r2ai

https://github.com/radareorg/r2ai

https://infosec.exchange/@dnakov

https://x.com/dnak0v

```
,______  .______ .______  ,___
: __   \ \____  |:      \ : __|
|  \____|/  ____||  _,_  || : |
|   :  \ \   .  ||   :   ||   |
|   |___\ \__:__||___|   ||   |
|___|        :       |___||___|
                      *
```

```
 .--.    .--.    .--.    .--.    .--.
_|_ |   _|_ |   _|_ |   _|_ |   _|_ |
0 0 |   0 0 |   0 0 |   0 0 |   0 0 |
||  |   ||  |   ||  |   ||  |   ||  |
||_.|   ||_.|   ||_.|   ||_.|   ||_.|
|   |   |   |   |   |   |   |   |   |
 `___'   `___'   `___'   `___'   `___'
```

What is r2ai?

- Your reversing assistant, integrated with radare2
- It can use both local and remote LLMs to automate reversing tasks

Why r2ai?

- radare2 has been around forever, LLMs already know a lot of its commands
- LLMs are getting better at reasoning, and can be used for reversing automation
- We want to push the limits of what LLMs can do for reversing
- I can’t remember the radare2 commands

Demo

```
[r2ai:0x00000000]> -h
```

1. What is r2ai?
2. Why r2ai?
3. Demo
4. Basic Usage
5. Auto Mode
6. Other features
7. Installation
8. What’s next?
9. Thanks!

Basic Usage

- `-M` or `-MM` to list the models we like
- use any GGUF model from huggingface `-m <user>/<repo>` (e.g. `-m meta-llama/Meta-Llama-3-8B-Instruct`)
- use any LLM from litellm `-m <provider>/<model>` (e.g. `-m openai/gpt-4o`)
- `-e` to set a configuration variable (e.g. `-e llm.temperature=1.0`)
- `:` to run a command (e.g. `:afl`)
- cli usage `r2ai <bin> -m <model> -c <prompt>`
- plugin usage
  - You can use all the r2ai commands inside `r2`, prefixed with `r2ai`
    - `r2ai -h`
    - `r2ai ' crack this binary for me`
    - `r2ai -m openai/gpt-4o`

Auto Mode

- `r2ai` auto mode can use recursive tool-calling to let LLMs execute radare2 commands and more
  - there are 3 basic tools: `r2cmd`, `run_python`, `execute_binary`
  - currently, you'll get best results with the latest remote models like `claude-3-5-sonnet` and `gpt-4o`
- Caution: auto mode can be dangerous, it can execute arbitrary code

Visual Mode

- `-VV` to enable visual mode (`textual` python package)
- Runs in auto mode only

Other features

- Web Server `-w` to run a openai api compatible local server
  - used by `decai` for awesome decompilation in multiple languages
  - checkout pancake’s talk at https://www.youtube.com/watch?v=KL1yi8FXCKI
- 🎙️ Voice Mode `-a` `-A`
- 📎 Clippy Mode `-r2`

Installation

1. Install `radare2`, preferably from source
2. Install `rlang-python` and `r2ai` with `r2pm`
   - `r2pm -ci rlang-python`
   - `r2pm -ci r2ai`
   - (optional) `r2pm -ci r2ai-plugin`
   - (optional) `r2pm -ci r2ai-server`

What’s next?

`r2ai` is under active development. Feedback is welcome!

- Currently experimenting with training small LLM models on radare2.
  - https://huggingface.co/dnakov
  - https://github.com/dnakov/r2ai-model
- Bug fixing, fighting python packaging
- MLX and VLLM integration
- Rewrite in C someday ™

Thanks!

- https://github.com/radareorg/r2ai
- https://infosec.exchange/@dnakov
- https://github.com/dnakov
- https://x.com/dnak0v
- https://github.com/dnakov/r2ai-model
- https://huggingface.co/dnakov