# （一）开源软件漏洞感知系统

## 系统背景:

开源软件广泛采用协同漏洞披露政策（Coordinated Vulnerability Disclosure，CVD）来管理开源软件漏洞。协同漏洞披露政策建议将发现的漏洞私下报告给开源软件维护人员，以便在漏洞正式披露之前不会公开讨论相关信息。开源软件维护人员进行隐秘漏洞修复，公开提交补丁，之后通过安全披露平台（National Vulnerability Database, NVD）来公布安全漏洞。开源软件用户通过安全披露平台感知到漏洞，之后应用补丁来消除安全隐患。然而，在这个过程中，安全漏洞可能会在公开信息渠道被提前讨论（例如，在GitHub、 JIRA， Bugzilla等社区中进行讨论）。这导致攻击者可以利用这些泄露的信息进行安全攻击直到开源软件用户从NVD平台感知到漏洞并修复。因此，只依赖于安全披露平台进行漏洞管理使得开源软件用户处于极度安全风险中，用户需要提前感知安全漏洞来进行提前防御。

## 主要功能

开源软件漏洞感知系统开发的主要目的是结合深度学习模型对可能存在于代码中的漏洞进行提前感知，主要功能模块包括：三个模块。

（1）代码变更：

用户可以方便管理代码变更提交，了解代码变更前后的差异。

（2）漏洞扫描：

基于用户代码变更提交，采用方法级数据增强的对比学习算法，构建漏洞扫描模型，识别代码中潜在的漏洞。

（3）漏洞感知：

如若识别了代码中潜在的漏洞，用户可以查询该漏洞所属的Common Weakness Enumeration (CWE) 种类及其在Common Vulnerability Scoring System (CVSS) 3.0下的可利用性风险等级，用户操作完成后可以退出系统。

## 开发环境

操作系统及版本：Windows 10 专业版

支撑软件及版本列表：PyCharm + Python-3.9 + IntelliJ + jdk-15.0.2 + Vue3

数据库环境：MongoDB

## 基本的架构体系

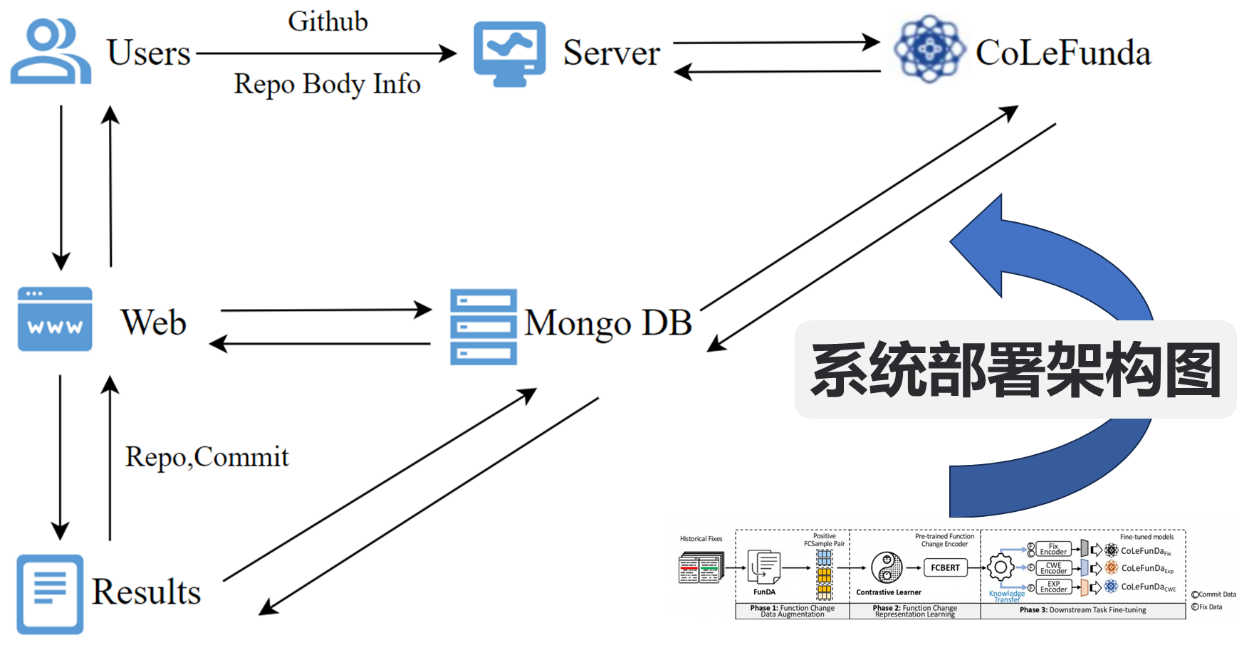


图 1 开源软件漏洞感知系统功能结构图

代码变更：用户可以方便管理代码变更提交，了解代码变更前后的差异。

漏洞扫描：基于用户代码变更提交，采用方法级数据增强的对比学习算法，构建漏洞扫描模型，识别代码中潜在的漏洞。

漏洞感知：如若识别了代码中潜在的漏洞，用户可以查询该漏洞所属的Common Weakness Enumeration (CWE) 种类及其在Common Vulnerability Scoring System (CVSS) 3.0下的可利用性风险等级，用户操作完成后可以退出系统。