安全玻璃盒

让安全更简单更智能

SCA 软件成分分析检测系统

产品手册

杭州孝道科技有限公司

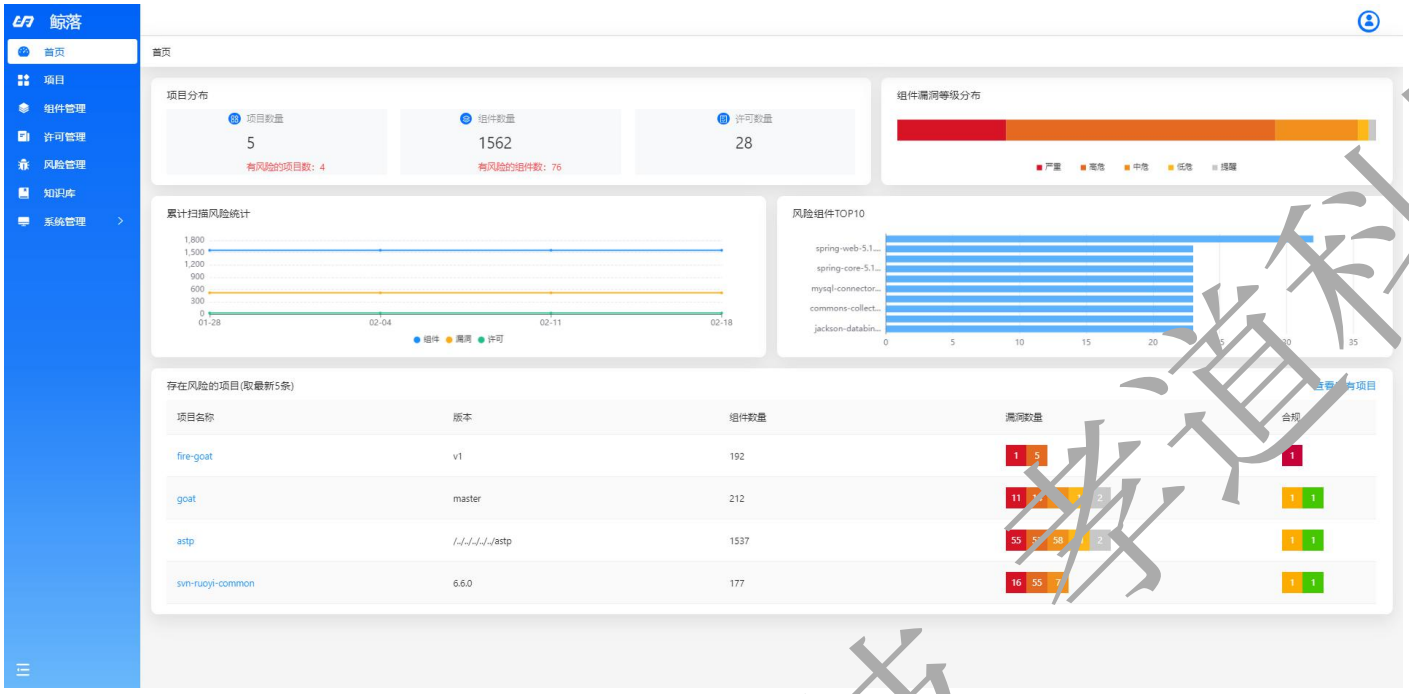
目录

1 系统登录

输入登录页面地址，打开登录页面，输入管理员分配的用户名及密码，即可登录成功，进入系统主页。

2 主页

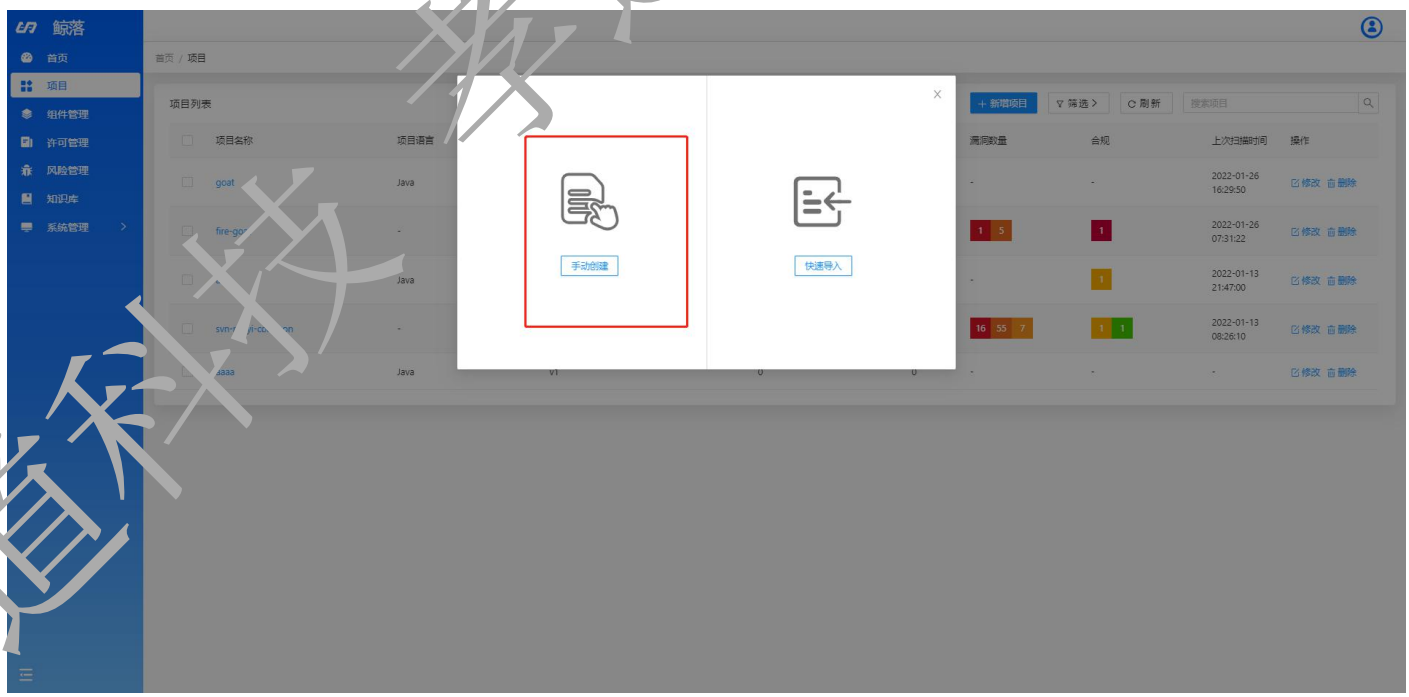
SCA 主页是对所有项目数据的统计，在主页我们可以查看到所有项目的不安全的组件漏洞情况、项目许可以及累计扫描风险趋势等情况统计，通过主页的数据展示，我们可以快速直观地了解到项目存在的风险及相关安全人员可以根据风险情况快速作出响应。



