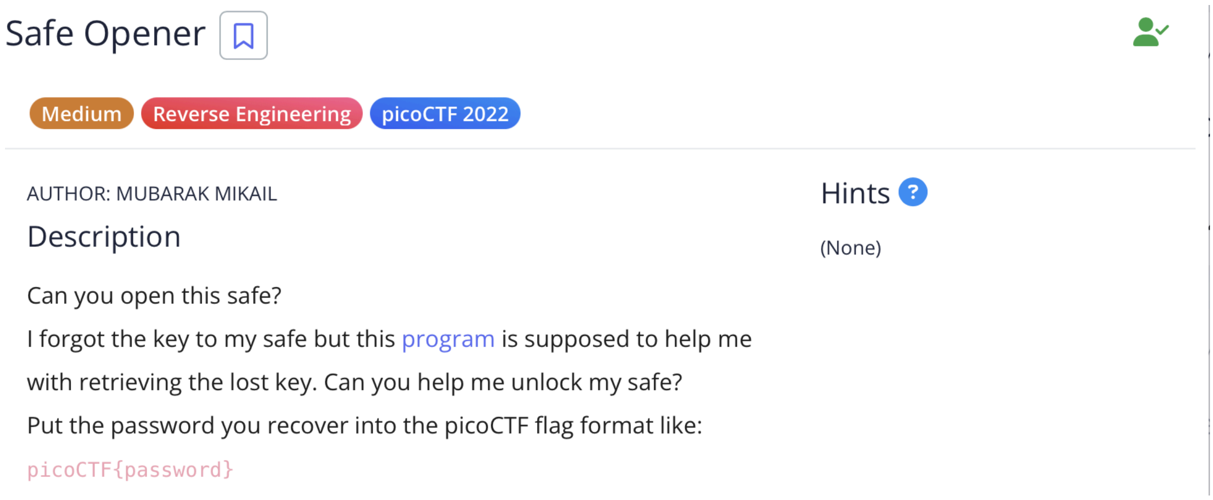


Safe Opener

Medium Reverse Engineering picoCTF 2022

AUTHOR: MUBARAK MIKAIL

Description

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?

