题目名称：威胁流量分析实现

一、 环境准备

1. 云主机数量：2 台、基础配置:8C 24G 100G+100G、 操作系统:Centos7.9
2. Python：要求存在 flask 框架、html 模版
3. Chrome：版本要求 110.0.0000.129 以上

二、 题目要求

1. 通过编写脚本实现不同类型、字段的日志数据可以统一入库（输出为 txt，每行一个日志）

- 标准：json 格式，所需字段：startattacktime、attacksrcip、destip、attacktype、payload
- 注意：如果目的 IP 或攻击类型为空设定为不符合标准的数据直接丢弃。
- Attacktype：需要通过自动化方式识别（类型包括 xss、sql 注入、目录扫描、命令注入、弱口令）

2. 通过代码实现流量分析界面展示（展示内容包含：攻击开始时间、攻击者 IP、受害者 IP，攻击类型、攻击详情）

三、评分标准

1. 使用自动化方法处理日志 20 分
2. 处理日志的准确性 30 分

3. 流量分析界面完整（包含所需字段展示） 20

4. 动态获取数据能力展示（数据写入 js，不得分，证明 通过接口发送数据）30

四、预计完成时间（标准答题时间 5 人 8 小时）

5 人 8 小时