



中北大学

NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

OpenKylin操作系统 安全分析工具

OpenKylin Operating System Security Analysis Tool

组名：NUC脚踏实地队

组员：刘鑫 乔嘉琛 谢幸

学校：中北大学

指导老师：张斌 张静



中北大学

NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

目录

Contents

01

项目概述

02

架构设计

03

成果展示



中北大学

NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

01

项目概述



中北大学
NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

项目目标



基于openkylin操作系统，实现linux的基线检查
与poc漏洞扫描，并给出修复建议，同时能够进
行大数据可视化展示。



中北大学

NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

基本任务

题目1

功能1： 实现系统安全配置基线检查

功能2： 形成安全基线检查报告

功能3： 系统基线检查安全评估

功能4： 实现系统总线服务接口
自动化安全检查基线

题目2

功能1： 实现安全漏洞
(POC/EXP)检查功能

功能2： 形成安全漏洞扫描报告

功能3： 系统安全漏洞评估

功能4： POC防逆向



中北大学

NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

增加的功能

可视化实时动态网
页展示检测结果



基线检查、漏洞扫描的修复

对任务的完成状况
生成日志报告

将对openkylin操作系统
安全检测和AI大模型相结合，制作openkylin检测
智能体



中北大学

NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

创新点

所有的检测结果以及数据库全部云端化，云服务器部署，全部支持公网IP访问

项目巧妙将AI大模型与操作系统安全分析结合起来，实现“AI+”国家战略目标

所有检测结果全部实现动态实时化检测



中北大学

NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

02

架构设计

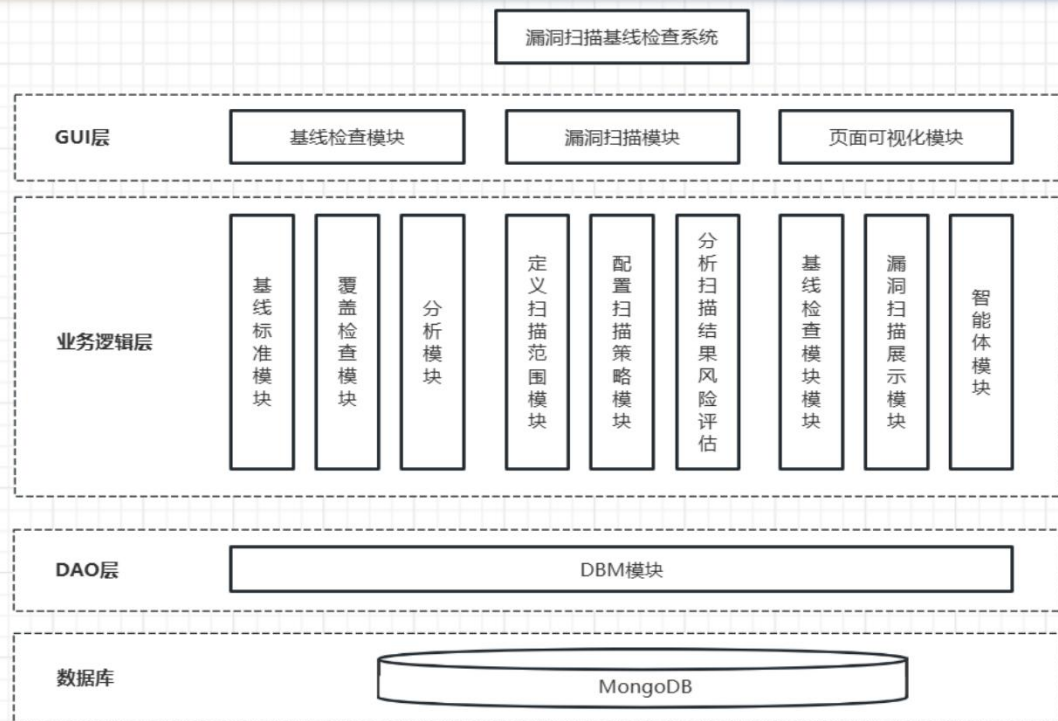


中北大学

NORTH UNIVERSITY OF CHINA

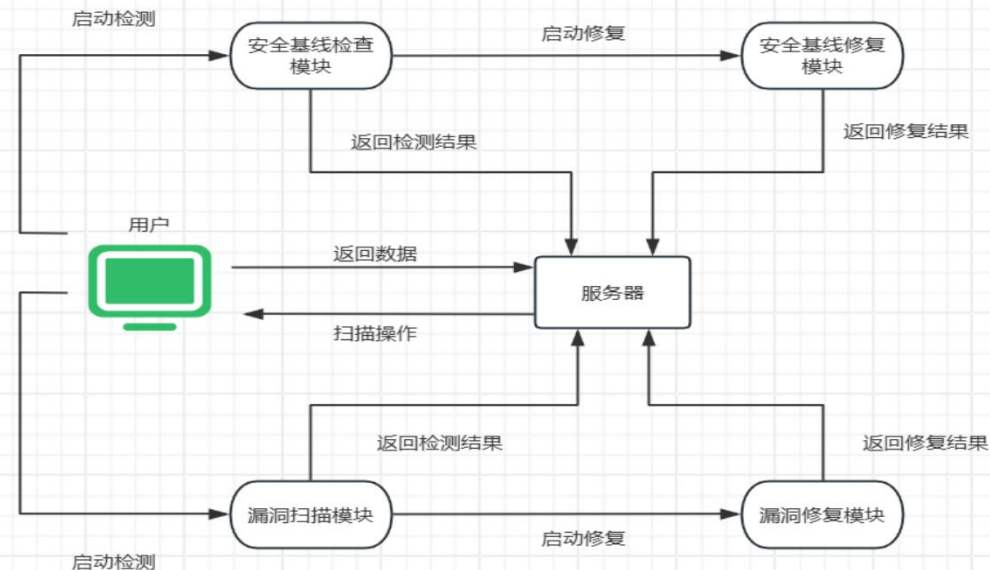


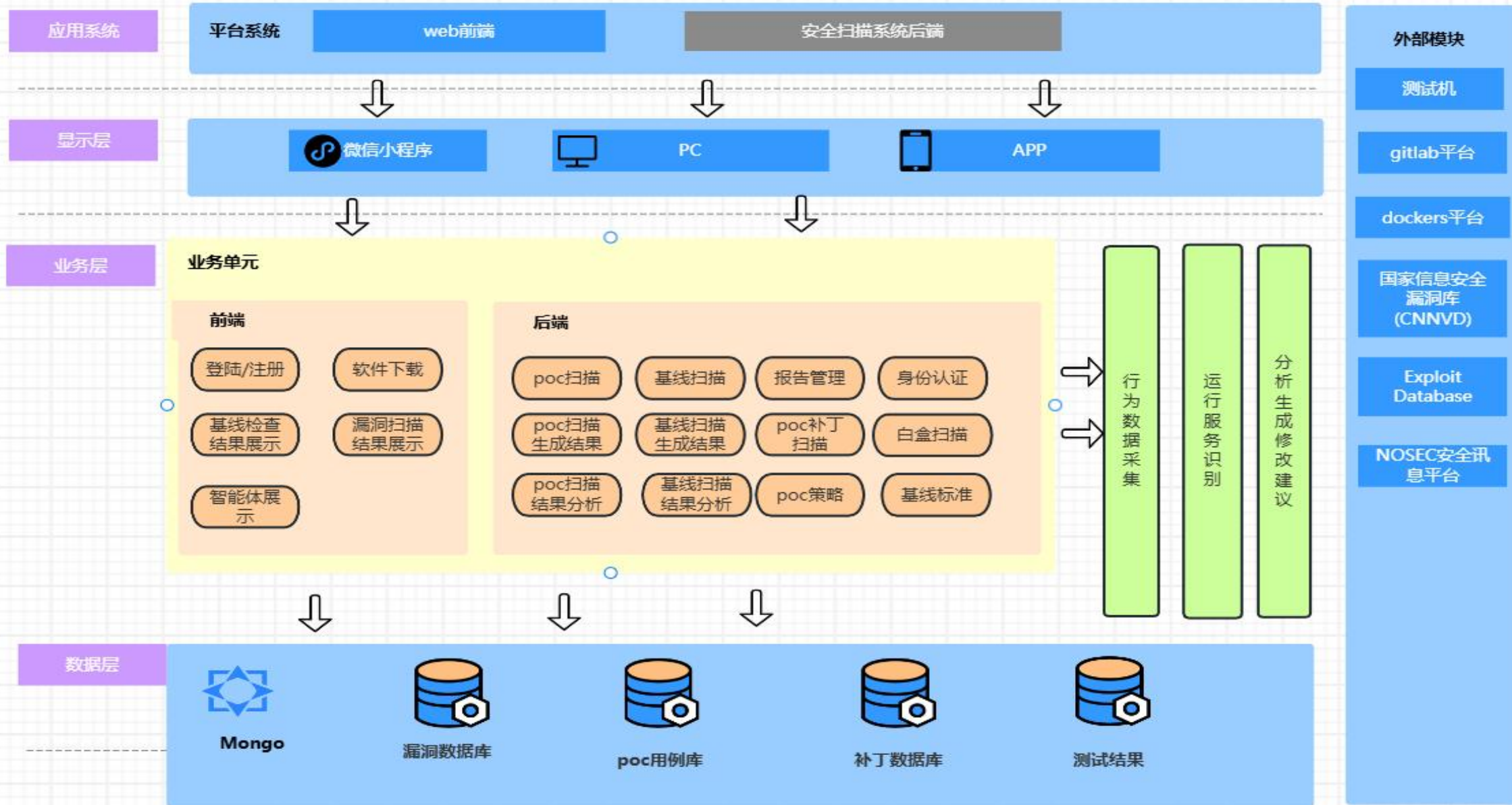
CSCC 全国大学生
计算机系统能力大赛



初步模块设计

初步流程设计







中北大学

NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

