# Project 1 User-Level System Call Hook Report

312706038 資管所 吳方庭

## #Task 1

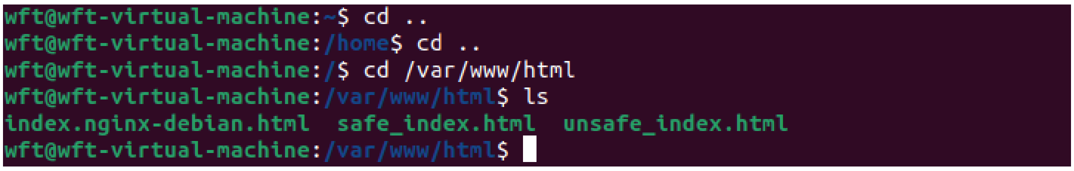
a. Task 1.1 Permission access - Setting up Nginx

- 安裝 Nginx

```
$ sudo apt update
$ sudo apt install nginx
$ sudo apt install apparmor-easyprof apparmor-notify apparmor-utils certspotter
```

- 將文件移動到根目錄

```
$ sudo mv safe_index.html /var/www/html/
$ sudo mv unsafe_index.html /var/www/html/
```



```
wft@wft-virtual-machine:~$ cd ..
wft@wft-virtual-machine:/home$ cd ..
wft@wft-virtual-machine:/$ cd /var/www/html
wft@wft-virtual-machine:/var/www/html$ ls
index.nginx-debian.html  safe_index.html  unsafe_index.html
wft@wft-virtual-machine:/var/www/html$ 
```

b. Task 1.2 Permission access - Creating AppArmor profile

- 創建設定檔

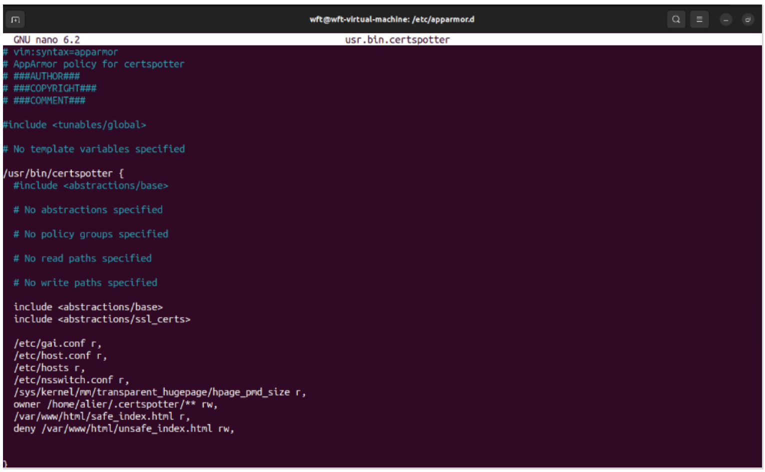
```
$ aa-easyprof /usr/bin/certspotter
$ aa-easyprof /usr/bin/certspotter > usr.bin.certspotter
$ sudo mv usr.bin.certspotter /etc/apparmor.d
```

- 進行規範設定

```
$ sudo nginx
$ sudo aa-logprof
```

- 在/etc/apparmor.d/usr.bin.certspotter 中加入以下設定

```
/var/www/html/safe_index.html r,
deny /var/www/html_unsafe.html rw,
```

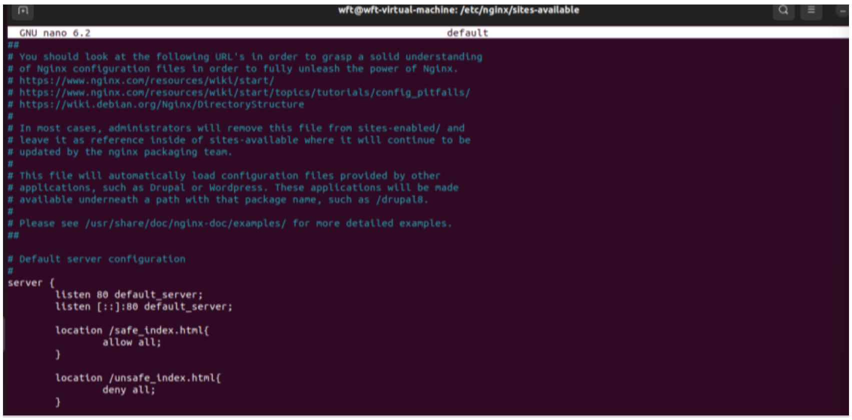


```
  GNU nano 6.2                                   usr.bin.certspotter
# vim:syntax=apparmor
# AppArmor policy for certspotter
# ###AUTHOR###
# ###COPYRIGHT###
# ###COMMENT###

#include <tunables/global>

# No template variables specified

/usr/bin/certspotter {
  #include <abstractions/base>

  # No abstractions specified

  # No policy groups specified

  # No read paths specified

  # No write paths specified

  include <abstractions/base>
  include <abstractions/ssl_certs>

  /etc/gai.conf r,
  /etc/host.conf r,
  /etc/hosts r,
  /etc/nsswitch.conf r,
  /sys/kernel/mm/transparent_hugepage/hpage_pmd_size r,
  owner /home/alier/.certspotter/** rw,
  /var/www/html/safe_index.html r,
  deny /var/www/html/unsafe_index.html rw,


}
```

- 將設定重新載入核心

```
$ sudo apparmor_parser -r /etc/apparmor.d/usr.bin.certspotter
```

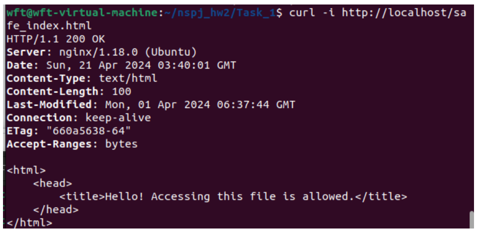
- 在/etc/nginx/sites-availbale/default 中加入兩個位置進行存取限制



