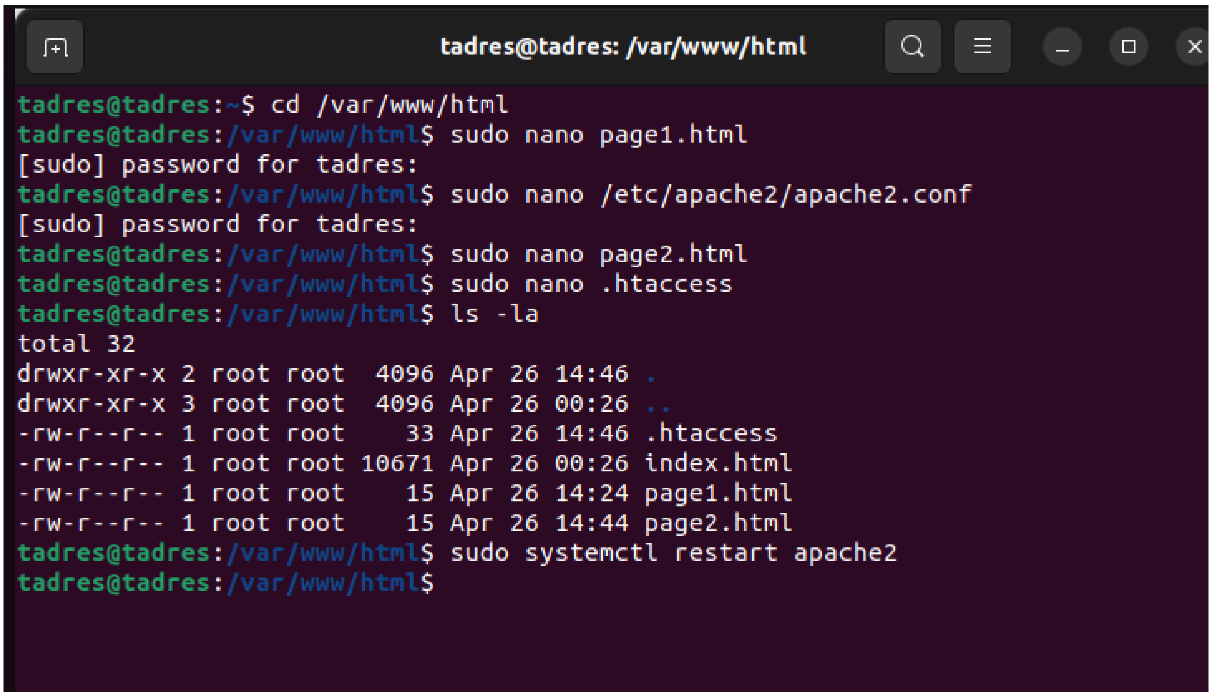
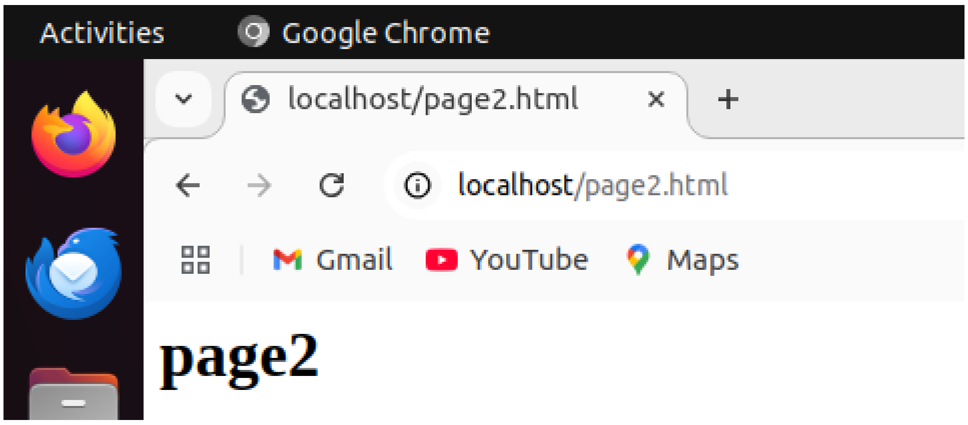
apache_lab1