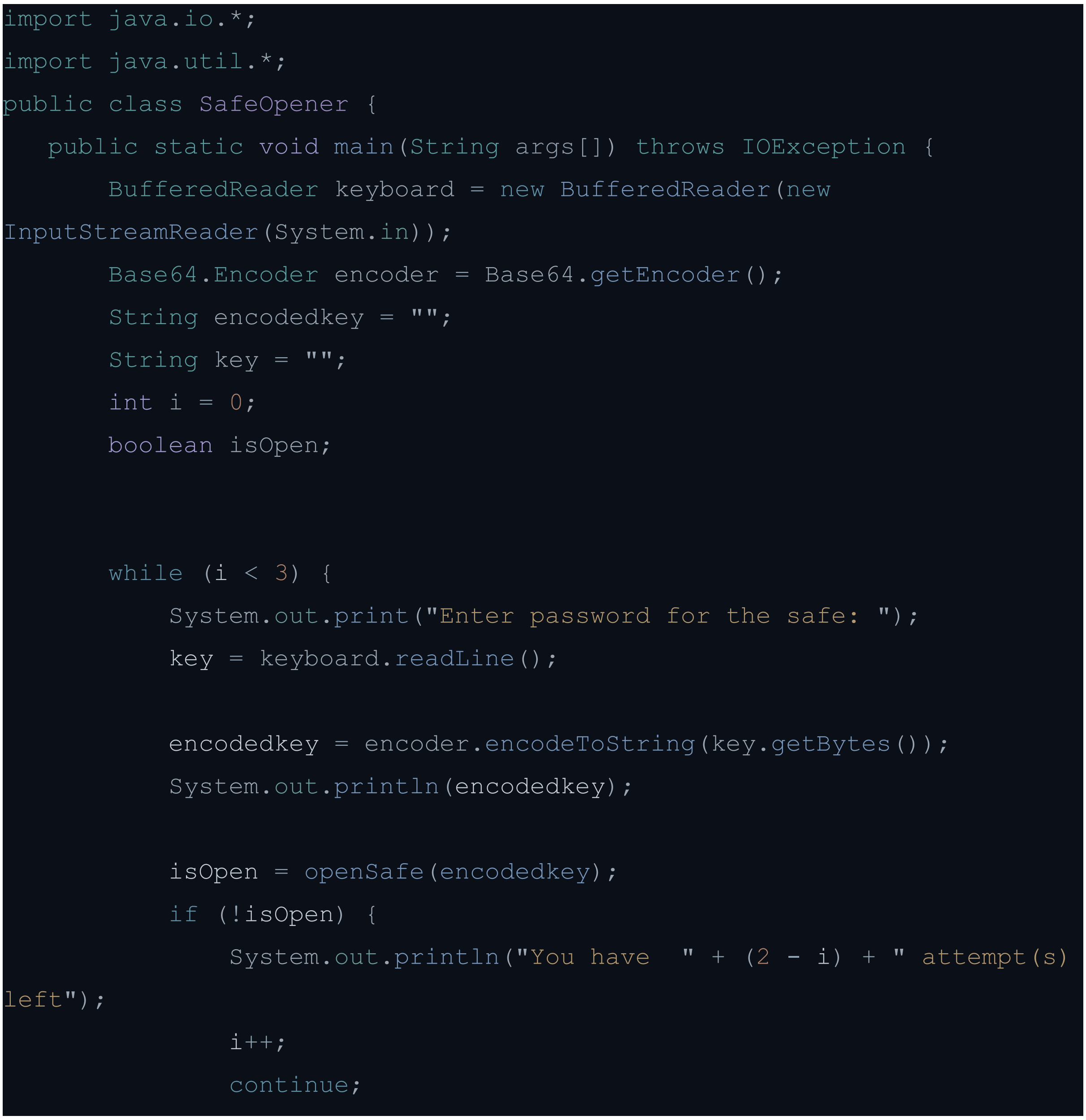
Put the password you recover into the picoCTF flag format like:

`picoCTF{password}`

Hints ?

(None)

Isi file :