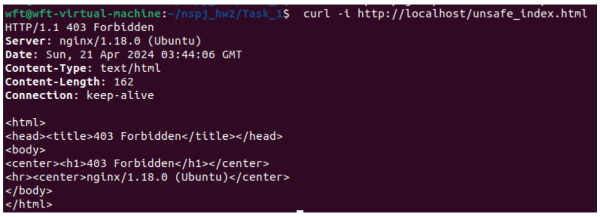
```
wft@wft-virtual-machine: /etc/nginx/sites-available
 GNU nano 6.2                                    default
##
# You should look at the following URL's in order to grasp a solid understanding
# of Nginx configuration files in order to fully unleash the power of Nginx.
# https://www.nginx.com/resources/wiki/start/
# https://www.nginx.com/resources/wiki/start/topics/tutorials/config_pitfalls/
# https://wiki.debian.org/Nginx/DirectoryStructure
#
# In most cases, administrators will remove this file from sites-enabled/ and
# leave it as reference inside of sites-available where it will continue to be
# updated by the nginx packaging team.
#
# This file will automatically load configuration files provided by other
# applications, such as Drupal or Wordpress. These applications will be made
# available underneath a path with that package name, such as /drupal8.
#
# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.
##

# Default server configuration
#
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        location /safe_index.html{
                allow all;
        }

        location /unsafe_index.html{
                deny all;
        }
```

- 重啟 nginx `$ sudo systemctl restart nginx`
- 測試結果

```
$ curl -i http://localhost/safe_index.html
$ curl -i http://localhost/unsafe_index.html
```



```
wft@wft-virtual-machine:~/nspj_hw2/Task_1$ curl -i http://localhost/sa
fe_index.html
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 21 Apr 2024 03:40:01 GMT
Content-Type: text/html
Content-Length: 100
Last-Modified: Mon, 01 Apr 2024 06:37:44 GMT
Connection: keep-alive
ETag: "660a5638-64"
Accept-Ranges: bytes

<html>
    <head>
        <title>Hello! Accessing this file is allowed.</title>
    </head>
</html>
```



```
wft@wft-virtual-machine:~/nspj_hw2/Task_1$  curl -i http://localhost/unsafe_index.html
HTTP/1.1 403 Forbidden
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 21 Apr 2024 03:44:06 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive

<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
```

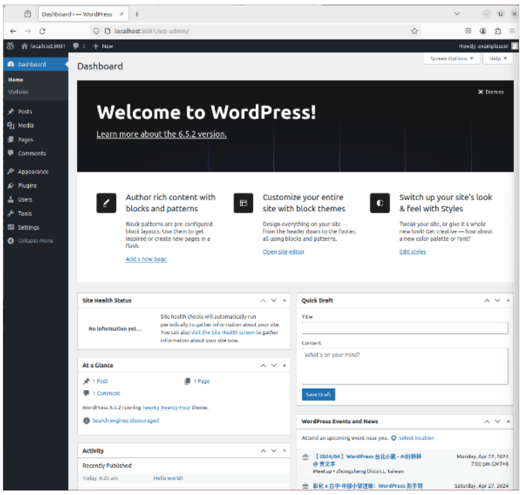
## #Task 2

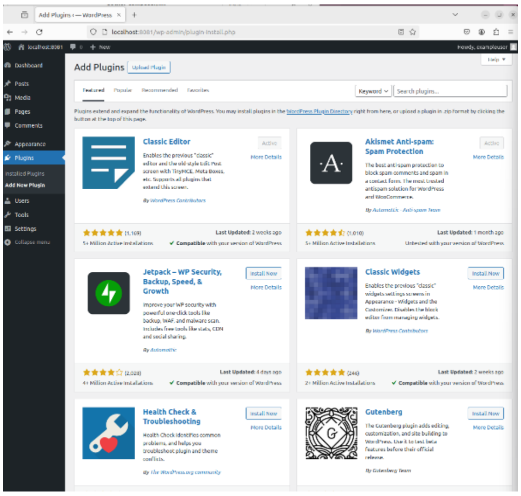
c. Task 2.1 Restrict a Container's Access to Resources - Setting up the container

