

同行专家业内评价意见书编号： 20250854398

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： 边振昆

学号： 22260082

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)

我在计算机技术领域有较为扎实的基础理论知识，主要掌握计算机系统的架构、操作系统、数据库原理以及网络协议等基本概念。此外，我对网络安全领域的相关知识有深入了解，特别是在网络攻防、信息加密和渗透测试等方面具有较强的理论基础。通过对常见攻击方式如DDoS攻击、SQL注入、XSS攻击等的研究，我熟悉了防火墙、入侵检测、入侵防御系统（IDS/IPS）等安全技术的原理和应用。在专业技术方面，我能够熟练使用各种网络安全工具，如Wireshark、Metasploit、Nmap等，进行漏洞扫描和安全评估。此外，我还掌握了编程语言和算法设计，能够独立开发和调试安全工具，解决实际安全问题。对于近些年兴起的大语言模型也进行了系统学习，并将其与实践进行了结合。

2. 工程实践的经历(不少于200字)

1. 杭州智语网络科技有限公司进行校外专业实践，研究课题为新型Web应用攻击检测与漏洞挖掘方法研究。
2. 杭州安恒信息技术股份有限公司实习，从事“恒脑”安全领域垂类大模型研发相关工作。
3. 腾讯科技（深圳）有限公司实习，从事网络安全研究以及大模型前沿技术的探索工作。
4. 参与国家重点研发计划课题：多模态边缘网络安全。
5. 参与泉城省实验室重点项目：园区网络动态高级防御算法与技术。
6. 参与浙江省科技计划项目：支撑行业应用的数据服务系统研究及应用示范。

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）

在杭州智语网络科技有限公司进行校外专业实践期间，我针对两个项目进行了研究与实现，研究方向之一是针对Spring框架漏洞的检测，另一个是针对无文件WebShell攻击的检测。我将这两项研究项目分为了上下两个半区，首先对Spring框架攻击与防守进行研究，最后着重对无文件WebShell攻击检测进行深入研究。

通过查阅相关论文和网上公开博客，我首先确定了针对Spring框架漏洞检测的学习路线：首先对Java语言以及Spring框架进行源码层面的学习，对最常见的攻击方式进行复现，随后对静态与动态分析技术进行探索，确定使用CodeQL作为静态分析的最重要技术，动态分析采用动态发送PoC，根据返回内容进行分析。通过整个学习与实践的流程，我对Java安全尤其是Spring框架的漏洞有了更加深刻的理解，并且对静态分析技术有了更深入的探索。企业也为我们提供了许多帮助，比如初期对于方法路线探索过程中与我一起确定思路，避免我多走很多弯路，还为我们提供了一些更硬核的资料学习，这使我收获颇丰。

无文件WebShell攻击检测的研究课题更让我确定了毕业论文的研究方向。企业实践使我对于无文件WebShell攻击的历史进程有了整体性的认知，无文件WebShell借助系统内存和合法工具执行恶意操作，隐蔽性更强，对于有效检测提出了巨大挑战。为应对该挑战，我设计并实现了一种基于RASP智能决策的检测方法。主要对以下三个方面进行了研究与实现：（1）提出了一种基于RASP的类行为分析检测技术，通过对Java无文件WebShell敏感方法进行动态监控，基于类的行为特征进行分析，筛选高危风险类，结合大语言模型进行初步判断，可覆盖绝大多数常见Java无文件WebShell；（2）提出了一种基于大语言模型与规则的数据增强技术，通过Prompt技术与规则匹配实现Java无文件WebShell样本的多样性与数据量层面的循环增强，解决Java无文件WebShell样本量不足以支撑模型训练的问题；（3）提出了一种基于大语言模型异构体的联合裁决检测技术，通过微调得到倾向不同的大语言模型，利用堆叠泛

化思想联合多个大语言模型异构体进行裁决，借助逻辑回归算法给出最终判断结果，有效提升整体检测能力。

通过对这两个课题的研究，我的学习能力得到了大幅提升，从以往的看到一个课题发怵成长到现在看到一个问题更加得心应手，解决问题的思想是相似的，不必慌张，一步一步走，做好调研、分析、设计与实现，问题也就迎刃而解了。

(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 [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
一种基于静态分析的Java框架自动化漏洞发掘构造方法	发明专利申请	2024年07月15日	申请号：202410943907.5	1/8	
一种基于静态分析与模拟执行的PowerShell反混淆方法	发明专利申请	2024年02月26日	申请号：202410208923.X	1/8	
第二届研究生网络安全创新大赛揭榜挑战赛全国一等奖	获奖	2023年11月14日		2/3	

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） 考核成绩： 84 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！	
申报人签名： 边振良	

22260082

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： ☒ 优秀 ☐ 良好 ☐ 合格 ☐ 不合格 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： ☐ 通过 ☐ 不通过（具体原因：_____） 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：22260082		姓名：边振昆		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：28.0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		研究生英语基础技能			1.0	68	公共学位课
2022-2023学年秋季学期		新时代中国特色社会主义思想理论与实践			2.0	92	公共学位课	2022-2023学年春季学期		科技创新案例探讨与实战			2.0	87	专业选修课
2022-2023学年秋冬学期		工程伦理			2.0	83	公共学位课	2022-2023学年春季学期		自然辩证法概论			1.0	88	公共学位课
2022-2023学年秋冬学期		高阶工程认知实践			3.0	85	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学年秋冬学期		研究生论文写作指导			1.0	67	专业学位课	2022-2023学年夏季学期		物联网信息安全技术与应用基础			2.0	94	专业学位课
2022-2023学年秋冬学期		研究生英语			2.0	87	公共学位课	2022-2023学年夏季学期		工程师创新创业思维			2.0	98	专业选修课
2022-2023学年冬季学期		产业技术发展前沿			1.5	82	专业学位课			硕士生读书报告			2.0	通过	
2022-2023学年冬季学期		工程中的有限元方法			2.0	98	专业选修课								

