به نام ایزد یکتا

گزارش اول آزمایشگاه سیستم‌عامل

­­

استاد: مهندس قاسمی

تهیه کننده: بردیا اردکانیان

۹۸۳۱۰۷۲

**دایرکتوری داخل میز‌کاری (Desktop) بسازید و تمامی مجوز‌های آن را به گونه‌ای تغییر دهید که فقط شما و اعضای گروه بتوانند بنویسند، بخوانند و در آن جست‌و‌جو کنند.**

شرح مراحل:

1. cd Desktop/
2. mkdir [foldername]
3. chmod ug+rwx [foldername]
4. ls -l

همانطور که در دستورات بالا مشاهده کردیم برای ساخت یک دایرکتوری داخل میزکار، طبق شکل 1-1 ابتدا با استفاده از دستور cd به آدرسDesktop رفتیم سپس با استفاده از دستورmkdir یک دایرکتوری جدید به اسم temp ساختیم.

بعد از دستورات وارد شدن به دایرکتوری و ساختن دایرکتوری temp؛ با استفاده از chmod مجوز‌های آن را تغییر دادیم. شرح هرکدام از الگومان‌های دستور به ترتیب آمده است:

* برای تغییر مجوزهای دایرکتوری برای همه، از "u" برای کاربران، "g" برای گروه، "o" برای دیگران، و "ugo" یا "a" (برای همه) استفاده می‌شود.
* برای اضافه کردن، گرفتن دسترسی از یک دایرکتوری به ترتیب از + و – استفاده می‌شود.
* برای تغییر دسترسی خواندن، نوشتن و اجرا کردن به ترتریب از r، w، x استفاده می‌شود. (به ترتیب read، write و execute)

بنابر این با استفاده از دستور ug+rwx به کاربر (u) و گروه (g) دسترسی خواند، نوشتن و اجرا کردن (rwx) اعطا (+) شد.