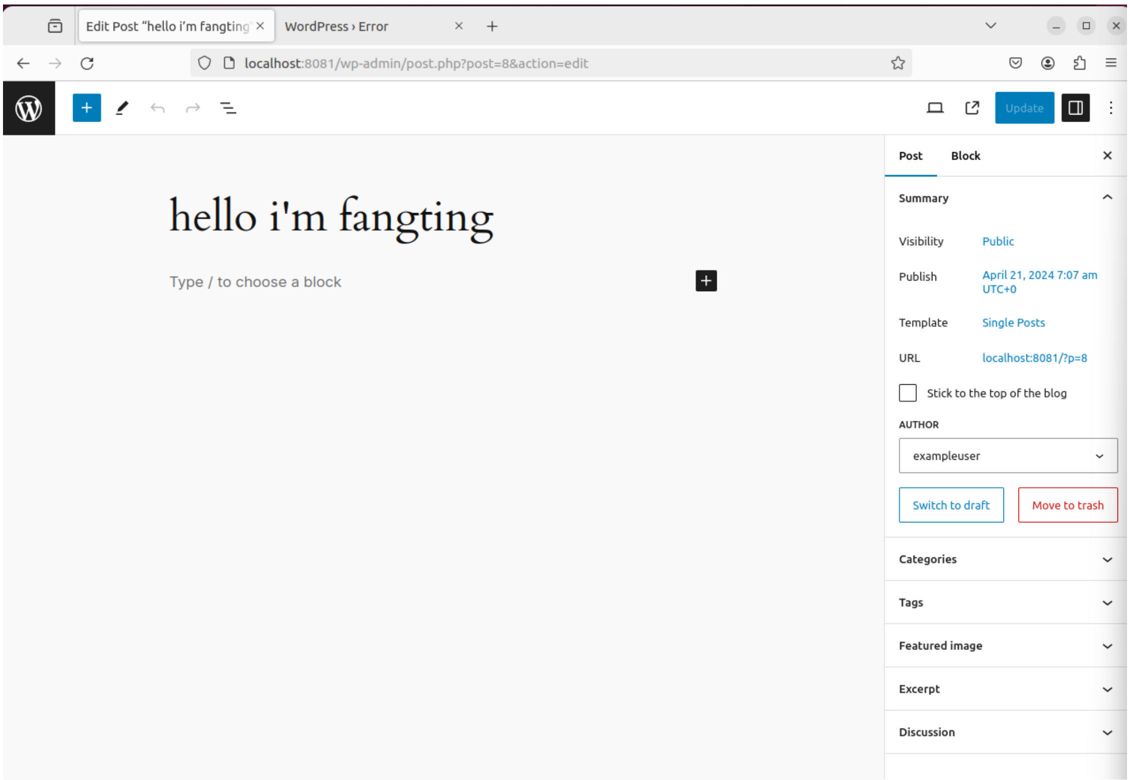
- 進入 Task_2 資料夾位置

```
$sudo apt-get update && apt-get install docker-compose
$sudo docker build -t nspj:latest .
$sudo docker-compose up
```

- ➢ 進入 localhost:8081 登入帳號，額外 Plugin Classic Editor 和 Akismet Anti-spam 及張貼一個新的文章。


Dashboard
Welcome to WordPress!
Learn more about the 6.5.2 version.
Author rich content with blocks and patterns
Customize your entire site with block themes
Switch up your site's look & feel with Styles
Site Health Status
Quick Draft
At a Glance
WordPress Events and News
Activity





localhost:8081/wp-admin/post.php?post=8&action=edit

hello i'm fangting

Type / to choose a block

Summary

Visibility Public

Publish April 21, 2024 7:07 am UTC+0

Template Single Posts

URL localhost:8081/?p=8

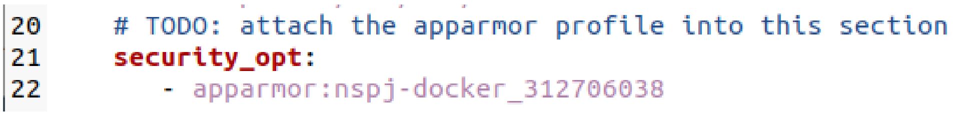
□ Stick to the top of the blog

AUTHOR

exampleuser

d. Task 2.2 Restrict a Container's Access to Resources - Creating AppArmor profile

- ➢ 在 apparmor.d 文件夾中創建 nspj-docker_312706038，並加入在 docker-compose.yml 中的 security_opt 項目中



```
    # TODO: attach the apparmor profile into this section
    security_opt:
        - apparmor:nspj-docker_312706038
```

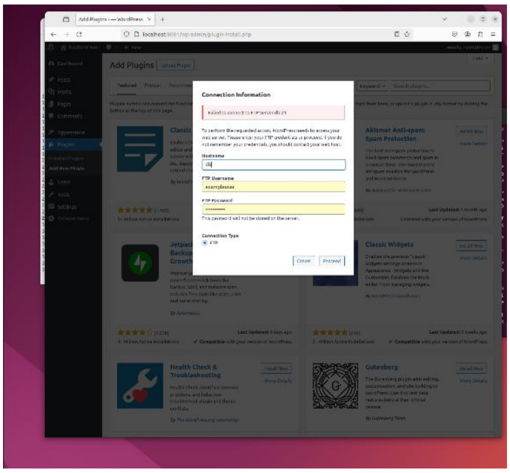
- ➢ 完成 nspj-docker_312706038 基本配置

$ sudo systemctl restart docker

$ sudo docker-compose up

$ sudo aa-logprof

- ➢ 修改 nspj-docker_312706038 配置內容，使在安裝 plugins 時連接 FTP 失敗，以及無法修改張貼內容。



Connection Information

Failed to connect to FTP Server db:21

To perform the requested action, WordPress needs to access your web server. Please enter your FTP credentials to proceed. If you do not remember your credentials, you should contact your web host.

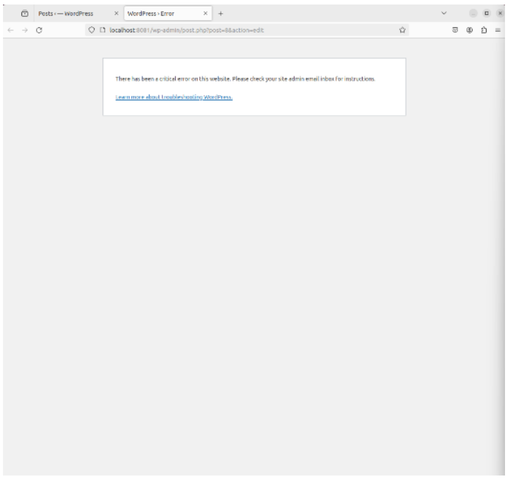
Hostname: db

FTP Username: exampleuser

FTP Password: ••••••••••••

This password will not be stored on the server.

