

【用户使用手册】docker方式

原理

当用户无法提供模型给平台时,则可以采用 docker 方式进行黑盒评测。

其基本原理是,用户首选从平台上下载要推理的基础数据集(例如干净样本)和子数据集(例如对抗样本),用自己的模型去分别推理 这两个数据集,将得到的推理结果(即 y)按格式保存成 JSON 文件,这个文件我们称作**中间结果**文件,平台再去按这个 JSON 文件的 内容去评测指标。

使用方法

1. 执行文件, 查看是否运行成功

python main.py

2. 本地编译 docker 镜像

docker build ./ -t demo:latest

注意: opencv-python 包,如果是在 macos 下编译,则需改成 opencv-python-headless 。

3. 登录重明平台,点击菜单「模型管理」→「提交模型」→模型格式选择镜像,可以看到下方显示本用户的 docker 命令,例如:



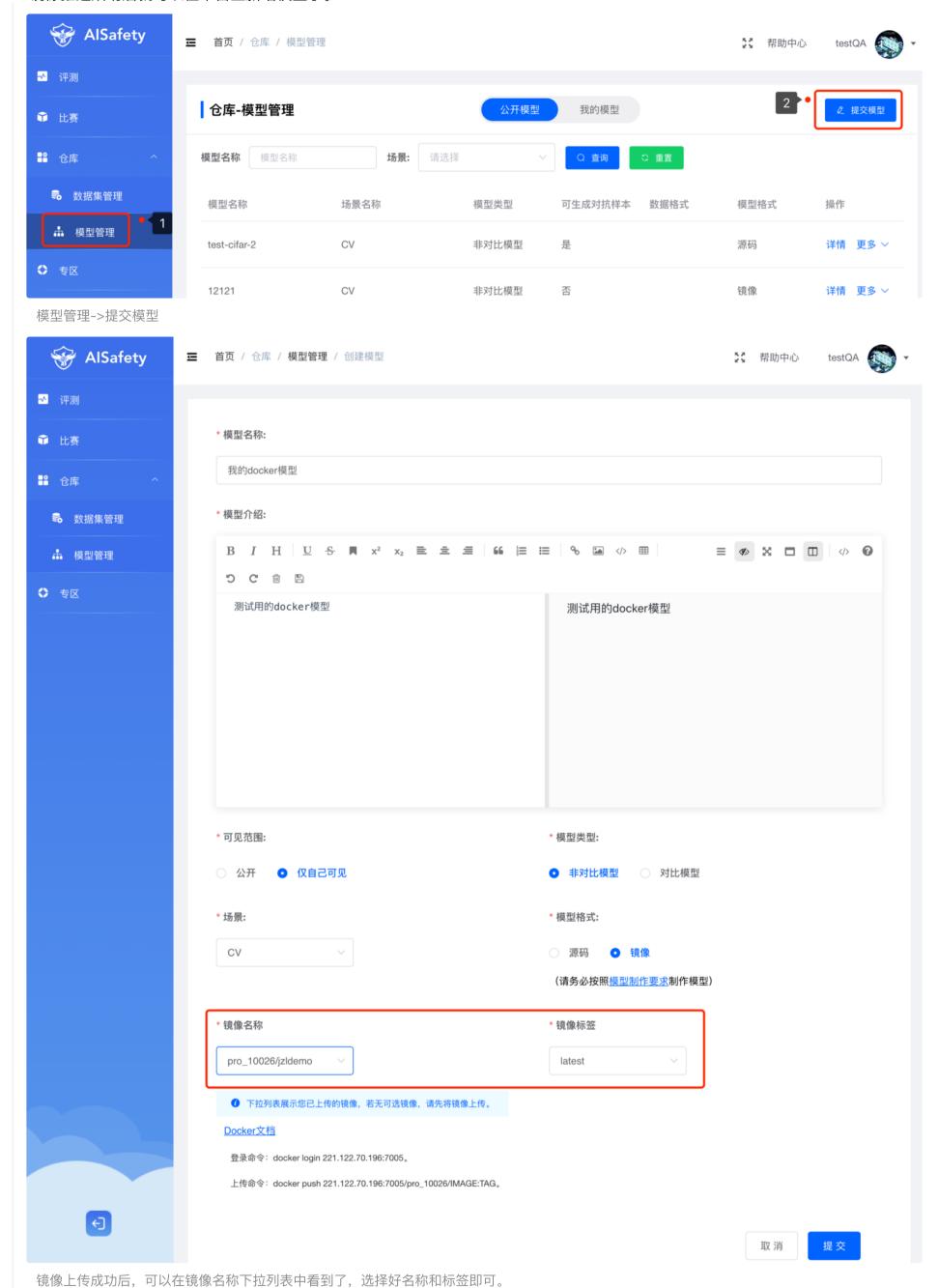
4. 修改镜像 tag,这一步是为了保证可以正常 push 到远程仓库。

注意修改后的tag前半部分必须和步骤3中上传命令的一致 221.122.70.196:7005/pro_10026/docker tag demo:latest 221.122.70.196:7005/pro_10026/jzldemo:latest

