

Introduction to Ghidra

23 Aug 2019

Sahil Dhar

xen1thLabs

SMART AND SAFE DIGITAL

Whoami



Sahil Dhar

Security Researcher

My area of expertise include Web and Mobile application security. Prior to joining Xen1thLabs, I have worked on numerous projects involving the security assessment of Web, Mobile, Thick clients, Network and Cloud Infrastructure for multiple fortune 500 companies.



@0x401

A former

Security Engineer

Security Consultant

Bug Bounty Hunter

Currently

Security Researcher

@Xen1thLabs

Content

- What is Ghidra
- Getting Started
- Ghidra Project Types
- Understanding Workspace
- Ghidra Scripting
- Limitations

01

What is Ghidra

What is Ghidra

- SRE Framework developed by NSA
- Supports shared projects
- Plugin based architecture
- Highly extensible
- Multi-platform support
- Undo ability



02

Getting Started

Getting Started with Ghidra

- Download the Java Development Kit (JDK) version 11 from <http://jdk.java.net/java-se-ri/11>
- Download the Ghidra zip file from <https://ghidra-sre.org> website
- Extract the downloaded ghidra.zip file
- Navigate to the extracted folder and execute ghidraRun file from commandline
- Provide the path to JDK home directory and we are good to go 😊

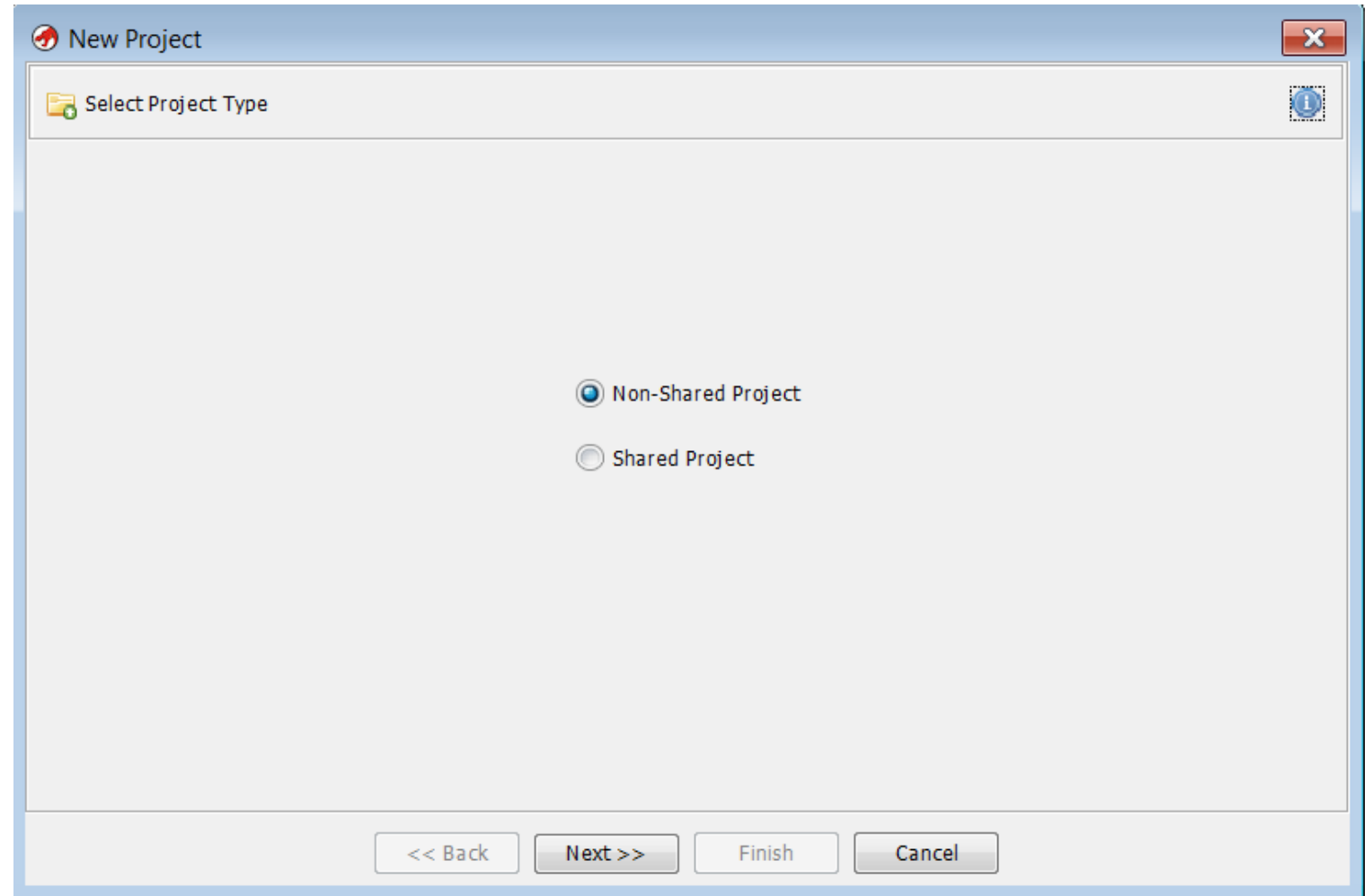
```
6142 ○ ./ghidraRun
*****
JDK 11+ could not be found and must be manually chosen!
*****
Enter path to JDK home directory: /path/to/jdk-11/bin
```

