基于 python 开发的入侵检测系统

1、 软件简介

本系统采用 B/S 的三层架构，以 Flask 作为 Web 框架，Vscode 集成开发环境为开发平台，并且使用面向对象程序设计技术对入侵检测系统进行设计与开发，后台数据的存储则是使用关系数据库 SQLite。在对系统的数据库、功能以及性能等内容进行深入分析与设计后，实现了一个功能齐全、操作简便的入侵检测系统。系统主要功能包括：信息搜集、端口扫描、入侵检测、流量捕捉、暴力破解等。

2、 硬件要求

处理器主频：2.20GHZ

硬盘最低空闲：10GB 可用硬盘空间

内存最低配置：2GB

3、 系统要求

操作系统：Windows10 以上

开发工具：Visual Studio Code

数据库：SQLite

4、 软件特色

在计算机技术高速发展的今天，入侵检测系统迎来了新的挑战与机遇。作为网络安全的重要防护攻击，该入侵检测系统提供了五大重要功能，以满足用户的需求：

（1）信息搜集：该模块利用 FOFA API 进行信息收集，能够查询并展示与目标相关的网络资产信息，帮助用户全面了解目标网络的安全状况。

（2）端口扫描：该模块能够扫描目标网络设备的开放端口，识别潜在的安全漏洞，并提供详细的扫描结果，以帮助用户及时采取安全措施。

（3）入侵检测：通过集成机器学习模型（如 CNN 和 LSTM），该模块能够实时监控网络流量，检测并识别异常活动或潜在入侵行为，确保网络的安全性。

（4）流量捕捉：该模块能够实时捕捉并分析网络流量，帮助用户监控网络数据包，识别异常流量，提升网络的安全监控能力。

（5）暴力破解：该模块能够对目标系统进行暴力破解测试，通过尝试多种密码组合，评估系统密码的安全性，并帮助用户识别和修复安全漏洞。

入侵检测系统注重用户体验，界面简洁友好，操作简便，并通过多种方式提高系统的安全性和可靠性，旨在为用户提供一套高效、安全的入侵检测解决方案。

5、 系统使用流程

5.1 系统注册界面

系统的注册界面如下图 5.1.1 所示，用户需要填写账号、密码等个人信息来注册入侵检测系统的账号。

图 5.1.1 系统的注册界面

5.2 系统登陆界面

用户注册完后，就可以登录系统了。系统的登录界面如图 5.2.1 所示。系统登录的过程可以描述如下：（1）用户（管理员）首先打开浏览器，访问系统；（2）浏览器跳出一个登录页面，用户（管理员）输入登录信息。（3）浏览器将输入的账号和密码、验证码发送到后台。（4）系统后台服务器接收请求，将输入数据进行比对，然后响应。