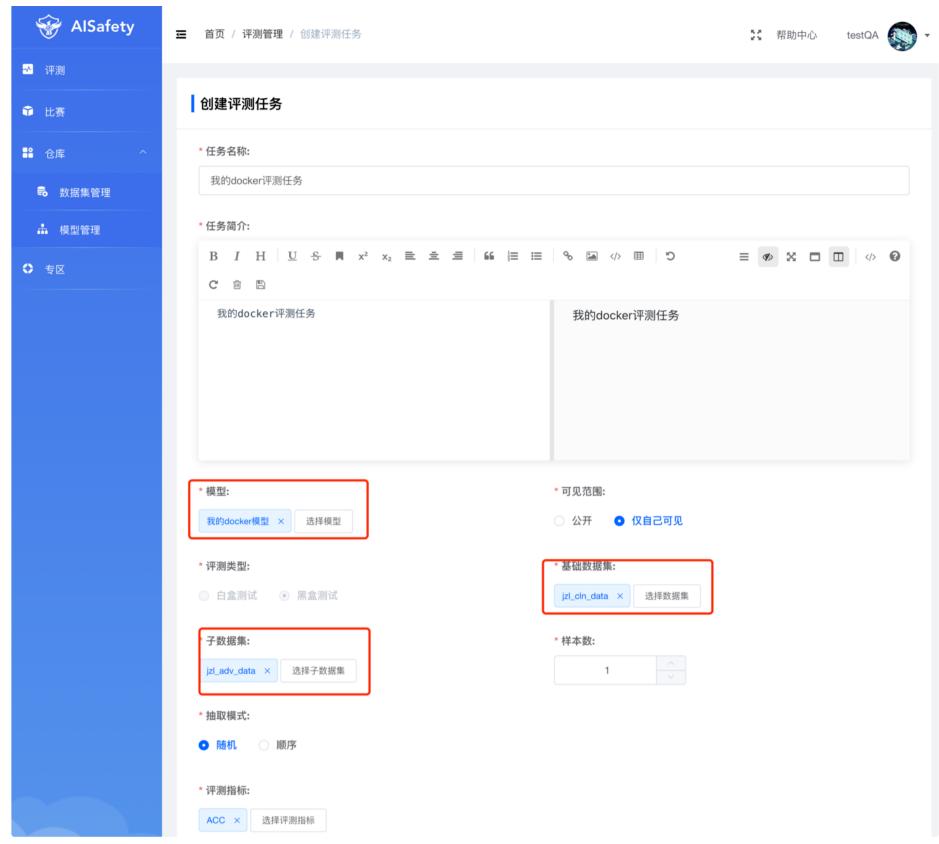
5. 将镜像推送到重明平台仓库

```
# 先登录,使用重明平台账号密码
docker login 221.122.70.196:7005
# 推送
docker push 221.122.70.196:7005/pro_10026/jzldemo:latest
```

6. 镜像推送成功后就可以在平台上新增模型了。

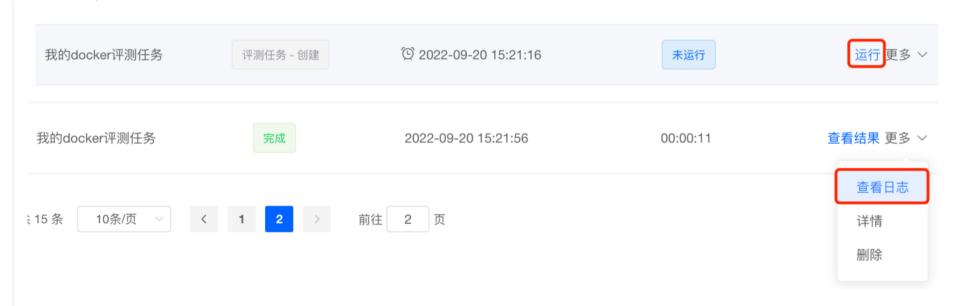


7. 创建评测任务,点击菜单栏「评测」→「创建评测」。



选择要评测的数据集,两个数据集可以通过环境变量传递给docker内的程序

8. 运行评测, 查看日志结果。



非目标攻击结果

评测进度: b'{"code":"0","msg":"","times":1663658515712}'

不存在target /childdataset/pgd/targets/pgd.txt

指标: ACC

IS_COMPARE_MODEL False
IS_PYTORCH_WHITE False

.