**初步用户手册**

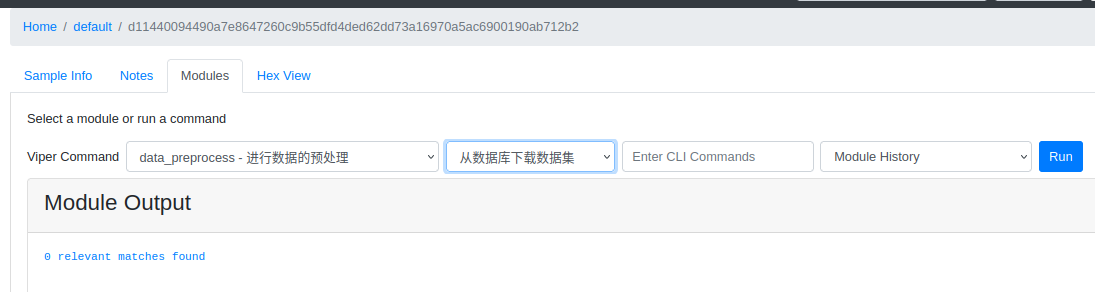
# 1数据预处理模块

## 1.1数据集下载

图形用户界面, 文本, 应用程序, Teams

描述已自动生成

上传任意文件，然后打开会话进入



将下拉框设置为上图所示，然后点击Run

图形用户界面, 应用程序

描述已自动生成

从中可以看出数据集下载完成

图形用户界面, 应用程序

描述已自动生成

可以查看路径，发现该数据集下载完成

## 1.2恶意代码转换成灰度图

图形用户界面, 文本, 应用程序

描述已自动生成

将下拉框设置为如图所示，然后点击Run

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图形用户界面, 应用程序

描述已自动生成

从文件夹中可以看到被处理成不同宽度的图片，这里主要使用的是256宽度的图片。

# 2模型训练模块

1. 编写模型训练脚本

文本

描述已自动生成

Model\_name:只能从设定的三种模型结构里面选择。

Image\_dim:这个参数建议选择使用256，因为自定义识别时是将图片转换成256宽度来识别。

Feature\_type:设置提取的特征是提取图片，对图片进行提取，使用image。

1. 将模型脚本上传

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 运行训练模块

图形用户界面, 文本, 应用程序

描述已自动生成

将下拉框参数设置为如上图，然后点击Run可以进行运行，该部分比较耗时，就不展示结果。

# 3恶意代码检查模块

1. 上传恶意代码

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 检查模型结构(可以查看内置的三个模型的结构)

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 进行恶意代码识别

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

将下拉框切换为如上，使用CNNMalware\_Model1来进行模型识别，可以显示使用的模型，预测为每一种恶意代码家族的概率以及最后的结果。

1. 切换不同模型进行识别

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

里面内置了三种检测的模型来进行识别，可以切换为其他的模型来进行识别。

1. 自定义检测方式

图形用户界面

低可信度描述已自动生成

需要修改配置文件cnn\_params.json文件

图形用户界面, 文本, 应用程序, 电子邮件, 网站

描述已自动生成

添加使用的模型名称以及模型参数的路径在里面。

(6)将结果上传至数据库

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

需要注意的是，必须确保恶意代码的标签只有一个，如果有多个标签，需要人工删除多余的，只保留一个，否则会进行报错提示。