同行专家业内评价意见书编号：20250854397

# 附件1

# 浙江工程师学院（浙江大学工程师学院）
# 同行专家业内评价意见书

姓名：张浩然

学号：22260095

申报工程师职称专业类别（领域）：电子信息

浙江工程师学院（浙江大学工程师学院）制

2025年03月19日

# 填表说明

一、本报告中相关的技术或数据如涉及知识产权保护、军工项目保密等内容，请作脱密处理。

二、请用宋体小四字号撰写本报告，可另行附页或增加页数，A4纸双面打印。

三、表中所涉及的签名都必须用蓝、黑色墨水笔，亲笔签名或签字章，不可以打印代替。

四、同行专家业内评价意见书编号由工程师学院填写，编号规则为：年份4位＋申报工程师职称专业类别(领域)4位+流水号3位，共11位。

# 一、个人申报

**（一）基本情况【围绕《浙江工程师学院（浙江大学工程师学院）工程类专业学位研究生工程师职称评审参考指标》，结合该专业类别(领域)工程师职称评审相关标准，举例说明】**

**1.对本专业基础理论知识和专业技术知识掌握情况(不少于200字)**

基础及专业知识：在本科及研究生期间系统修读了高等数学、线性代数、概率论与数理统计等数学基础课程，以及计算机组成原理、编译原理、汇编语言、操作系统原理、软件体系结构、数据结构、算法设计与分析、面向对象的程序设计、机器学习技术等计算机技术核心课程，具备扎实的计算机科学与技术理论基础，掌握C/C++、Java、Python、Bash、JavaScript、SQL等编程语言，能够熟练运用相关理论解决复杂工程问题。

行业知识：本人持续关注计算机技术前沿发展动态，熟悉工业界和学术界采用的新技术，特别是在操作系统内核与虚拟化技术的模糊测试研究领域有深入理解，如Syzkaller、AFL、Morphuzz、v-shuttle等模糊测试框架，并能够在其基础上予加以改进，取得更好的漏洞挖掘效果。

默会性工程知识：通过参与省级、国家级网络安全演练（护网）及实际项目，本人积累了丰富的工程实践经验。熟练模糊测试技术在真实软件中的应用，能够独立挖掘安全漏洞。掌握Web攻击、网络钓鱼、应急响应、逆向分析、免杀技术等多方面的实战经验。

跨专业领域知识：在人工智能与网络安全交叉领域，本人深入研究了常见的机器学习模型（如CNN、RNN、Transformer等）的原理，能够实施针对卷积神经网络的对抗样本攻击，以及针对大语言模型（LLM）的提示词注入攻击、越狱攻击等攻击手段，具有较强的跨领域学习与创新能力。

**2.工程实践的经历(不少于200字)**

1. 网络安全攻防实践

2023年，作为攻击方参与杭州市淳安县护网、杭州市亚运护网及浙江省护网行动，获得省三等奖的成绩。同年8月，作为防守方参与华夏银行总部的国家级护网行动实现零失分，获得客户的高度认可并收到感谢信。这些实战经历不仅提升了我的网络安全实战能力，也提提升了我的软件分析技术。

2. 专业实践训练

2023年至2024年，我在杭州智语网络科技有限公司进行专业实践，主导开发了一套用于挖掘公司产品的潜在漏洞的内存错误检测工具。经过6个月的研发，成功设计并实现了fslSan，一个基于影子内存编码和相对寻址插桩的C/C++内存错误检测工具。该工具显著提升了漏洞检测效率。本次专业实践训练使我深入掌握了编译原理，并且锻炼了我的组织协调能力，体现了技术创新与工程实践的结合。

3.

美团基础安全部门实习经历

2024年4月至6月，在美团基础安全部门实习期间，以蓝军视角对美团APP及其协议进行逆向分析，挖掘两个POI和一个SKU泄露接口，并分析了libmtguard.so中的mtgSig算法及传感器参数，提出风控对抗策略。此外，针对样本的重打包绕过机制进行了研究并提出了解决方案。本次实习使我接触到了一些数据安全对抗涉及的具体攻防方法，积攒了风控对抗的经验，以及提升了逆向分析技术水平。