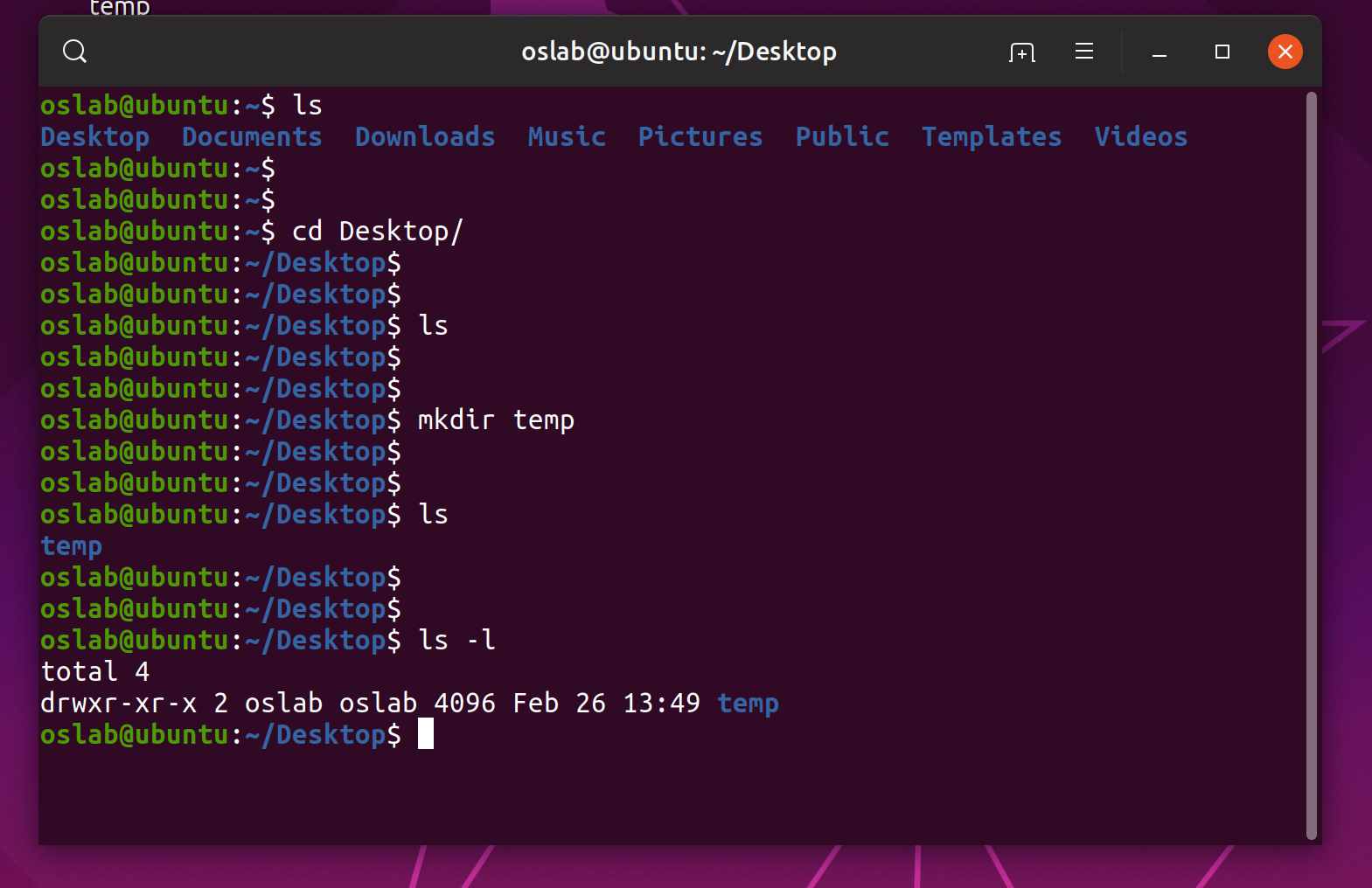
ممکن است لازم باشد بدانید که چگونه مجوزهای کد عددی را در لینوکس تغییر دهید، بنابراین برای انجام این کار به جای "r"، "w" یا "x" از اعداد استفاده می‌کنید.