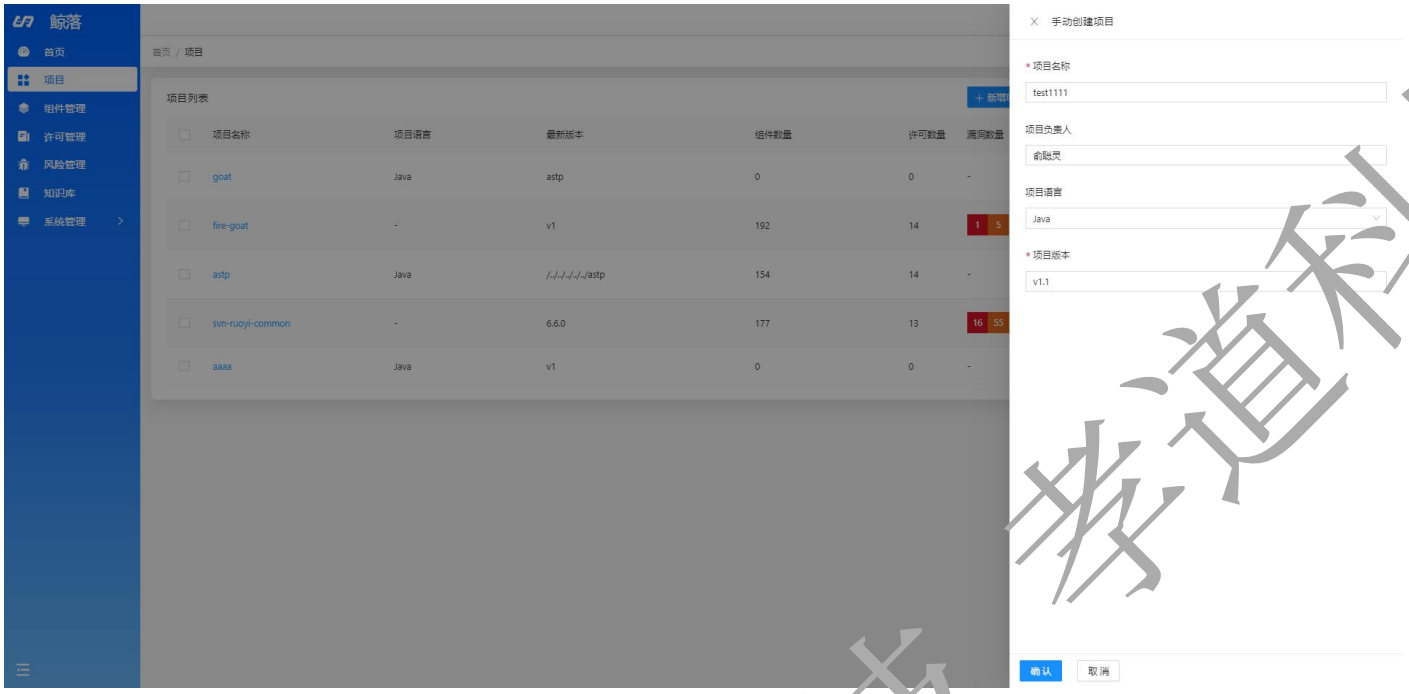
3 创建项目

3.1 手动创建

点击右上角新增项目，选择手动创建



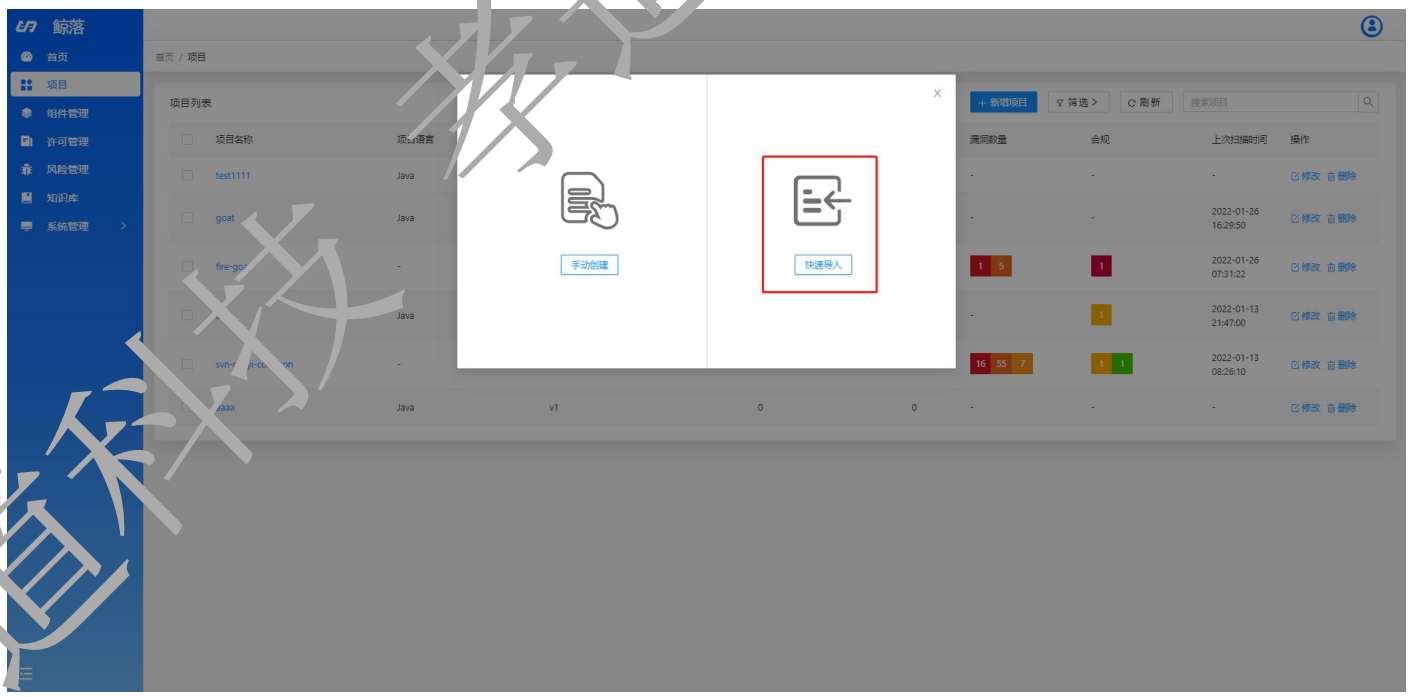
按照页面提示填写项目信息



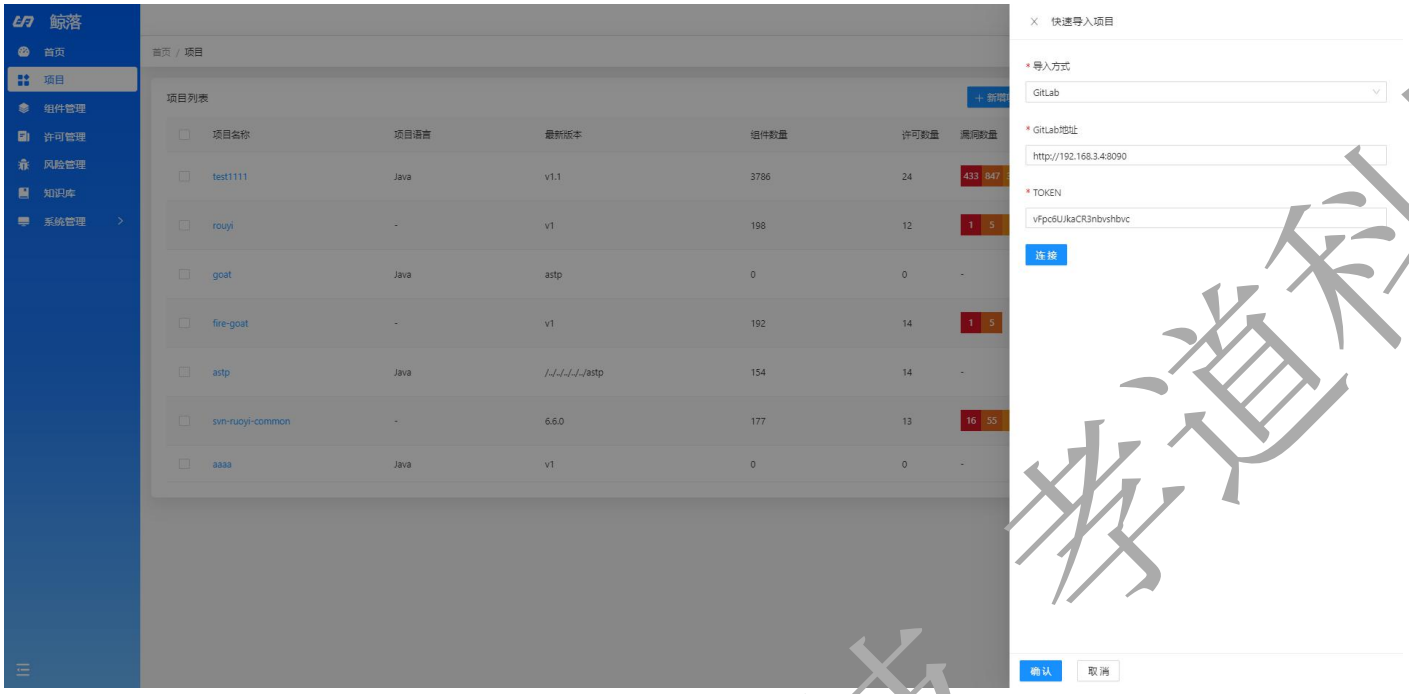
3.2 快速导入

3.2.1 Gitlab 导入

点击右上角新增项目，选择快速导入

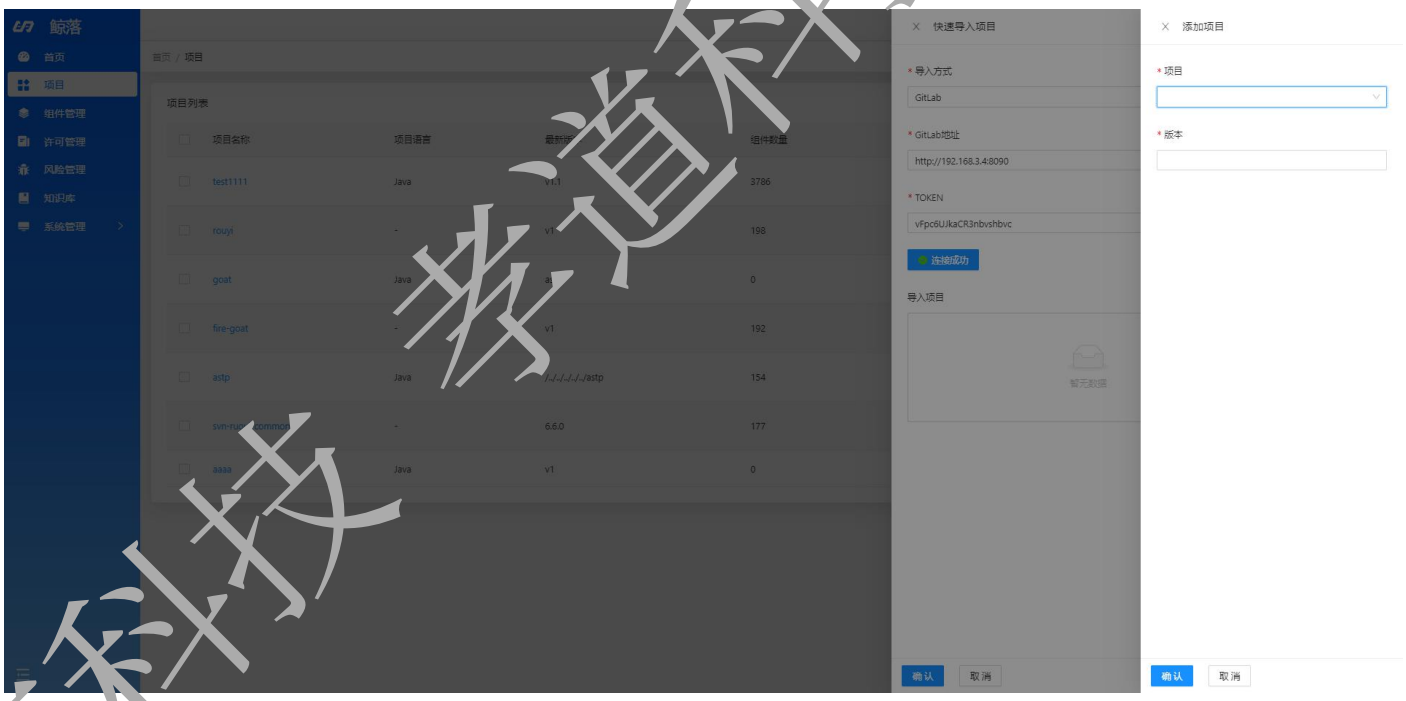


选择远程仓库类型为 Gitlab，添加地址和链接凭证后可以连接到对应的远程仓库

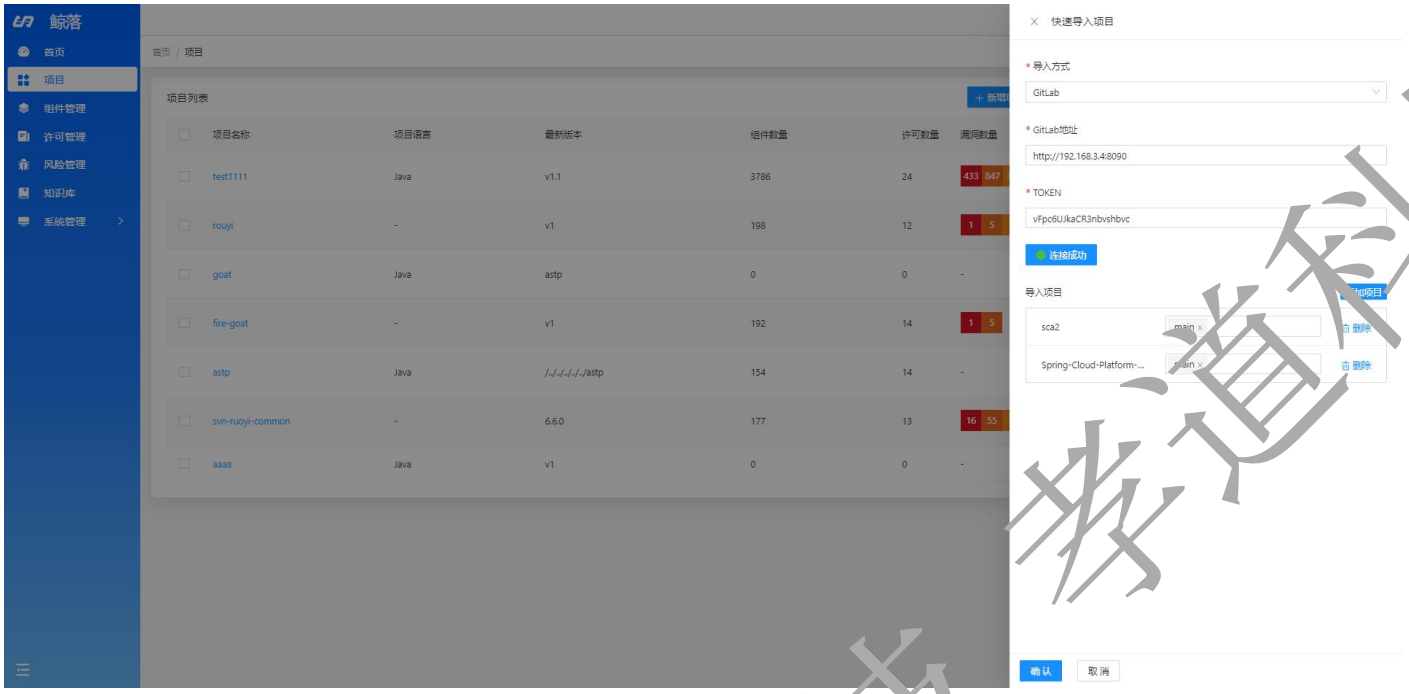


连接成功后，会拉取远程仓库的项目列表，根据需要可以选择需要的项目以及对应的版本，进行导入

导入成功

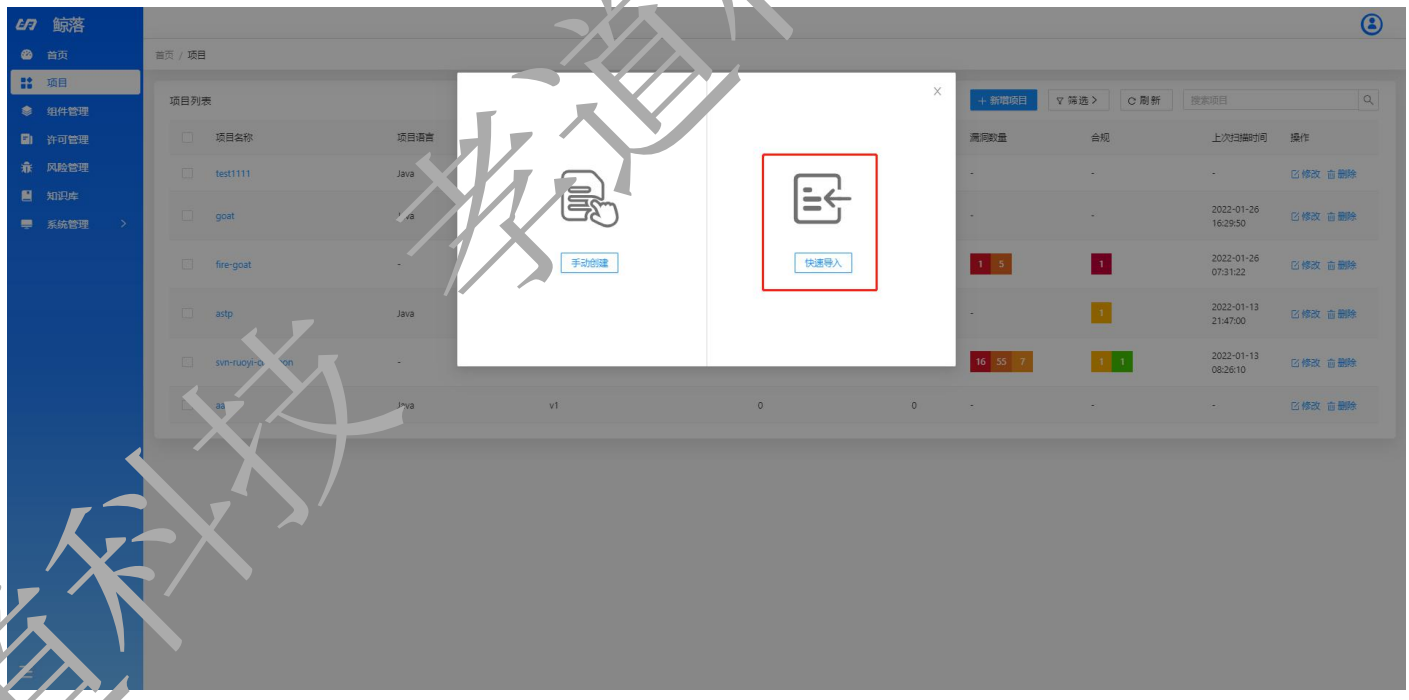


可以根据需要导入多个项目以及版本

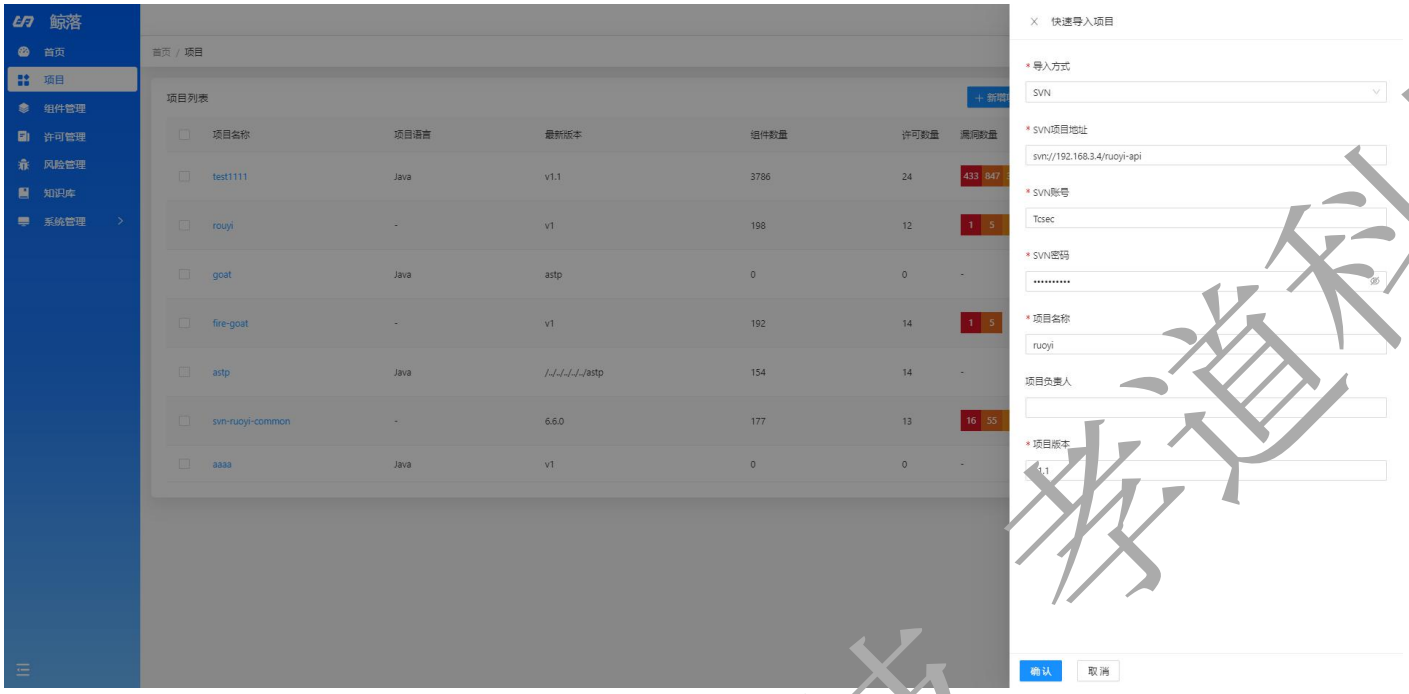


3.2.2 SVN 导入

点击右上角新增项目，选择快速导入



选择远程仓库类型为 SVN，需要填写 SVN 中具体项目文件夹的地址，单次只能导入一个项目的一个版本，保存成功后，即可创建对应的项目以及版本。



