**题目1：基于静态分析的二进制代码CWE漏洞检测定位**

**一、题目背景：**

随着软件规模的扩大，二进制代码中的安全漏洞（如缓冲区溢出、整数溢出、硬编码密钥等）已成为网络攻击的主要入口。静态分析技术无需执行代码即可通过数据流/控制流建模等方法识别潜在漏洞模式，但面对大规模二进制代码时，也存在资源消耗高、误报漏报率难以平衡、结果可验证性不足等挑战。本赛题要求参赛者设计兼顾性能与精度的静态分析方案，推动二进制安全分析技术的实用化突破。

**二、题目描述：**

给定一个固件代码测试集，选手需要设计实现一个二进制静态漏洞检测工具，能够检测测试集样本中存在多种常见漏洞类型（如越界写入、整数溢出、释放后重用、缓冲区溢出、命令注入、加密强度不足、硬编码密钥等），并定位漏洞代码位置，能够输出漏洞类型、代码偏移地址、触发路径，支持漏洞模式的规则编写与扩展。

工具分析过程需控制内存占用≤8GB，且对100MB以上二进制文件的分析时间≤30分钟。

**三、考察选手二进制静态分析漏洞识别、性能优化能力，挑战内容如下：**

1、二进制静态分析漏洞识别：能否构建精准的数据流/控制流模型，识别输入源（Source）到危险操作（Sink）的传播路径。

2、性能优化能力：算法复杂度控制与硬件资源管理策略。

**三、交付件**

1、工具源代码。

2、工具设计说明书：技术原理详细描述。

3、二进制程序及部署操作说明。

**四、评价方式**：

从如下几个层面评价工具得分：

1、检测出的漏洞数量与误报率：选手需要提供每个检测漏洞的漏洞位置、漏洞类型、反汇编代码、触发路径、危险信息等用于评估是否误报。

2、适应性与扩展性：是否支持扩展现有漏洞模式的规则，以及能够对新的漏洞模式的添加规则。

3、创新性：是否有创新的思路、算法或方法在程序中得以应用。

加分项：工具分析过程需控制内存占用≤8GB，且对100MB以上二进制文件的分析时间≤30分钟，内存开销越低越好、分析时间越快越好。

**五、咨询邮箱：** liuxing@valiantsec.com