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





(12) 发明专利申请

(10) 申请公布号 CN 119128891 A

(43) 申请公布日 2024. 12. 13

(21) 申请号 202410943907.5

(22) 申请日 2024.07.15

(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 边振昆 吴春明 刘智扬 张浩然
汪昌兴 陶逸铭 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 21/57 (2013.01)

G06F 8/53 (2018.01)

G06F 11/36 (2006.01)

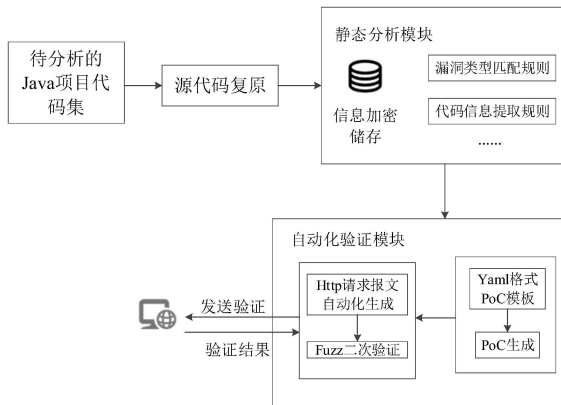
权利要求书2页 说明书4页 附图1页

(54) 发明名称

一种基于静态分析的Java框架自动化漏洞
发掘构造方法

(57) 摘要

本发明提供一种基于静态分析的Java框架自动化漏洞发掘构造方法,用于提高Java框架开发的应用安全性测试效率,解决人工费时费力的同时漏洞发掘效率与准确率低下的问题。本构造方法使用多种静态分析技术联合对代码进行静态分析,发掘可能存在的漏洞点,接着进行自动化验证技术与Fuzz模糊测试技术对漏洞点进行动态验证可达性与可利用性,最终实现Java框架漏洞的自动化挖掘与验证的全流程自动化。





(12) 发明专利申请

(10) 申请公布号 CN 118211216 A

(43) 申请公布日 2024. 06. 18

(21) 申请号 202410208923.X

(22) 申请日 2024.02.26

(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 边振昆 吴春明 张浩然 刘智扬
陶逸铭 汪昌兴 魏之千
买买江·克然木(74) 专利代理机构 杭州求是专利事务有限公司
33200

专利代理师 邱启旺

(51) Int. Cl.

G06F 21/56 (2013.01)

G06F 21/57 (2013.01)

G06F 21/55 (2013.01)

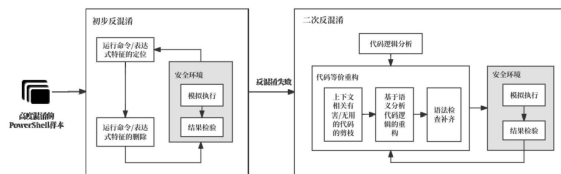
权利要求书2页 说明书4页 附图1页

(54) 发明名称

一种基于静态分析与模拟执行的PowerShell反混淆方法

(57) 摘要

本发明公开了一种基于静态分析与模拟执行的PowerShell反混淆方法,通过使用黑名单与模拟执行方法进行初步反混淆,尝试对关键数据进行提取与漏洞挖掘。二次反混淆中引入符号执行思想,尝试解决对初步反混淆后的PowerShell文件存在的代码逻辑混淆问题,在保证语义正确的前提下,依据静态分析中符号执行思想对多路径分支代码进行自动化调整,从而可以对关键信息进行进一步提取或对漏洞进行成功挖掘。





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: FSL-Aucltral

指导教师: 吴春明

参赛队员：刘智扬、边振昆、王正誥

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·一等奖

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

注册编号: W20230116004



(12) 发明专利申请

(10) 申请公布号 CN 119089440 A

(43) 申请公布日 2024. 12. 06

(21) 申请号 202411063326.9

(22) 申请日 2024.08.05

(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 刘智扬 吴春明 边振昆 张浩然
汪昌兴 陶逸铭 买买江·克然木

(74) 专利代理机构 杭州求是专利事务有限公司
33200

专利代理师 邱启旺

(51) Int.Cl.

G06F 21/56 (2013.01)

G06F 21/57 (2013.01)

G06F 21/60 (2013.01)

权利要求书2页 说明书4页 附图1页

(54) 发明名称

一种SpringBoot Web应用程序漏洞挖掘和验证的模糊测试方法

(57) 摘要

本发明公开了一种SpringBoot Web应用程序漏洞挖掘和验证的模糊测试方法,在饮用软件投入市场前,需要人工审计大量代码,挖掘出漏洞并验证该漏洞的可利用性,提高代码安全。本发明基于CodeQL静态分析、Fuzz等技术,挖掘SpringBoot Web应用程序漏洞并验证该漏洞的可利用性,最终提供利用成功的HTTP报文。





边振昆

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



Corendil 龙音