0 华为安全实验室实习

2024年7月至9月，在华为安全实验室暑期实习期间，实习内容是复现CVE、源码审计和Linux的IPC组件与虚拟化驱动的漏洞挖掘。通过编写syzlang和针对性优化syzkaller mutator，将特定目标的模糊测试覆盖率由baseline的15%提高至50%，跑出3个不同类型的crash。这些工作让我对Linux内核、syzkaller的原理以及安卓平台的Linux特性有了更深的认识，同时提高了我应对压力和挑战的能力。

4. 开源社区贡献与跨团队协作能力

积极参与开源社区工作，在Qemu和Linux内核项目中贡献了多个代码补丁，并与社区开发人员紧密合作，提出了有效的修复方案。相关贡献记录如下：
CVE-2024-49863修复补丁：https://lore.kernel.org/linux-cve-announce/2024102110-CVE-2024-49863-6a74@gregkh/
Linux内核补丁提交：https://lkml.org/lkml/2025/1/11/81
Qemu项目补丁提交：https://patchwork.kernel.org/project/qemu-devel/patch/20240917181256.634732-8-mjt@tls.msk.ru/

这些经历不仅提升了我对开源系统的理解，还培养了我跨语言、跨国的沟通和协作能力。

**3.在实际工作中综合运用所学知识解决复杂工程问题的案例（不少于1000字）**

fslSan——基于llvm的C/C++内存错误动态检测框架
一、公司概况：
杭州智语网络科技有限公司（以下简称“小语智能”）是一家依托于浙江大学计算机学院，专注智能客服营销及大数据创新服务的高新技术企业。小语智能公司核心成员均来自浙江大学、阿里巴巴等知名学校和企业，科研团队由众多人工智能领域教授、博士、硕士组成，具有极强的研发实力和创新能力。
小语智能自成立以来，以智能语音AI为基础，获得多项国家发明专利及软件著作权。该公司提供安全研究的实践岗位，工作内容为开发一套模糊测试框架，发掘公司产品的潜在漏洞。
二、项目来源：
内存漏洞是编码者疏忽导致的软件缺陷，可能会带来拒绝服务、数据泄露、远程代码执行等问题，商业产品中出现的软件漏洞，通常如果被黑灰产利用，会严重危害用户隐私，从而导致销量下降，甚至违反《数据安全法》，收到有关部门的处罚。因此，编码安全性是软件公司不得不重视的一项问题。越来越多的公司采用单元测试、代码评审、模糊测试等方法检测编码软件的漏洞，从而在产品发布前将其修复，将损失降到最低。目前业界普遍使用Address Sanitizer（以下简称ASan）来检测C/C++程序的内存错误问题。传统的 Asan是一

C/C++内存错误检测工具，可以发现代码中的诸多安全问题。但是Address Sanitizer在设计上并非完备，很多情况可能导致漏报。如何设计一套更精确的内存错误检测机制，同时兼顾性能和易用性，是一个具有挑战性的课题。

三、研究路线：

该项目基于llvm 15.0框架，在保持 Asan 高效性的前提下AddressSanitizer的基础上对影子内存进行编码，实现O(1)时间复杂度的内存区域定位。该项目继承了 Asan 的影子内存（Shadow Memory）、插桩模块（Instrumentation）和运行时库（Run-time Library）三个主要部件。本人在项目中负责释放后重使用的检测机制设计和代码实现。经过6个月的研发实践，设计并实现了fslSan，一个基于影子内存编码和相对寻址插桩的C/C++内存错误检测工具。对于空间内存错误，FslSan通过重新设计 shadow memory 的赋值与检测机制，使用基于扩展标志位的编码存储偏移信息，可以检测出 Asan 所能检测到空间类型的全部错误，还可以实现缓冲区非连续访问错误的检测。对于时间内存错误，FslSan 通过对指针地址插桩，标记了指针所指向内存的释放状态，并在解引用和指针值传递时插桩，独立实现了向上的别名分析和向下的值传递链追踪，从而实现指针层面的 UAF 检测。该项目以常数级别的额外开销实现了Asan所不能识别的通过逻辑错误访问合法地址的内存越界访问和释放后重引用运行时检测。后续的优化可以考虑提升插桩指令的效率，使得运行开销接近ASan。