* 0 = بدون مجوز
* 1 = اجرا کنید
* 2 = بنویس
* 4 = بخوانید

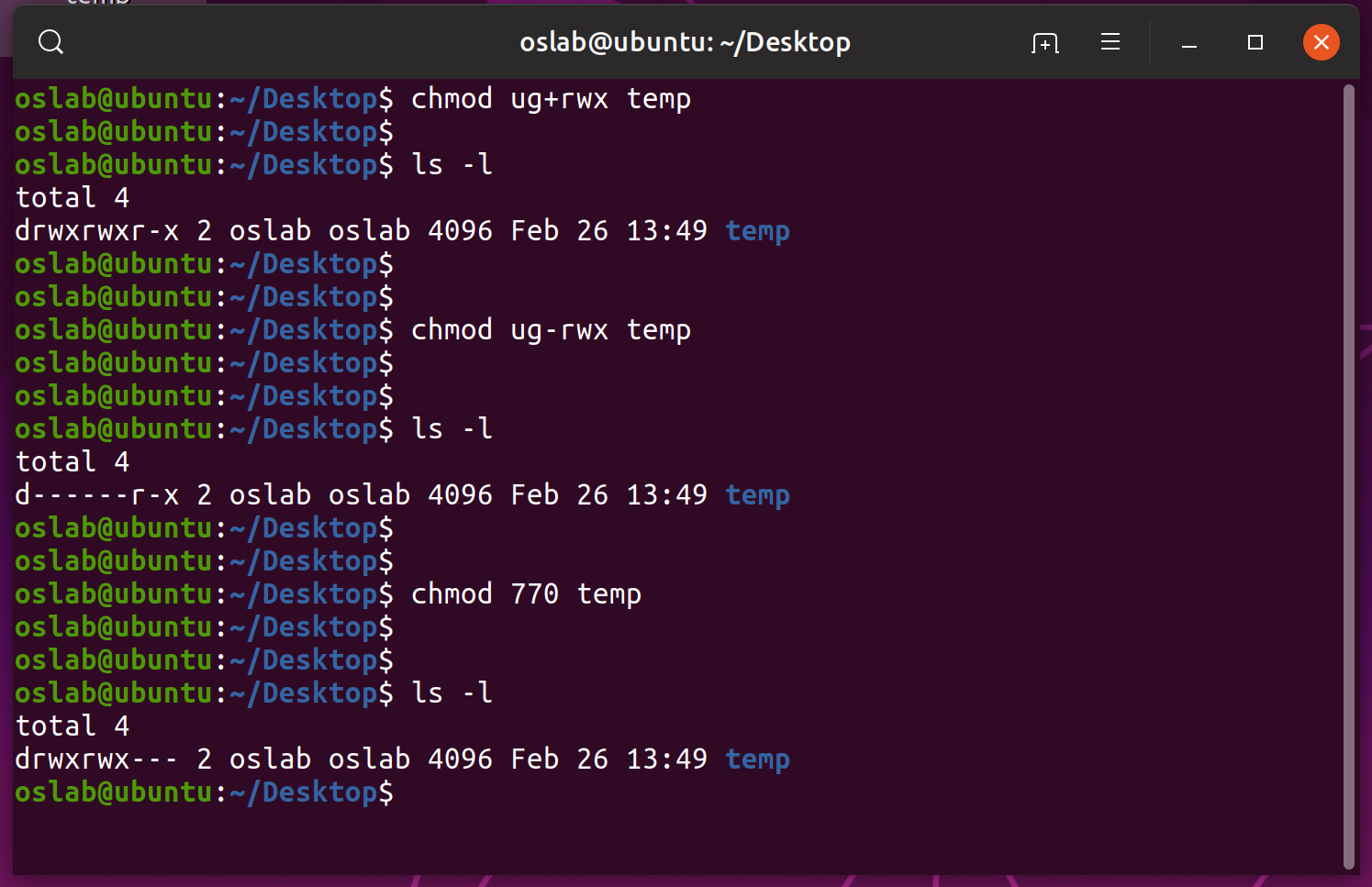
اساساً، بسته به سطح مجوزی که می خواهید بدهید، اعداد را جمع می کنید.

همچنین اعطا دسترسی به ترتیب برای کاربر، گروه و دیگران به صورت xxx است که به جای هر x جمع اعداد سطح دستری داده می‌شود.

بنابر‌این برای انجام دستور فوق می‌توان از chmod 770 نیز استفاده کرد. چرا 770؟ چون 0 اخر مربوط به دیگران (others) می‌باشد و قرار نیست دسترسی اعطا شود.



شکل 1-1



شکل 1-2

همچنین می‌توان با استفاده از ls -l سطح دسترسی را مورد برسی قرار داد. با مقایسه شکل 1-1 و 1-2 این تغییرات قابل مشاهده است.

