chess 部署

环境需求:

Mac 电脑一台，需要安装 python3.x 和 redis

macOs 系统应该无特殊要求

iPhone 需要越狱，iOS >= iOS13.0

目录介绍:

```
➜  WMCTF ls -l
total 32
-rw-r--r--@ 1 momo  staff  6386  8  3 10:18 WMCTF 2022 挑战赛 chess writeup.md
-rw-r--r--@ 1 momo  staff  2794  8 11 10:23 WMCTF Chess
drwxr-xr-x  5 momo  staff   160  7 20 16:42 chess
-rw-r--r--  1 momo  staff   881  8  3 10:14 chess_patch.py
drwxr-xr-x  4 momo  staff   128  8  3 14:12 chess_server
drwxr-xr-x  6 momo  staff   192  8 11 10:48 release
```

`./WMCTF 2022 挑战赛 chess writeup.md` 为赛题 writeup

`./WMCTF Chess` 为记录的一些 flag 或者测试用例

`./chess` 目录下为 iOS 赛题源代码

`./chess_patch.py` 为 IDAPython 的 patch 脚本，用来 patch svc 0x80

`./chess_server` 目录下为 webserver 的源码

一般情况下需要关心的只有 `./release` 目录下的文件:

```
➜  WMCTF ls -l release
total 9624
-rw-r--r--@ 1 momo  staff   557048  8 11 10:41 chess.ipa
-rw-r--r--@ 1 momo  staff   557048  8 11 10:41 chess_flag.ipa
-rwxr-xr-x  1 momo  staff  3803642  8 11 10:11 chess_server
-rw-r--r--  1 momo  staff     2397  8 10 15:42 inject.py
-rw-r--r--  1 momo  staff       27  8 11 10:19 requirements.txt
```

`./release/chess.ipa` 是提供给选手的 ipa 文件

`./release/chess_flag.ipa` 是部署在真实 iPhone 上的 ipa。**安装包中有真实 flag，切勿提供给选手**

`./release/chess_server` 是一个用 rust 编写的简单 webserver

`./release/inject.py` 是一个循环执行的脚本，用来从 redis 队列中取任务并执行

`./release/requirements.txt` python 脚本依赖

部署：

Mac 安装 python 依赖 `pip install -r requirements.txt`

iPhone 越狱后在 cydia source 中添加 `https://build.frida.re/` 源，并搜索安装 frida 插件

iPhone 通过数据线连接 Mac，确保只有一台设备连接，在 Mac 端执行 `frida-ls-devices` 显示设备则成功

启动 Mac 本地 redis 服务 `redis-server`，使用默认 6379 端口

启动 webserver 监听 `cd ./release/ && ./chess_server` ，监听地址为：`0.0.0.0:1024`

通过 `curl http://127.0.0.1:1024/chess?urlscheme=Y2hlc3M6Ly93d3cuYXBwbGUuY29t` 测试是否启动成功

正常情况下此时接口接收到请求会往 redis 队列中写一个任务，并且 python 检测到队列中出现任务会取出任务，并且通过 frida 拉起客户端进行执行

该接口会返回一个当前提交的 task_id，选手需要通过该 task_id 来查询自己提交的任务是否执行完成，测试接口：`curl http://127.0.0.1:1024/query?task_id=b6fad70d97cf475fcae6a3125092ec78`。

该 webserver 共提供了两个 get 请求接口，格式分别为：

```
// 提交任务接口参数是：选手输入的 urlscheme base64 后发送
http://127.0.0.1:1024/chess?urlscheme=Y2hlc3M6Ly93d3cuYXBwbGUuY29t
// 查询任务接口参数是：提交任务时返回的任务id
http://127.0.0.1:1024/query?task_id=b6fad70d97cf475fcae6a3125092ec78
```

请严格按照该文档请求，建议前端做一些短时间防止重复点击的逻辑处理，没时间做一些完善的容错处理了😭

当 webserver 启动时也会在子线程启动一个定时脚本用来处理队列中的任务，请确保启动 webserver 前已经连接好 iPhone 设备，确认已启动 redis server。

所以！！！！！实际启动服务阶段需要做的事情：

```
连接好 iPhone
启动 redis-server 服务
cd ./release/ && ./chess_server
```

即可！！