
SPQR

Ghidra:
a new player in the RE scene

by Blaze

$ whoami

Giulio Ginesi [@blazef104, @blaze911]

24 years old, student of MSc in Cybersecurity.

Interested in hardware security and binary analysis.

Short experience in the CTFs world.

Many other interests: skiing, planes, climbing, reading and science.

So Ghidra is here?

Hacker Fantastic
@hackerfantastic

Segui

Here is a screen shot that proves RCE in the JDWP service when running Ghidra in debug mode. The issue is that the NSA left an asterisk * instead of something sane like "127.0.0.1" - exposing JDWP to all interfaces and allowing exploitation. It's not default, but a bugdoor.

SwiftOnSecurity @SwiftOnSecurity · 12 h
When they realize you'll run anything if it's hosted on Github and this was the secret all along

Traduci il Tweet

18 285 1376

Aaron Gallagher @aagallag · 21 h
Should government email + real names be shared with the world? #ghidra

Traduci il Tweet

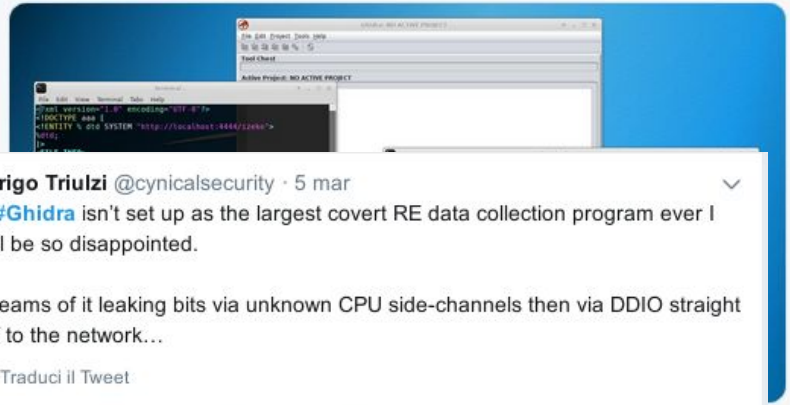
```
commit 6c909a46cdb9f56af0be73062852ccac79ee89a1
Author: Christopher Tubbs <christopher.l.tubbs.civ@mail.mil>
Date:   Thu Feb 28 22:43:12 2019 -0500

    Add skeleton repository files
```

evariste.gal is e Tavis Ormandy hanno messo Mi piace

sghctoma @sghctoma · 1 h
it's Java.. so of course it's susceptible to XXE.. kids, don't accept #Ghidra projects from strangers!

Traduci il Tweet



Arrigo Triulzi @cynicalsecurity · 5 mar
If #Ghidra isn't set up as the largest covert RE data collection program ever I will be so disappointed.

Dreams of it leaking bits via unknown CPU side-channels then via DDIO straight off to the network…

