# Fuzzing KDE Libraries: A Totally Serious Guide

## Introduction

Fuzzing KDE is fun. Fuzzing KDE is dangerous. here’s a short writeup that doesn’t do anything useful but looks like it does.

## Target: libkonqueror++

We are gonna fuzz a fake kde library called libkonqueror++. it does something with html css, and, javascript.

### Why fuzz it?

Because bugs…

## Setup

You need:

* clang (for -fsanitize=address,fuzzer)
* bash
* libkonqueror++ (ofc)`
* A cat (optional but boosts morale)

## Code snippet

#include <konqueror/fake.h>  
  
extern "C" int LLVMFuzzerTestOneInput(const uint8\_t \*data, size\_t size)   
 // Feed data to konqueror  
 return 0;  
}