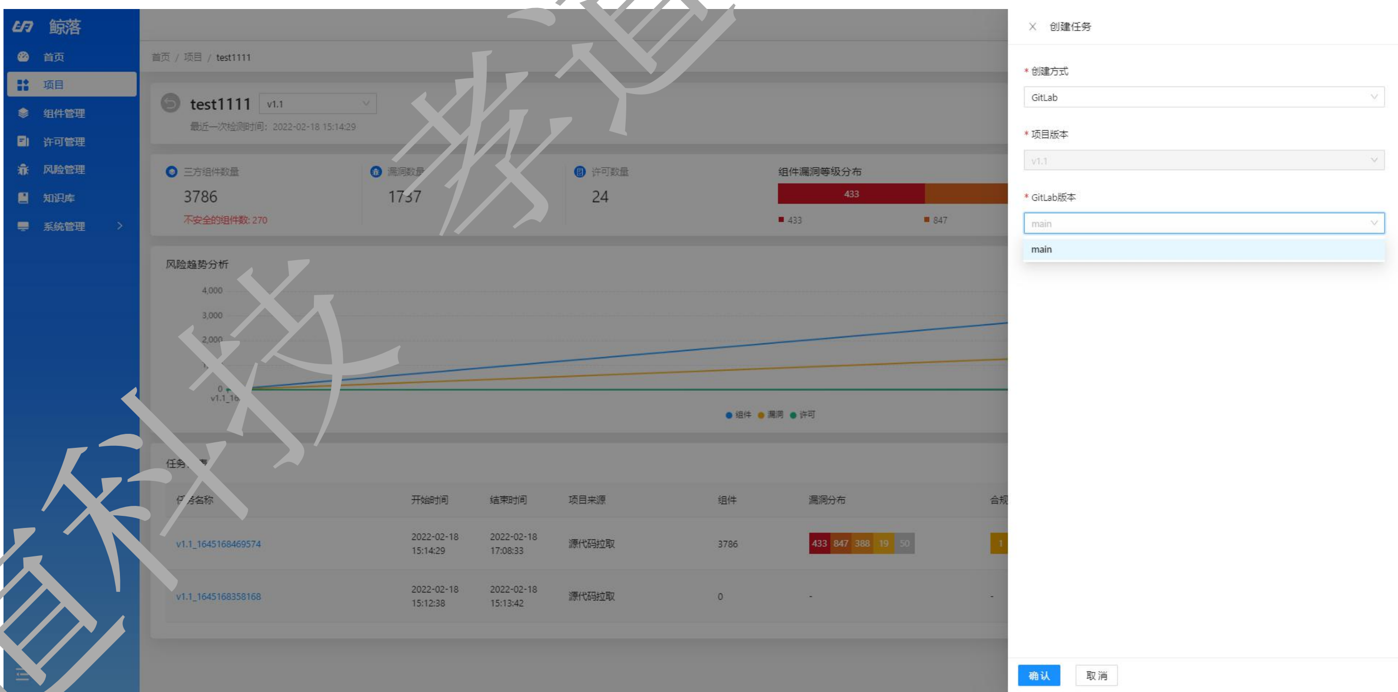
4 创建扫描任务

4.1 文件上传

如下图所示，我们支持物料文件（500m 以内 jar 格式的文件）、二进制文件（500m 以内的 jar 包或者 war 包）以及源代码（500m 以内 zip、rar、tar 或者 tar.gz 格式的文件）三种类型文件的上传，将文件上传，点击保存后系统将会自动进行扫描分析。

4.2 Gitlab 获取

当已经在项目设置中对 Git 进行配置后，可以选择 Gitlab 创建方式，根据已经配置的地址、token 以及项目获取到需要创建任务项目的分支，您可以根据需要选择对应的分支进行任务的创建。



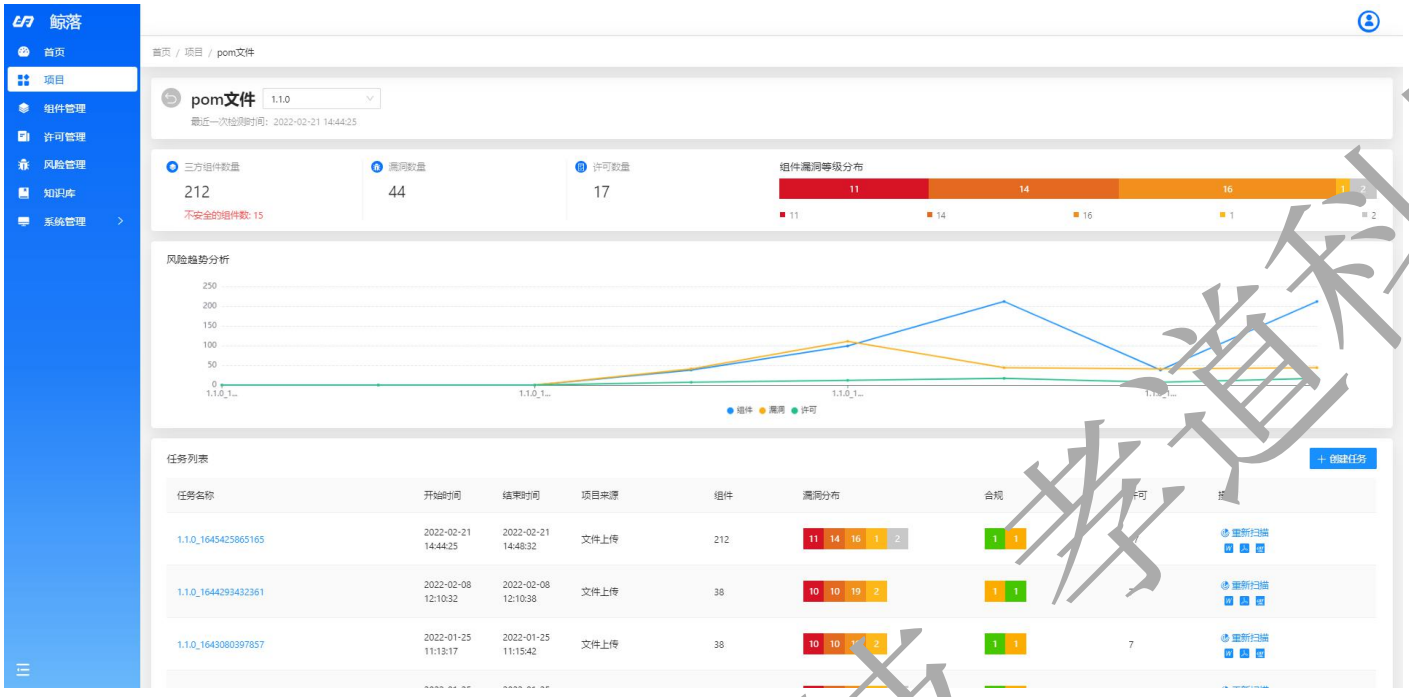
4.3 SVN 获取

通过 SVN 创建任务时，需要填写具体的项目文件夹地址，SVN 账号以及密码，您可以根据需要选择对应的项目文件夹进行任务的创建。

5 项目

5.1 总览

项目总览页面主对当前项目数据的统计，在这里您可以查看到当前项目基本信息、组件数量、漏洞危害等级及状态分布情况、风险趋势分析以及扫描的任务列表。通过总览页面，您可以快速直观地了解到当前项目所存在的风险情况。在扫描任务列表，可以根据需要以 word、pdf 以及 csv 三种形式导出扫描任务报告。