03

Project Types

Project Types

- Non-Shared Project
- Shared Project



Project Types – Shared Projects (Quick Start)

➤ <INSTALL_DIR>/server/

- ghidraSvr.bat
- server.conf
- svrAdmin.bat

➤ Ghidra server configuration (server.conf)

```
1. ghidra.repositories.dir=./repositories
2. wrapper.app.parameter.1=-a0
3. wrapper.app.parameter.2=-u
4. wrapper.app.parameter.3=-ip192.168.0.107
5. wrapper.app.parameter.4=${ghidra.repositories.dir}
```

➤ Adding new user to Ghidra server

```
~: svrAdmin.bat -add tester //default password: changeme
```

➤ Starting ghidra server as console

```
~: ghidraSvr.bat console
```

➤ <INSTALL_DIR>/support/launch.properties

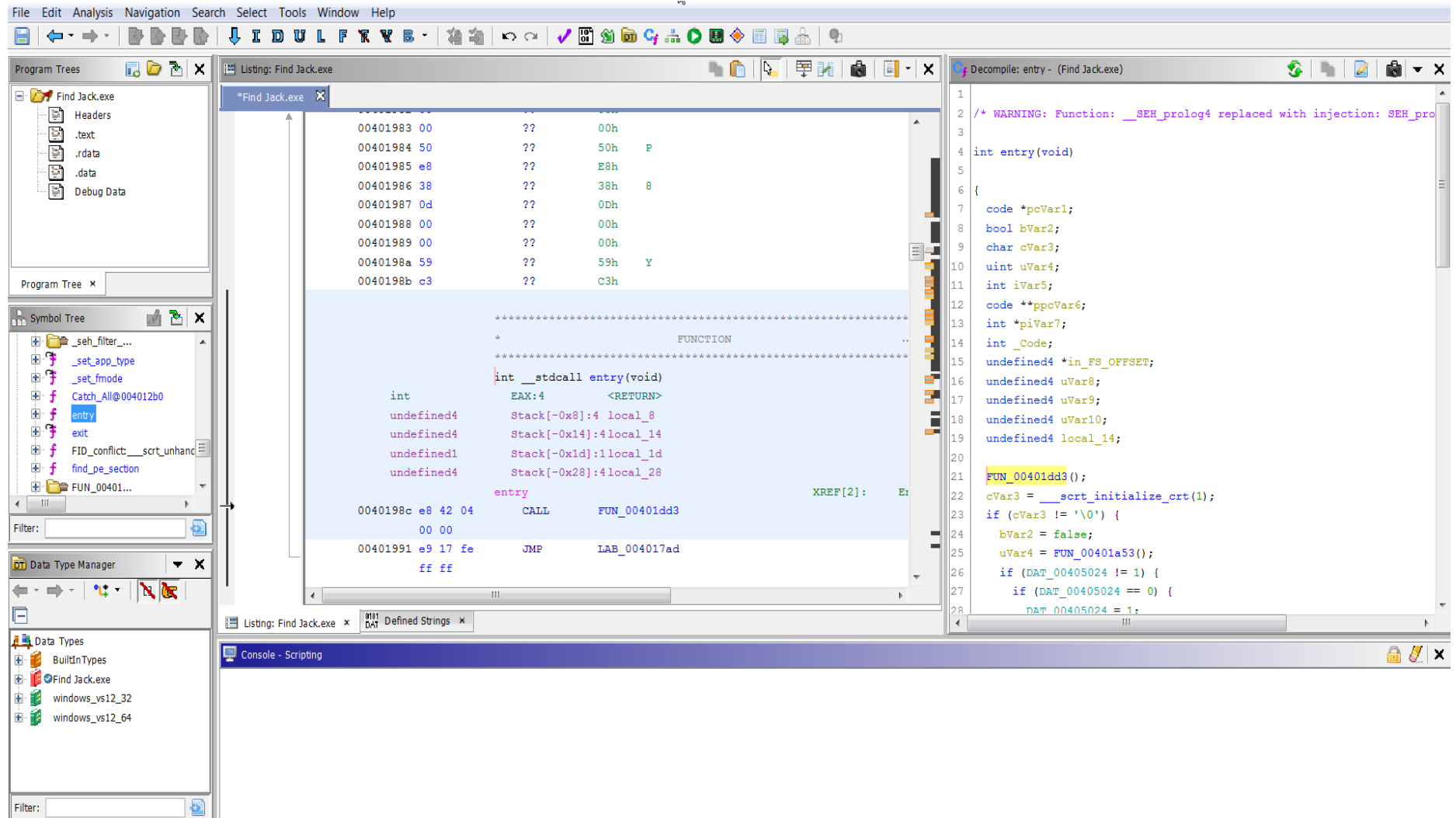
```
~: VMARGS=-Duser.name=tester
```

04

Understanding Workspace

Understanding Workspace

- Program trees
- Symbol trees
- Data type manager
- Listing window
- Decompiler window
- Function call graph
- Function graph