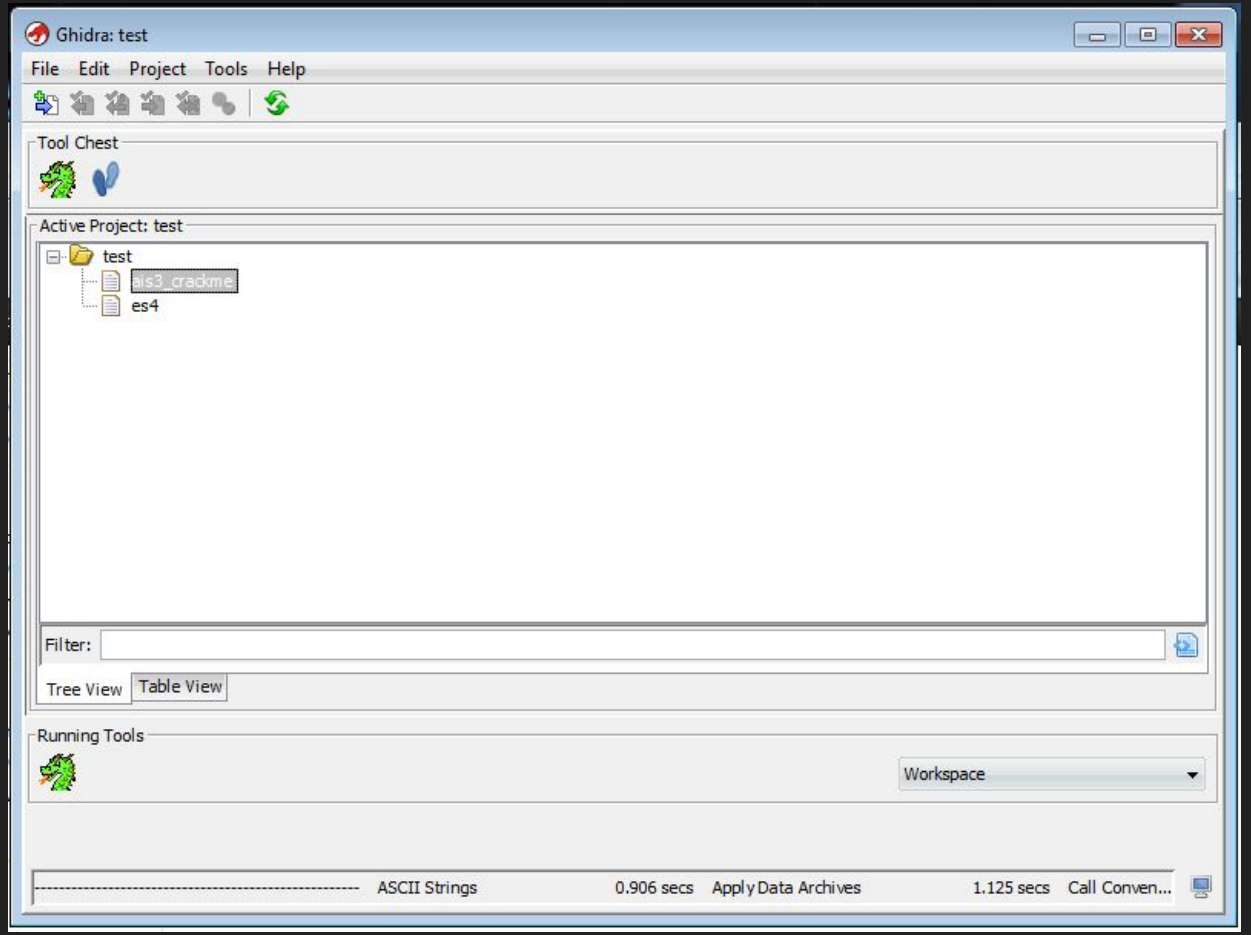
Traduci il Tweet

2 11 47

Dragons

Project manager

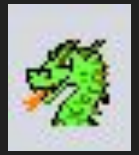
- Everything is a project
- Built in version control
- Direct access to the decompiler