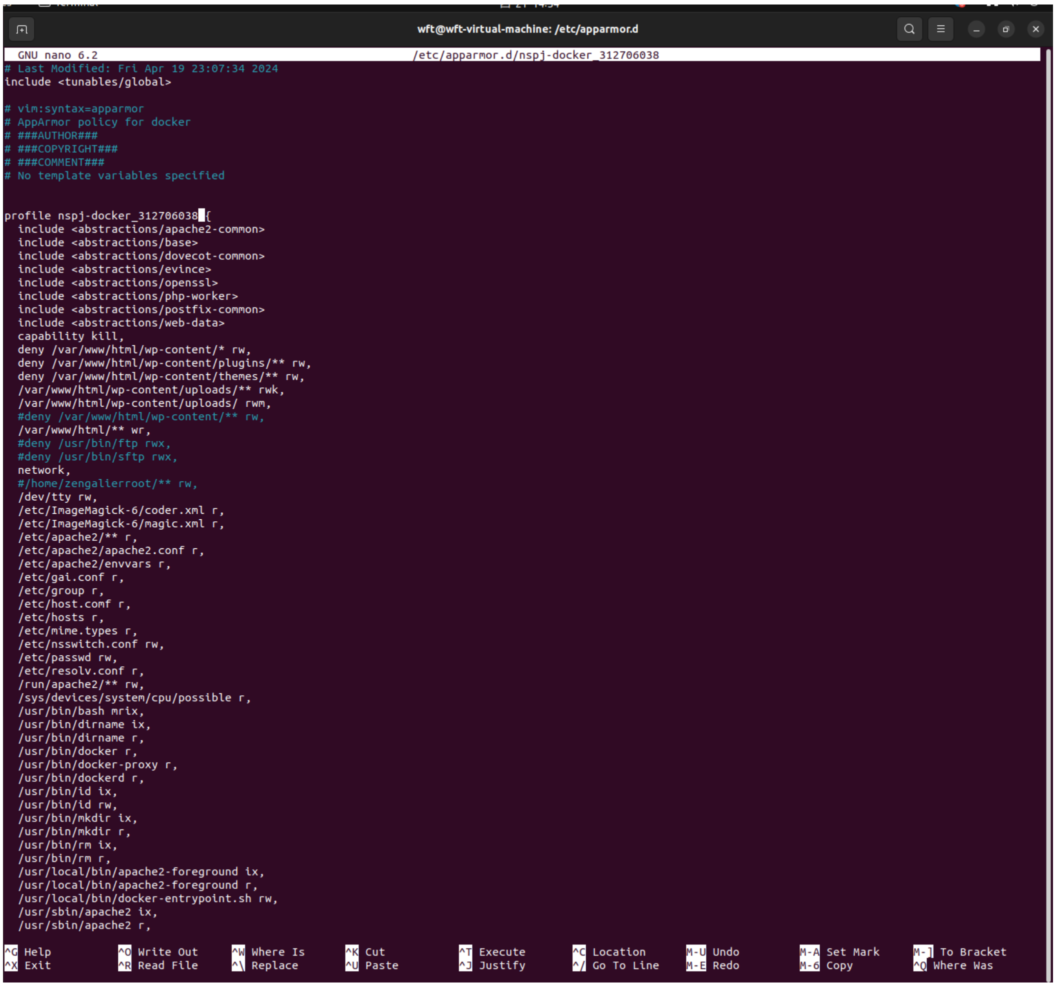
Connection Type
● FTP



localhost:8081/wp-admin/post.php?post=8&action=edit

There has been a critical error on this website. Please check your site admin email inbox for instructions.

Learn more about troubleshooting WordPress.



```
  GNU nano 6.2                     /etc/apparmor.d/nspj-docker_312706038
# Last Modified: Fri Apr 19 23:07:34 2024
include <tunables/global>

# vim:syntax=apparmor
# AppArmor policy for docker
# ###AUTHOR###
# ###COPYRIGHT###
# ###COMMENT###
# No template variables specified


profile nspj-docker_312706038 {
  include <abstractions/apache2-common>
  include <abstractions/base>
  include <abstractions/dovecot-common>
  include <abstractions/evince>
  include <abstractions/openssl>
  include <abstractions/php-worker>
  include <abstractions/postfix-common>
  include <abstractions/web-data>
  capability kill,
  deny /var/www/html/wp-content/* rw,
  deny /var/www/html/wp-content/plugins/** rw,
  deny /var/www/html/wp-content/themes/** rw,
  /var/www/html/wp-content/uploads/** rwk,
  /var/www/html/wp-content/uploads/ rwm,
  #deny /var/www/html/wp-content/** rw,
  /var/www/html/** wr,
  #deny /usr/bin/ftp rwx,
  #deny /usr/bin/sftp rwx,
  network,
  #/home/zengalierroot/** rw,
  /dev/tty rw,
  /etc/ImageMagick-6/coder.xml r,
  /etc/ImageMagick-6/magic.xml r,
  /etc/apache2/** r,
  /etc/apache2/apache2.conf r,
  /etc/apache2/envvars r,
  /etc/gai.conf r,
  /etc/group r,
  /etc/host.conf r,
  /etc/hosts r,
  /etc/mime.types r,
  /etc/nsswitch.conf rw,
  /etc/passwd rw,
  /etc/resolv.conf r,
  /run/apache2/** rw,
  /sys/devices/system/cpu/possible r,
  /usr/bin/bash mrix,
  /usr/bin/dirname ix,
  /usr/bin/dirname r,
  /usr/bin/docker r,
  /usr/bin/docker-proxy r,
  /usr/bin/dockerd r,
  /usr/bin/id ix,
  /usr/bin/id rw,
  /usr/bin/mkdir ix,
  /usr/bin/mkdir r,
  /usr/bin/rm ix,
  /usr/bin/rm r,
  /usr/local/bin/apache2-foreground ix,
  /usr/local/bin/apache2-foreground r,
  /usr/local/bin/docker-entrypoint.sh rw,
  /usr/sbin/apache2 ix,
  /usr/sbin/apache2 r,
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^Q Where Was
```

e. Additions & Difficulties　# 另外 task1.2 有完成第二種方法:

- ➢ 使用 aa-easyprof 命令建立一個 Nginx 的 AppArmor 配置檔

$ aa-easyprof /usr/sbin/nginx

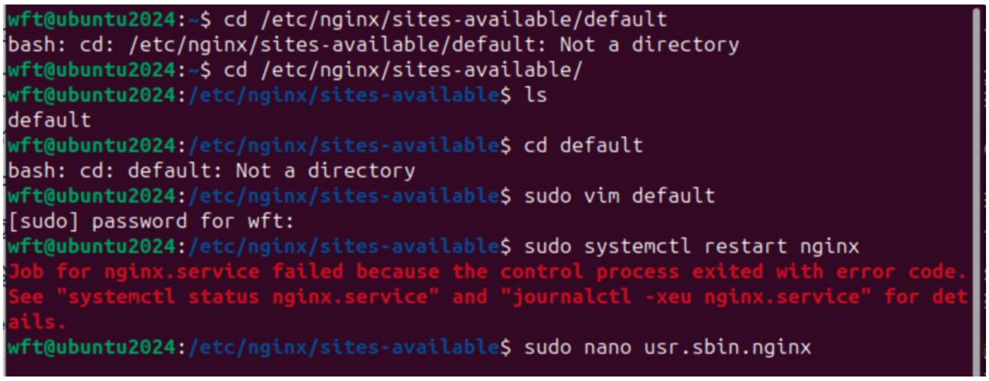
```
$ aa-easyprof /usr/sbin/nginx > nspj-nginx_312706038
$ sudo mv nspj-nginx_312706038 /etc/apparmor.d
```

- ➢ 使用 apparmor_parser 命令重新加載 AppArmor 配置文件，並重啟 Nginx

```
$ sudo apparmor_parser -r /etc/apparmor.d/nspj-nginx_312706038
$ sudo systemctl restart nginx
```

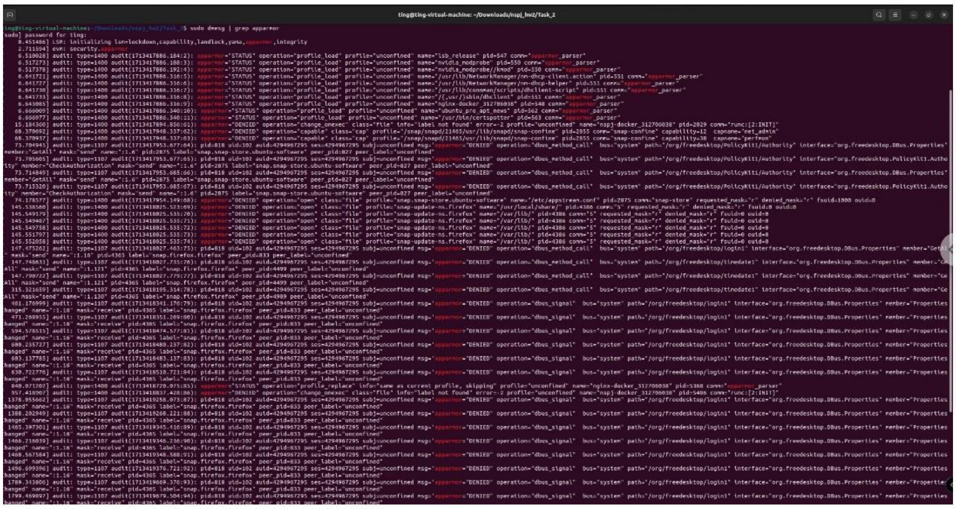
- ➢ 如果 Nginx 服務啟動失敗，使用 grep 命令檢查 AppArmor 的 log 檔，查找權限被 denied 原因

```
$ sudo grep -i apparmor /var/log/syslog
```



```
wft@ubuntu2024:~$ cd /etc/nginx/sites-available/default
bash: cd: /etc/nginx/sites-available/default: Not a directory
wft@ubuntu2024:~$ cd /etc/nginx/sites-available/
wft@ubuntu2024:/etc/nginx/sites-available$ ls
default
wft@ubuntu2024:/etc/nginx/sites-available$ cd default
bash: cd: default: Not a directory
wft@ubuntu2024:/etc/nginx/sites-available$ sudo vim default
[sudo] password for wft:
wft@ubuntu2024:/etc/nginx/sites-available$ sudo systemctl restart nginx
Job for nginx.service failed because the control process exited with error code.
See "systemctl status nginx.service" and "journalctl -xeu nginx.service" for det
ails.
wft@ubuntu2024:/etc/nginx/sites-available$ sudo nano usr.sbin.nginx
```