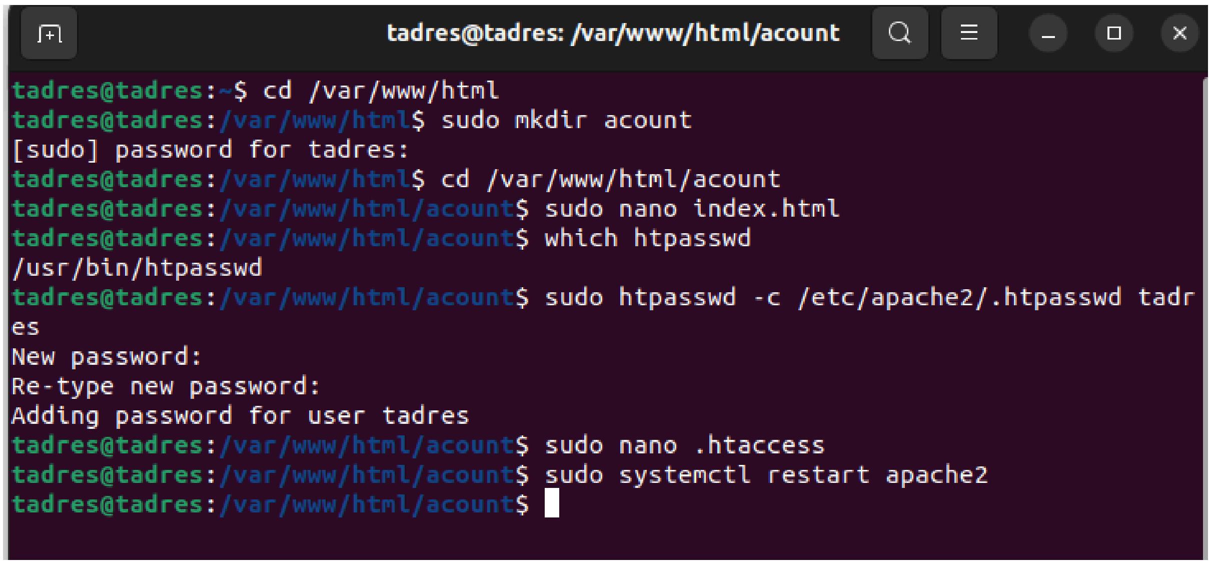
2-Create two simple html pages named “page1.html, page2.html” then use the suitable
directive to automatically redirect from localhost/page1.html to localhost/page2.html.



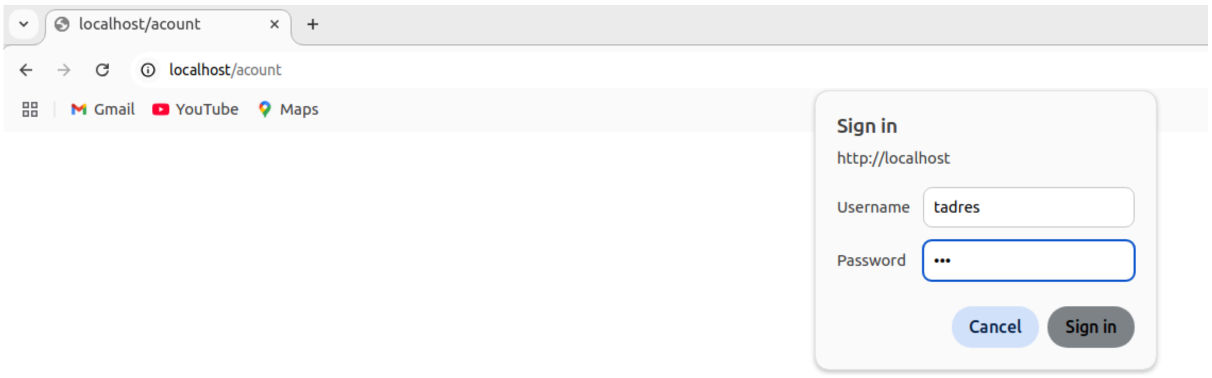
```
tadres@tadres:~$ cd /var/www/html
tadres@tadres:/var/www/html$ sudo nano page1.html
[sudo] password for tadres:
tadres@tadres:/var/www/html$ sudo nano /etc/apache2/apache2.conf
[sudo] password for tadres:
tadres@tadres:/var/www/html$ sudo nano page2.html
tadres@tadres:/var/www/html$ sudo nano .htaccess
tadres@tadres:/var/www/html$ ls -la
total 32
drwxr-xr-x 2 root root  4096 Apr 26 14:46 .
drwxr-xr-x 3 root root  4096 Apr 26 00:26 ..
-rw-r--r-- 1 root root    33 Apr 26 14:46 .htaccess
-rw-r--r-- 1 root root 10671 Apr 26 00:26 index.html
-rw-r--r-- 1 root root    15 Apr 26 14:24 page1.html
-rw-r--r-- 1 root root    15 Apr 26 14:44 page2.html
tadres@tadres:/var/www/html$ sudo systemctl restart apache2
tadres@tadres:/var/www/html$
```



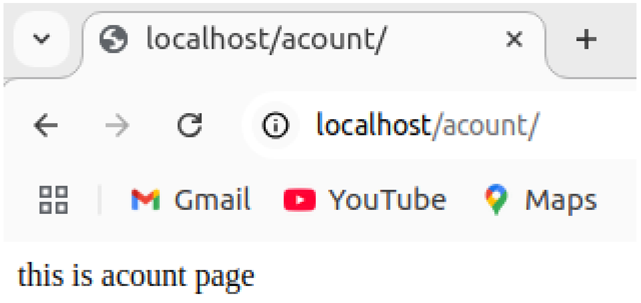
3-Ask for user name and password when accessing a directory.



```
tadres@tadres:~$ cd /var/www/html
tadres@tadres:/var/www/html$ sudo mkdir acount
[sudo] password for tadres:
tadres@tadres:/var/www/html$ cd /var/www/html/acount
tadres@tadres:/var/www/html/acount$ sudo nano index.html
tadres@tadres:/var/www/html/acount$ which htpasswd
/usr/bin/htpasswd
tadres@tadres:/var/www/html/acount$ sudo htpasswd -c /etc/apache2/.htpasswd tadr
es
New password:
Re-type new password:
Adding password for user tadres
tadres@tadres:/var/www/html/acount$ sudo nano .htaccess
tadres@tadres:/var/www/html/acount$ sudo systemctl restart apache2
tadres@tadres:/var/www/html/acount$
```

