Fuzzer Research

Jack Foley

September 28, 2024

Contents

1 Introduction

This document will outline the research done to start the work on the 4th Software Development Final Year Project (FYP). This project was created by Dr. Chris Meudec and is based on the idea of creating a fuzzer for the C programming language.

2 Fuzzing

Fuzzing is a method of testing software by using broken, random or usual data as an input into the software which is being tested. The idea of fuzzing is that it will find bugs and other issues that traditional software testing methods, such as unit testing, will not find as easily. There are some different types of fuzzing, such as white-box, grey-box and black-box fuzzing. There are also different approaches, dumb fuzzing or smart fuzzing.

2.1 White-box Fuzzing

White-box fuzzing, also known as smart fuzzing, is a technique that is used to identify flaws such as memory spikes and leaks (temporary denial-of-service), buffer overruns (remote code execution), unhandled exceptions, read access violations (AVs), and thread hangs (permanent denial-of-service). [1]

2.2 Black-box Fuzzing

2.3 Grey-box Fuzzing

Grey-box fuzzing is a well-known and commonly used fuzzing technique that is used for testing software and finding vulnerabilities. Differing from white-box and [2]

References

[1] J. Neystadt. *Automated penetration testing with white-box fuzzing*. Microsoft Learn. Available at: `https://learn.microsoft.com/en-us/previous-versions/software-testing/cc162782(v=msdn.10)?redirectedfrom=MSDN` (Accessed: 28 September 2024). 2009.

[2] Van-Thuan Pham et al. "Smart Greybox Fuzzing". In: *IEEE Transactions on Software Engineering* 47.9 (2021), pp. 1980–1997. DOI: `10.1109/TSE.2019.2941681`.