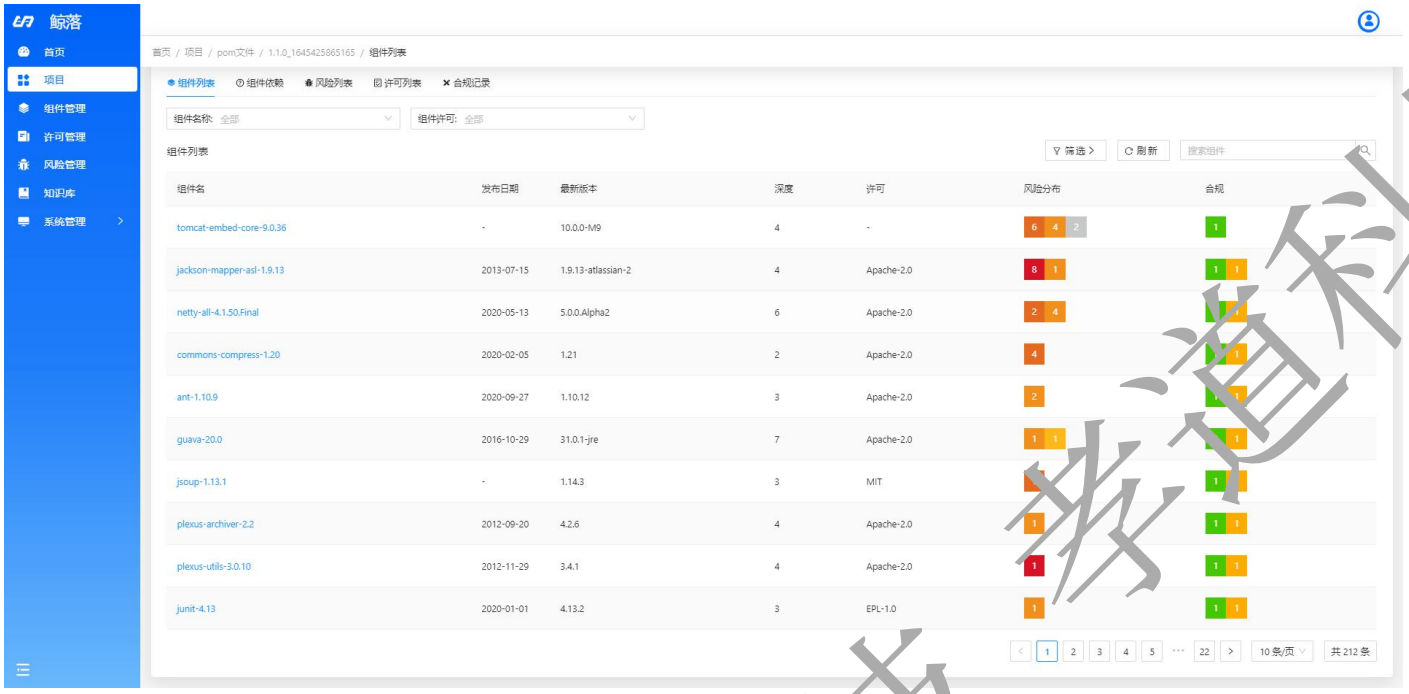


5.2 任务详情

如下图所示，顶部的任务结果统计展示了有关该任务的组件以及漏洞数量分布，并对组件危害分布、组件漏洞比例分布以及组件使用年限分布进行了统计。

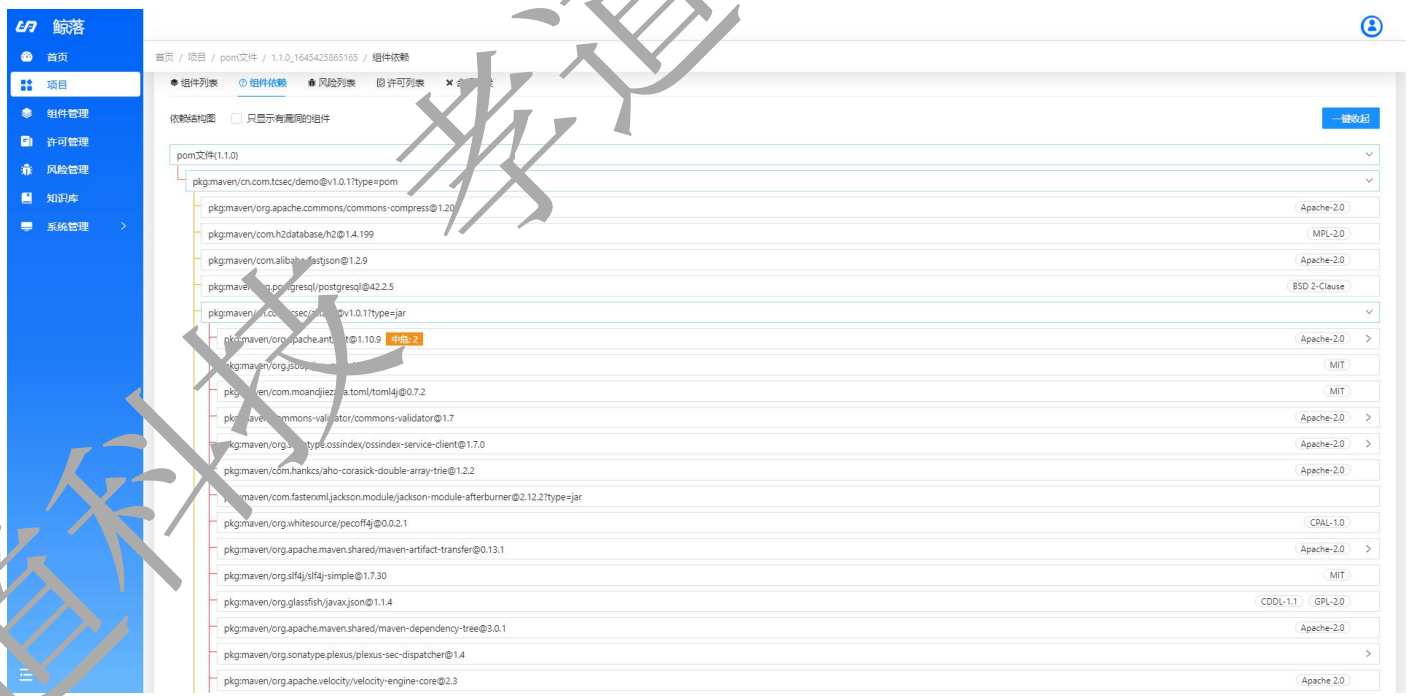
5.2.1 组件列表

组件列表展示了本次扫描任务中，所有扫描的组件信息。列表中展示了组件的基本信息，包括组件的名称、发布日期、最新版本、许可、风险分布以及合规情况。您可以通过组件名称、组件许可和搜索框来搜索对应的组件。



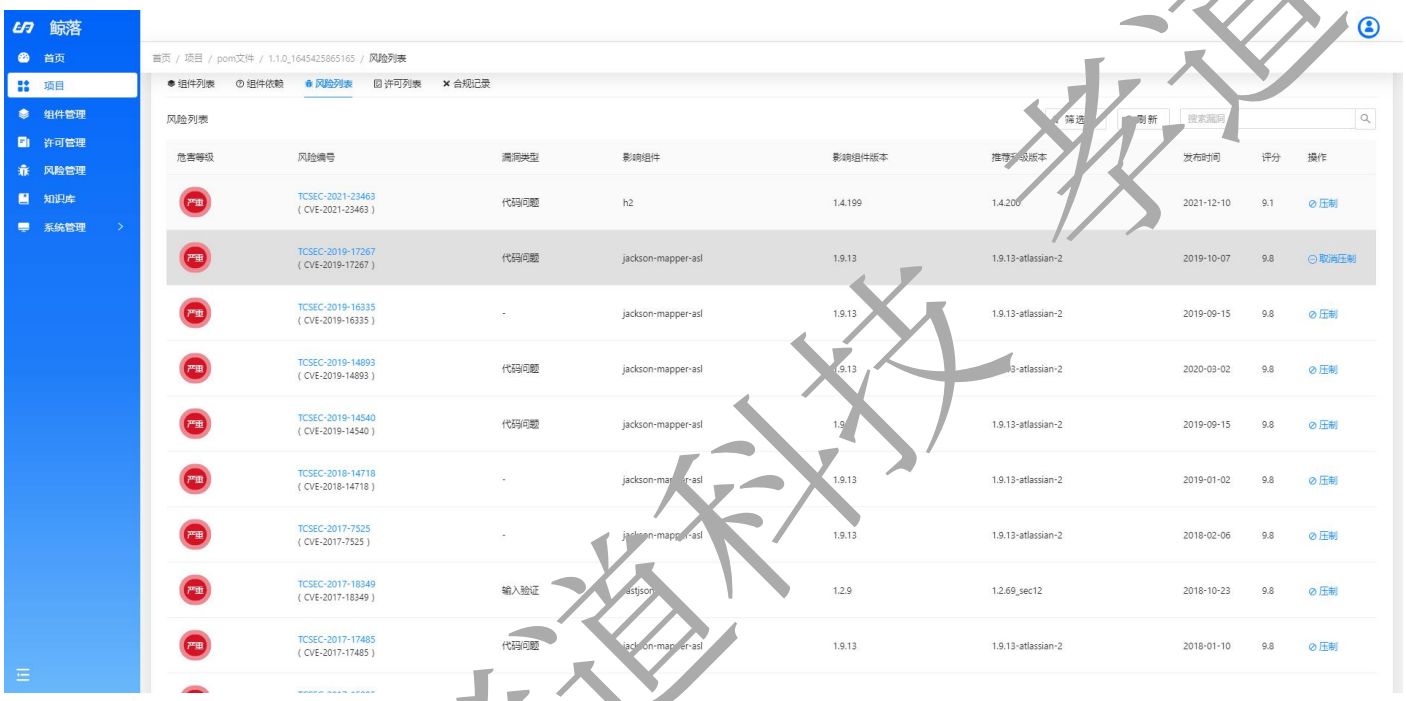
5.2.2 组件依赖

组件依赖将本次任务中扫描到的组件依赖关系以树状图的形式进行展示，组件的基本信息、组件存在的漏洞以及许可都会展示到依赖树中，可以通过顶部的勾选查看有漏洞的组件。



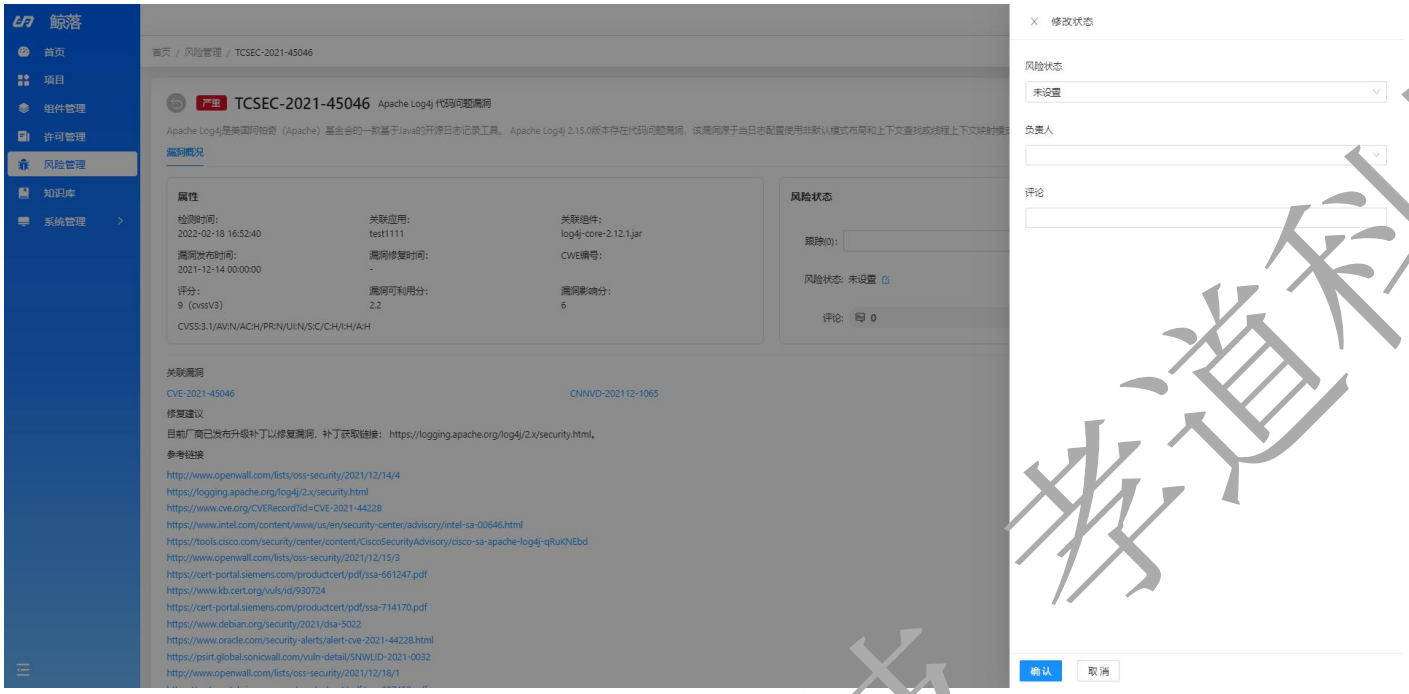
5.2.3 风险列表

风险列表展示了本次扫描任务中，所有组件包含的漏洞信息。列表中展示了危害等级、风险编号、漏洞类型、影响组件、影响组件版本、推荐升级版本、发布时间、评分以及压制操作。您可以通过漏洞类型、危害等级、搜索框来筛选对应的漏洞。当对某个漏洞进行压制后，无法再对该漏洞进行操作，并且再次扫描的时候该漏洞也将被继续压制。