四、实践情况：

在实践过程中，我运用所学的编译原理知识解决了一系列复杂问题，通过自研的数据流分析和别名分析算法，实现了在编译过程进行解引用检测和传递链分析。

为了保证设计质量，我们对检测算法进行了多次迭代。例如，对于跨chunk溢出检测，最初的方法是在检测到有相对寻址的中间代码时，对基址也进行shadow检测，在每次访问内存前，获得基址所在chunk的size值（-0x8偏移），减去0x10与访问偏移量比对大小。但是如果访问的是中间的位置，那么无法通过偏移获得size；我们还考虑过在非连续访存情况下：在每次malloc后，将chunk的size字段和prev_size字段设置为一些特殊的内容，针对每次getelementptr指令，从getelementptr基址往前寻找，找到该chunk的size字段和prev Size字段，获得偏移。在free时恢复size字段和prev_size字段。但是考虑到寻找size字段和prev_size字段的时间消耗问题，这个方案还不能满足我们的要求。最终，经过深入思考我们发现问题的重点在于如何在时空复杂度尽可能小的前提下，判断getelementptr操作的基地址与目的地址之间有无redzone。最后，我们修改了shadow的映射机制，充分利用shadow byte的编码，用中间三位存储距离chunk尾地址的偏移量，并采用类似Unicode编码的拼接机制，在shadow byte中编码了距离chunk尾的偏移大小。对于UAF检测，我们考虑过给指针加一个metadata，但是metadata如何和指针存放地址的映射无法满足复杂度的要求。我们还考虑过让malloc指针先指向metadata，并给指针绑定一个nonce，再从matadata找到真实地址。访问的时候判断nonce是否匹配来确定是否UAF。但是由于解码状态下的free不好同步会导致漏报，以及系统调用的结构体不能处理加密指针的问题，这个方案最终被我们抛弃。我最后采用了标识指针的地址，对内存分配、访问和释放函数进行插桩从而进行检测的方案。

作为本次实践项目的领导者，除了核心部分的设计与编码外，我还负责了分工以及日程安排。我们把时间分成了算法设计阶段，编码实现阶段和测试以及报告撰写阶段，并为每一个阶段都设置了里程碑时间点。在最重要的设计和实现阶段，我们框架学习和算法设计同步进行。前几周学习llvm原理和ASan源码，并广泛阅读论文，开始提出思路，从第四周开始编码。因此，这次实践也锻炼了我的合作能力。

五、取得成效：

我们提出了FslSan——基于影子内存编码和指针解引用插桩的C/C++内存错误检测工具。Fslan 是一个基于 LLVM-15 设计的内存错误　　检测工具。我们使用 Juliet1.3 测试集对FslSan的功能进行了验证，结果表明FslSan的所有功能均达到了预期目标，同时在未加额外优化的情况下，时间和空间复杂度均接近 Asan。该工程的创新点在于改进了 Asan 的影子内存机制与部分插桩代码，把影子内存每一个比特的作用发挥到了极致，在继承了Asan强大的内存错误检测功能的基础上，解决了 Asan 无法检测到的多种漏报问题。由于llvm框架前后端分离的特性，FslSan的插桩处理目标是中间代码，因此我们的框架支持多种编译前端也就是多种编程语言，除了传统的C/C++之外还有 Ada, D, Delphi, Fortran, Haskell, Objective-C 和 Swift 等。因此，该框架是多语言多平台支持的，可以为PC、移动设备、物联网嵌入式系统等的构建的软件进行内存错误检测。最后，我们的检测方案参加了华为杯全国研究生网络安全大赛揭榜挑战赛，获得了二等奖。

六、其他项目（基于fslSan的下游模糊测试框架）

为了解决Native代码接口复杂、闭源分析编写模糊测试驱动需要大量人工成本的问题，我设计并实现了一套JNI库模糊测试自动化框架。通过自动化进行解析函数签名、生成Frida代码、Hook目标函数调用提取变异种子、根据函数签名将模糊测试输入转化为jvm内部状态等过程，该项目达成了以较低的人工成本将闭源JNI代码接入AFL等模糊测试工具的目标。此外，我还编写了图形化界面，可以一键Fuzz目标APK的JNI函数。支持自动生成的JNI函数参数类型包括原始类型、引用类型和多维数组等。