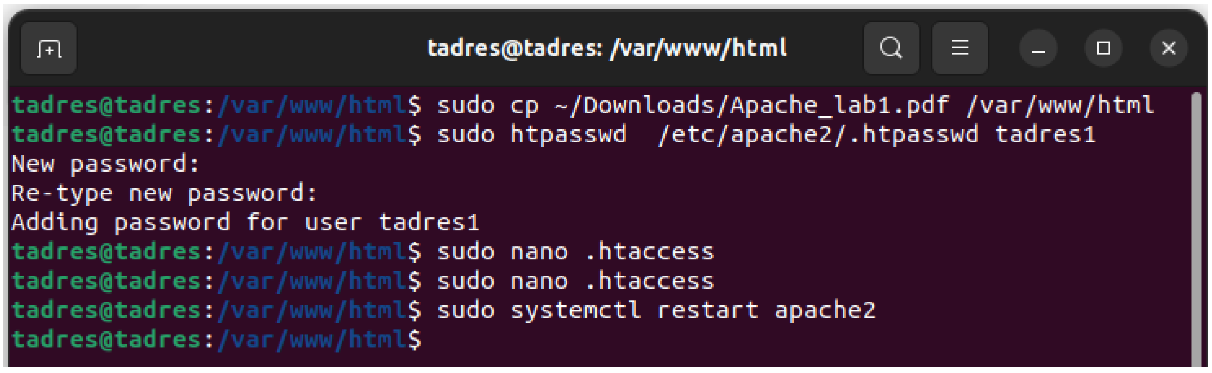


Sign in
http://localhost
Username: tadres
Password: •••

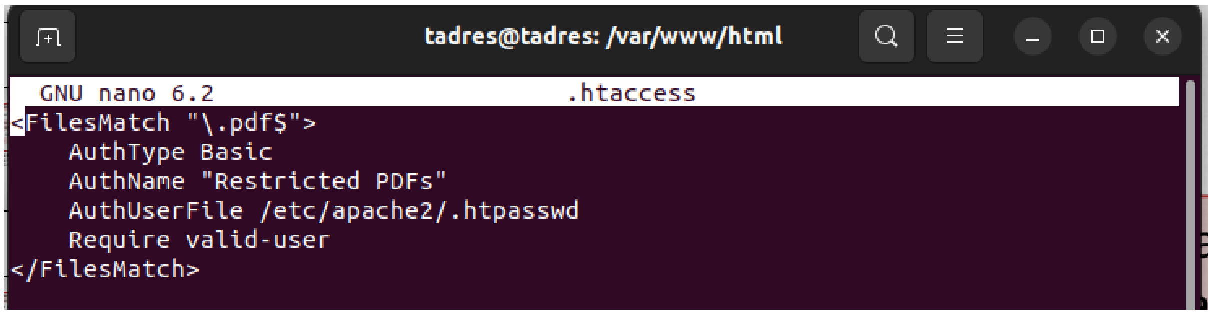


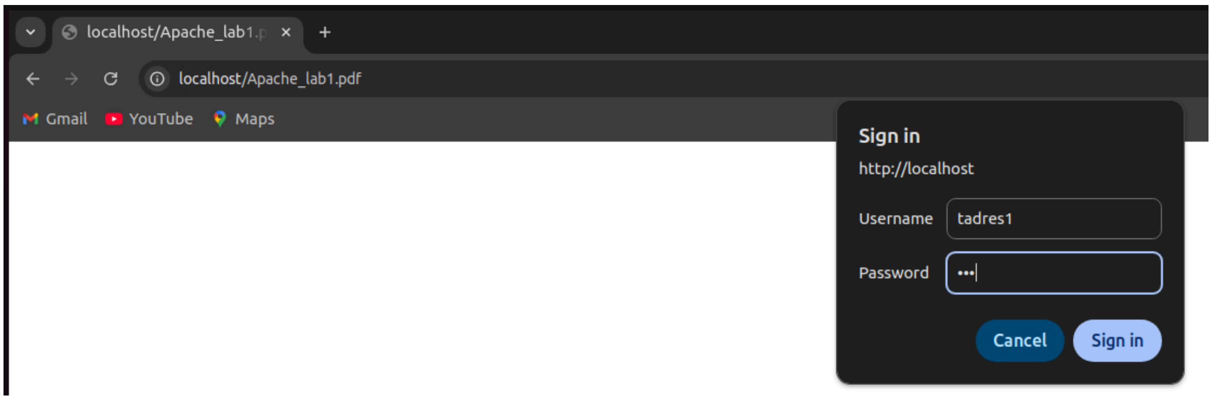
this is acount page

4-Apply authentication before downloading PDF files.