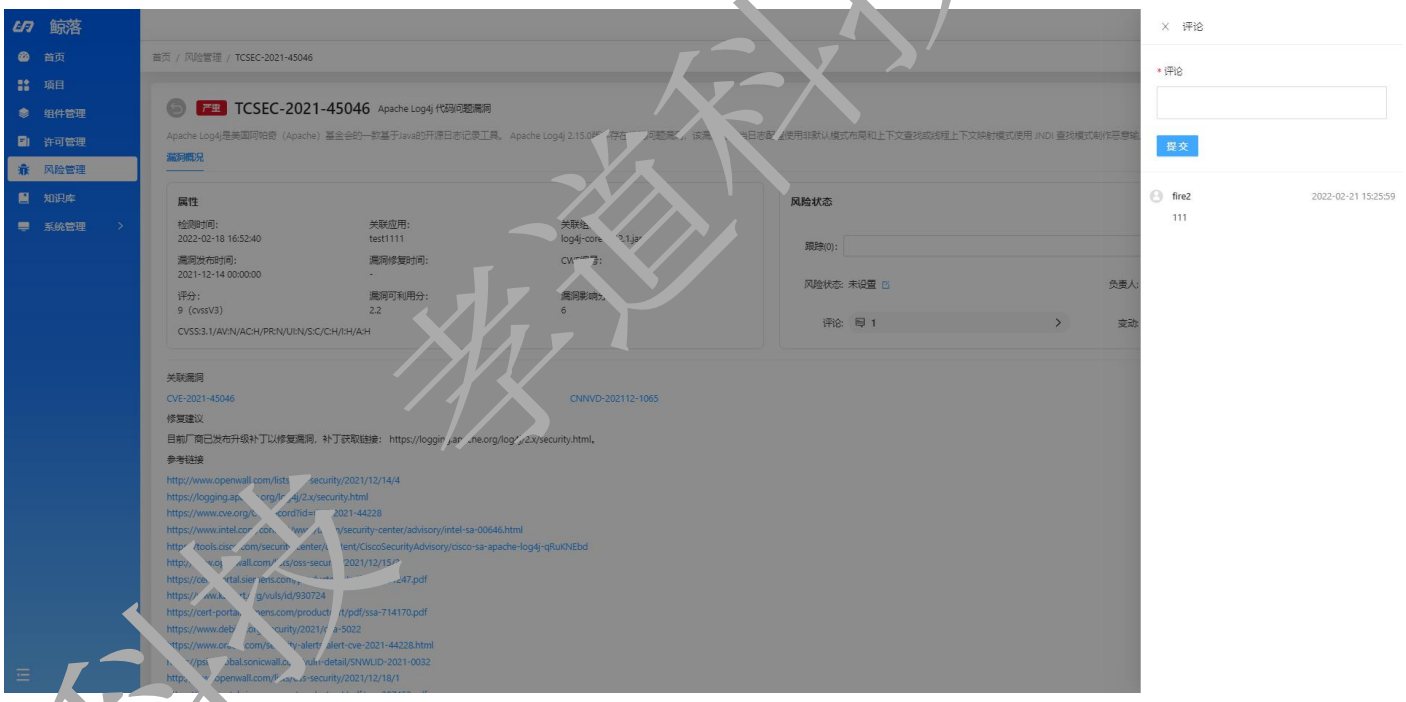


进入到漏洞详情，在风险状态处中，在状态栏中您可以为该漏洞创建 JIRA/禅道问题，我们会对该漏洞创建的所有问题进行跟踪。

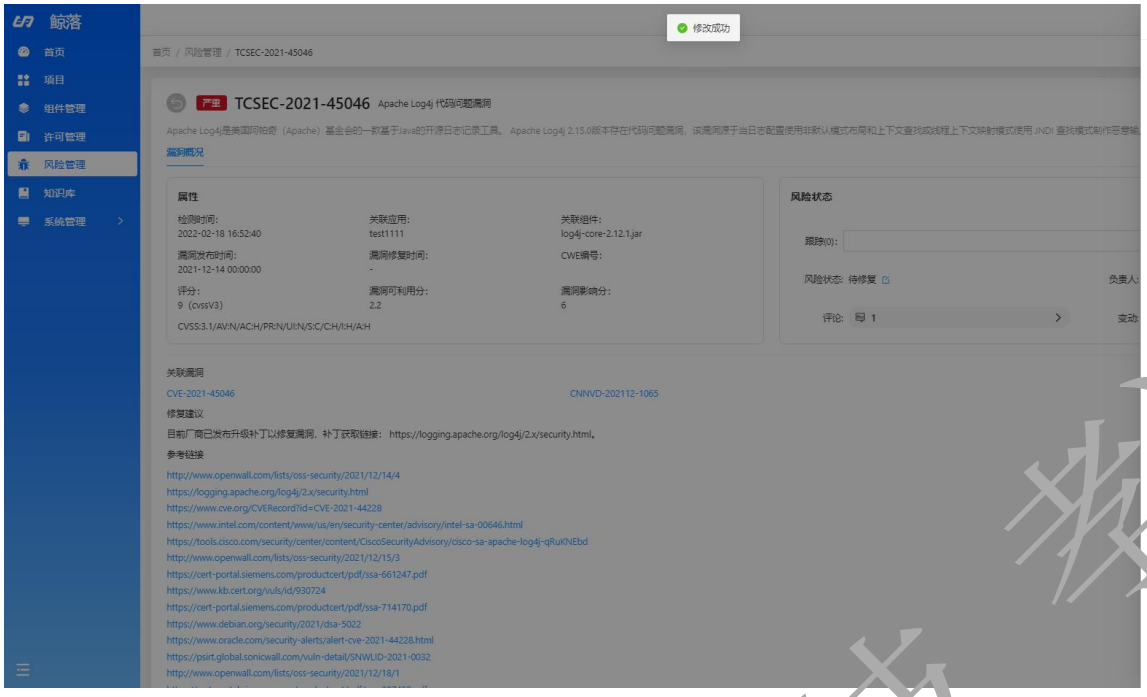
点击编辑状态，您可以对漏洞状态进行修改，且可以对当前状态进行备注。您可以将该漏洞分配给其他用户，方便对漏洞进行及时有效的处理。



点击评论栏，您可以看到所有用户对该漏洞留下的评论。

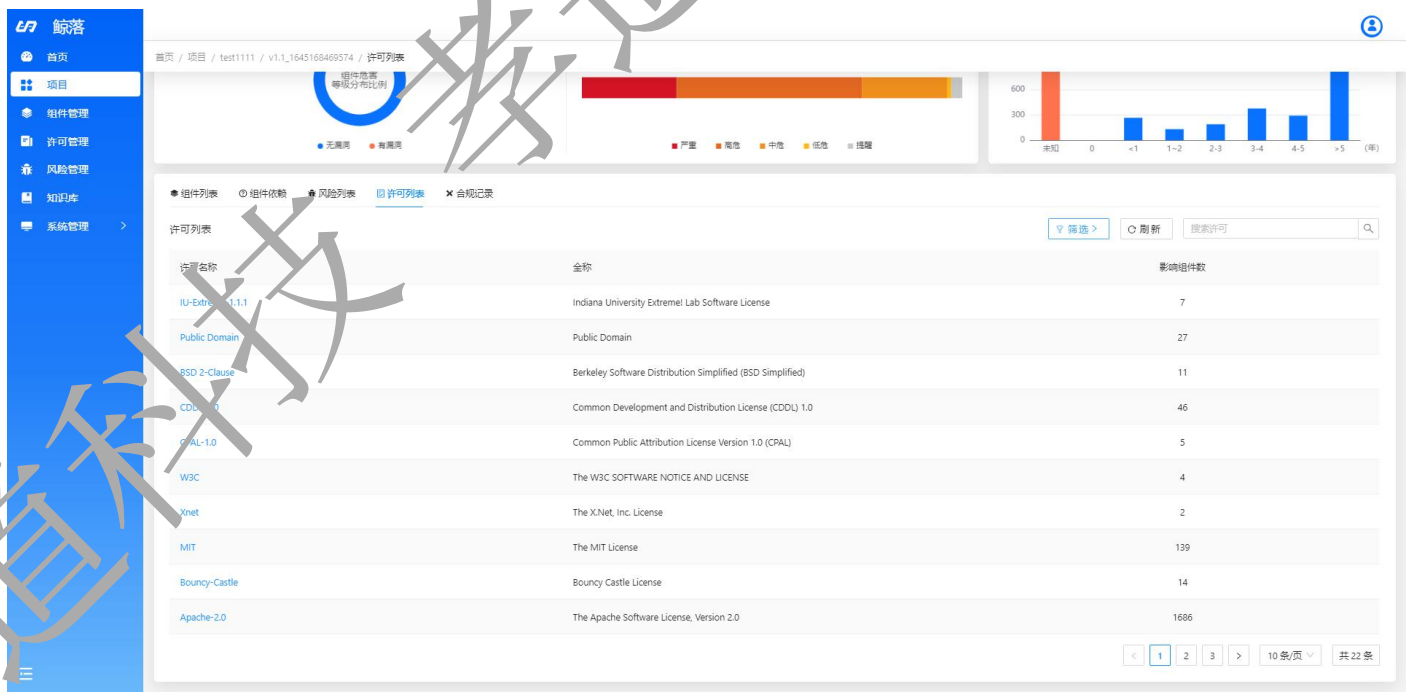


同样，在状态栏中也会展示目前该漏洞被分配的负责人，以及所有用户对该漏洞进行的状态变更操作。



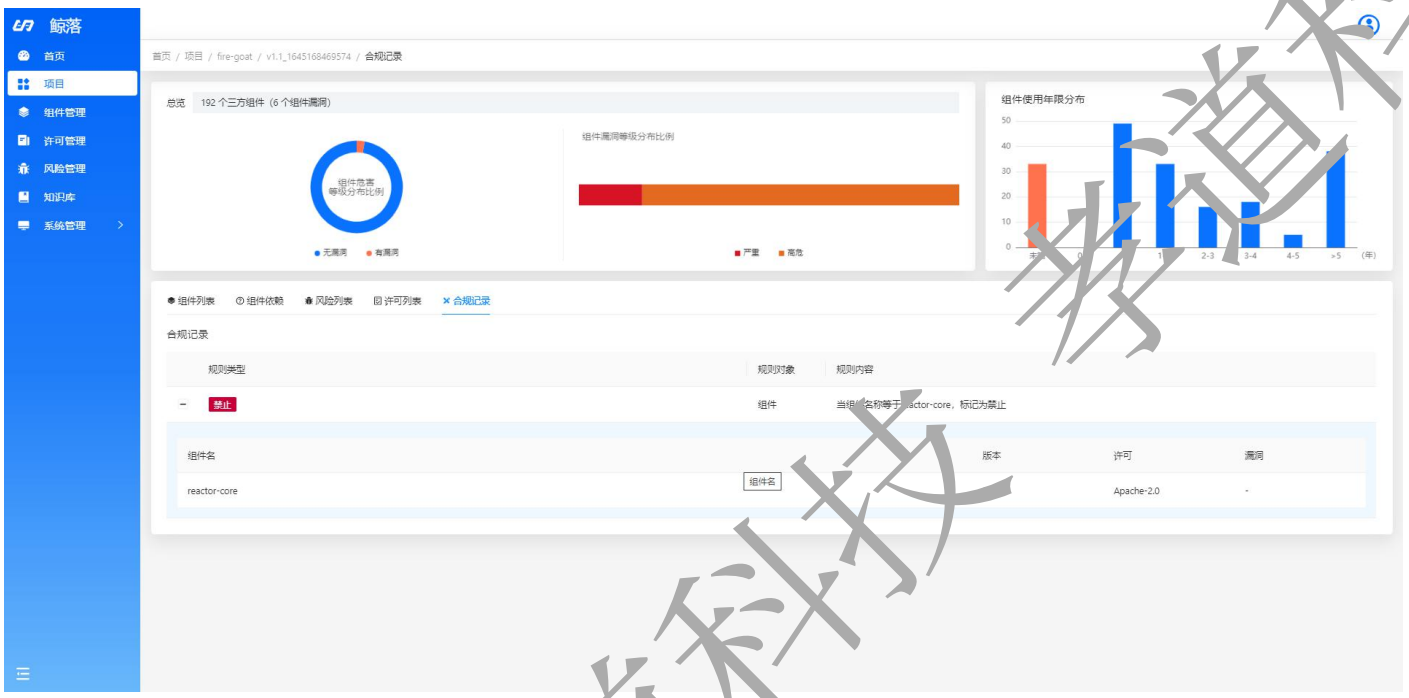
5.2.4 许可列表

许可列表展示了本次扫描任务中，所有组件使用的许可信息。列表中展示了许可名称、许可全称以及影响的组件数量。您可以按许可名称、搜索筛选查看许可。



5.2.5 合规记录

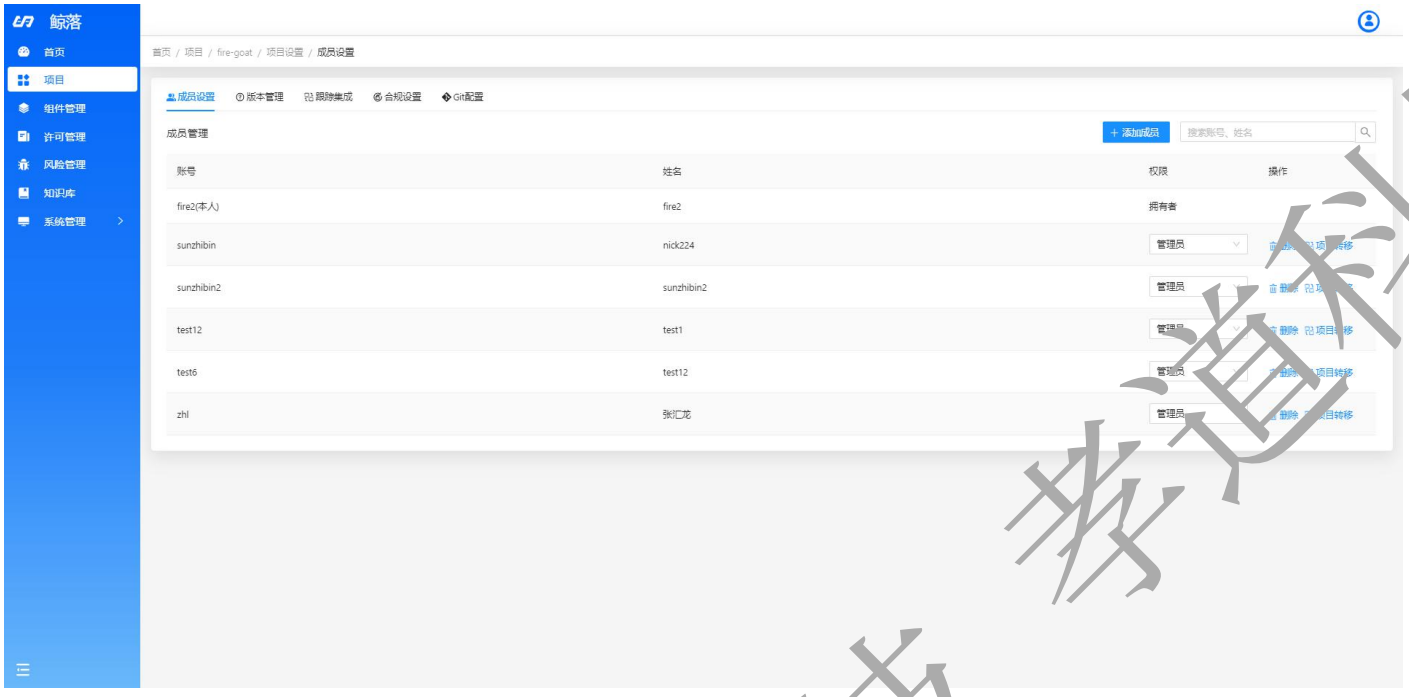
合规记录中展示本次扫描中，不符合项目合规的记录，展开该条规则，可以查看具体不符合规则的对象详情。