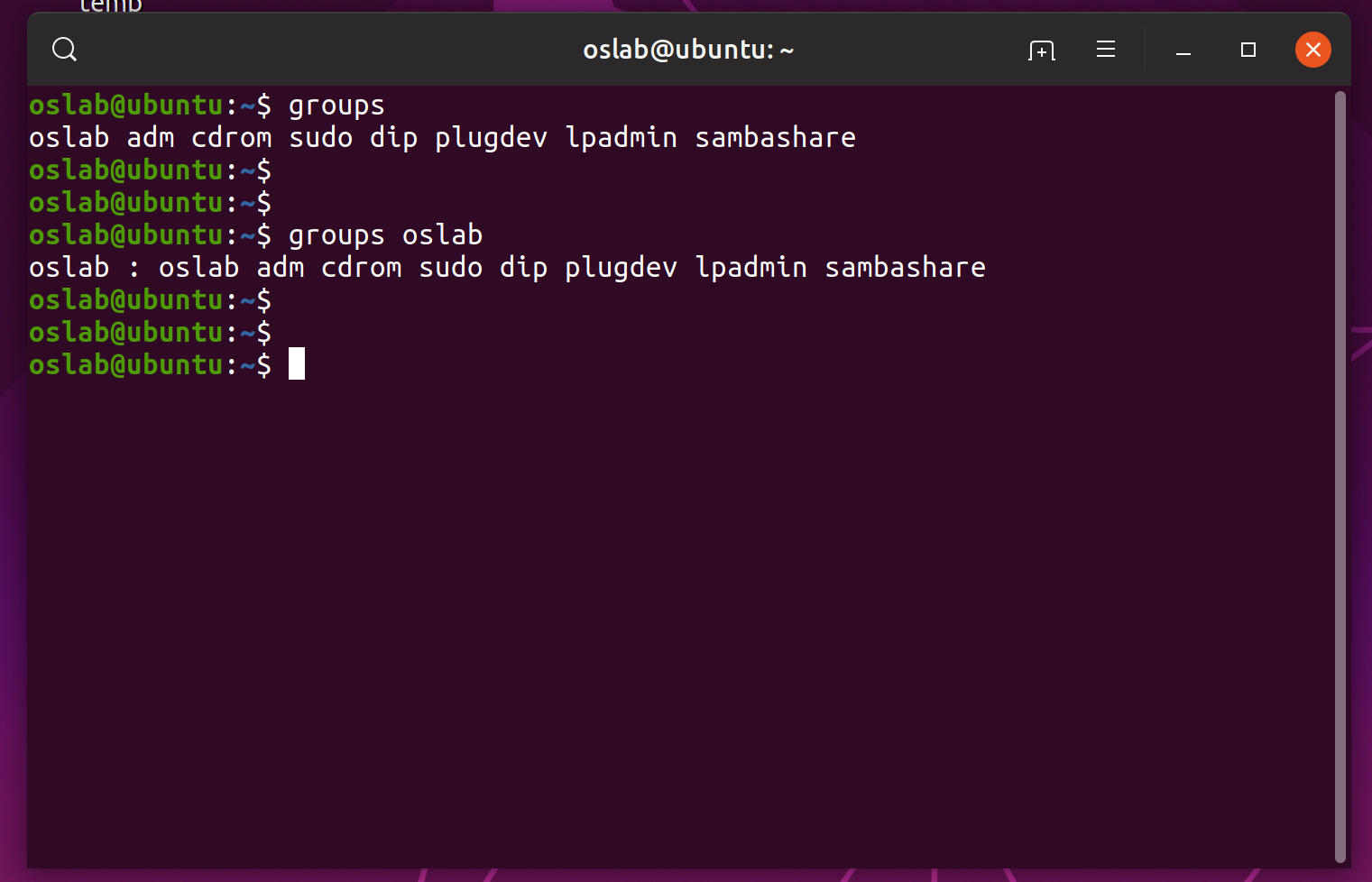
**گروه‌هایی که شما در آن عضو هستید را لیست کنید، سپس مالکیت فایل فعلی را به یکی دگر از گروه‌های خود بدهید.**

لیست کردن گروه‌های که کاربر oslab در آن هستند:

1. groups [username]…

* دستور groups نام گروه های اصلی و مکمل را برای هر نام کاربری داده شده یا فرآیند فعلی را در صورت عدم وجود نام چاپ می کند.
* اگر بیش از یک نام داده شود، نام هر کاربر قبل از لیست گروه های آن کاربر چاپ می شود و نام کاربری با علامت دونقطه از لیست گروه جدا می شود.