针对内核态虚拟化设备的研究，我提出了云计算环境下基于 Host 控制层扩展攻击面的威胁模型，并基于此威胁模型开发了适用于内核态 VHost 虚拟设备的模糊测试框架vhfuzz。从理论上对传统内核态虚拟设备模糊测试的架构进行了深入剖析，以虚拟设备的客户机总线地址转化为宿主机虚拟地址这一底层过程为切入点，优化了模糊测试架构，实现了目标虚拟化设备和 VMM 的解耦。具体贡献有

（1）设计了仅包含 VHost 虚拟设备的轻量级虚拟机管理程序vhvmm，降低了冗余虚拟化组件的开销，实现高效地初始化目标设备；
（2）提出了基于客户机请求模拟和数据注入的内核态虚拟设备模糊测试方法，并设计了针对客户机侧 VHost设备功能的数据注入组件 vhio 和 vhtlb。基于 I/O 转换后备缓存注入和 VRing接口拦截技术，分别针对底层 VRing驱动和顶层设备进行模糊测试，实现了更高的测试覆盖率；
（3）设计了数据调度算法，实现了模糊测试数据调度器 vhsched。数据调度器允许 vhtlb 组件动态获取模糊测试输入，从而提高了注入数据的匹配率和模糊测试效率。

相比于其他框架，vhfuzz 的初始化速度提升了59%，单次样例执行速度提升了6.7 倍；在代码探索能力上，vhfuzz 相比于仅针对宿主机控制面的内核模糊测试软件Syzkaller，其整体覆盖率表现由 45% 提升到 71%。实验表明 vhfuzz具有显著的效率和覆盖率优势。vhfuzz 框架成功挖掘了 7 个存在于上游 Linux内核主线的软件缺陷。

**（二）取得的业绩（代表作）【限填3项，须提交证明原件（包括发表的论文、出版的著作、专利证书、获奖证书、科技项目立项文件或合同、企业证明等）供核实，并提供复印件一份】**

1.
**公开成果代表作【论文发表、专利成果、软件著作权、标准规范与行业工法制定、著作编写、科技成果获奖、学位论文等】**

| 成果名称 | 成果类别<br>[含论文、授权专利（含发明专利申请）、软件著作权、标准、工法、著作、获奖、学位论文等] | 发表时间/授权或申请时间等 | 刊物名称/专利授权或申请号等 | 本人排名/总人数 | 备注 |
|---|---|---|---|---|---|
| 一种基于配置模糊匹配的安卓应用组成成分分析方法 | 发明专利申请 | 2024年07月24日 | 申请号：202410996860.9 | 1/8 | |
| 一种基于指针解引用插桩的C/C++释放后重引用动态检测方法 | 发明专利申请 | 2024年07月23日 | 申请号：202410996856.2 | 1/8 | |
| 第二届华为杯研究生网络安全创新大赛揭榜挑战赛 | 获奖 | 2023年11月01日 | | 2/4 | 二等奖（第2名） |

**2.其他代表作【主持或参与的课题研究项目、科技成果应用转化推广、企业技术难题解决方案、自主研发设计的产品或样机、技术报告、设计图纸、软课题研究报告、可行性研究报告、规划设计方案、施工或调试报告、工程实验、技术培训教材、推动行业发展中发挥的作用及取得的经济社会效益等】**

| （三）在校期间课程、专业实践训练及学位论文相关情况 | |
|---|---|
| 课程成绩情况 | 按课程学分核算的平均成绩： 87 分 |
| 专业实践训练时间及考核情况(具有三年及以上工作经历的不作要求) | 累计时间： 1.5 年（要求1年及以上）<br>考核成绩： 79 分 |
| **本人承诺** | |
| **个人声明：本人上述所填资料均为真实有效，如有虚假，愿承担一切责任，特此声明！**<br><br>**申报人签名：**张浩然 | |

2226095

## 二、日常表现考核评价及申报材料审核公示结果

| | |
|---|---|
| 日常表现考核评价 | 非定向生由德育导师考核评价、定向生由所在工作单位考核评价：<br>☑优秀 ☐良好 ☐合格 ☐不合格<br>德育导师/定向生所在工作单位分管领导签字（公章）：　　年　月　日 |
| 申报材料审核公示 | 根据评审条件，工程师学院已对申报人员进行材料审核（学位课程成绩、专业实践训练时间及考核、学位论文、代表作等情况），并将符合要求的申报材料在学院网站公示不少于5个工作日，具体公示结果如下：<br>☐通过 ☐不通过（具体原因：　　）<br>工程师学院教学管理办公室审核签字（公章）：　　年　月　日 |