5.3 项目设置

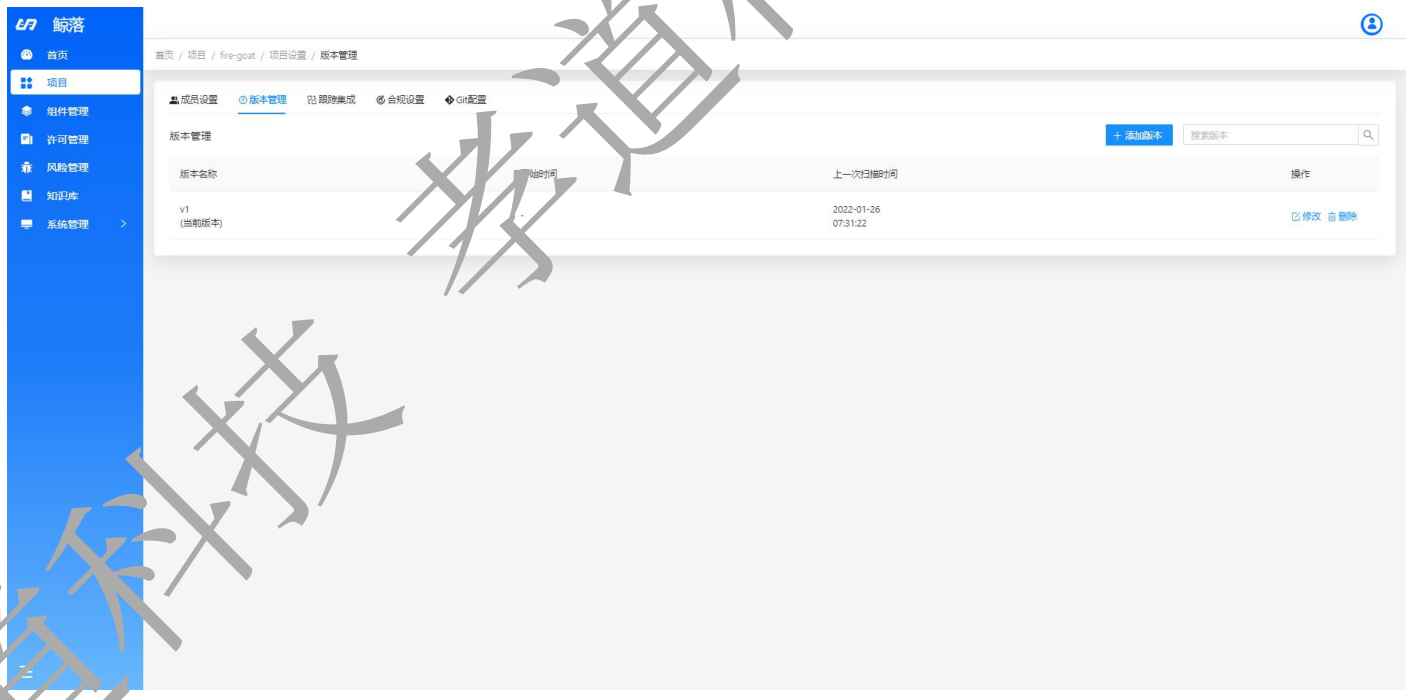
5.3.1 成员设置

项目拥有者或者项目管理员，可以根据实际需要对项目的成员进行添加、删除或者修改项目权限，项目成员可以查看项目的详情、为项目创建扫描任务。



5.3.2 版本管理

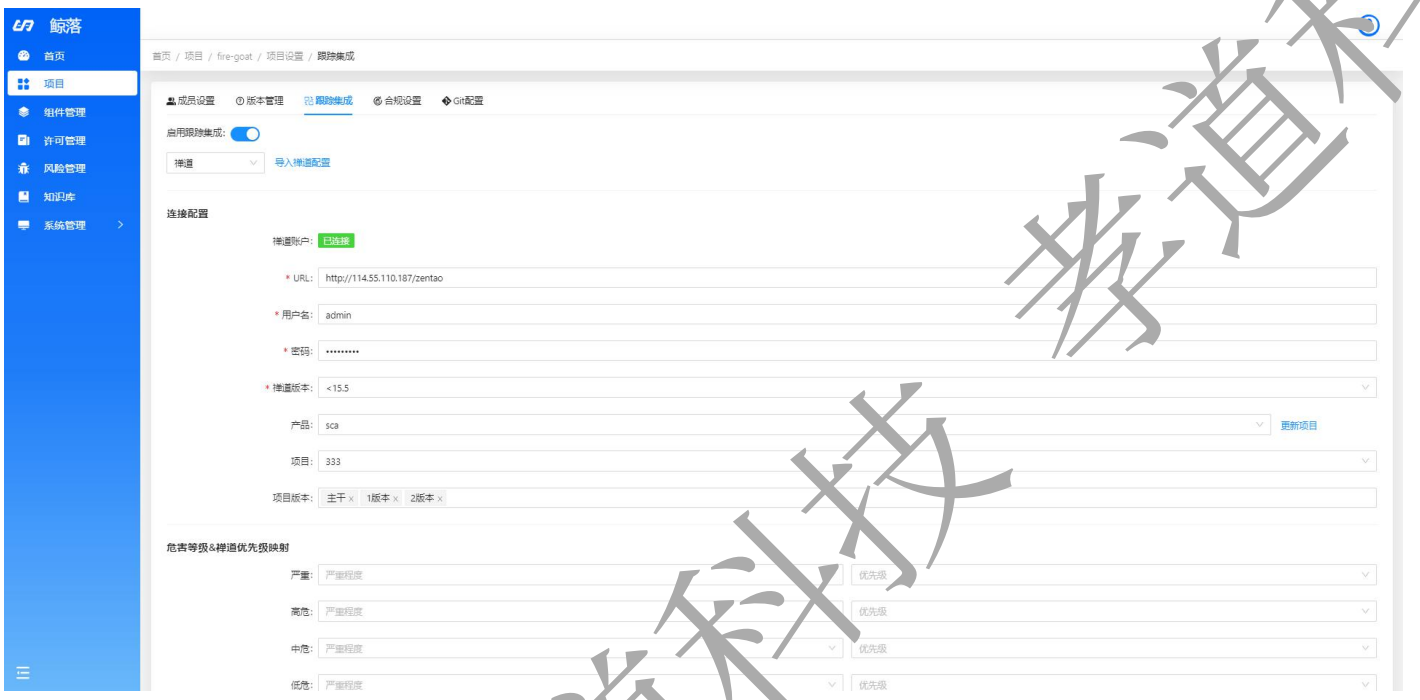
当项目存在多个版本时候，可以通过改功能对项目版本进行管理。



5.3.3 跟踪集成

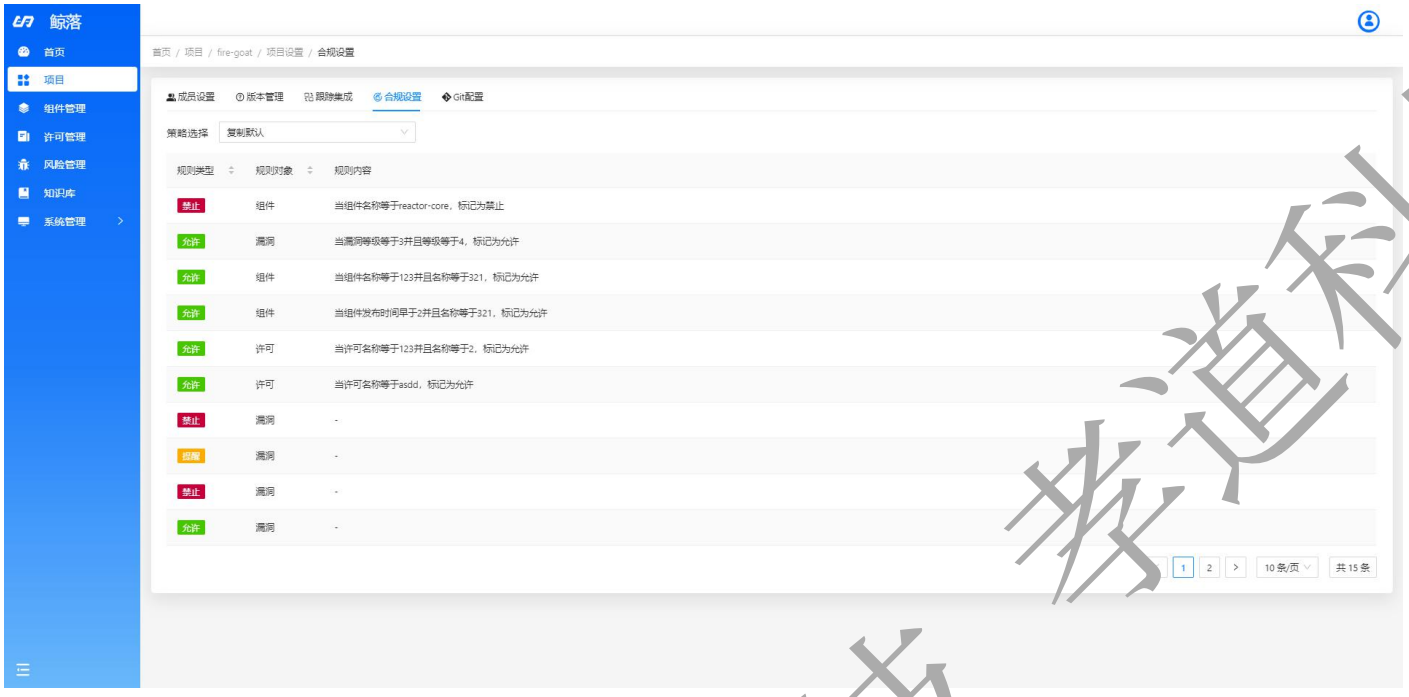
启用 JIRA/禅道跟踪集成，可对 SCA 平台三方组件存在的漏洞进行跟踪管理。您可以在 JIRA 或禅

道平台创建项目，在 SCA 的项目-项目设置-跟踪集成中，配置 JIRA 或禅道的账户信息并连接到 JIRA 或禅道平台，连接成功后，可选择创建问题所属的项目（正常情况下，项目一一对应），并配置 SCA 危害等级与 JIRA 或禅道优先级的映射，之后选择问题类型，点击保存完成配置，然后就可以在项目风险列表创建 JIRA 或者禅道问题了。



5.3.4 合规设置

管理员可以根据项目的需要为项目选择对应的合规策略，选择对应的策略后，下方的策略列表会展示该策略包含的具体策略内容。如果项目选择了对应的策略，在任务扫描的时候，系统将会根据策略内容，将满足规则的条目进行标记并体现在任务扫描结果当中。