شکل 2-1 هر 2 حالت را به نمایش کشیده است.



شکل 2-1

عوض کردن مالکیت فایل فعلی:

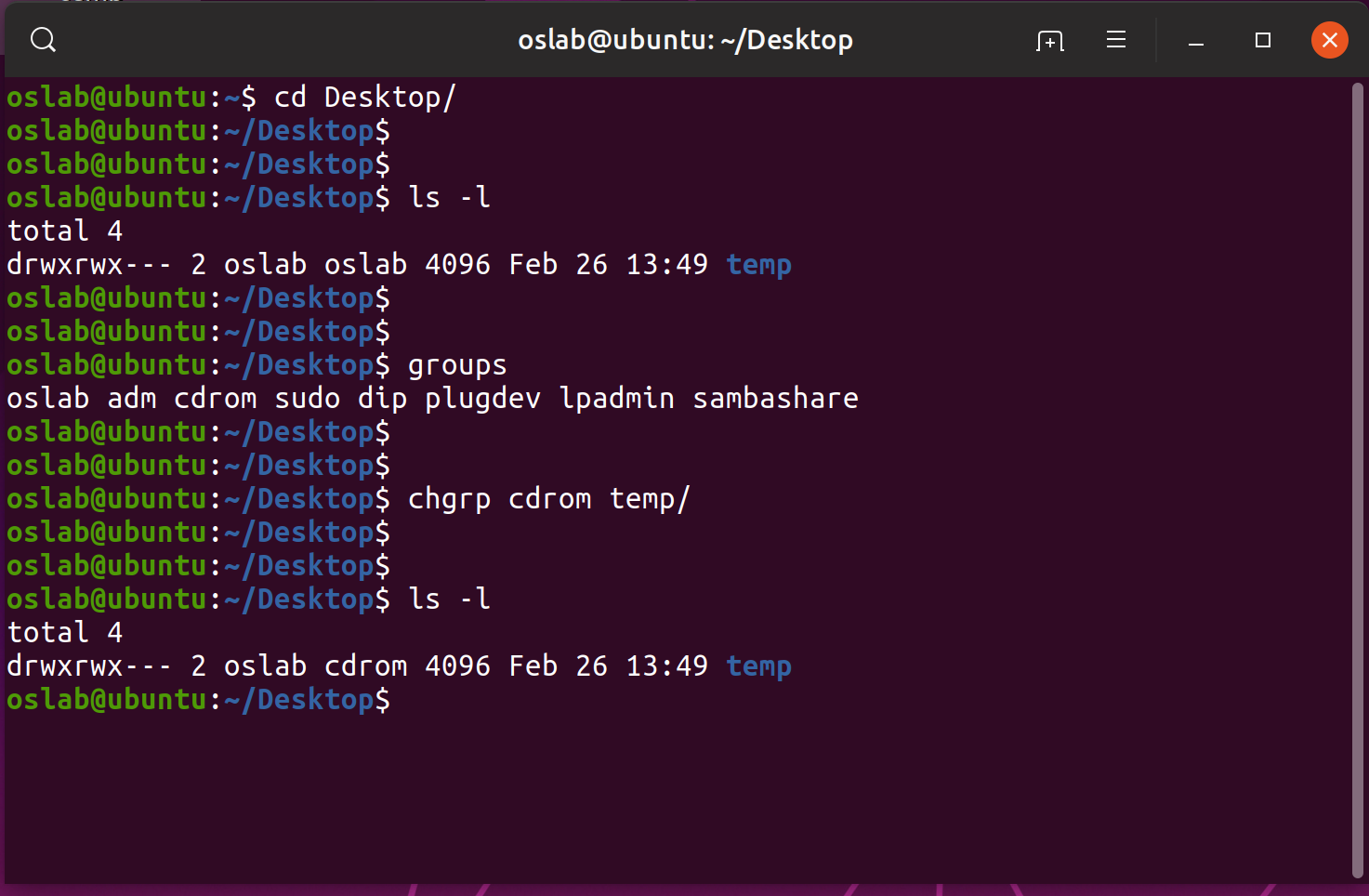
1. chgrp [groupname] [foldername]

