**赛题3：智能化未知漏洞攻击检测以及**

**自动防御闭环**

**一、题目背景：**

随着对外提供服务或接口的业务场景增多，面向用户的访问权限或接口没有充分验证或验证逻辑问题突显，例如越权/未授权漏洞、业务逻辑漏洞以及设备或数据库配置失误导致的安全事件造成敏感数据泄露、直接经济损失或恶意操作等严重后果（比如数据库误配置外网导致数据泄露、API接口未授权漏洞被攻击利用，业务系统存在接口逻辑漏洞导致信息泄露或提权）。此类攻击与业务场景高度相关存在场景差异性，不存在确定性的攻击特征，传统检测基于预置的专家规则在面对此类未知漏洞攻击时无法预定义规则检测，这一直是漏洞扫描和漏洞检测的难点问题，导致防御滞后，闭环时间长。

**二、题目描述：**

赛题需要结合业务场景解决未知漏洞攻击防御问题，核心任务是从大量正常请求行为数据中识别异常行为。目标是基于智能化算法，通过攻击行为识别（如调用顺序、参数组合、攻击目标等），判断攻击者攻击意图（权限滥用、数据窃取等）和攻击载荷等，检测未知漏洞利用攻击，并自动生成和优化漏洞防御规则，实现在线的威胁自动发现和响应闭环。

本赛题需要完整实现以下两个功能：

（1）攻击意图识别和漏洞定位：根据业务场景正常流量特点，结合攻击流量上下文识别攻击意图和结果，判断漏洞类型、漏洞载荷及漏洞点。

（2）自动化防御策略生成：根据识别出的攻击行为和漏洞，结合已有防御规则，自动生成相应的防御策略，并能根据反馈自动优化。

**三、考察选手数据挖掘能力和算法应用能力，挑战内容如下：**

1、有效识别攻击意图和漏洞位置，确保准确率达到95%以上，检测时间<=1H

2、根据识别的攻击意图和漏洞位置，自动生成和优化防御规则，误报率<=10%

**四、交付件**

1、工具源代码。

2、工具源代码技术说明书：工具使用关键技术原理的详细描述，代码功能实现的详细描述。

**五、评价方式**：

请根据提供的比赛环境，包括流量数据集和可添加规则的开源入侵检测环境，利用智能化算法，实现赛题目标，评判标准如下：

1、漏洞发现数量与检测时间：评估程序能否全面地发现给定流量包中的未知漏洞，同时确保检测时间短且资源消耗低。

2、防御规则的可用性与生成时间：评估程序生成的防御规则误报率、漏报率，同时确保响应时间较短且资源消耗低。

3、报告质量：评估选手提交的报告是否清晰详细，是否包含可运行的源代码。

4、创新性：是否有创新的思路、算法或方法在程序中得以应用。

5、编程技能：评估选手编写程序代码的质量和运行效率。

**六、咨询邮箱：** baiyang72@huawei.com

**七、赛题答疑与交流链接：**

https://www.chaspark.com/#/races/competitions/1124132265686347776