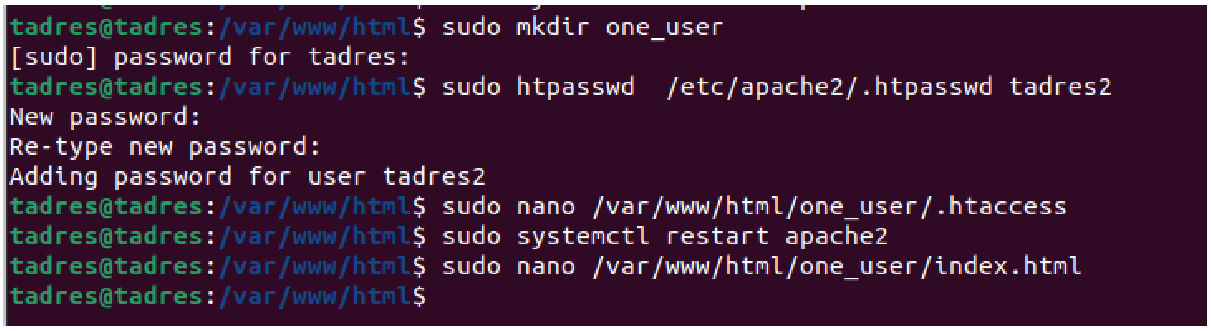


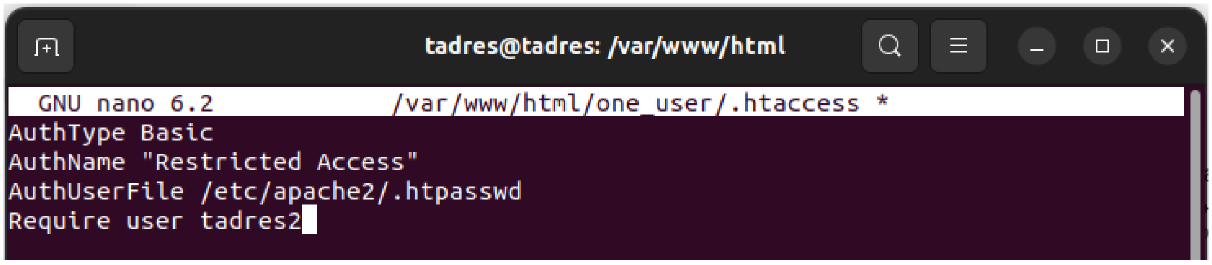
```
tadres@tadres:/var/www/html$ sudo cp ~/Downloads/Apache_lab1.pdf /var/www/html
tadres@tadres:/var/www/html$ sudo htpasswd  /etc/apache2/.htpasswd tadres1
New password:
Re-type new password:
Adding password for user tadres1
tadres@tadres:/var/www/html$ sudo nano .htaccess
tadres@tadres:/var/www/html$ sudo nano .htaccess
tadres@tadres:/var/www/html$ sudo systemctl restart apache2
tadres@tadres:/var/www/html$
```

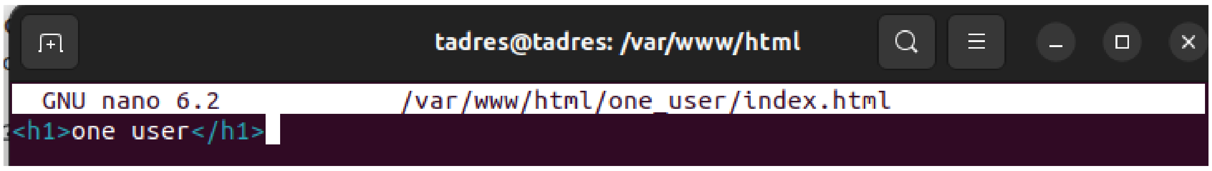

```
  GNU nano 6.2                          .htaccess
<FilesMatch "\.pdf$">
    AuthType Basic
    AuthName "Restricted PDFs"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
</FilesMatch>
```