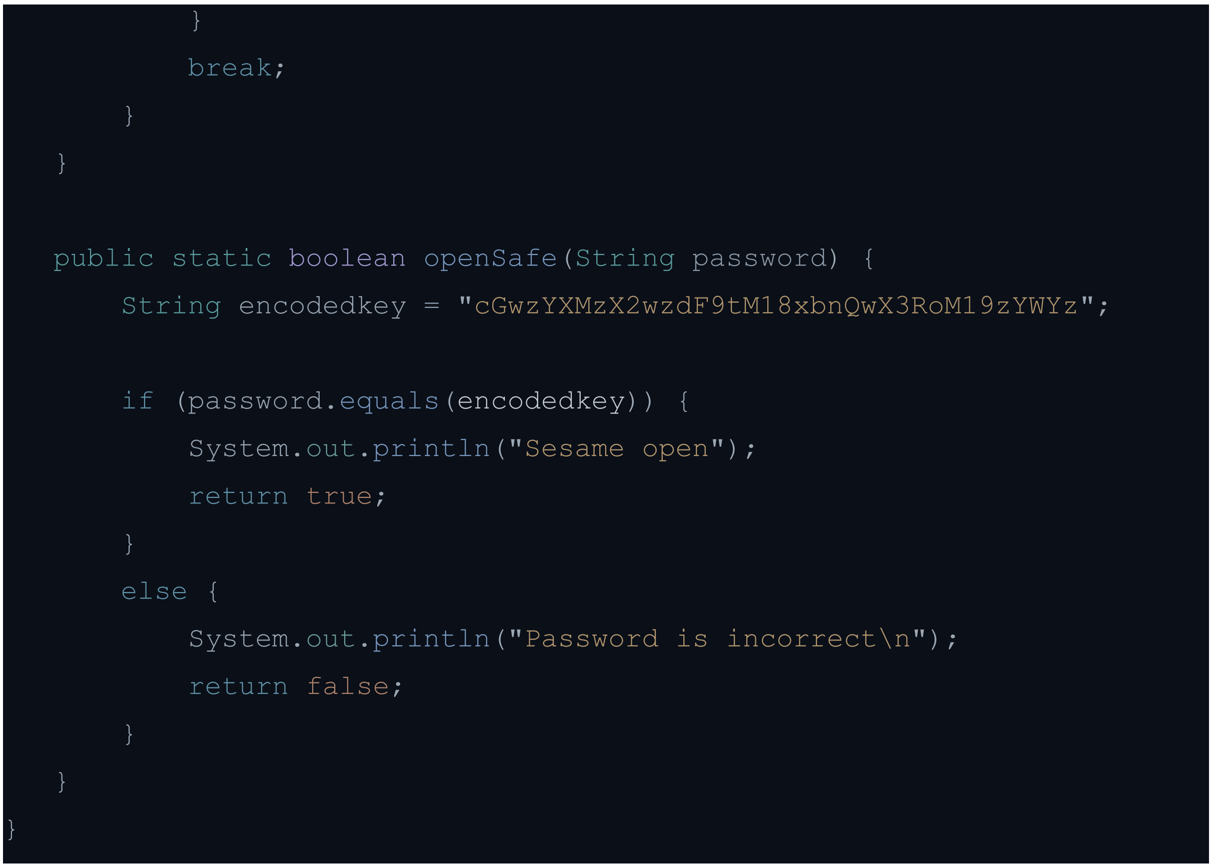


```
import java.io.*;
import java.util.*;
public class SafeOpener {
   public static void main(String args[]) throws IOException {
       BufferedReader keyboard = new BufferedReader(new
InputStreamReader(System.in));
       Base64.Encoder encoder = Base64.getEncoder();
       String encodedkey = "";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


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

           encodedkey = encoder.encodeToString(key.getBytes());
           System.out.println(encodedkey);

           isOpen = openSafe(encodedkey);
           if (!isOpen) {
               System.out.println("You have  " + (2 - i) + " attempt(s)
left");
               i++;
               continue;
```



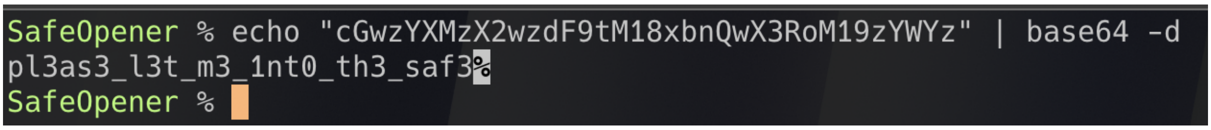
```
            }
            break;
        }
    }

    public static boolean openSafe(String password) {
        String encodedkey = "cGwzYXMzX2wzdF9tM18xbnQwX3RoM19zYWYz";

        if (password.equals(encodedkey)) {
            System.out.println("Sesame open");
            return true;
        }
        else {
            System.out.println("Password is incorrect\n");
            return false;
        }
    }
}
```

Pada source code di atas, terlihat bahwa sistem menerima input sebanyak 3 kali kesempatan dengan inputan berupa password. Password yang diinput tersebut akan di encoding dengan algoritma base64, nah jika hasil encoding sama dengan encodedkey yang ada pada fungsi openSafe, maka akan mengembalikan nilai true dan akan masuk ke dalam sistem.

Artinya disini, kita bisa melakukan decoding dari isi encodedkey dengan algoritma base64 juga seperti berikut :



```
SafeOpener % echo "cGwzYXMzX2wzdF9tM18xbnQwX3RoM19zYWYz" | base64 -d
pl3as3_l3t_m3_1nt0_th3_saf3%
SafeOpener %
```

Flag : picoCTF{pl3as3_l3t_m3_1nt0_th3_saf3}