# 浙 江 大 学 研 究 生 院

## 攻读硕士学位研究生成绩表

| 学号：22260095 | 姓名：张浩然 | 性别：男 | 学院：工程师学院 | 专业：计算机技术 | 学制：2.5年 |
|---|---|---|---|---|---|
| 毕业时最低应获：26.0学分 | 已获得：29.0学分 | 入学年月：2022-09 | 毕业年月： | | |
| 学位证书号： | 毕业证书号： | 授予学位： | | | |

| 学习时间 | 课程名称 | 备注 | 学分 | 成绩 | 课程性质 | 学习时间 | 课程名称 | 备注 | 学分 | 成绩 | 课程性质 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2022-2023学年秋季学期 | 工程技术创新前沿 | | 1.5 | 87 | 专业学位课 | 2022-2023学年春季学期 | 自然辩证法概论 | | 1.0 | 68 | 专业学位课 |
| 2022-2023学年冬季学期 | 物联网操作系统与边缘计算 | | 2.0 | 92 | 专业选修课 | 2022-2023学年春季学期 | 研究生英语基础技能 | | 1.0 | 75 | 公共学位课 |
| 2022-2023学年秋冬学期 | 高阶工程认知实践 | | 3.0 | 91 | 专业学位课 | 2022-2023学年春夏学期 | 移动互联网智能设备应用设计与实践 | | 3.0 | 96 | 专业学位课 |
| 2022-2023学年冬季学期 | 新时代中国特色社会主义理论与实践 | | 2.0 | 89 | 专业学位课 | 2022-2023学年春夏学期 | 密码学基础理论 | | 2.0 | 80 | 跨专业课 |
| 2022-2023学年秋冬学期 | 数据分析的概率统计基础 | | 3.0 | 68 | 专业选修课 | 2022-2023学年夏季学期 | 物联网信息安全技术与应用基础 | | 2.0 | 95 | 专业选修课 |
| 2022-2023学年冬季学期 | 研究生英语 | | 2.0 | 89 | 专业学位课 | 2022-2023学年夏季学期 | 研究生论文写作指导 | | 1.0 | 96 | 专业选修课 |
| 2022-2023学年秋冬学期 | 工程伦理 | | 2.0 | 96 | 专业学位课 | | 硕士生读书报告 | | 2.0 | 通过 | |
| 2022-2023学年冬季学期 | 产业技术发展前沿 | | 1.5 | 90 | 专业学位课 | | | | | | |
| | | | | | | | | | | | |

说明：1. 研究生课程按三种方法计分：百分制，两级制（通过、不通过），五级制（优、良、中、及格、不及格）。

2. 备注中“*”表示重修课程。

学院成绩校核章：

成绩校核人：张梦依

打印日期：2025-03-20

浙江大学研究生院（60）成绩校核章

(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119046135 A
(43)申请公布日 2024.11.29

(21)申请号 202410996856.2

(22)申请日 2024.07.24

(71)申请人 浙江大学
地址 310058 浙江省杭州市西湖区余杭塘路866号

(72)发明人 张浩然 陶逸铭 吴春明 汪昌兴 魏之千 边振昆 刘智扬 买买江·克然木

(74)专利代理机构 杭州求是专利事务所有限公司 33200
专利代理师 邱启旺

(51)Int.Cl.
*G06F 11/36*(2006.01)
*G06F 21/57*(2013.01)
*G06F 8/71*(2018.01)

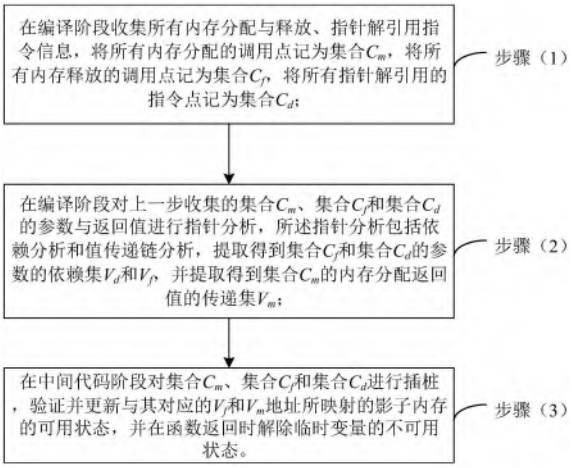
权利要求书3页 说明书6页 附图1页

(54)发明名称

一种基于指针解引用插桩的C/C++释放后重引用动态检测方法

(57)摘要

本发明公开了一种基于指针解引用插桩的C/C++释放后重引用动态检测方法,在执行软件测试时,传统的Address Sanitizer无法检测到地址合法的逻辑错误,本发明通过数据流分析和对GetElementPtr指令进行插桩,实现对指针重使用内存错误的动态检测。




