题　　目：二进制代码漏洞智能检测关键技术研究

摘要：近年来，随着互联网与软件技术的不断发展，软件的安全性以及网络空间安全这一概念越来越受到关注，与此同时针对于软件的安全测试愈发重要。Fuzz（模糊测试）作为二进制漏洞挖掘中的重要方法，为安全领域贡献了许许多多的0day漏洞。Libfuzzer作为LLVM项目中的一员，帮助安全研究人员编写出了许多功能迥异的fuzzer，发现了许多软件安全问题。

本文首先介绍软件软件的测试方法，并且着重分析了以fuzz为代表的黑盒测试方法，并且介绍了当前发现的比较常见的安全漏洞形式。

重点介绍了fuzz测试的主要工具libfuzzer的使用以及其功能的分析，并且利用libfuzzer对现存的两个漏洞CVE-2014-0160、CVE-2016-5180进行了复现，从源码层面剖析了漏洞的成因并且编写了fuzz程序对其进行挖掘。

本文研究的基于libfuzzer编写的fuzz程序在一定程度上可以有助于挖掘更多的安全漏洞，并且针对于不同的测试样例可以编写针对性更强的fuzz程序进行漏洞挖掘。

关键词：软件安全测试；fuzz；模糊测试；漏洞挖掘；libfuzzer；llvm

Abstract： In recent years, with the continuous development of the Internet and software technology, the concepts of software security and cyberspace security have received increasing attention. At the same time, security testing for software has become increasingly important. As an important method in binary vulnerability mining, Fuzz (fuzzing test) has contributed many 0day vulnerabilities to the security field. As a member of the LLVM project, Libfuzzer helped security researchers write many fuzzers with very different functions and found many software security problems.

This article first introduces the testing methods of software and software, and focuses on analyzing the black box testing method represented by fuzz, and introduces the more common forms of security vulnerabilities that are currently found.

It mainly introduces the use of libfuzzer, the main tool for fuzz testing, and the analysis of its functions, and uses libfuzzer to reproduce the two existing vulnerabilities CVE-2014-0160 and CVE-2016-5180, and analyzes the causes of the vulnerability from the source And wrote a fuzz program to mine it.

The fuzz program written in this paper based on libfuzzer can help to dig more security holes to a certain extent, and can write more targeted fuzz programs for vulnerability mining for different test samples.

Keywords: software security testing; fuzz; fuzzing; vulnerability mining; libfuzzer; llvm