

# Panda

发表于 2021-01-08 更新于 2021-01-09 分类于 [Challenge](#) , [2020](#) , [CSICTF](#) , [Forensics](#)  
[Challenge](#) | [2020](#) | [CSICTF](#) | [Forensics](#) | [Panda](#)

[点击此处](#)获得更好的阅读体验

---

## WriteUp来源

<https://dunsp4rce.github.io/csictf-2020/forensics/2020/07/22/Panda.html>

by AnandSaminathan

## 题目描述

*I wanted to send this file to AJ1479 but I did not want anyone else to see what's inside it, so I protected it with a pin.*

## 题目考点

## 解题思路

*The given zip file is password protected, which can be cracked using fcrackzip or john:*

```
1 fcrackzip -v -u -D -p rockyou.txt panda.zip
```

*The password was 2611. After extracting the zip file using the password, we got two images, one was the messed up version of the other. On analysing using xxd, it was clear that some parts of the original image was replaced in the messed up image (with the flag). A simple Go program which prints the changed bytes (the flag):*

```
1 package main
2 import (
3     "io/ioutil"
4     "fmt"
5 )
6 func main() {
7     corrupted, err1 := ioutil.ReadFile("panda1.jpg")
8     original, err2 := ioutil.ReadFile("panda.jpg")
9     if err1 != nil || err2 != nil {
10        fmt.Printf("Error loading the files")
11    }
12    for i, cur := range original {
13        if cur != corrupted[i] {
14            fmt.Printf("%c", corrupted[i])
15        }
16    }
17    return
18 }
```

## Flag

```
1 csictf{kung_fu_p4nd4}
```

- 本文作者: [CTFHub](#)
- 本文链接: <https://writeup.ctfhub.com/Challenge/2020/CSICTF/Forensics/t2bxWNQYBxQ8RrAhhqEquc.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[# Challenge](#) [# 2020](#) [# CSICTF](#) [# Forensics](#)

[unseen](#)

[In Your Eyes](#)