.
.,sisandprotectorandroids+.
..nemesisandprotectorandroidsn:.
.emesisandprotectorandroidsnemes..
..isandp,..,rotectorandro,..,idsnem.
.isisandp..rotectorandroid..snemisis.
,andprotectorandroidsnemisisandprotec.
.torandroidsnemesisandprotectorandroid.
.snemisisandprotectorandroidsnemesisan:
.dprotectorandroidsnemesisandprotector.
drozer Console (v2.3.4)

intents.fuzzinozer



intents.fuzzinozer – running examples

```
dz> run intents.fuzzinozer --fuzzing_intent
--package_name com.google.android.gms --template_fuzz_parameters_number 6

dz> run intents.fuzzinozer --complete_test
--package_name com.google.android.gms --save_state

dz> run intents.fuzzinozer --complete_test
--package_name com.google.android.gms --reload_state "1 1 5 5 5"

dz> run intents.fuzzinozer --run_seed
seedfile_com.google.android.gms_NullPointerException.txt

dz> run intents.fuzzinozer --broadcast_intent
--package_name com.google.android.gms

$ drozer console connect -c
"run intents.fuzzinozer --broadcast_intent -test_all"
```

Results

IllegalStateException

javaNullPointerException

javaClassNotFoundException

SecurityException

DoS attack

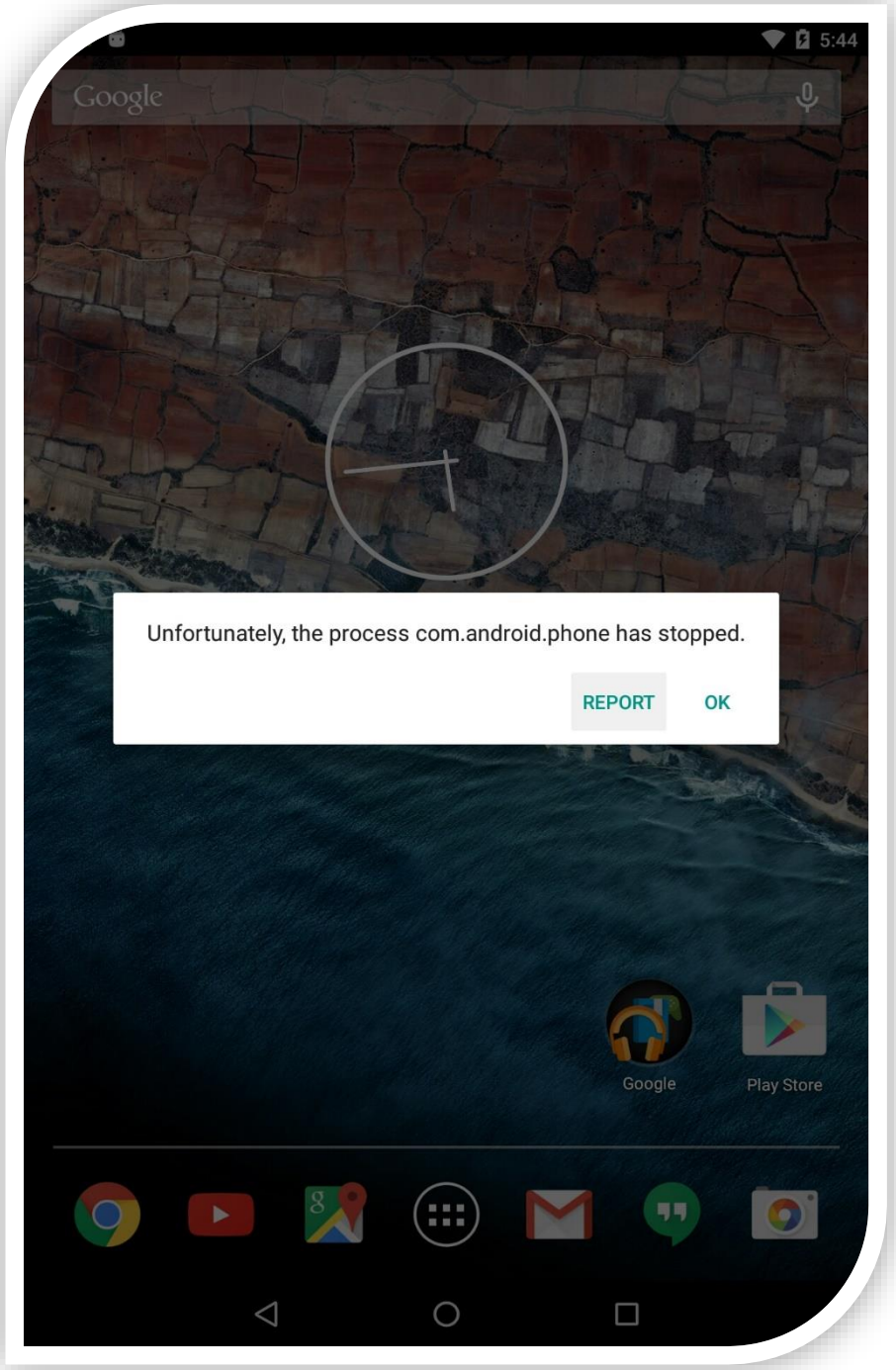
DoS attack

DoS attack

ClassCastException

NumberFormatException

IllegalArgumentException



https://www.flickr.com/photos/codex41/9725166177

https://github.com/fuzzing