03

结果展示



中北大学

NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

访问网址: <http://152.136.142.183:8080/baseline>

基线检测可视化



53	6其他配置操作	No advice	检查FTP用户上传的文件所具有的权限	No result
54	6其他配置操作	No advice	检查历史命令设置	No result
55	6其他配置操作	No advice	检查是否设置SSH成功登录后Banner	No result
56	6其他配置操作	参考基线检测配置手册	检查是否配置定时自动屏幕锁定(适用于图形化界面)	对具有图形化界面的设备应配置定时自动屏幕锁定,此检查项建议调整
57	6其他配置操作	No advice	检查是否关闭多ip绑定	No result
58	6其他配置操作	参考基线检测配置手册	检查是否安装OS补丁	及时安装操作系统补丁保证系统稳定性,此检查项建议系统管理员根据系统情况自行判断
59	6其他配置操作	No advice	检查磁盘空间占用率	No result
60	6其他配置操作	参考基线检测配置手册	检查是否按组进行账号管理	该项配置主要偏向于对系统用户的管理,如账户已分组管理,该检查项可以跳过,此检查项建议系统管理员根据系统情况自行判断
61	6其他配置操作	参考基线检测配置手册	检查是否按用户分配账号	该项配置主要偏向于对系统用户的管理,如有未知账号,请及时调整与关闭,此检查项建议系统管理员根据系统情况自行判断



