南京邮电大学
毕 业 设 计（论 文）

题　　目　定向覆盖模糊测试工具的设计与实现

专　　业　计算机科学与技术

学生姓名　雷尚远

班级学号　B190303　B19030334

指导老师　王子元

指导单位　计算机学院、网络学院、网络空间安全学院

日期：　2023 年 3 月 x 日至 2023 年 6 月 x 日

毕业设计（论文）原创性声明

本人郑重声明：所提交的毕业设计（论文），是本人在导师指导下，独立进行研究工作所取得的成果。除文中已注明引用的内容外，本毕业设计（论文）不包含任何其他个人或集体已经发表或撰写过的作品成果。对本研究做出过重要贡献的个人和集体，均已在文中以明确方式标明并表示了谢意。

论文作者签名：

日期：　　年　　月　　日

摘　要

模糊测试（Fuzzing）是一种通过向目标系统提供非预期的输入并监视异常结果来发现软件安全漏洞的方法，是软件安全领域常用的方法之一。由于代码覆盖率与漏洞覆盖率密切相关，大多数模糊测试工具都是以代码覆盖率为导向。然而，由于大多数被覆盖测试的代码可能并不包含漏洞，这使得盲目地扩展代码覆盖率的方式在实际测试时效率较低。极端情况尤为如此。与盲目增加代码覆盖率的模糊测试不同，定向覆盖的灰盒模糊测试（DGF）将大部分时间用于检测特定目标区域（例如，易出错代码段）而不会浪费资源于不相关的部分。因此，DGF 特别适用于补丁测试、漏洞复现以及特殊漏洞检测等场景。目前，DGF 已成为一个快速发展的研究方向。基于一些先进的定向覆盖模糊测试工具的研究和相关调查，本文主要做了以下点工作：

(1) 基于现有的模糊测试工具框架 AFL（American Fuzzy Lop）以及 AFLGo 做了定向覆盖策略的设计和集成；
(2) 实现了简单的定向覆盖的模糊测试命令行工具；
(3) 针对相应的公开通用漏洞集（CVE）做了复现及定向实验对比测试。

此外本文亦通过分析工具设计以及实现过程中的局限性与不足，对于未来该方向的研究发展做出了一些展望。

关键词： 模糊测试；定向覆盖模糊测试；灰盒测试；软件安全

ABSTRACT

Fuzzing is a method of discovering software security vulnerabilities by providing unexpected inputs to a target system and monitoring for abnormal results. It is one of the commonly used methods in the field of software security. As code coverage is closely related to vulnerability coverage, most fuzz testing tools are guided by code coverage. However, blindly extending code coverage may be inefficient in practical testing since most of the covered code may not contain vulnerabilities, especially for corner cases. In contrast to blind code coverage-based fuzz testing, directed grey-box fuzzing (DGF) spends most of its time detecting specific target regions (such as error-prone code segments) rather than wasting resources on irrelevant parts. Thus, DGF is particularly suitable for scenarios such as patch testing, bug reproduction, and special bug detection. For now, DGF has become a fast-growing research area. Based on some advanced directed coverage fuzz testing tools and relevant investigations, this article mainly focuses on the following points of work:

(1) Designed and integrated a directed coverage strategy based on the existing fuzzy testing tool framework AFL (American Fuzzy Lop) and AFLGo；
(2) Implemented a simple command-line tool for directed fuzz testing；
(3) conducted reproductions and directed experiments on corresponding public vulnerability databases (CVE) for comparative testing。

In addition, this article also provides some prospects for the future research and development of this direction by analyzing the limitations and deficiencies in the design and implementation process of the tool.

Keywords: Fuzzing；Directed Greybox Fuzzing；Greybox test；Software Security

目　　录

第一章　绪论

1.1 背景分析

1.2 国内外研究现状

1.3 研究内容

1.4 论文结构

第二章　　相关技术研究

2.1 模糊测试技术

2.1.1 黑盒模糊测试技术

2.1.2 白盒模糊测试技术

2.1.3 灰盒模糊测试技术

2.2 定向模糊测试技术

2.2.1 白盒定向模糊测试技术

2.2.2 灰盒定向模糊测试技术

2.3 研究动机

2.4 本章小结

第三章　　基于 AFLGo 的定向模糊测试策略集成

3.1 模糊测试技术

3.1.1 黑盒模糊测试技术

3.1.2 白盒模糊测试技术

3.1.3 灰盒模糊测试技术

3.2 定向模糊测试技术

3.2.1 白盒定向模糊测试技术

3.2.2 灰盒定向模糊测试技术

3.3 研究动机

3.4 本章小结

这是一个参考文献示例[1]

第四章　　需要几章自己加一下！

结束语

致　谢

本论文采用 LaTeX 模版编写的，是基于南京邮电大学 2021 年理工艺教类的 Word 模板进行严格迁移编写的。本模板地址https://github.com/dhiyu/NJUPT-Bachelor感谢 imguozr（https://github.com/imguozr/NJUPThesis-Bachelor ）和 lemoxiao（https://github.com/lemoxiao/NJUPThesis-Scholar ）的工作，为本模板的形成奠定了大量的基础。

参考文献

[1] Lv J, Xu M, Feng L, et al. Progressive identification of true labels for partial-label learning[C]// International Conference on Machine Learning. PMLR, 2020: 6500-6510.

附录 A

1 本科期间的学术成果发表情况

- 发表一篇 Nature
- 获得了诺贝尔奖
- 当选足球先生
- 开发了 1nm 光刻机一台

2 本科期间的获奖情况

- 设计了一块 RTX5090
- 准备移民火星
- 去太阳上面看看