CN 119046135 A

(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119045877 A
(43)申请公布日 2024.11.29

(21)申请号 202410996860.9
(22)申请日 2024.07.24
(71)申请人 浙江大学
地址 310058 浙江省杭州市西湖区余杭塘路866号
(72)发明人 张浩然 刘智扬 吴春明 边振昆 陶逸铭 汪昌兴 魏之千 买买江·克然木
(74)专利代理机构 杭州求是专利事务所有限公司 33200
专利代理师 邱启旺
(51)Int.Cl.
*G06F 8/74*(2018.01)
*G06F 8/71*(2018.01)
*G06F 8/53*(2018.01)
*G06F 18/22*(2023.01)
*G06F 18/10*(2023.01)

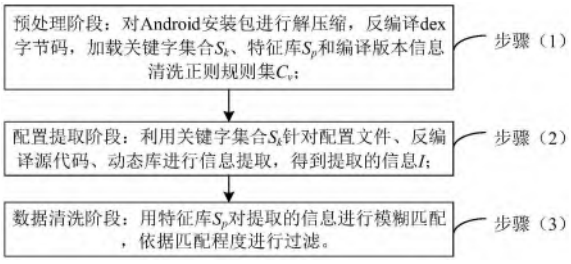
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种基于配置模糊匹配的安卓应用组成成分分析方法

(57)摘要

本发明公开了一种基于配置模糊匹配的安卓应用组成成分分析方法。在进行移动应用软件分析时,提取第三方组件是一件费时费力的事情。本发明通过对可能出现SDK信息的配置文件与代码进行针对性搜索与提取,并基于特征库模糊匹配对结果进行过滤,实现对APK组成成分和硬编码密钥情况的静态分析。




CN 119045877 A

CPIPC
中国研究生
创新实践系列大赛

中国研究生创新实践系列大赛

# 获奖证书

参赛单位：浙江大学
参赛作品：fslSan——基于llvm15.x的C/C++内存错误检测工具
指导教师：吴春明
参赛队员：陶逸铭、张浩然、汪昌兴、魏之千

荣获“华为杯”第二届中国研究生网络安全创新大赛

# 揭榜挑战赛·二等奖

中国学位与研究生教育学会　　中国科协青少年科技中心

二〇二三年十一月

证书编号：W2023012006

DataCon

张浩然

在DataCon2022大数据安全分析竞赛
软件安全赛道中荣获

# 一等奖

特发此证，以资鼓励。

DataCon组委会
2022年12月

主办单位：奇安信 清华大学 网络科学与网络空间研究院 Institute for Network Sciences and Cyberspace
蚂蚁集团 ANT GROUP 腾讯安全大数据实验室 TENCENT SECURITY BIG DATA LAB Coremail论客

S7

# 第七届 强网杯

## 全国网络安全挑战赛

指导单位：中央网信办　河南省人民政府
主办单位：信息工程大学　河南省委网信办
河南省教育厅　郑州市人民政府

## 线下赛

# 获奖证书

获奖等级：二等奖

参赛单位：浙江大学

战队名称：AAA

参赛队员：康锦辉、韩　数
张浩然、谢天晰

“强网杯”全国网络安全挑战赛
竞赛组织委员会
2024年1月

XCTF
国际网络攻防联赛

# XCTF INTERNATIONAL COMPETITION
# TPCTF 2023

## THIS CERTIFICATE IS PROUDLY PRESENTED TO

## 张浩然

## FOR WINNING



November,27,2023
Date

Chair of Technical Committee

# 荣誉证书

CERTIFICATE OF HONOR

张浩然 ：

您出的题目被第六届浙江省大学生网络与信息安全竞赛组委会采用。

特发此证，以资鼓励！

浙江省大学生网络与信息安全竞赛组委会

二〇一三年十一月