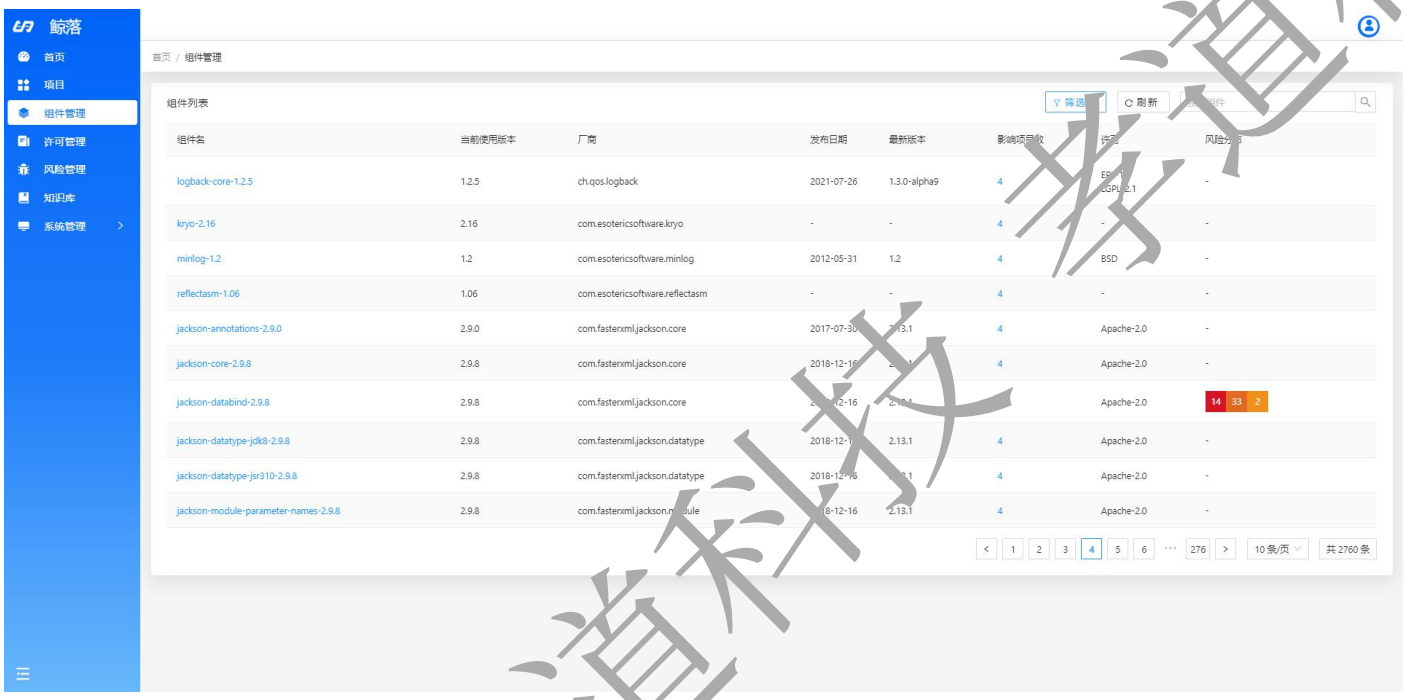


5.3.5 Git 配置

Gitlab 配置成功后，可以在创建任务时，通过拉取的形式对项目的分支进行自动创建以及扫描。

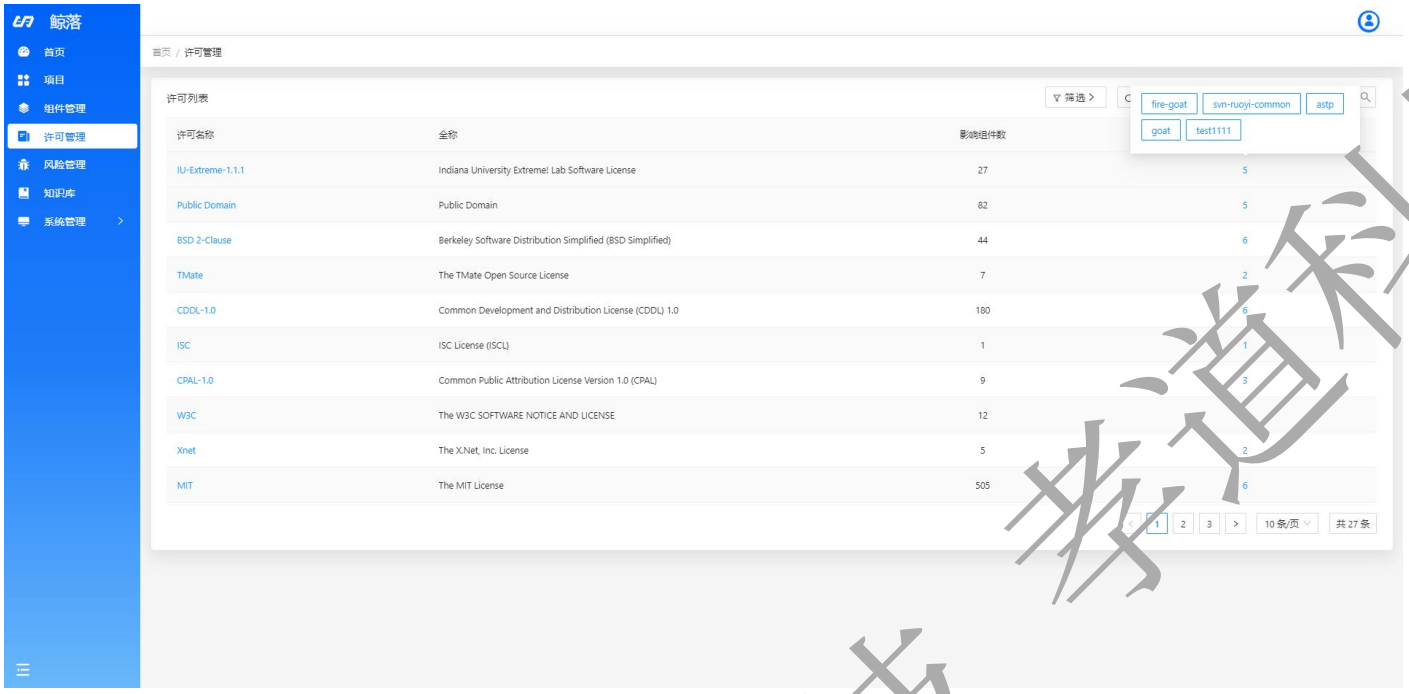
5 组件管理

组件列表展示了所有被测项目包含的组件信息。列表中展示了组件的基本信息，包括组件名称、当前使用版本、厂商、发布日期、最新版本、影响项目、许可、风险分布等。您可以通过组件名称、组件许可、搜索框来筛选对应的组件。



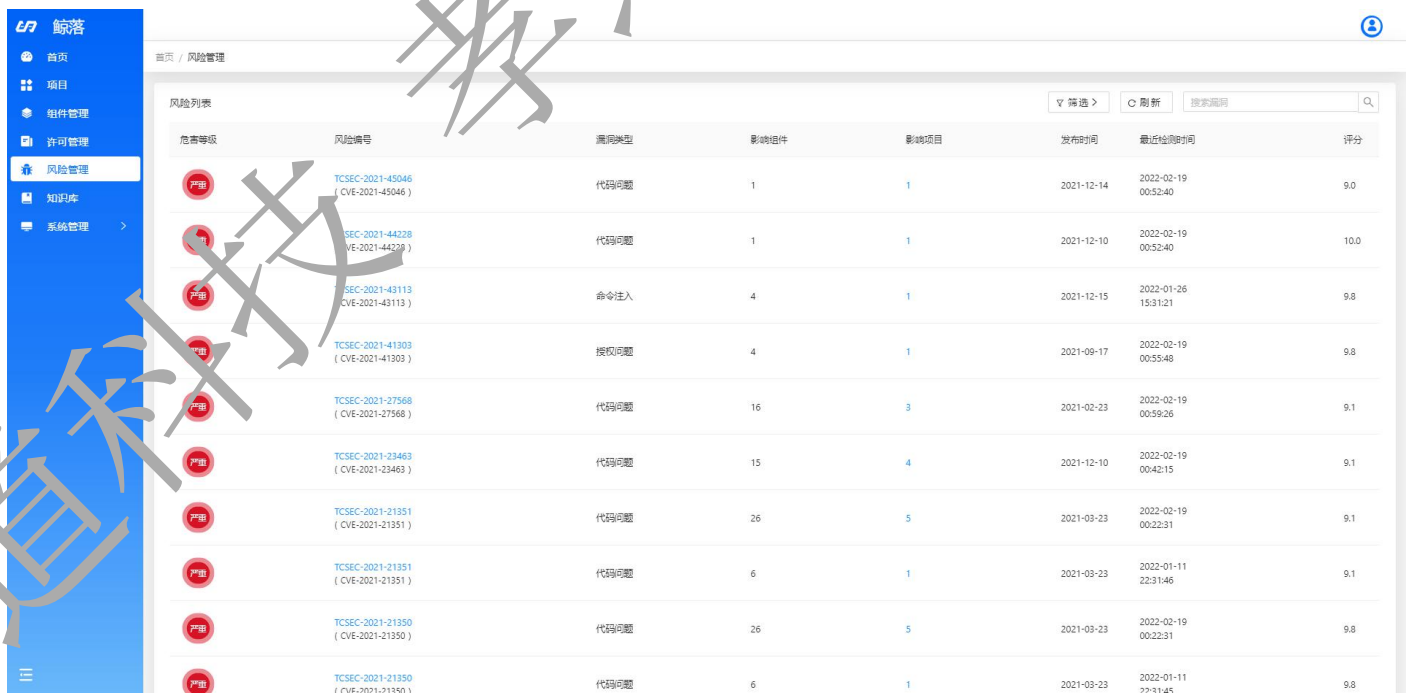
6 许可管理

许可列表展示了所有被测项目的组件包含的许可信息。列表中展示了许可的基本信息，包括许可名称、全程、影响组件、影响项目等。您可以通过许可名称、搜索框来筛选对应的许可。



7 风险管理

风险列表风险列表展示了系统中所有被测项目组所有组件包含的漏洞信息。列表中展示了危害等级、风险编号、漏洞类型、影响组件、影响项目、发布时间、评分。您可以通过漏洞类型、危害等级、搜索框来筛选对应的漏洞。



8 知识库

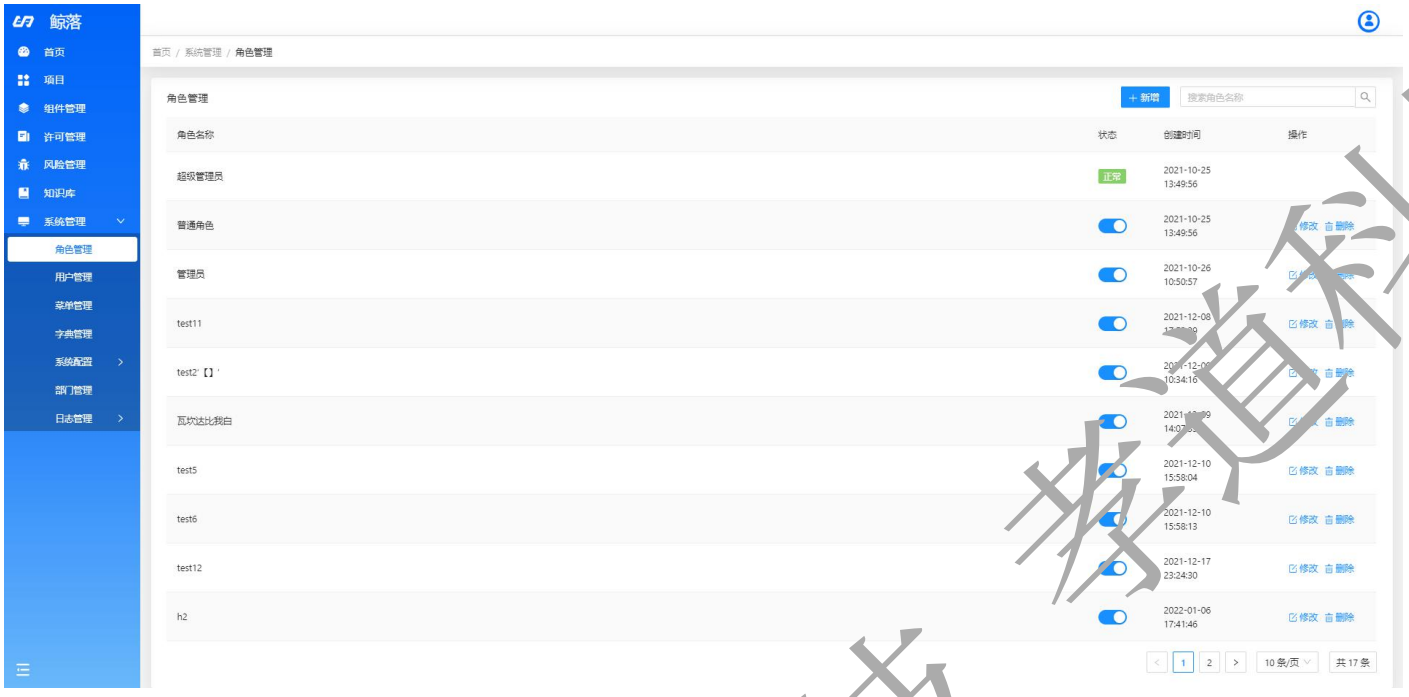
在测试或者交付验收环节，针对开源安全风险进行处路往往会投入更大的工作量和成本。通过使用左移开源安全治理工具的方式，将开源安全风险治理集成到软件开发全生命 周期过程中。在需求设计、组件选型、编码集成等早期研发过程中及早发现开源风险问题，从而降低开源安全治理成本。向左移（Shift Left）是在软件开发过程早期尽可能多地检测问题的核心理念。问题组件在软件选型阶段就得到规避，可以减少 90%的修复成本。