با صدور این دستورات می توانید گروهی از فایل ها و دایرکتوری ها را در لینوکس تغییر دهید:

* **chgrp groupname filename**
* **chgrp groupname foldername**

توجه داشته باشید که قبل از اینکه بتوانید گروه‌ها را به فایل ها و دایرکتوری ها اختصاص دهید، گروه باید خارج شود.

بنابر این با کمک دستور chgrp cdrom temp گروه cdrom را به دایرکتوری ساخته شده در بخش 1 به پوشه اضافه می‌شود. همچنین در نهایت با کمک ls -l صحت عملکرد را چک می‌کنیم. (شکل 2-2)



شکل 2-2

**این دستور چه کاري انجام میدهد ؟**

**chmod 4664 file.txt**

همانطور که در بخش اول توضیح داده شد chmod دسترسی اعطا می‌کند یا می‌گیرد. پس در مرحله اول متوجه می‌شویم دسترسی file.txt عوض می‌شود.

همانطور که در بخش اول گفته شد 6 جمع 2 و 4 که همان read و write هستند می‌باشند. همچنین 4 به تنهایی مفهوم read را دارد. پس 664 به group و user دسترسی خواندن و نوشتن و به other دسترسی خواندن را اعطا می‌کند.

رغم اول چطور؟ رقم 4 كه در سمت چپ 4464 آمده نشان دهنده ى يكSpecial Permission می‌باشد که در این جا عدد 4، بیت دسترسی SUID را به فايل مورد نظر مى‌دهد و تنها بر روی فایل هایی با قابلیت execute (x) تاثیر دارد.

در واقع اگر بر روی یک فایل با قابلیت execute تنظیم شود زمانى كه آن فایل را اجرا می كنيم، آن فایل به جای آنکه با دسترسی فرد اجرا کننده فایل اجرا شود با دسترسی صاحب فایل اجرا می‌شود.

برای اطلاعات بیشتر از سطح‌های دسترسی خاص:

# Special privileges of Linux: SUID SGID and SBIT

Time：2019-8-5

**1、**[**SUID**](https://developpaper.com/tag/suid/)The important role is to allow other users to have the privileges of the program owner when executing the program with SUID.

A direct example is the passwd command: [root@localhost www] ll/usr/bin/passwd

– rwsr-xr-x 1 root 31736 August 22, 2010/usr/bin/passwd

Passwd has the right to execute only root, but it grants SUID privileges and other users temporarily have the right to root when they execute.

**2、**[**SGID**](https://developpaper.com/tag/sgid/)To use directories so that programs under directories temporarily gain ownership when they execute: [root@localhost www] ll/usr/bin/locate