登录模块运行效果如下：

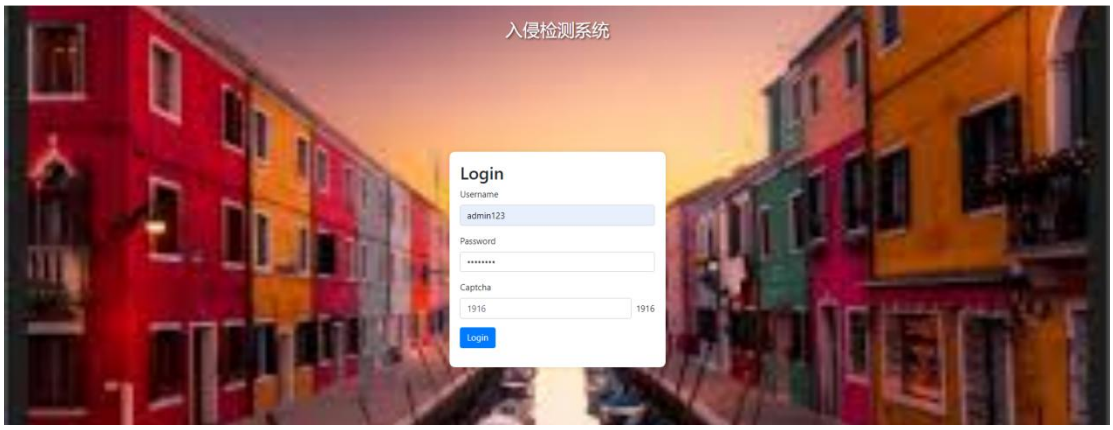

图 5.2.1 系统的登录界面

（2）当用户（管理员）登录进入系统后所看到的主页界面如下图 5.2.2 所示。主页页面显示了入侵检测系统的五大功能。

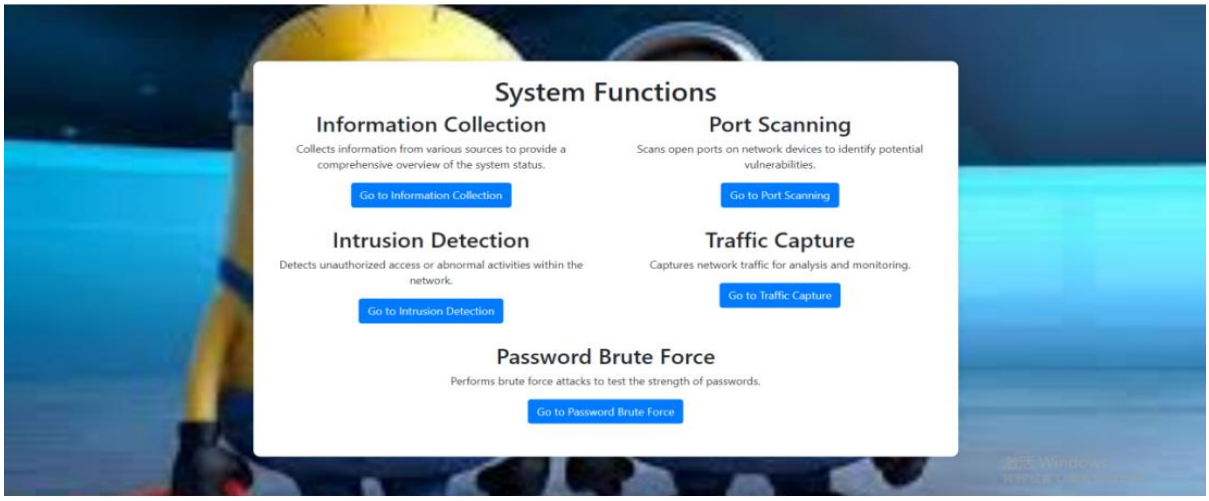

图 5.2.2 系统主页界面

5.3 信息搜集界面

本界面主要是调用 FOFA 网站的接口，对于用户（管理员）来说，他们可以通过 fofa 的相关语法对他们想查的网站进行相关的信息搜寻。图 5.3.1 为信息搜集界面。

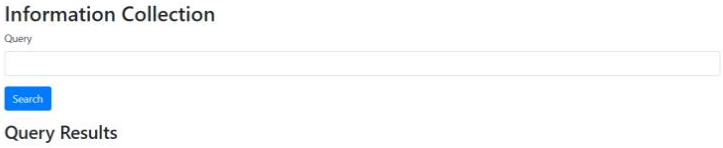

图 5.3.1 信息搜集界面

5.4 端口扫描界面

端口扫描界面能够扫描目标网络设备或主机的开放端口，识别潜在的安全漏洞，并提供详细的扫描结果，以帮助用户及时采取安全措施。图 5.4.1 是端口扫描界面，这里以百度网站为例，进行 80 和 1111 端口的扫描，发现百度的 80 端口开着，1111 端口关着。