DEMO

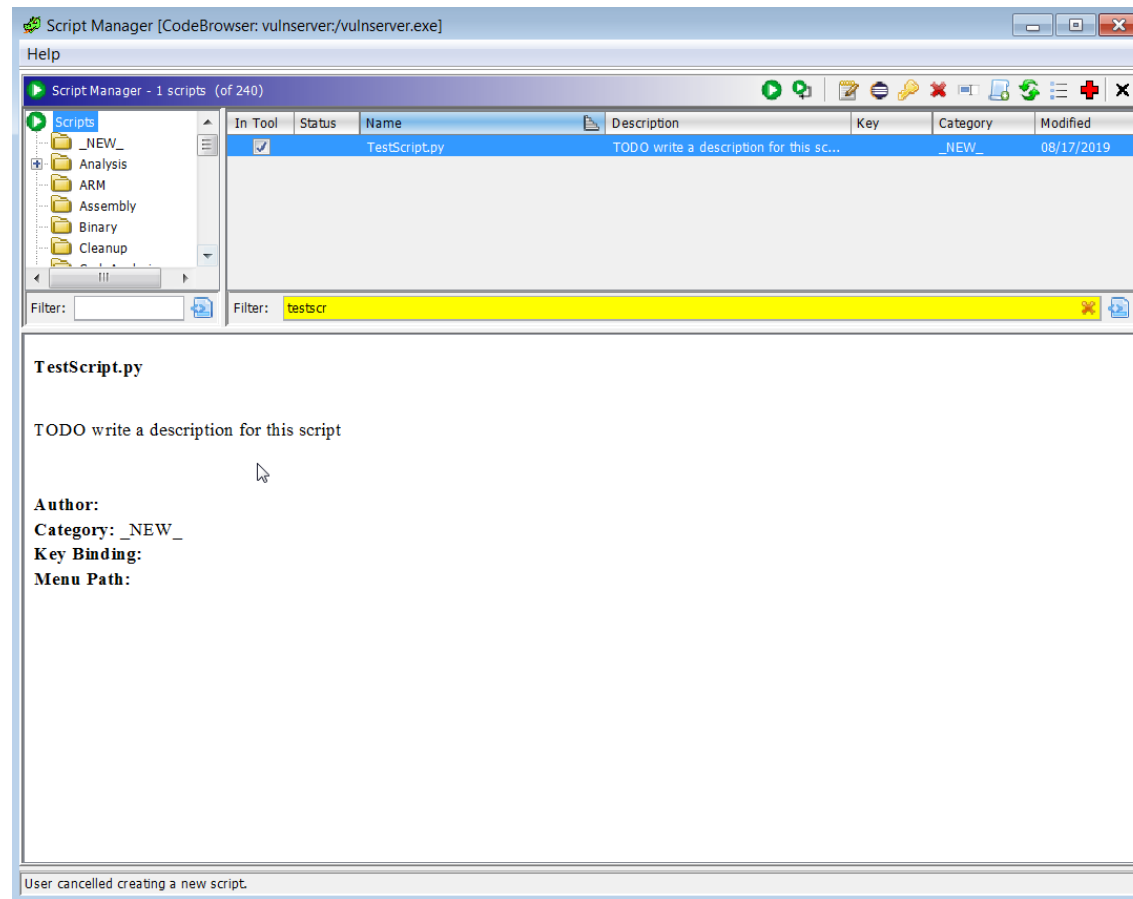
Reverse Engineering Workflow with Ghidra

05

Ghidra Scripting

Ghidra Scripting – Getting Started

- Navigate to Script Manager via menu Windows > Script Manager
- Click on  icon and select the language Java or Python
- Select your <SCRIPT_DIR> and name of your script file
- Click on  icon to edit the script
- Execute your script by clicking on  icon





DEMO

Getting Started with Ghidra Scripting



DEMO

Vulnerability Discovery Automation with Ghidra

Limitations

- No way to X-ref from decompiler
- Variables cannot be mapped
- Variables representation cannot be changed in decompiler
- No debugging support

References

- <https://ghidra-sre.org/>
- <https://ghidra-sre.org/InstallationGuide.html>
- https://ghidra.re/ghidra_docs/api/ghidra/program/model/listing/Program.html
- <https://github.com/JeremyBlackthorne/Ghidra-Keybindings>
- https://github.com/ghidraninja/ghidra_scripts

Questions ?

Thank you 😊