– rwx-s-x 1 root s locate 38464 August 24, 2010/usr/bin/locate

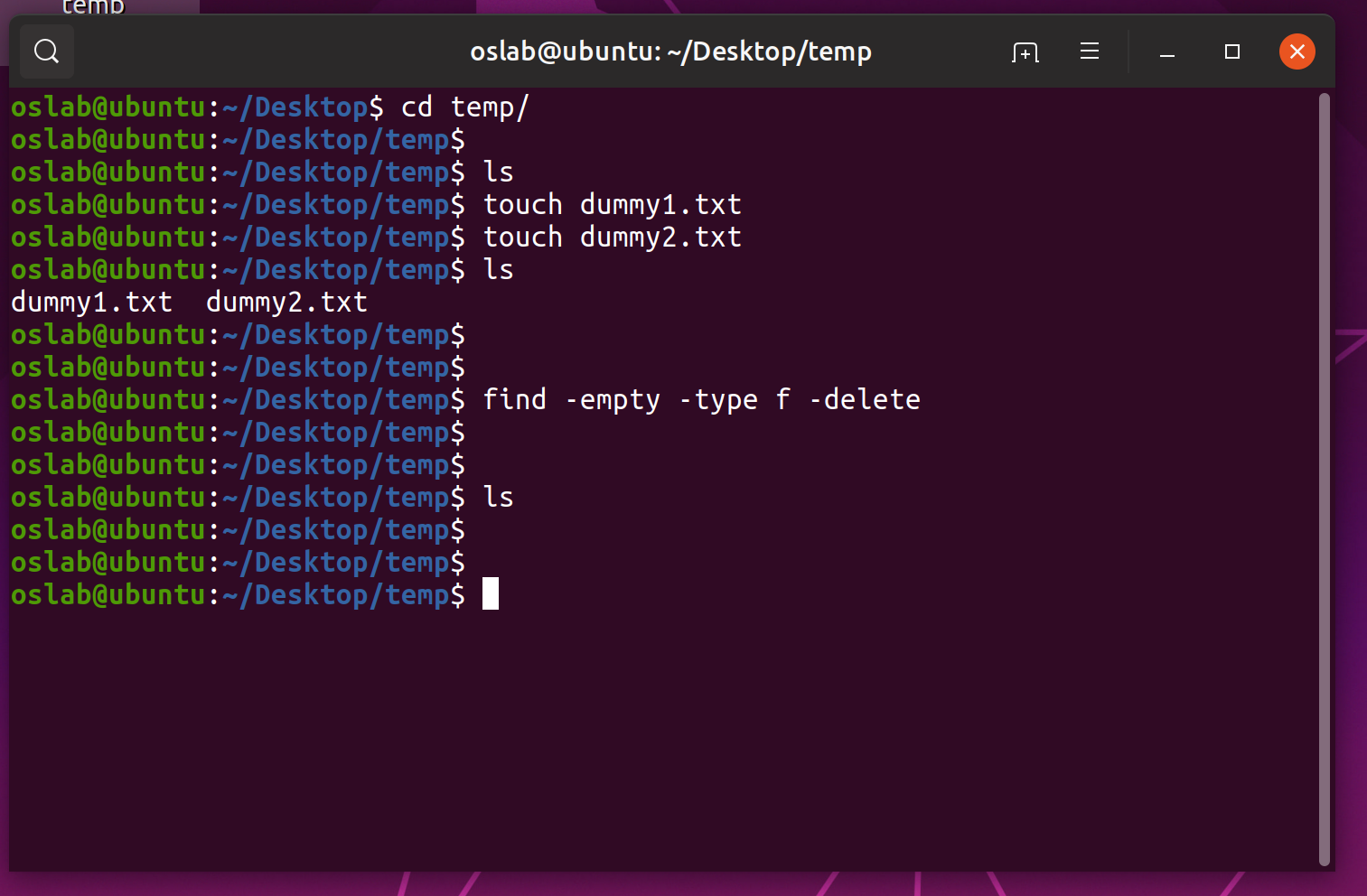
**3、**[**SBIT**](https://developpaper.com/tag/sbit/)For directory use, files in this directory can only be deleted by themselves and root: [root@localhost www] ll/ | grep “tmp”

Drwxrwxrwt. 6 root 4096 November 18 15:38 TMP

**درون کل دایرکتوري هاي موجود، فایلهاي خالی را پیدا کرده و پاك کنید (اینکار باید در یک خط دستور انجام شود).**

1. Find -empty -type f -delete

در دایرکتوری temp مقداری فایل خالی به اصطلاح dummy درست کردیم. در نهایت به کمک دستور بالا آنها را پاک کردیم. برای صحت از عملیات با کمک ls تمامی فایل‌های دایرکتوری را لیست کردیم. (شکل 4-1)



شکل 4-1