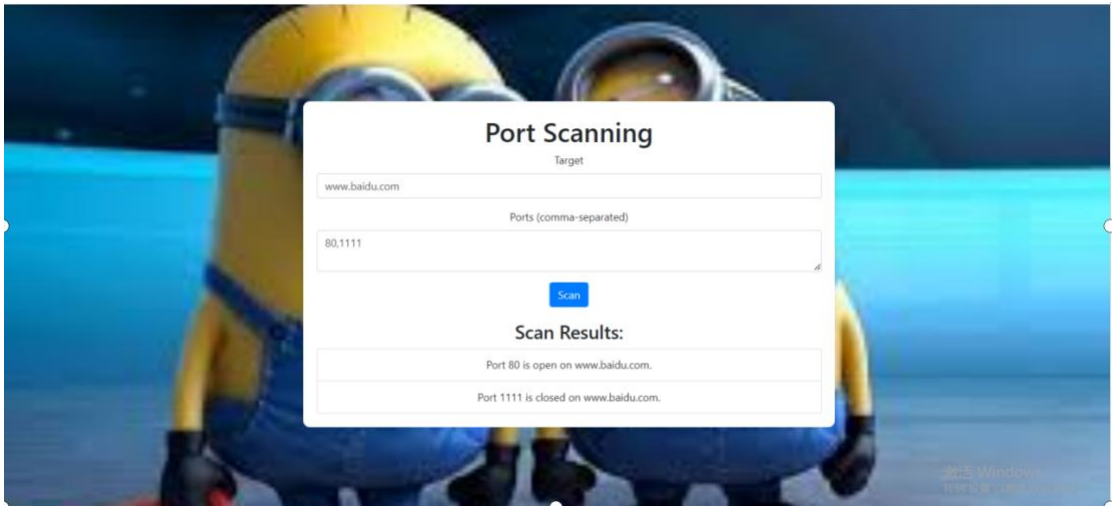

图 5.4.1 端口扫描界面

5.5 入侵检测界面

该模块通过提供两种机器学习模型（如 CNN 和 LSTM），实时监控网络流量，检测并识别异常活动或潜在入侵行为，确保网络的安全性。用户通过上传需要监控的网络流量（训练集和测试集）以及选择模型，便能通过模型训练来对相关的网络流量是否异常进行检测。下面是用户上传数据和选择模型的界面：