中北大学
NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

访问网址: <http://152.136.142.183:8080/bug>

漏洞扫描可视化



检测时间: 2024-08-14 09:00:36

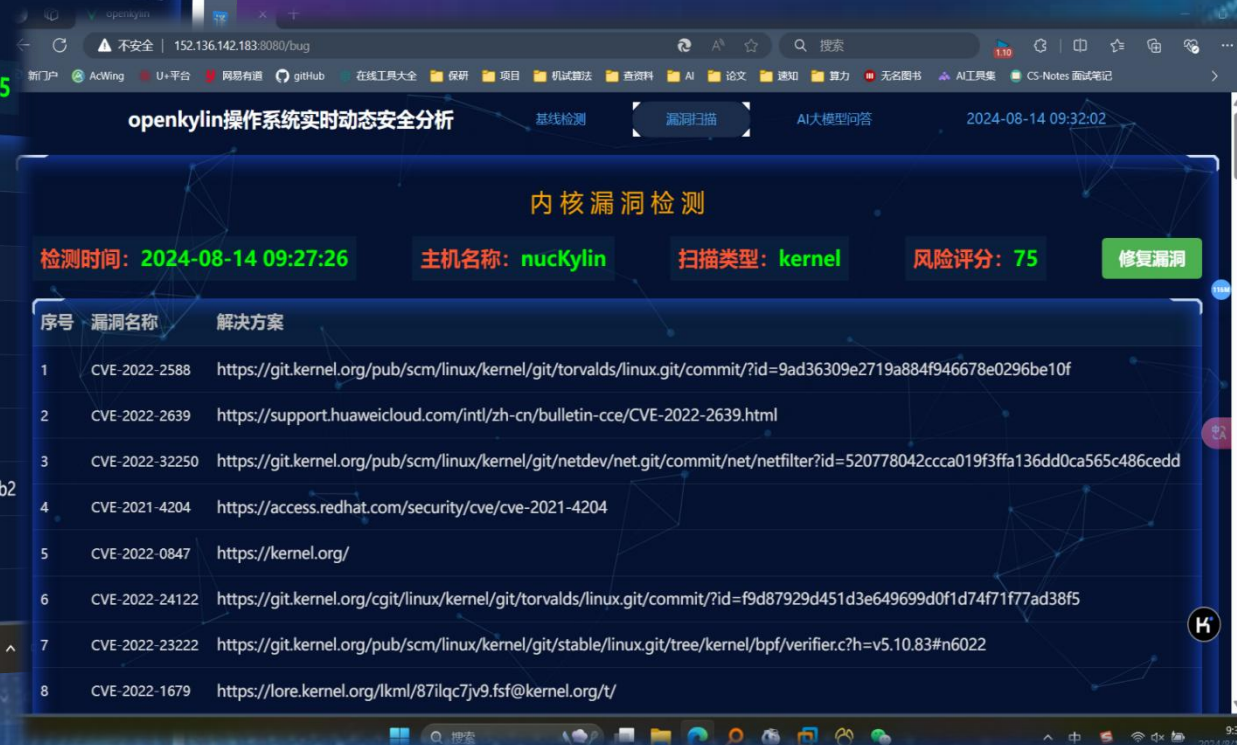
系统漏洞检测

主机名称: nuckKylin

扫描类型: System

风险评分: 75

序号	漏洞名称	解决方案
1	KVE-2022-0206	https://kylinos.cn/support/loophole/patch/1874.html
2	KVE-2022-0231	https://kylinos.cn/support/loophole/patch/1331.html
3	KVE-2022-0210	https://kylinos.cn/support/loophole/patch/1329.html
4	KVE-2022-0207	https://kylinos.cn/support/loophole/patch/1329.html
5	KVE-2022-0205	https://kylinos.cn/support/loophole/patch/2370.html
6	CVE-2022-1292	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=1ad73b4d27bd8c1b369a3cd453681d3a4f1bb9b2
7	CVE-2021-3156	https://vigilance.fr/vulnerability/libarchive-write-access-via-Symlink-Modes-Times-Flags-Modification-37590
8	CVE-2023-0054	https://github.com/vim/vim/commit/3ac1d97a1d9353490493d30088256360435f7731



