

LinkedIn: [Kelvin Kimotho](#)

Medium

Reverse Engineering

picoCTF 2022

AUTHOR: MUBARAK MIKAIL

Hints ?

## Description

(None)

Can you open this safe?

I forgot the key to my safe but this program is supposed to help me with retrieving the lost key. Can you help me unlock my safe?

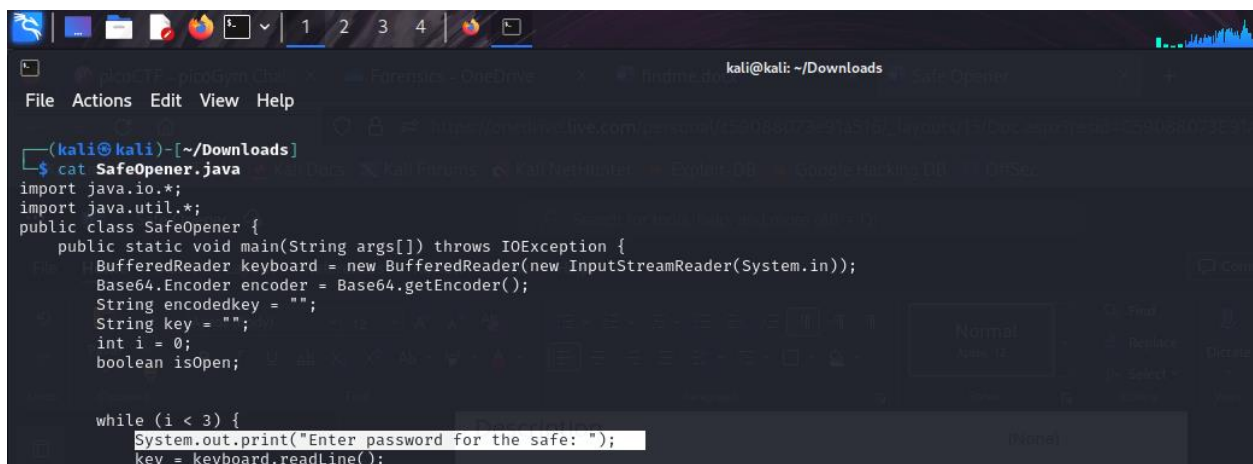
Put the password you recover into the picoCTF flag format like:

picoCTF{password}

## Solution

This task involved analyzing a java program trying to get the correct password required when running the program.

The program requires the user to enter a password then the program encrypts it using a **base64** encoding before comparing it with the expected password.



```
(kali@kali)-[~/Downloads]
$ cat SafeOpener.java
import java.io.*;
import java.util.*;

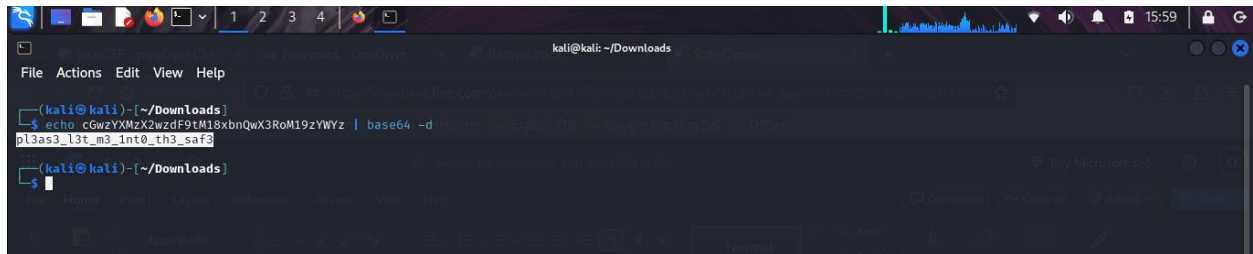
public class SafeOpener {
    public static void main(String args[]) throws IOException {
        BufferedReader keyboard = new BufferedReader(new InputStreamReader(System.in));
        Base64.Encoder encoder = Base64.getEncoder();
        String encodedkey = "";
        String key = "";
        int i = 0;
        boolean isOpen;

        while (i < 3) {
            System.out.print("Enter password for the safe: ");
            key = keyboard.readLine();
```

Knowing how the program works, I went ahead looking for the value being compared to the

encrypted password entered by the user. The expected password was

**cGwzYXMzX2wzdF9tM18xbnQwX3RoM19zYWYz** in base64 encoding. I went ahead and decoded the base64 encoding and this is what i got **pl3as3\_l3t\_m3\_1nt0\_th3\_saf3**.

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~/Downloads'. The terminal shows a command prompt where the user has entered the base64 string 'cGwzYXMzX2wzdF9tM18xbnQwX3RoM19zYWYz' and used the 'base64 -d' command to decode it. The output of the command is 'pl3as3\_l3t\_m3\_1nt0\_th3\_saf3'. The terminal has a dark background with light-colored text. The window's top bar shows various system icons and the time '15:59'.

To create the flag, I just added the decoded string within the brackets **{ }** considering the pico ctf flag format **picoCTF{pl3as3\_l3t\_m3\_1nt0\_th3\_saf3}** was the flag.