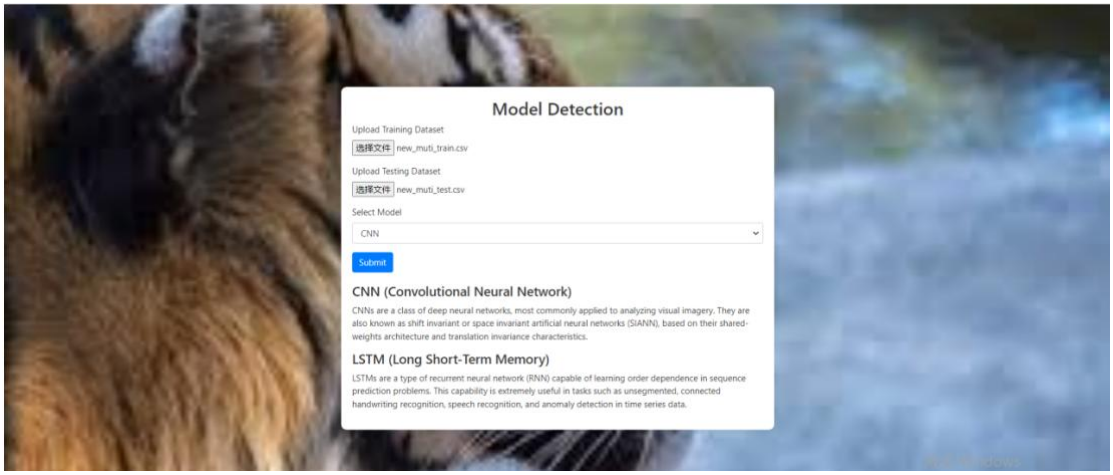

图 5.5.1 上传数据和选择模型的界面

接着，模块会对上传的训练集和测试集的分布进行可视化，如图 5.5.2 所示：

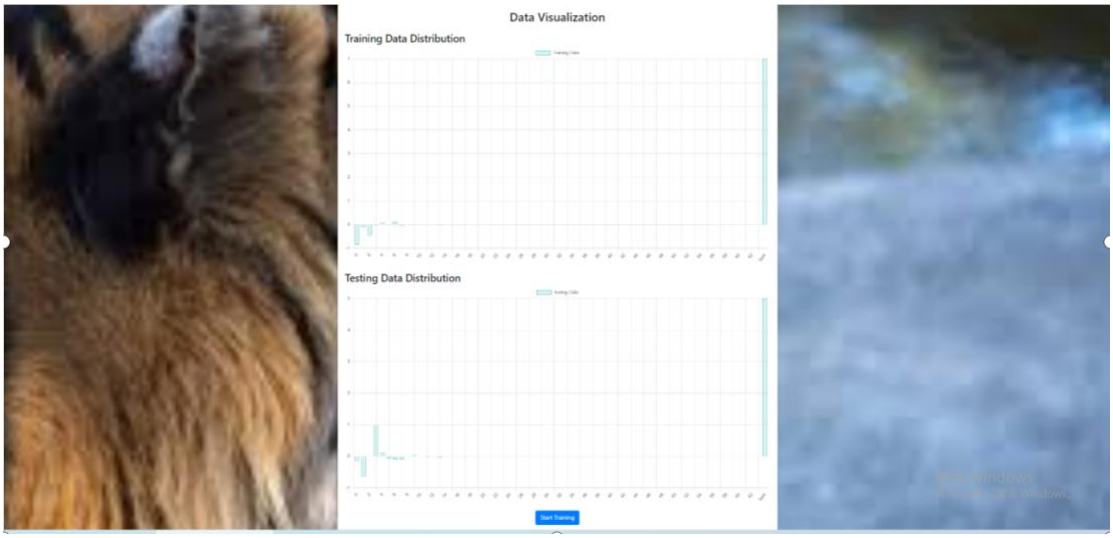

图 5.5.2 数据可视化界面

然后点击最下方“开始训练”按钮，进行训练：

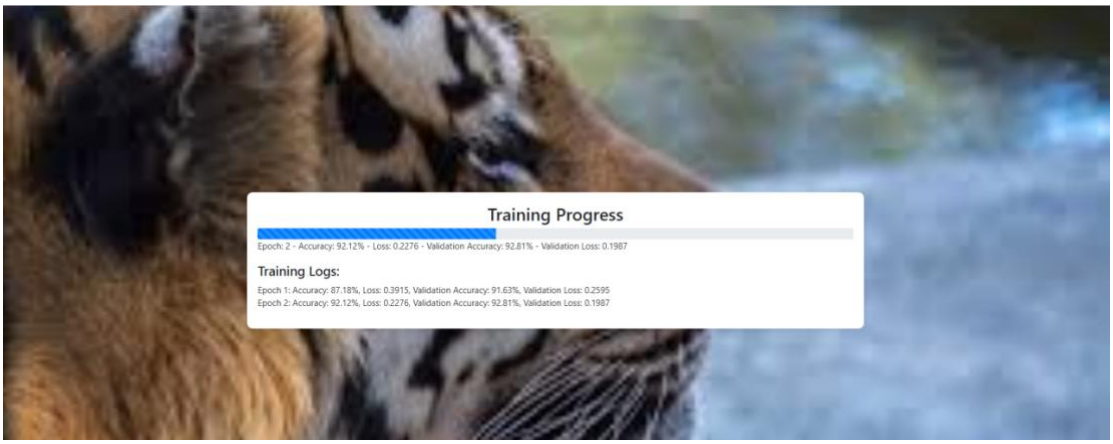

图 5.5.3 训练过程界面

最终训练结果如下：

图 5.5.4 训练结果界面

5.6 流量捕捉界面

在流量捕捉界面，这里调用了 wireshark 的 tshark 模块用于返回监控结果。用户通过输入需要监视的网络接口和监控时间，会对其进行相应的观测。图 5.6.1 是流量捕捉的输入页面，这里以 win10 电脑的 WLAN 为例，持续监视 30s。

