**赛题2：开源代码提交安全相关性分析**

**一、题目背景：**

开源项目每天有大量的代码提交，在这些代码提交中，有feature的合入，有bug的修复，有代码架构的优化等等，在这些提交中，也有很多是安全漏洞的相关修复。如何能够精准识别这些修复是和安全漏洞相关，关系到下游产品能否快速合入这些补丁，消减现网产品的安全风险。

目前各大主流社区都有对应的漏洞管理能力，能够对多数的漏洞实现主动管理，但是因为社区代码量大，每天更新较多，无法完成对所有提交的管理，如果能够自动化的识别到提交是漏洞相关，进而针对性管理是社区漏洞管理的重要难题。

**二、题目描述：**

参赛选手实现一个自动化分析工具，具备如下能力：

1：能够实时感知OpenHarmony社区(以<https://www.openharmony.cn/download>开源代码仓库地址链接介绍信息为准)的提交；

2：针对每一笔提交进行分析和标识，区分出提交类别（安全漏洞类提交需要单独标识）

3：分析安全漏洞相关提交修复的潜在安全问题 ，形成简要的描述和CWE信息；

4：分析此问题在社区所有分支中是否涉及（需要评判的分支包含master/OpenHarmony-4.1-Release/OpenHarmony-5.0.3-Release/OpenHarmony-5.1.0-Release）；

5：如果上述分支涉及此漏洞，需要分析上述分支上是否完成了相关修复；

**三、考察选手漏洞识别和挖掘能力，挑战内容如下：**

1、网页爬虫，能够快速实时全面完整的收集到目标信息。

2、具备丰富安全漏洞知识，能够识别各类安全相关修复。

3、需要有自动化/智能化安全分析能力，识别代码安全修复特征。

4、具备代码分析或验证能力，尤其是针对差异化代码能否识别相同/相似安全问题的分析或验证能力。

**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。

3、工具使用说明书及DEMO演示视频，说明工具运行的依赖环境和操作说明。

4、针对社区指定时间段（比赛当月及上月）所有代码提交的分析报告（主要指的是识别是否安全漏洞相关提交的分析报告），针对是安全类问题提交的需要给出对应判断主要依据和分析逻辑。

备注：

1：OpenHarmony社区官网安全主页（https://www.openharmony.cn/security/overview）安全漏洞披露链接中历史披露漏洞可以作为工具样本进行验证。

2：commit message等非代码性信息可以作为分析辅助参考，而不应该拿来作为分析的主要参数和判定引子。

**五、评价方式**：

1、准确性：识别的安全漏洞相关提交的准确度，尽可能不误报。

2、完整性：是否能够完整识别到所有安全相关提交，尽可能不漏报。

3、分支是否涉及的准确性和完整性。

备注：

1：能够尽可能多的识别的安全相关提交会有对应正向加分；

2：误报问题会有对应的负向扣分；

3：因为分支代码差异不同，而能够识别到对应安全问题的会有对应正向加分；

4：识别的安全修复类型（比如越界、信息泄露等）数量会有对应的权重分数；

5：能够快速/实时/准确的分析也是评判的重要引子；

6：普通DOS类/功能类等非传统意义健壮性问题不作为安全类问题；

**六、咨询邮箱：**

zhangadong@huawei.com

**七：赛题互动交流答疑社区链接：**

https://www.chaspark.com/#/races/competitions/1124131390662258688