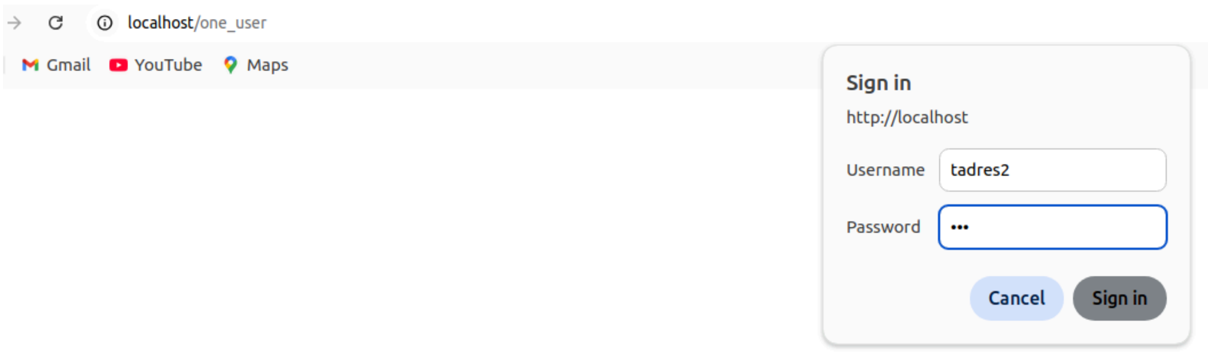

Sign in
http://localhost
Username: tadres1
Password: •••

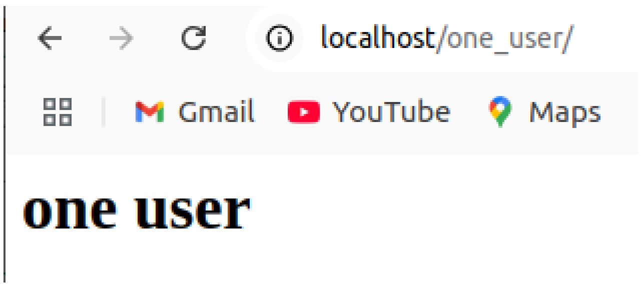
5-Create a directory then allow access to one of your classmates only.


```
tadres@tadres:/var/www/html$ sudo mkdir one_user
[sudo] password for tadres:
tadres@tadres:/var/www/html$ sudo htpasswd  /etc/apache2/.htpasswd tadres2
New password:
Re-type new password:
Adding password for user tadres2
tadres@tadres:/var/www/html$ sudo nano /var/www/html/one_user/.htaccess
tadres@tadres:/var/www/html$ sudo systemctl restart apache2
tadres@tadres:/var/www/html$ sudo nano /var/www/html/one_user/index.html
tadres@tadres:/var/www/html$
```


```
  GNU nano 6.2                /var/www/html/one_user/.htaccess *
AuthType Basic
AuthName "Restricted Access"
AuthUserFile /etc/apache2/.htpasswd
Require user tadres2
```

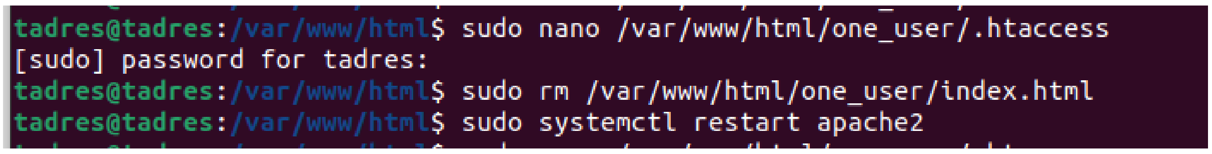

```
  GNU nano 6.2                /var/www/html/one_user/index.html
<h1>one user</h1>
```



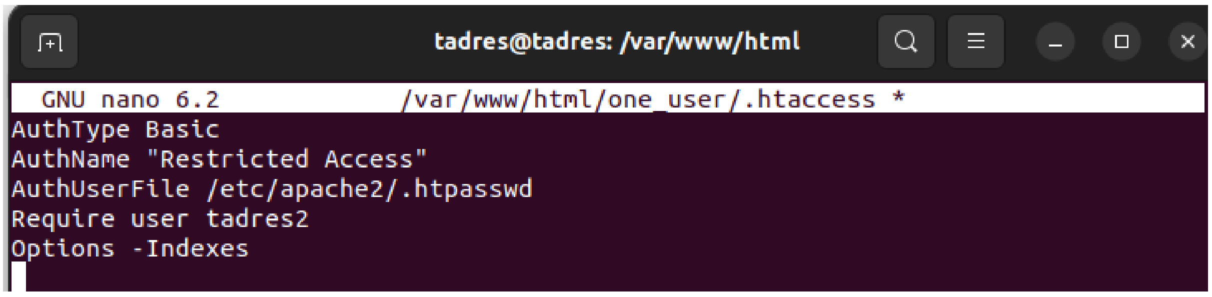


one user

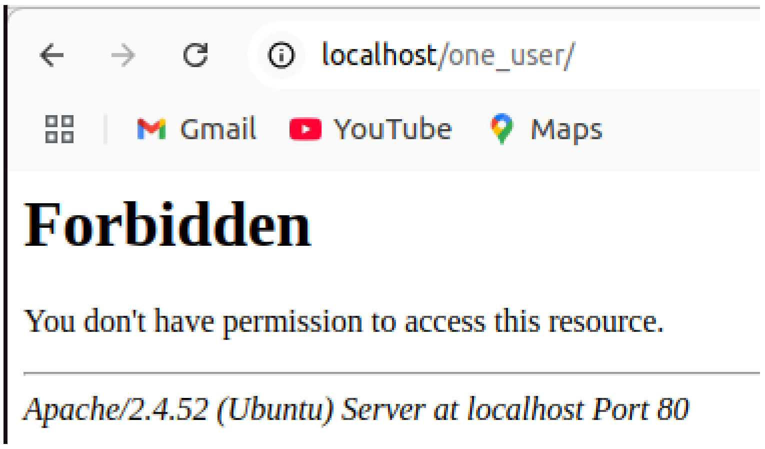
6-Disable listing the directory content (hint use indexs).



```
tadres@tadres:/var/www/html$ sudo nano /var/www/html/one_user/.htaccess
[sudo] password for tadres:
tadres@tadres:/var/www/html$ sudo rm /var/www/html/one_user/index.html
tadres@tadres:/var/www/html$ sudo systemctl restart apache2
```



```
  GNU nano 6.2             /var/www/html/one_user/.htaccess *
AuthType Basic
AuthName "Restricted Access"
AuthUserFile /etc/apache2/.htpasswd
Require user tadres2
Options -Indexes
```