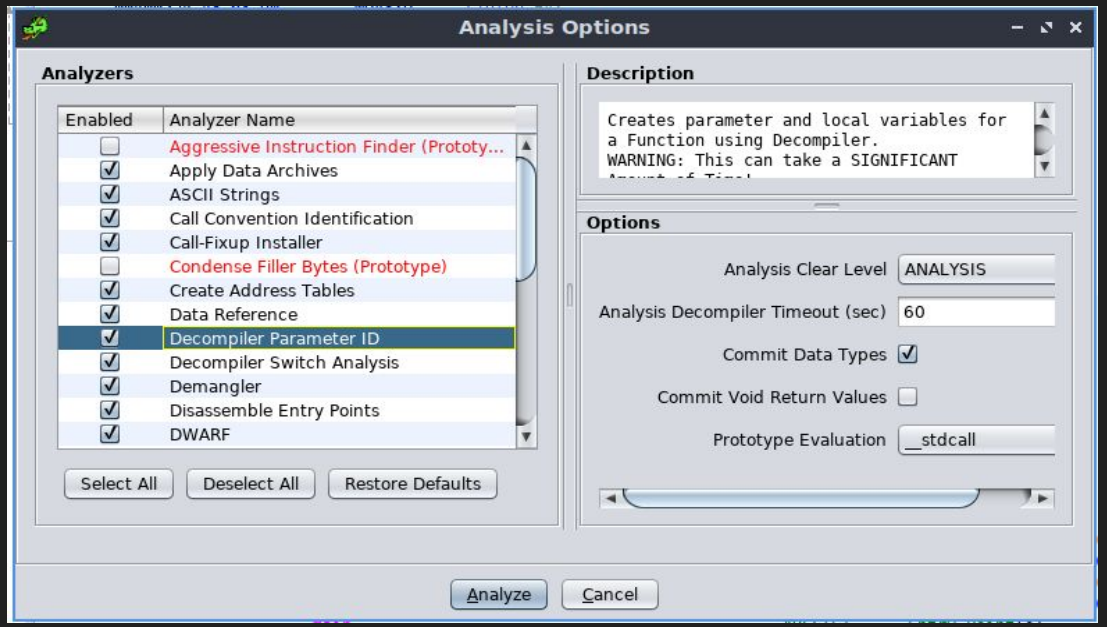
Short intro

- Ghidra is organized as a collection of plugins which can be dynamically loaded
- A tool is just 1 (or more) plugin and their configuration
- Everyone can write his tool to extend Ghidra functionalities

