

12 Days of Ghidra

Nathan R

[Twitter](#) | [Mastodon](#)

Day 1 – Crackme

Editing Function Signatures

Ghidra's analysis is a best guess

- Params and return values are often not the correct type

Ghidra allows you to edit the function signature

- Improves readability
 - array index in decompilation
 - Pointer types

RE challenge 1 -> adding correct function signatures

Ghidra Variable Types

Default variable names do not provide much context

- pVar1, pVar2, undefined8

Can be useful as you go along to rename variables to what you think they might be used for (keybind -> L)

- Remember strings from yesterday? Use them to help you :)

For instance - password_maybe, sus_checking_password

Can help you build a more complete picture as you go

Day 1 Crackme

You should RE the static check to produce the correct password string.

Suggestions:

1. Setup correct function signature for main
2. Modify variable names and types to help improve the decompilation

Hints:

- Consider how different data types impact the length of data read