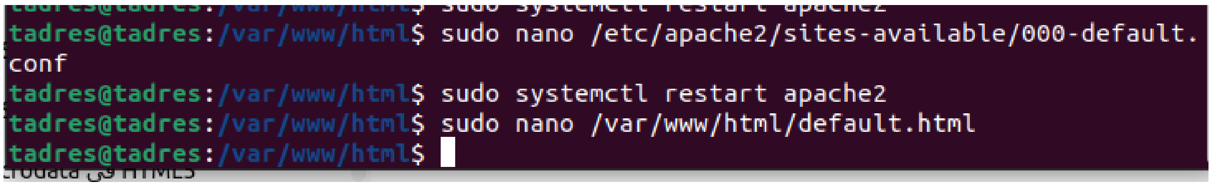


Forbidden

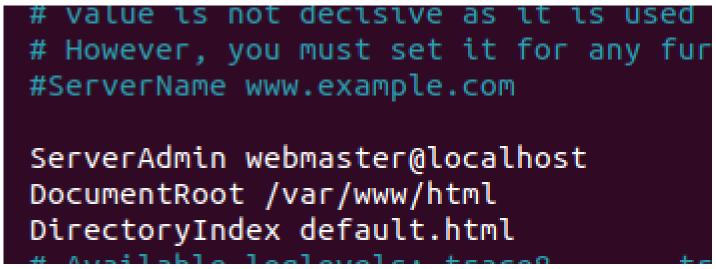
You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at localhost Port 80

7-Change the default index page to be default.html instead of index.html (use DirectoryIndex)

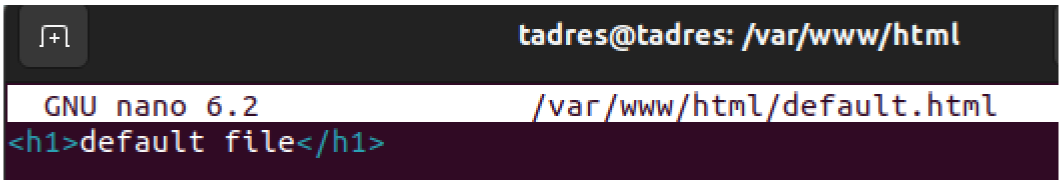


```
tadres@tadres:/var/www/html$ sudo nano /etc/apache2/sites-available/000-default.
conf
tadres@tadres:/var/www/html$ sudo systemctl restart apache2
tadres@tadres:/var/www/html$ sudo nano /var/www/html/default.html
tadres@tadres:/var/www/html$ 
```

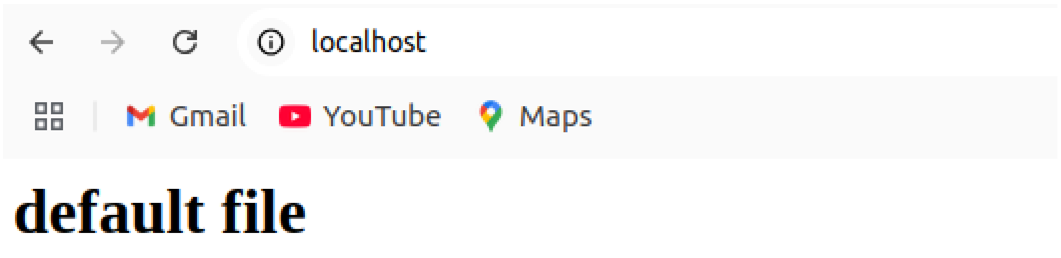


```
 # value is not decisive as it is used
 # However, you must set it for any fur
 #ServerName www.example.com

 ServerAdmin webmaster@localhost
 DocumentRoot /var/www/html
 DirectoryIndex default.html
```

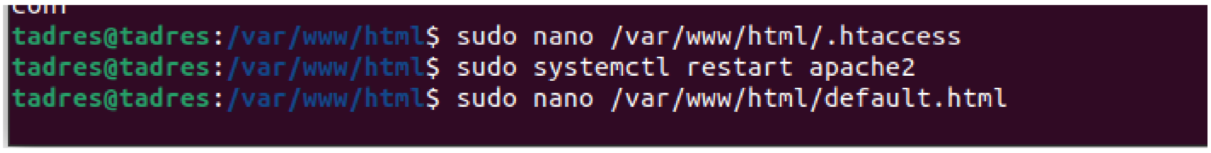


```
tadres@tadres: /var/www/html
  GNU nano 6.2                   /var/www/html/default.html
<h1>default file</h1>
```

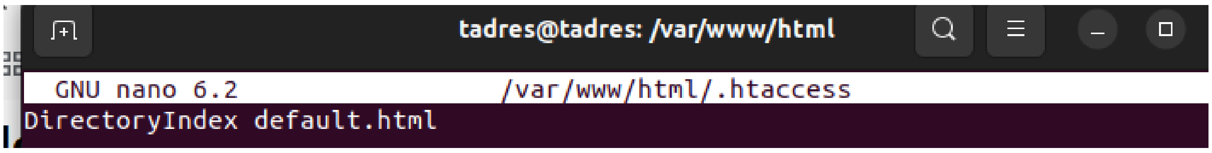


default file

another solve:

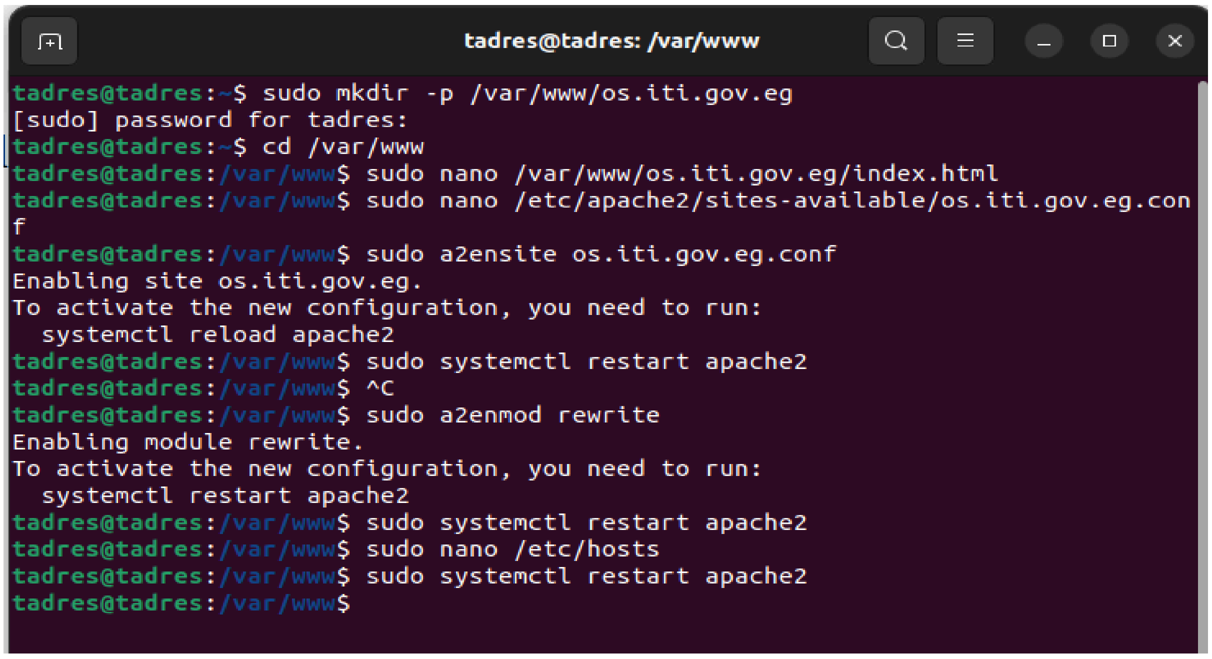


```
tadres@tadres:/var/www/html$ sudo nano /var/www/html/.htaccess
tadres@tadres:/var/www/html$ sudo systemctl restart apache2
tadres@tadres:/var/www/html$ sudo nano /var/www/html/default.html
```

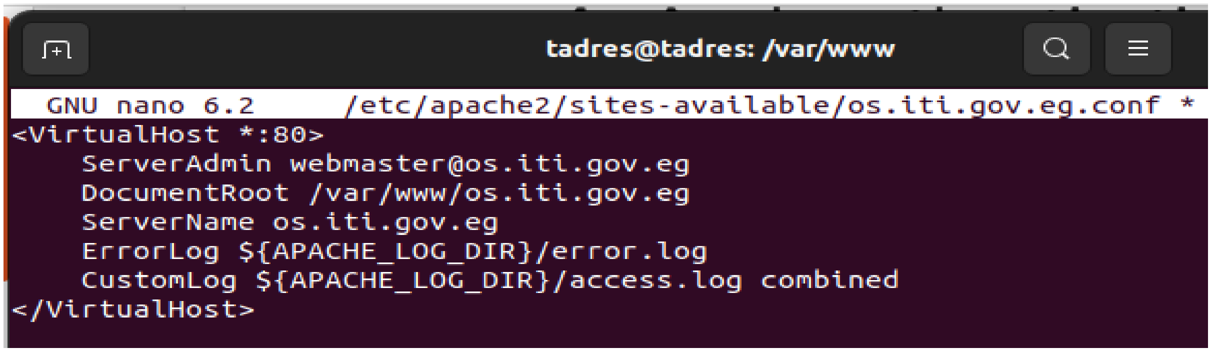


```
tadres@tadres: /var/www/html
  GNU nano 6.2                /var/www/html/.htaccess
DirectoryIndex default.html
```

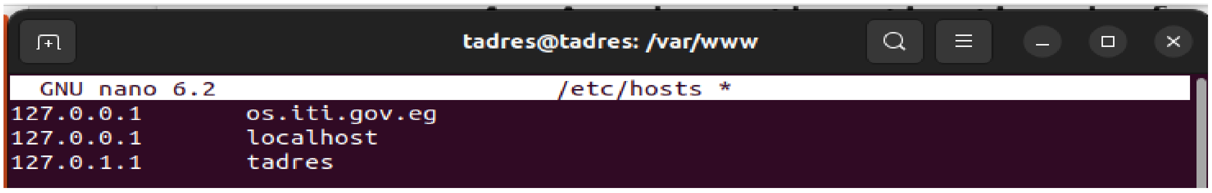
8-Create virtualhost for os.iti.gov.eg website