- ➢ 根據 log 檔，在 nspj-nginx_312706038 配置文件中加入對應的權限允許規則，並重新加載配置檔，再次重啟 Nginx



ting@ting-virtual-machine: ~/Downloads/nspj_hw2/Task_2

```
ting@ting-virtual-machine:~/Downloads/nspj_hw2/Task_2$ sudo dmesg | grep apparmor
sudo] password for ting:
    0.451486] LSM: initializing lsm=lockdown,capability,landlock,yama,apparmor,integrity
    2.711594] evm: security.apparmor
    6.510028] audit: type=1400 audit(1713417886.184:2): apparmor="STATUS" operation="profile_load" profile="unconfined" name="lsb_release" pid=547 comm="apparmor_parser"
    6.517273] audit: type=1400 audit(1713417886.188:3): apparmor="STATUS" operation="profile_load" profile="unconfined" name="nvidia_modprobe" pid=550 comm="apparmor_parser"
    6.517378] audit: type=1400 audit(1713417886.192:4): apparmor="STATUS" operation="profile_load" profile="unconfined" name="nvidia_modprobe//kmod" pid=550 comm="apparmor_parser"
    6.641721] audit: type=1400 audit(1713417886.316:5): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-client.action" pid=551 comm="apparmor_parser"
    6.641727] audit: type=1400 audit(1713417886.316:6): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-helper" pid=551 comm="apparmor_parser"
    6.641730] audit: type=1400 audit(1713417886.316:7): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/connman/scripts/dhclient-script" pid=551 comm="apparmor_parser"
    6.641733] audit: type=1400 audit(1713417886.316:8): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/{,usr/}sbin/dhclient" pid=551 comm="apparmor_parser"
    6.643085] audit: type=1400 audit(1713417886.316:9): apparmor="STATUS" operation="profile_load" profile="unconfined" name="nginx-docker_312706038" pid=548 comm="apparmor_parser"
    6.666009] audit: type=1400 audit(1713417886.340:10): apparmor="STATUS" operation="profile_load" profile="unconfined" name="ubuntu_pro_apt_news" pid=562 comm="apparmor_parser"
    6.666977] audit: type=1400 audit(1713417886.340:11): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/certspotter" pid=563 comm="apparmor_parser"
   15.184360] audit: type=1400 audit(1713417894.856:61): apparmor="DENIED" operation="change_onexec" class="file" info="label not found" error=-2 profile="unconfined" name="nspj-docker_312706038" pid=2029 comm="runc:[2:INIT]"
   68.370692] audit: type=1400 audit(1713417948.337:62): apparmor="DENIED" operation="capable" class="cap" profile="/snap/snapd/21465/usr/lib/snapd/snap-confine" pid=2855 comm="snap-confine" capability=12  capname="net_admin"
   68.370937] audit: type=1400 audit(1713417948.337:63): apparmor="DENIED" operation="capable" class="cap" profile="/snap/snapd/21465/usr/lib/snapd/snap-confine" pid=2855 comm="snap-confine" capability=38  capname="perfmon"
   73.704945] audit: type=1107 audit(1713417953.677:64): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/PolicyKit1/Authority" interface="org.freedesktop.DBus.Properties"
member="GetAll" mask="send" name=":1.6" pid=2875 label="snap.snap-store.ubuntu-software" peer_pid=827 peer_label="unconfined"
   73.705605] audit: type=1107 audit(1713417953.677:65): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/PolicyKit1/Authority" interface="org.freedesktop.PolicyKit1.Autho
ity" member="CheckAuthorization" mask="send" name=":1.6" pid=2875 label="snap.snap-store.ubuntu-software" peer_pid=827 peer_label="unconfined"
   73.714849] audit: type=1107 audit(1713417953.685:66): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/PolicyKit1/Authority" interface="org.freedesktop.DBus.Properties"
member="GetAll" mask="send" name=":1.6" pid=2875 label="snap.snap-store.ubuntu-software" peer_pid=827 peer_label="unconfined"
   73.715320] audit: type=1107 audit(1713417953.685:67): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/PolicyKit1/Authority" interface="org.freedesktop.PolicyKit1.Autho
ity" member="CheckAuthorization" mask="send" name=":1.6" pid=2875 label="snap.snap-store.ubuntu-software" peer_pid=827 peer_label="unconfined"
   74.178577] audit: type=1400 audit(1713417954.149:68): apparmor="DENIED" operation="open" class="file" profile="snap.snap-store.ubuntu-software" name="/etc/appstream.conf" pid=2875 comm="snap-store" requested_mask="r" denied_mask="r" fsuid=1000 ouid=0
  145.538560] audit: type=1400 audit(1713418025.523:69): apparmor="DENIED" operation="open" class="file" profile="snap-update-ns.firefox" name="/usr/local/share/" pid=4386 comm="5" requested_mask="r" denied_mask="r" fsuid=0 ouid=0
  145.549179] audit: type=1400 audit(1713418025.535:70): apparmor="DENIED" operation="open" class="file" profile="snap-update-ns.firefox" name="/var/lib/" pid=4386 comm="5" requested_mask="r" denied_mask="r" fsuid=0 ouid=0
  145.549487] audit: type=1400 audit(1713418025.535:71): apparmor="DENIED" operation="open" class="file" profile="snap-update-ns.firefox" name="/var/lib/" pid=4386 comm="5" requested_mask="r" denied_mask="r" fsuid=0 ouid=0
  145.549758] audit: type=1400 audit(1713418025.535:72): apparmor="DENIED" operation="open" class="file" profile="snap-update-ns.firefox" name="/var/lib/" pid=4386 comm="5" requested_mask="r" denied_mask="r" fsuid=0 ouid=0
  145.551797] audit: type=1400 audit(1713418025.535:73): apparmor="DENIED" operation="open" class="file" profile="snap-update-ns.firefox" name="/var/lib/" pid=4386 comm="5" requested_mask="r" denied_mask="r" fsuid=0 ouid=0
  145.552058] audit: type=1400 audit(1713418025.535:74): apparmor="DENIED" operation="open" class="file" profile="snap-update-ns.firefox" name="/var/lib/" pid=4386 comm="5" requested_mask="r" denied_mask="r" fsuid=0 ouid=0
  147.475262] audit: type=1107 audit(1713418027.463:75): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="GetAl
" mask="send" name=":1.16" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
  147.740631] audit: type=1107 audit(1713418027.735:76): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/timedate1" interface="org.freedesktop.DBus.Properties" member="Ge
All" mask="send" name=":1.121" pid=4365 label="snap.firefox.firefox" peer_pid=4499 peer_label="unconfined"
  147.790722] audit: type=1107 audit(1713418027.779:77): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/timedate1" interface="org.freedesktop.DBus.Properties" member="Ge
All" mask="send" name=":1.121" pid=4365 label="snap.firefox.firefox" peer_pid=4499 peer_label="unconfined"
  315.321659] audit: type=1107 audit(1713418195.314:78): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/timedate1" interface="org.freedesktop.DBus.Properties" member="Ge
All" mask="send" name=":1.130" pid=4365 label="snap.firefox.firefox" peer_pid=4909 peer_label="unconfined"
  461.176999] audit: type=1107 audit(1713418341.176:79): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
  471.268955] audit: type=1107 audit(1713418351.269:80): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
  594.578515] audit: type=1107 audit(1713418474.577:81): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
  600.235727] audit: type=1107 audit(1713418480.237:82): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
  603.137785] audit: type=1107 audit(1713418483.137:83): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
  630.722776] audit: type=1107 audit(1713418510.721:84): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
  840.071202] audit: type=1400 audit(1713418720.075:85): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="nginx-docker_312706038" pid=5388 comm="apparmor_parser"
  957.418907] audit: type=1400 audit(1713418837.428:86): apparmor="DENIED" operation="change_onexec" class="file" info="label not found" error=-2 profile="unconfined" name="nspj-docker_312706038" pid=5406 comm="runc:[2:INIT]"
 1378.055662] audit: type=1107 audit(1713419258.073:87): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
 1388.202949] audit: type=1107 audit(1713419268.221:88): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
 1465.397301] audit: type=1107 audit(1713419345.416:89): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
 1466.218039] audit: type=1107 audit(1713419346.236:90): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
 1468.567584] audit: type=1107 audit(1713419348.588:91): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
 1496.699396] audit: type=1107 audit(1713419376.721:92): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
 1789.343806] audit: type=1107 audit(1713419669.376:93): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
 1799.469897] audit: type=1107 audit(1713419679.504:94): pid=818 uid=102 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_signal"  bus="system" path="/org/freedesktop/login1" interface="org.freedesktop.DBus.Properties" member="Properties
hanged" name=":1.16" mask="receive" pid=4365 label="snap.firefox.firefox" peer_pid=833 peer_label="unconfined"
```