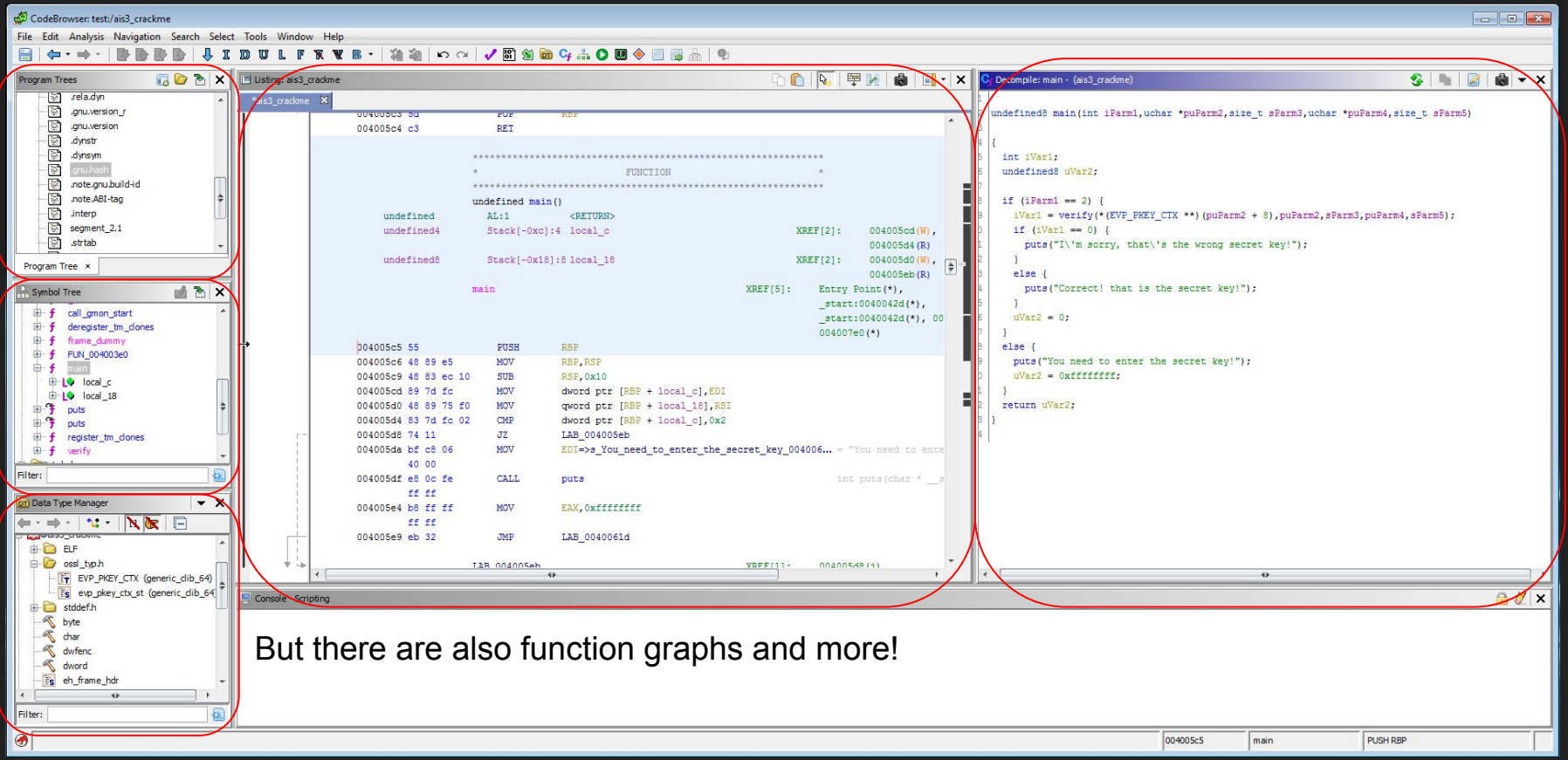
Auto analysis



- The first and most interesting thing that you should run!
  - The usual magic here
- It can be run in multiple steps and can be “augmented” using custom plugins.