您可以根据组件名称、许可名称或漏洞编号等对当前所需了解的内容进行搜索查看，以提前了解是否存在风险能否使用到项目当中去，从而避免不必要的修复成本。

9 系统管理

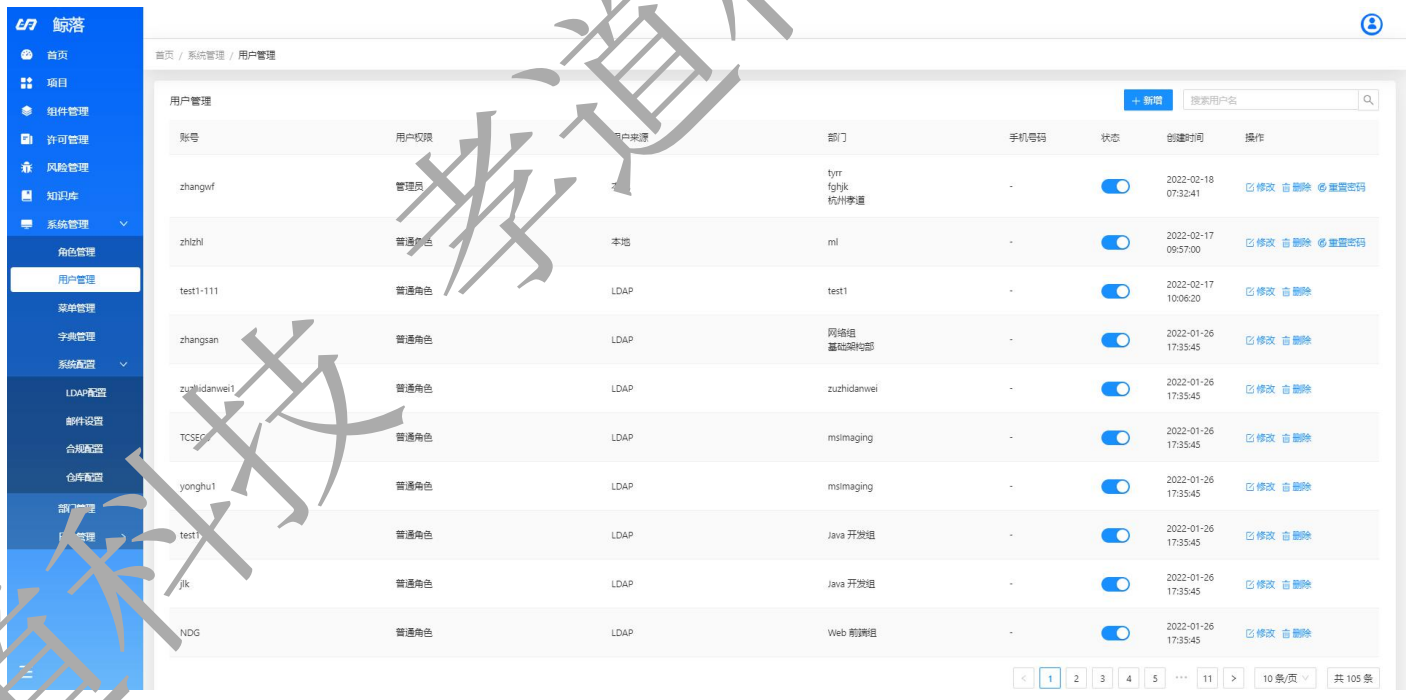
9.1 角色管理

您可以根据需要为不同的岗位所需的权限需要创建对应的角色。



9.2 用户管理

您可以根据实际需要为某个角色添加用户。



9.3 系统配置

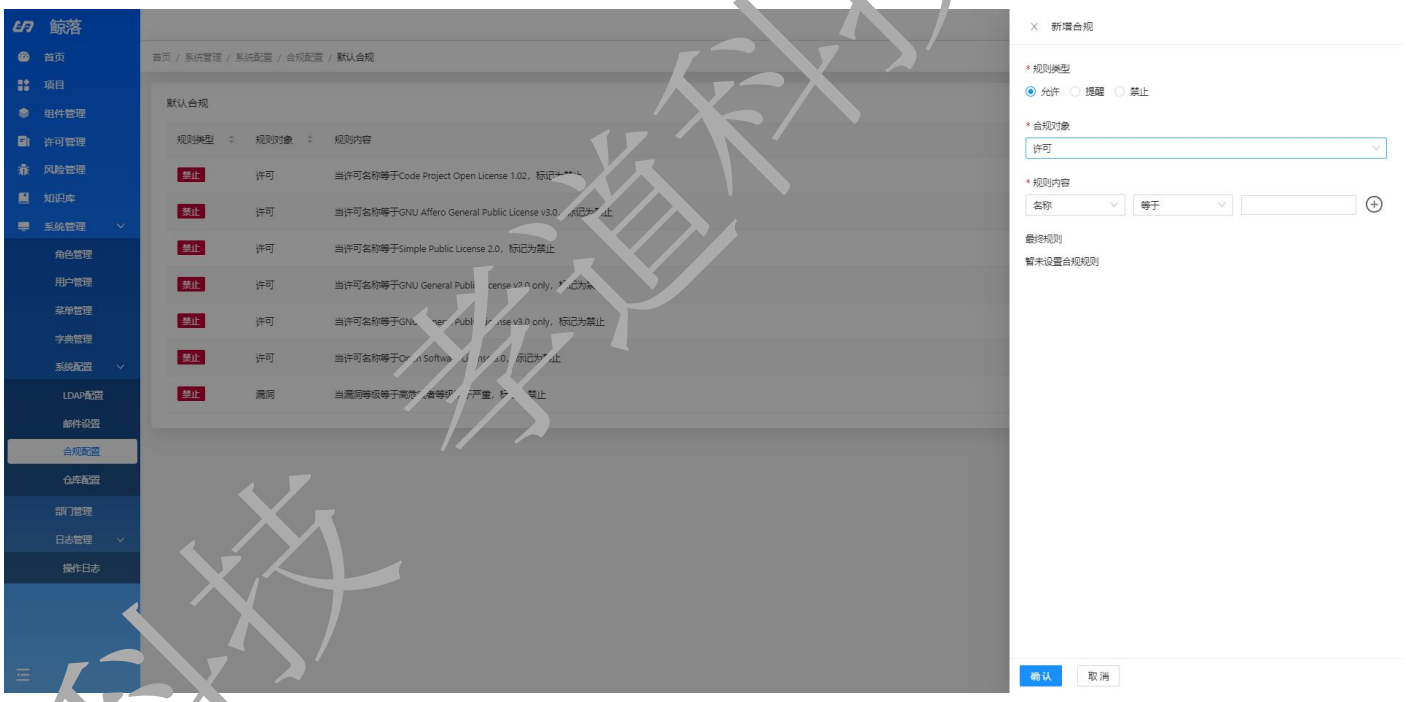
9.3.1 LDAP 配置

LDAP 配置完成并启用后，即可同步 LDAP 服务器上的用户信息到 SCA 平台，用户即可以使用 LDAP 账户进行登录。

9.3.2 合规配置

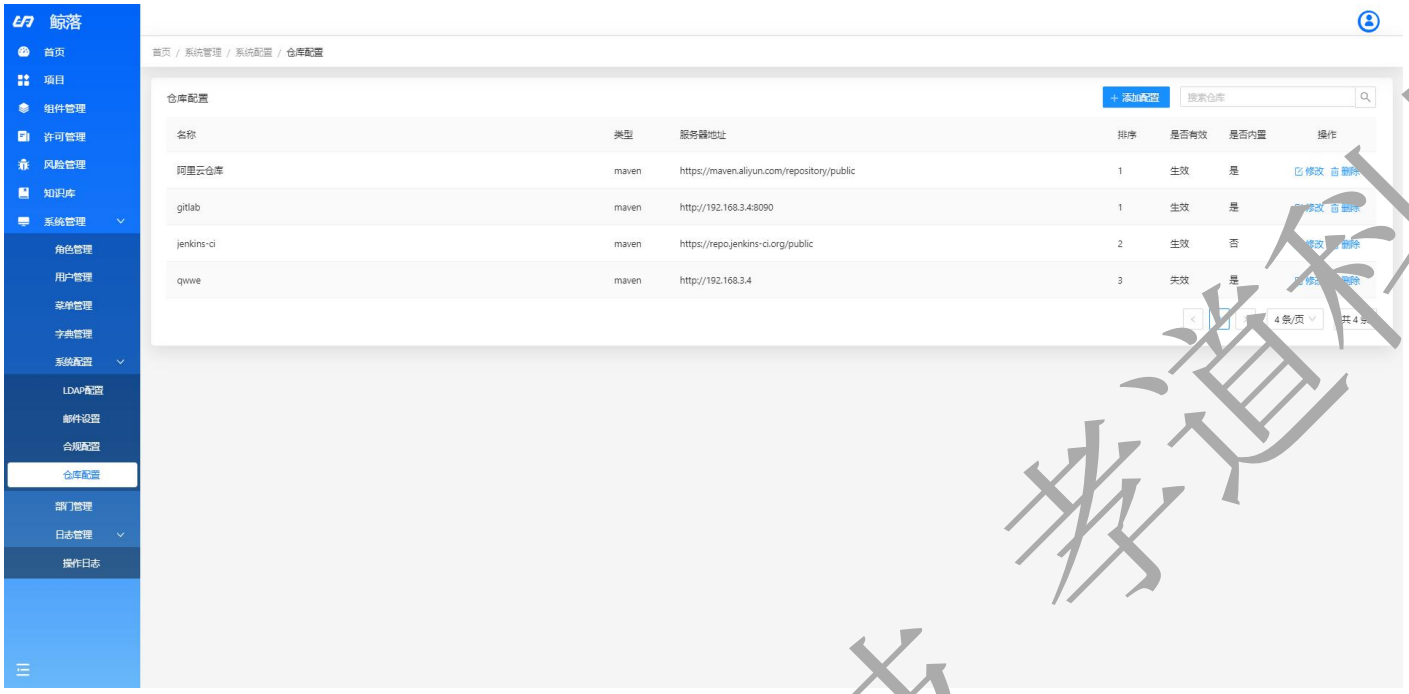
您可以针对不同项目的需求来设置不同的合规策略。

规则类型分为允许、提醒、禁止三种，可以针对许可、组件和漏洞三种对象进行设置。



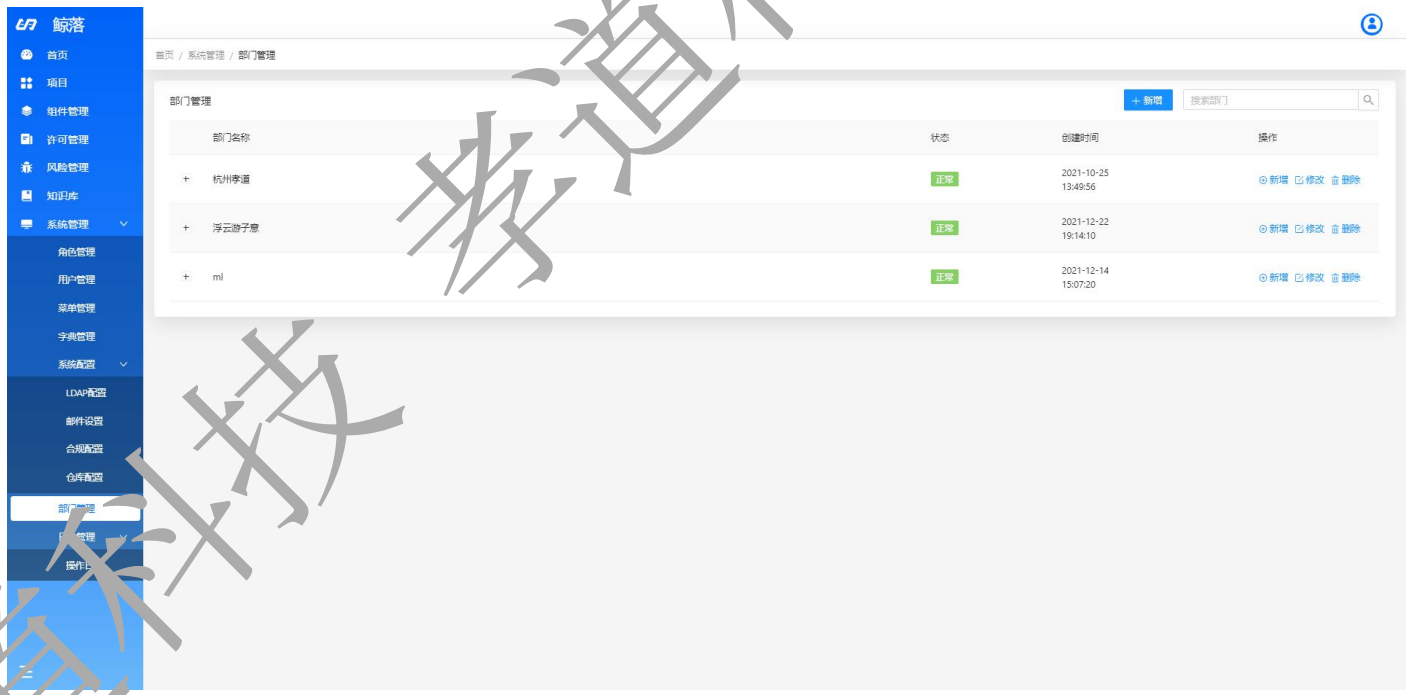
9.3.3 仓库配置

您可以根据需要配置公司的私服地址以方便分析过程中能获取所需的组件信息。



9.7 部门管理

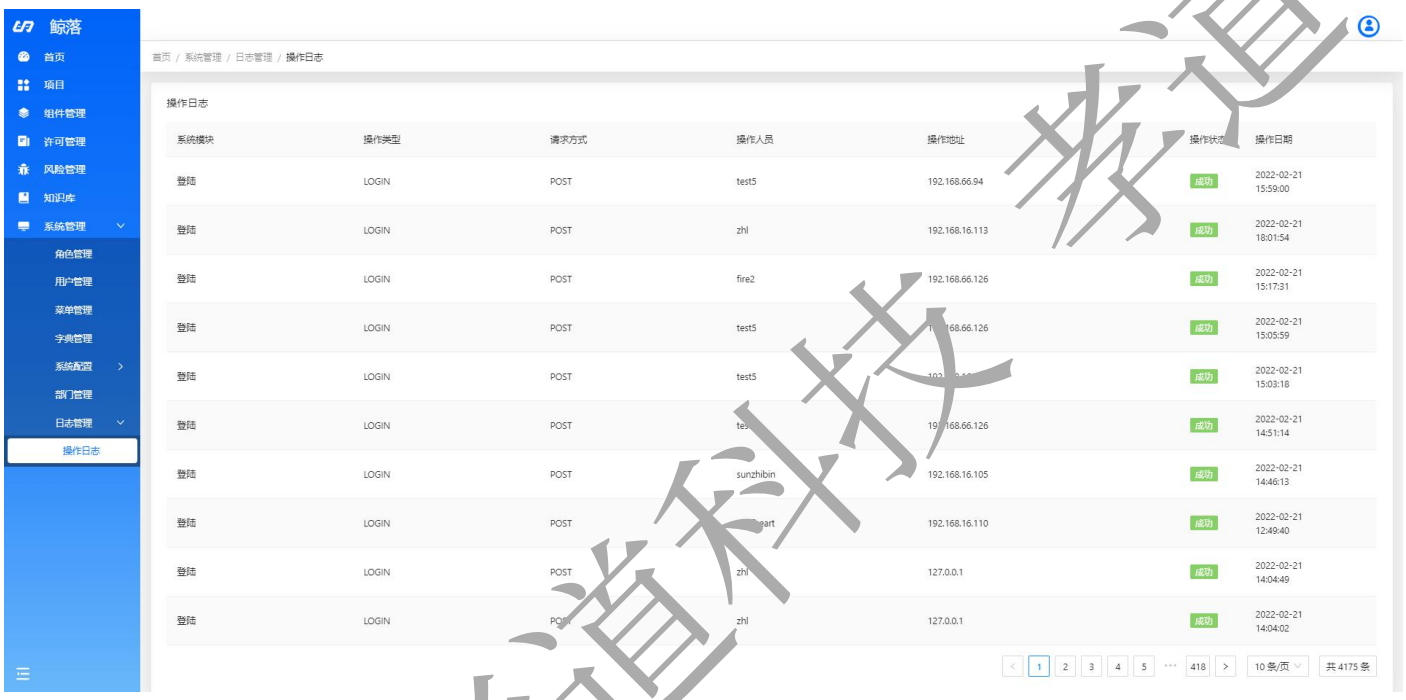
您可以根据公司组织架构对部门进行管理。



9.8 日志管理

9.8.1 操作日志

操作日志记录了登录、退出、新增、修改、删除、下载等操作的日志以及相应的搜索，当系统出现异常问题时，可以在此处追踪原因。



10 用户中心

10.1 基本资料设置

您可以在个人设置中修改当前账户的个人信息及密码。