

---

## STASH HOUSE

---

FRANKLIN DIAZ

September 25th, 2025



University of Colorado **Denver**

## Summary

In this project paper we will consider the issue of a "dirty" local development environment, and precisely what to do about it. Using freely available Open Source tools and a few easy to remember patterns we can work in a much more efficient and secure manner.

- First we look at how to set up a workable solution for storing credentials.
- Next we do some local search and cleanup to get our systems in order.
- Finally, we will see how we can still easily use these credentials though they remain encrypted at rest and in transit to our "vault" from now on.

# Contents

Summary . . . . .	i
<b>1 Introduction</b>	<b>1</b>
<b>2 Finding Secrets on Local Machine</b>	<b>2</b>
<b>3 Demonstration</b>	<b>3</b>
3.1 Setting Up . . . . .	3

## Chapter 1

# Introduction

## Chapter 2

# Finding Secrets on Local Machine

There is a BASH shells script that can be used to scan the local files for unsecured credentials that may be a candidate for encryption and safe storage.

## Chapter 3

# Demonstration

### 3.1 Setting Up

The same repository where this paper can be downloaded has the tools described in this and future chapters.