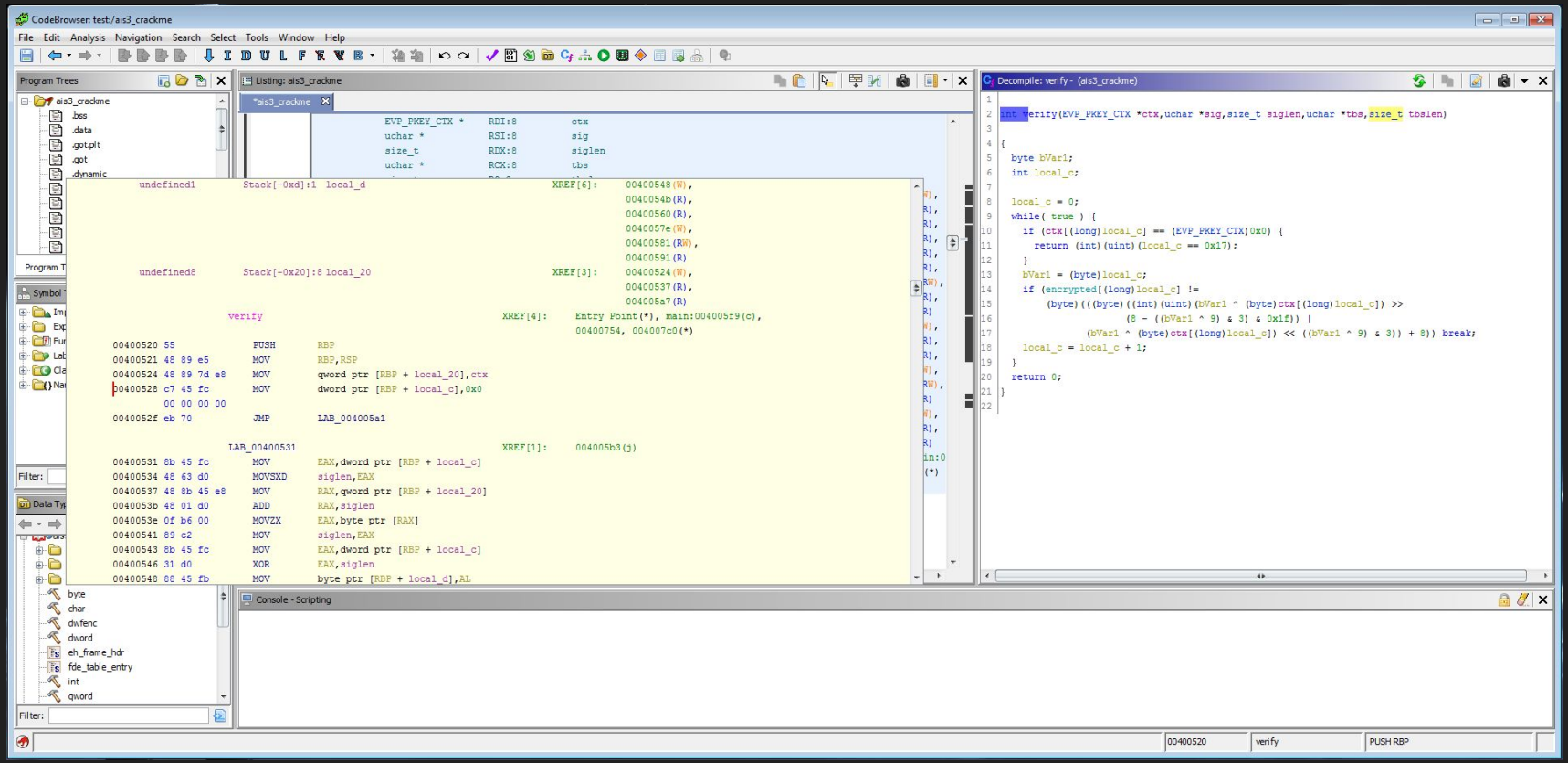


Main interface



But there are also function graphs and more!

Code navigation



Cheat Sheet

https://ghidra-sre.org/CheatSheet.html

Scripting

Ghidra can be extended in two main ways:

- Java (it is its main language)
- Python via the Jython implementation (py 2.7)
- The api is huge!

Nice framework to switch between IDA, Ghidra scripts and viceversa.

- https://github.com/daenerys-sre/source

Scripting (2)

```
import subprocess
import tempfile
import os
import csv
from ghidra.program.model.listing import CodeUnit

def add_bookmark_comment(addr, text):
      cu = currentProgram.getListing().getCodeUnitAt(addr)
      createBookmark(addr, "binwalk", text)
      cu.setComment(CodeUnit.EOL_COMMENT, text)

file_location = currentProgram.getDomainFile().getMetadata()["Executable
Location"]
_, result_file = tempfile.mkstemp()
```

Scripting (3)

```
try:
      subprocess.call(["binwalk", "-c", "-f", result_file, file_location])
      with open(result_file) as csvfile:
            reader = csv.reader(csvfile, delimiter=',', quotechar='"')
            for row in reader:
                  try:
                        addr = currentProgram.minAddress.add(int(row[0]))
                  except:
                        continue

                  text = row[2]
                  add_bookmark_comment(addr, text)
except Exception as e:
      print("Failed")
      print(e)

os.unlink(result_file)
```

A small and unfair comparison

- **Ghidra (vs IDA and redare)**
  - **has Ctrl+z**
  - **no debugger, sorry :(**
  - **collaborative projects**
  - **free and (not yet) open**
  - **looks like it can easily handle large files**
  - **is new but is almost as mature as IDA**

DEMO

References

- http://ghidra.re/courses/GhidraClass
- http://0xeb.net/2019/03/ghidra-a-quick-overview
- http://ghidra.re/ghidra_docs/api/index.html