检测时间: 2024-08-14 09:27:26

主机名称: nuckKylin

扫描类型: kernel

风险评分: 75

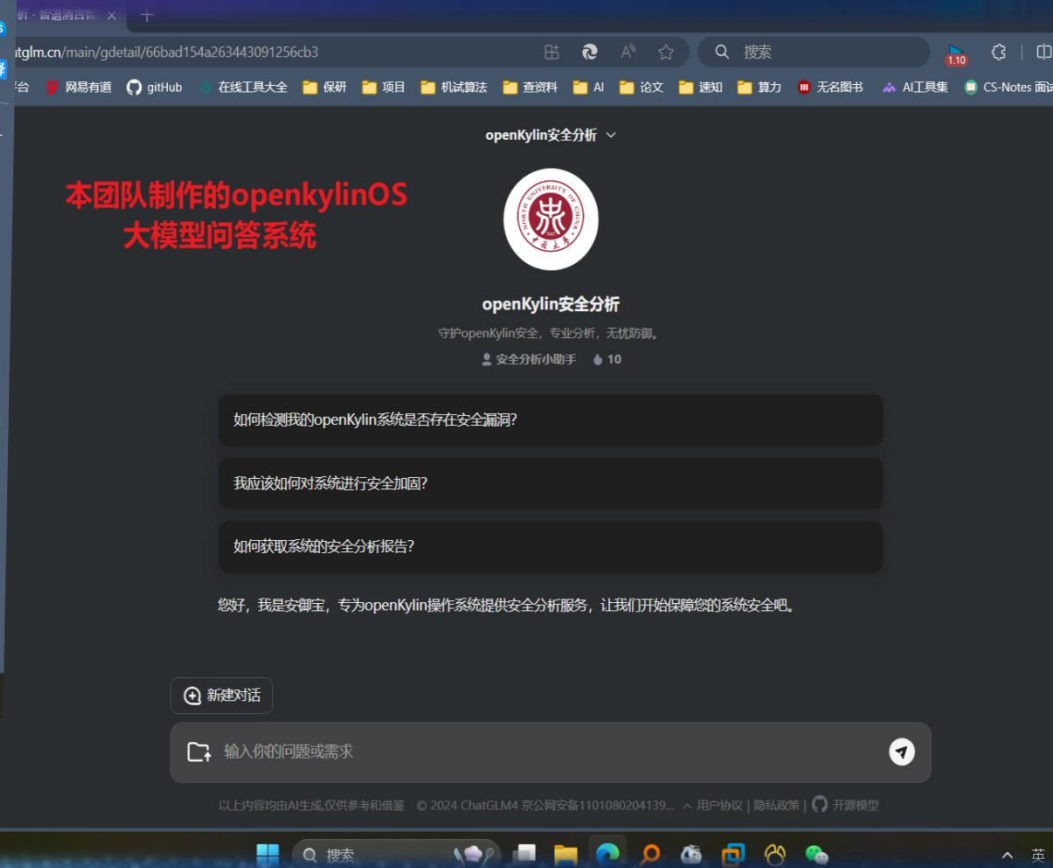
修复漏洞

序号	漏洞名称	解决方案
1	CVE-2022-2588	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=9ad36309e2719a884f946678e0296be10f
2	CVE-2022-2639	https://support.huaweicloud.com/intl-zh-cn/bulletin-cce/CVE-2022-2639.html
3	CVE-2022-32250	https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/net/netfilter?id=520778042ccca019f3ffa136dd0ca565c486cedd
4	CVE-2021-4204	https://access.redhat.com/security/cve/cve-2021-4204
5	CVE-2022-0847	https://kernel.org/
6	CVE-2022-24122	https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=f9d87929d451d3e649699d0f1d74f71f77ad38f5
7	CVE-2022-23222	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/tree/kernel/bpf/verifier.c?h=v5.10.83#n6022
8	CVE-2022-1679	https://lore.kernel.org/lkml/871qc7jv9.fsf@kernel.org/t/



访问网址: <http://152.136.142.183:8080/llm>

漏洞扫描可视化





中北大学

NORTH UNIVERSITY OF CHINA



CSCC 全国大学生
计算机系统能力大赛

感谢各位评委老师

OpenKylin操作系统安全分析工具