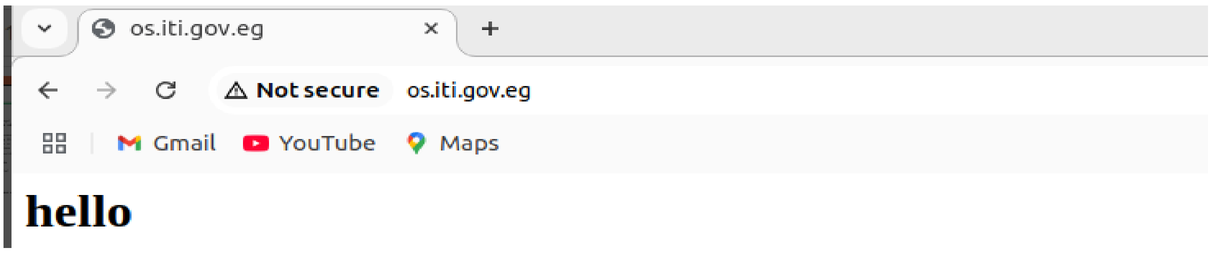
```
tadres@tadres:~$ sudo mkdir -p /var/www/os.iti.gov.eg
[sudo] password for tadres:
tadres@tadres:~$ cd /var/www
tadres@tadres:/var/www$ sudo nano /var/www/os.iti.gov.eg/index.html
tadres@tadres:/var/www$ sudo nano /etc/apache2/sites-available/os.iti.gov.eg.con
f
tadres@tadres:/var/www$ sudo a2ensite os.iti.gov.eg.conf
Enabling site os.iti.gov.eg.
To activate the new configuration, you need to run:
  systemctl reload apache2
tadres@tadres:/var/www$ sudo systemctl restart apache2
tadres@tadres:/var/www$ ^C
tadres@tadres:/var/www$ sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
tadres@tadres:/var/www$ sudo systemctl restart apache2
tadres@tadres:/var/www$ sudo nano /etc/hosts
tadres@tadres:/var/www$ sudo systemctl restart apache2
tadres@tadres:/var/www$
```



```
  GNU nano 6.2      /etc/apache2/sites-available/os.iti.gov.eg.conf *
<VirtualHost *:80>
    ServerAdmin webmaster@os.iti.gov.eg
    DocumentRoot /var/www/os.iti.gov.eg
    ServerName os.iti.gov.eg
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

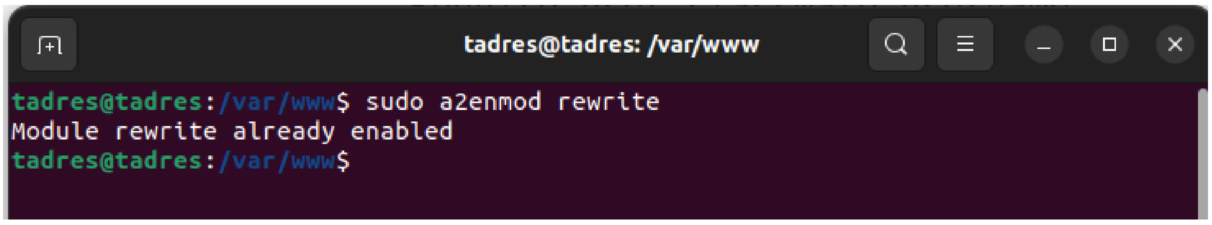


```
  GNU nano 6.2                              /etc/hosts *
127.0.0.1         os.iti.gov.eg
127.0.0.1         localhost
127.0.1.1         tadres
```



hello

9-Enable rewrite module



```
tadres@tadres:/var/www$ sudo a2enmod rewrite
Module rewrite already enabled
tadres@tadres:/var/www$
```

10-What is the importance of rewrite module?

The Importance of the Rewrite Module in Apache (mod_rewrite)
The Rewrite Module (mod_rewrite) in Apache is a powerful tool for URL manipulation and redirection. It allows servers to rewrite requested URLs on the fly, improving SEO, security, and user experience.

Key Benefits:
SEO-Friendly URLs: Converts dynamic URLs (e.g., ?id=123) into clean, readable paths (e.g., /products/123).

Redirection & Routing: Redirects old URLs to new ones (301/302) and manages internal URL routing.

Security: Blocks malicious requests, hides file extensions, and preventshotlinking.

Flexibility: Works with conditions (RewriteCond) and rules (RewriteRule) for complex URL handling.

Backward Compatibility: Ensures old links still work after website restructuring.

Example Use Cases:
Redirecting HTTP to HTTPS.

Making URLs user-friendly (/blog/post-title instead of /blog.php?id=42).

Preventing access to sensitive files.

Since it operates at the server level, mod_rewrite is efficient and widely used in modern web development.