图 5.6.1 流量捕捉的输入界面

监视的结果如下：

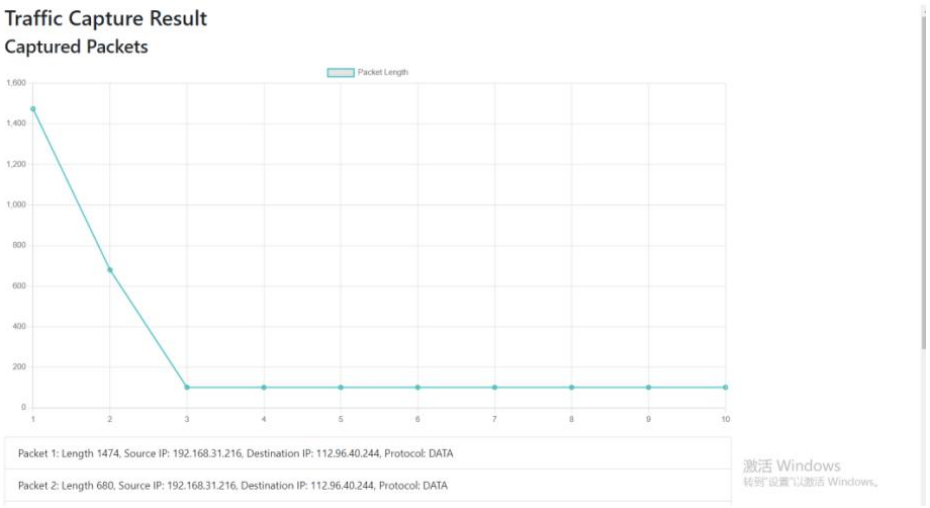

图 5.6.2 流量捕捉的结果界面

当输入错误的网络接口时，会出现以下报错：

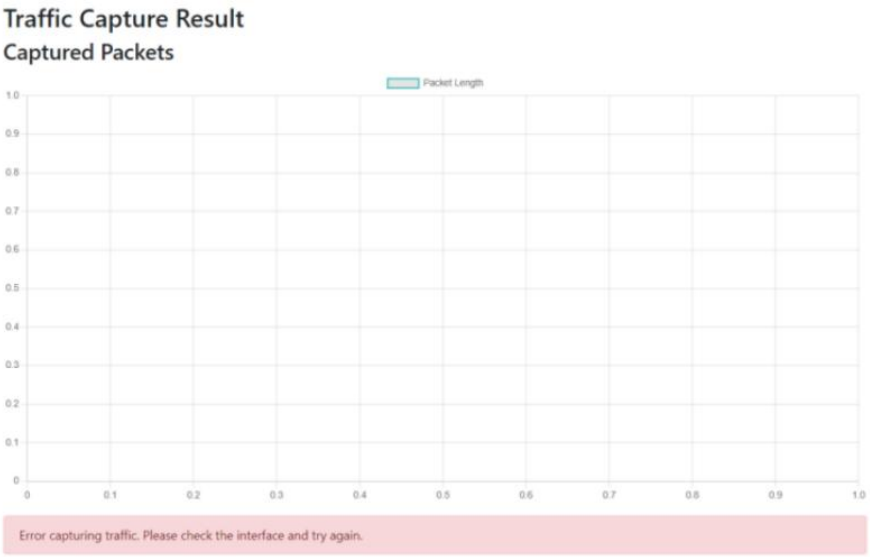

图 5.6.3 流量捕捉的报错界面

5.7 暴力破解界面

该模块能够对目标系统进行暴力破解测试，通过尝试多种密码组合，评估系统密码的安全性，并帮助用户识别和修复安全漏洞。图 5.7.1 是暴力破解需要输入的相关信息（包含目标系统、用户名和密码字典），这里以 win10 为例。