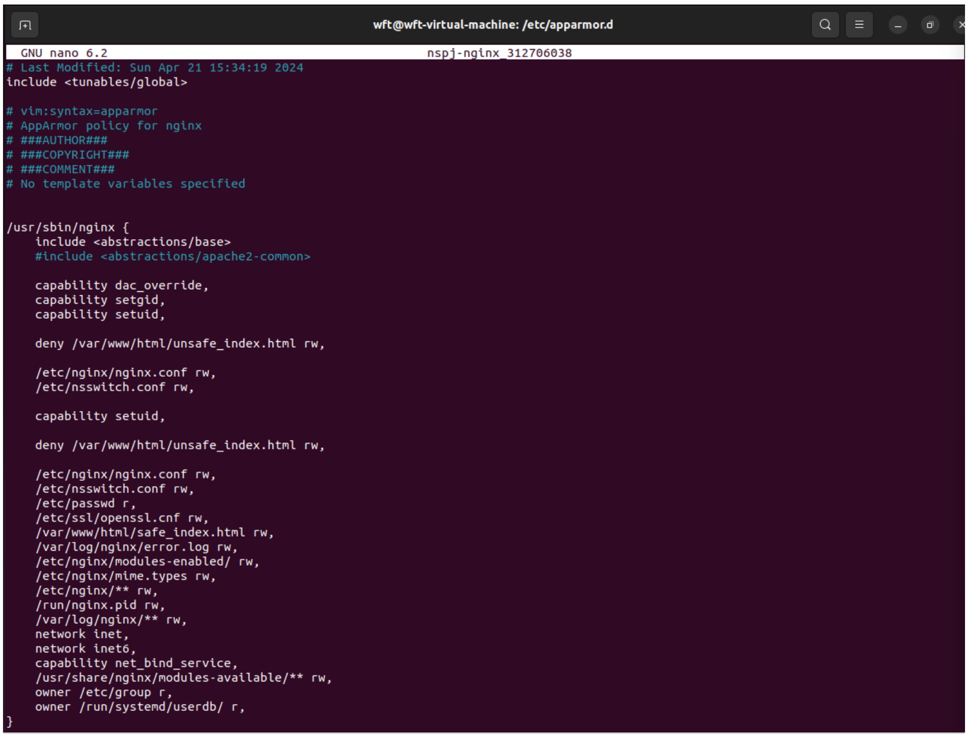
(出現的錯誤如上圖):

```
Apr 21 11:01:38 wft-virtual-machine kernel: [    145.717876] audit:
type=1107 audit(1713668498.468:83): pid=780 uid=102 auid=4294967295
ses=4294967295 subj=unconfined msg='apparmor="DENIED"
operation="dbus_method_call"    bus="system"
path="/org/freedesktop/RealtimeKit1"
interface="org.freedesktop.RealtimeKit1" member="MakeThreadRealtime"
mask="send" name="org.freedesktop.RealtimeKit1" pid=4974
```

```
label="snap.telegram-desktop.telegram-desktop" peer_pid=1232
peer_label="unconfined"

Apr 19 20:29:09 ting-virtual-machine kernel: [ 2588.109949] audit:
type=1400 audit(1713529749.303:202): apparmor="DENIED"
operation="open" class="file" profile="nspj-docker_312706038"
name="/usr/lib/x86_64-linux-gnu/libc.so.6" pid=14428 comm="docker-
entrypoi" requested_mask="r" denied_mask="r" fsuid=0 ouid=0
```

- 進行規範設定
  `$ sudo systemctl restart nginx` 和 `$ sudo aa-logprof`
- 在 nspj-nginx_312706038 檔加入以下條件

