

API访问风险评估

背景

某企业为了和保护数据安全，对API访问做了统计，安全团队从服务器上收集到了一天的访问日志数据。这些日志记录了所有对企业内部系统的访问请求，包括正常用户访问和潜在的恶意攻击行为。为了评估API安全威胁并制定相应的防护措施，需要对这些访问日志进行深入分析。

日志文件包含以下字段：

- 访问时间：请求发生的具体时间
- 访问IP：发起请求的客户端IP地址
- 请求URL：被访问的具体资源路径
- HTTP状态码：服务器响应状态
- user-agent：客户端标识信息

企业内部系统包括：认证系统（auth）、人力资源系统（hr）、财务系统（finance）、客户关系管理系统（crm）、监控系统（monitoring）、供应链系统（supply）、研发系统（rd）、法务系统（legal）、外部接口系统（external）。

题干说明

1. 以小时为单位，分析一天工作时间（9:00-17:00）内各小时的访问量分布，找出企业业务高峰时间段。其中，访问高峰时段定义为：该小时的访问量超过9:00-17:00 全时段内平均每小时访问量的时间段。

【评测标准】 请提交访问高峰时段的小时数（24小时制），多个小时按照从小到大排序，用英文逗号分隔。

举例说明，若分析结果显示9点、10点、14点、15点、16点为高峰时段，则答案为：9,10,14,15,16

2. 统计各个业务系统在一天中的访问量，找出访问量前三的系统。

【评测标准】 请提交访问量前三的系统名称，按访问量从大到小，使用英文逗号连接。转换位小写md5提交。

举例说明，若统计到前三访问量的系统如下：

代码块

```
1  认证系统      1333
2  人力资源系统   1222
3  财务系统      1111
```

答案可以通过下面的命令转换为32位小写md5。

代码块

```
1  echo -n "认证系统,人力资源系统,财务系统" | md5sum
```

最终提交的md5为：b1eded0ab5dc654b434e6bc1eb00c377

3. 检测高频访问行为，识别可能的恶意 IP。高频访问行为定义为：同一 IP 在任意一个自然分钟内（即每连续 60 秒且起始时间为整点或整分，如 08:05:00-08:05:59）对同一个接口的请求次数超过 30 次。

【评测标准】 请提交检测到的异常IP数量。若检测到3个异常IP，则答案为：3

4. 为了保障数据安全，公司内部仅允许正常用户的浏览器的User-Agent和开发使用的postman、curl、requests等工具对API进行访问。请检查User-Agent，找到使用其他工具访问API的IP地址。

【评测标准】 请提交使用恶意User-Agent的IP数量。若检测到23个使用恶意User-Agent的IP，则答案为：23