CS-412 Software Security Lab 2

Fuzzing Lab Report
Spring Semester 2025

Project: Tmux

Luca Di Bello (SCIPER 367552) Federico Villa (SCIPER XYZ)
Noah El Hassanie (SCIPER 404885) Cristina Morad (SCIPER 405241)

Submitted: May 8, 2025

Abstract

Briefly summarize goals, target project, and high-level results (coverage gains, crash triaged).

1 Introduction

Outline the assignment objectives and your chosen OSS-Fuzz project.

2 Methodology

Describe your environment, hardware, OSS-Fuzz setup, and how you conducted each experiment.

3 Part 1: Baseline Evaluation

3.1 With Seed Corpus

List the exact build/run commands and point to `run_w_corpus.sh`.

3.2 Without Seed Corpus

List the exact build/run commands and point to `run_wo_corpus.sh`.

3.3 Coverage Comparison

Discuss coverage percentages and key observations.

4 Part 2: Coverage Gaps

4.1 Region A

Justification of significance; why existing harness misses it.

4.2 Region B

Justification of significance; why existing harness misses it.

5 Part 3: Fuzzer Improvements

5.1 Improvement 1 (Region A)

Describe changes, refer to `improve1/run_improve1.sh`, and summarize coverage delta.

5.2 Improvement 2 (Region B)

Describe changes, refer to `improve2/run_improve2.sh`, and summarize coverage delta.

6 Part 4: Crash Analysis

Detail crash reproduction (`run_poc.sh`), ASAN log snippet, root cause, proposed patch, and exploitability.

7 Conclusion and Future Work

Summarize achievements and outline possible next steps.