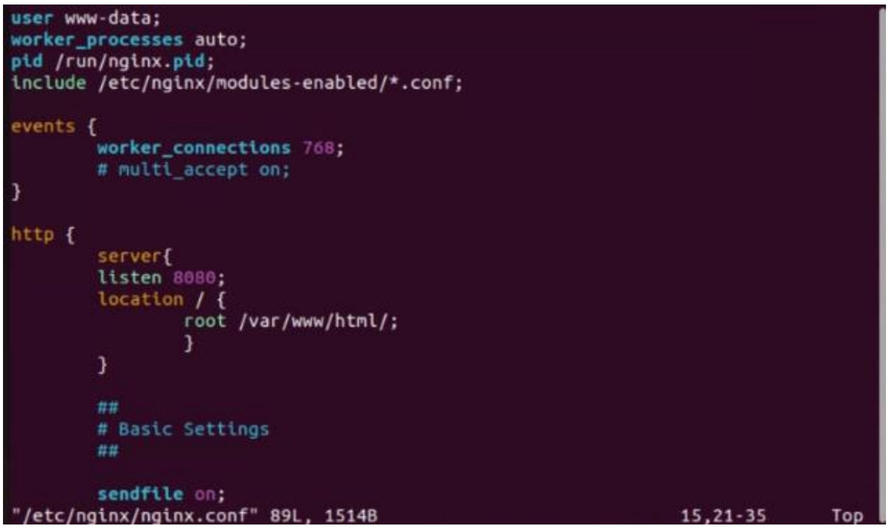
```
/var/www/html/safe_index.html rw,
deny /var/www/html/unsafe_index.html rw,
```



```
  GNU nano 6.2                                          nspj-nginx_312706038
# Last Modified: Sun Apr 21 15:34:19 2024
include <tunables/global>

# vim:syntax=apparmor
# AppArmor policy for nginx
# ###AUTHOR###
# ###COPYRIGHT###
# ###COMMENT###
# No template variables specified


/usr/sbin/nginx {
    include <abstractions/base>
    #include <abstractions/apache2-common>

    capability dac_override,
    capability setgid,
    capability setuid,

    deny /var/www/html/unsafe_index.html rw,

    /etc/nginx/nginx.conf rw,
    /etc/nsswitch.conf rw,

    capability setuid,

    deny /var/www/html/unsafe_index.html rw,

    /etc/nginx/nginx.conf rw,
    /etc/nsswitch.conf rw,
    /etc/passwd r,
    /etc/ssl/openssl.cnf rw,
    /var/www/html/safe_index.html rw,
    /var/log/nginx/error.log rw,
    /etc/nginx/modules-enabled/ rw,
    /etc/nginx/mime.types rw,
    /etc/nginx/** rw,
    /run/nginx.pid rw,
    /var/log/nginx/** rw,
    network inet,
    network inet6,
    capability net_bind_service,
    /usr/share/nginx/modules-available/** rw,
    owner /etc/group r,
    owner /run/systemd/userdb/ r,
}
```

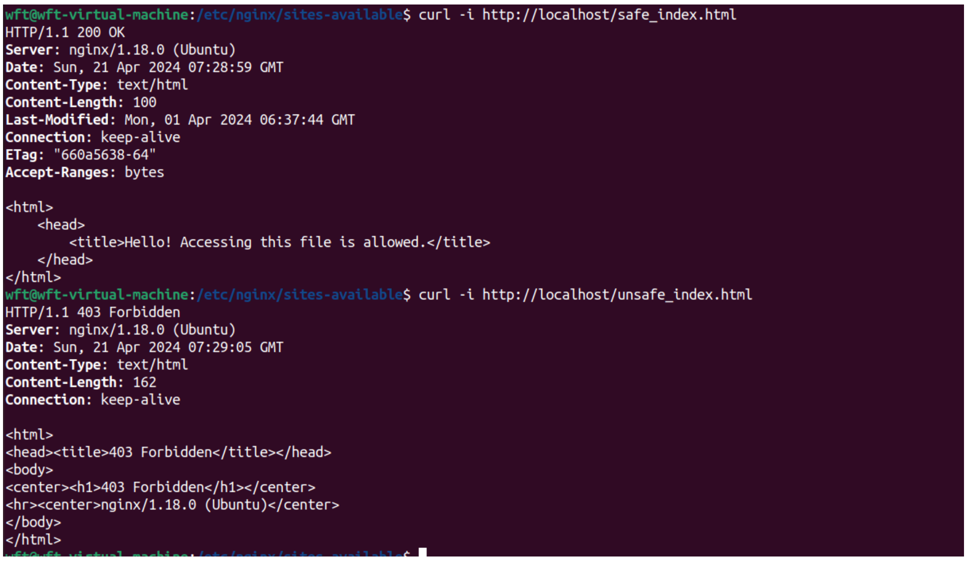
- 錯誤顯示，需要修改 usr.sbin.nginx 和 nginx.conf 的內容。
  使用 `$ nginx -t` 指令，發現是語法編譯錯誤。

- 修改 nginx.conf 的內容



```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
        worker_connections 768;
        # multi_accept on;
}

http {
        server{
        listen 8080;
        location / {
                root /var/www/html/;
                }
        }

        ##
        # Basic Settings
        ##

        sendfile on;
"/etc/nginx/nginx.conf" 89L, 1514B                              15,21-35      Top
```

- 最後成功測試



```
wft@wft-virtual-machine:/etc/nginx/sites-available$ curl -i http://localhost/safe_index.html
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 21 Apr 2024 07:28:59 GMT
Content-Type: text/html
Content-Length: 100
Last-Modified: Mon, 01 Apr 2024 06:37:44 GMT
Connection: keep-alive
ETag: "660a5638-64"
Accept-Ranges: bytes

<html>
    <head>
        <title>Hello! Accessing this file is allowed.</title>
    </head>
</html>
wft@wft-virtual-machine:/etc/nginx/sites-available$ curl -i http://localhost/unsafe_index.html
HTTP/1.1 403 Forbidden
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 21 Apr 2024 07:29:05 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive

<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
wft@wft-virtual-machine:/etc/nginx/sites-available$
```