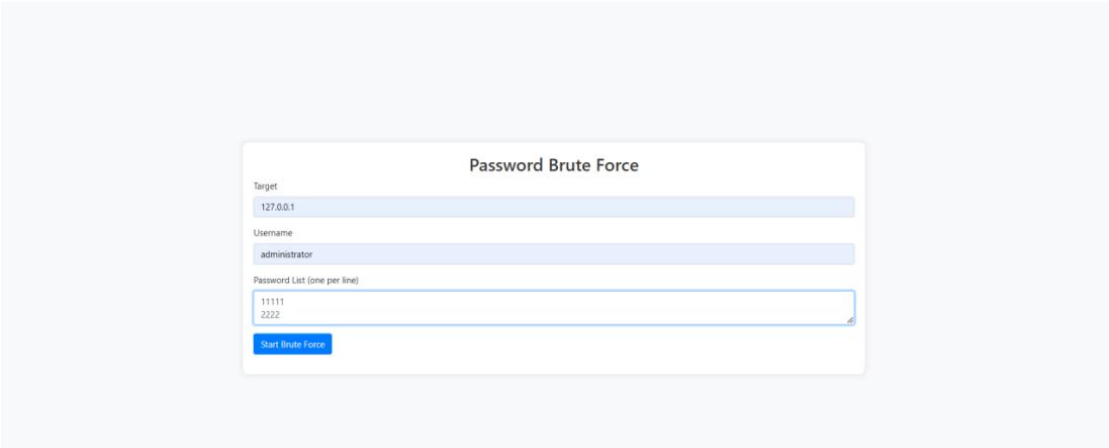

图 5.7.1 暴力破解的相关信息

下面是结果：

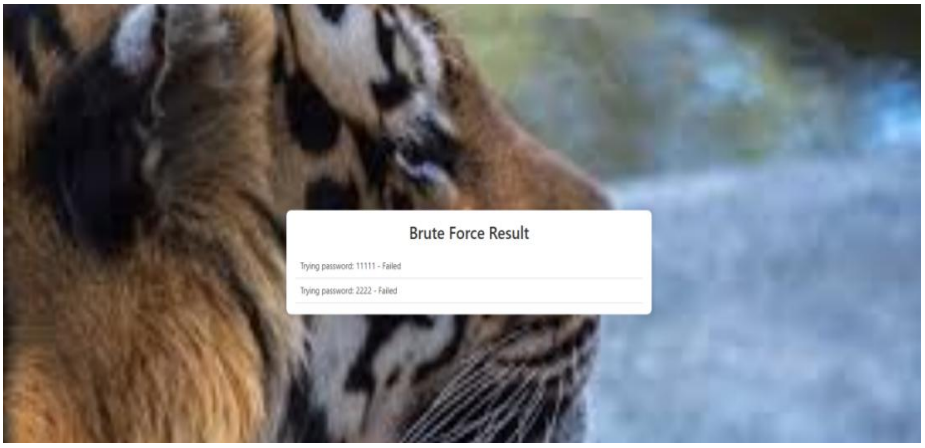

图 5.7.2 暴力破解结果

5.8 用户表界面

这里主要用来查看已注册的用户，表中包含账号和加密的密码，如图 5.8.1 所示。

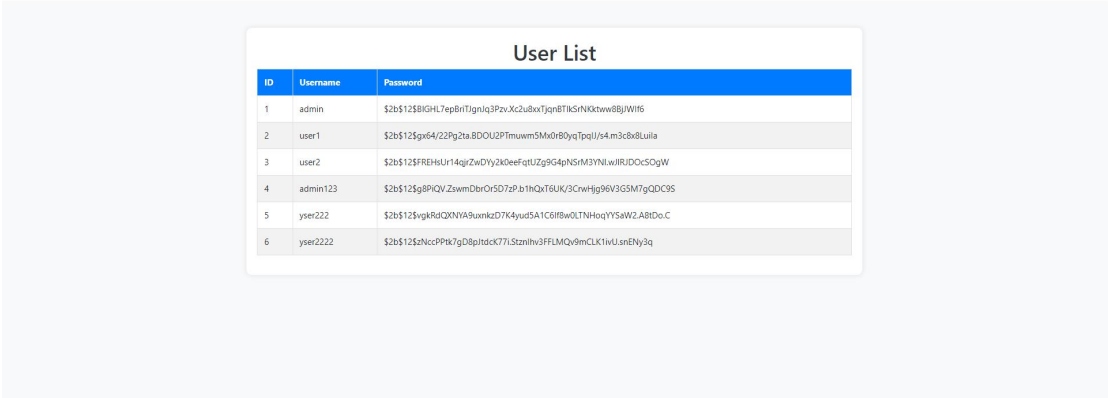

图 5.8.1 用户表界面