

## 網路安全實務 Project2 Report

資管所 312706026

### Task 1.1

先執行指令進行安裝：

```
$ sudo apt update
```

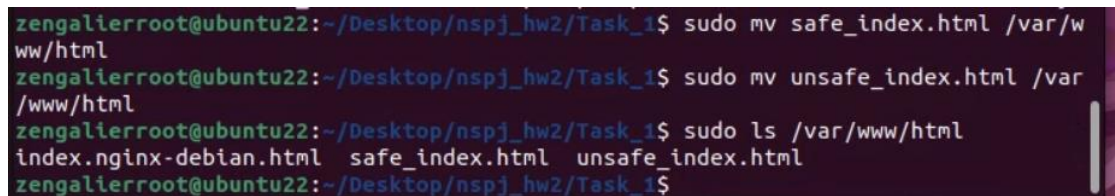
```
$ sudo apt install nginx
```

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

然後使用下面兩個指令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/
```



```
zengalierroot@ubuntu22:~/Desktop/nspj_hw2/Task_1$ sudo mv safe_index.html /var/w
ww/html
zengalierroot@ubuntu22:~/Desktop/nspj_hw2/Task_1$ sudo mv unsafe_index.html /var
/www/html
zengalierroot@ubuntu22:~/Desktop/nspj_hw2/Task_1$ sudo ls /var/www/html
index.nginx-debian.html  safe_index.html  unsafe_index.html
zengalierroot@ubuntu22:~/Desktop/nspj_hw2/Task_1$
```

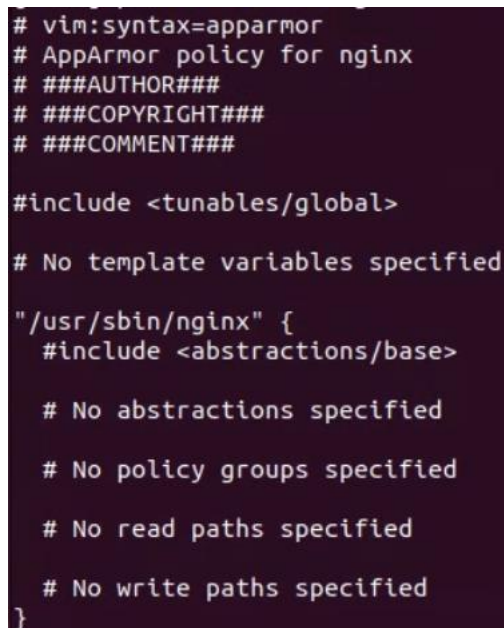
### Task1.2（方法二）：

使用下面三個指令得到我們的設定檔：

```
$ aa-easyprof /usr/sbin/nginx
```

```
$ aa-easyprof /usr/sbin/nginx > nspj-nginx_312706026
```

```
$ sudo mv nspj-nginx_312706026 /etc/apparmor.d
```



```
# vim:syntax=apparmor
# AppArmor policy for nginx
# ####AUTHOR###
# ####COPYRIGHT###
# ####COMMENT###

#include <tunables/global>

# No template variables specified

"/usr/sbin/nginx" {
    #include <abstractions/base>

    # No abstractions specified

    # No policy groups specified

    # No read paths specified

    # No write paths specified
}
```

然後\$ sudo apparmor\_parser -r /etc/apparmor.d/ nspj-nginx\_312706026 和\$ sudo systemctl restart nginx 和 \$ sudo aa-logprof 進行規範設定，全部點選 A 或 S

接著進入/etc/apparmor.d/ nspj-nginx\_312706026 添加下面兩行：

/var/www/html/safe\_index.html rw,

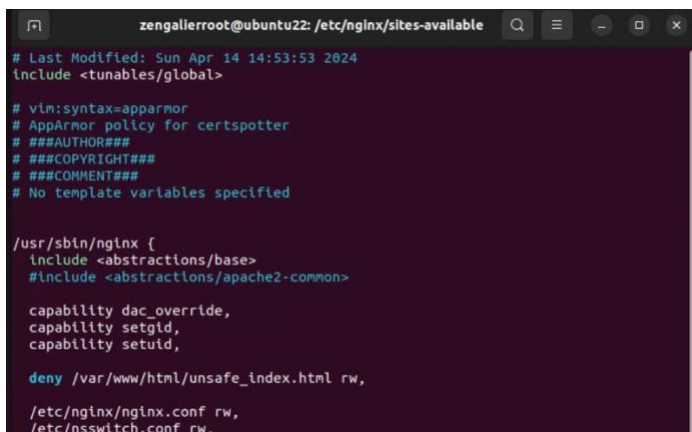
deny /var/www/html\_unsafe.html rw

然後\$ sudo apparmor\_parser -r /etc/apparmor.d/ nspj-nginx\_312706026 和\$ sudo systemctl restart nginx，若出現 Job for nginx.service failed because the control process exited with error code，則\$ sudo grep -i apparmor /var/log/syslog 檢查 AppArmor 日誌，若內容出現類似以下 apparmor=" DENIED"，則在 nspj-nginx\_312706026 中添加允許，直到\$ sudo systemctl restart nginx 不會出現錯誤。

```
Apr 14 15:02:24 ubuntu22 kernel: [ 6692.364856] audit: type=1400 audit(1713078144.195:138): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/sbin/nginx" pid=5240 comm="apparmor_parser"
Apr 14 15:02:27 ubuntu22 kernel: [ 6696.089014] audit: type=1400 audit(1713078147.919:139): apparmor="DENIED" operation="open" class="file" profile="/usr/sbin/nginx" name="/etc/nginx/mime.types" pid=5245 comm="nginx" requested_mask="r" denied_mask="r" fsuid=0 ouid=0
```

接著\$ curl -i http://localhost/safe\_index.html，若執行後一直無法執行結束，則需檢查 sudo tail -f /var/log/nginx/error.log，並根據錯誤提示修改 usr.sbin. nginx 和 nginx.conf（當修改該文件保存後，可先\$ sudo nginx -t 檢查是否有語法錯誤）的內容。

最終得到的 nspj-nginx\_312706026 內容如下：



```
zengallerroot@ubuntu22: /etc/nginx/sites-available
# Last Modified: Sun Apr 14 14:53:53 2024
include <tunables/global>

# vim:syntax=apparmor
# AppArmor policy for certspotter
# ###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.html rw,

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

```
zengallerroot@ubuntu22: /etc/nginx/sites-available
capability setuid,

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

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

}

36,1 Bot
```

nginx.conf 的內容如下：(更改端口為非特權端口 8080)

```
zengallerroot@ubuntu22: /etc/nginx/sites-available
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\$ curl -i http://localhost:8080/safe\_index.html 和\$ curl -i http://localhost:8080/unsafe\_index.html 後，會得到的畫面為：

```
zengallerroot@ubuntu22: ~/Desktop/nspj_hw2/Task_2
Step 12/12 : RUN chown -R www-data:www-data /var/www/html
--> Running in 5d0ce9dfe4af
Removing intermediate container 5d0ce9dfe4af
--> 143477cb45ca
Successfully built 143477cb45ca
Successfully tagged nspj:latest
zengallerroot@ubuntu22: ~/Desktop/nspj_hw2/Task_2$ curl -i http://localhost:8080/safe_index.html
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 14 Apr 2024 08:46:00 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>
zengallerroot@ubuntu22: ~/Desktop/nspj_hw2/Task_2$
```

```
zengallierroot@ubuntu22: ~/Desktop/nspj_hw2/Task_2
Accept-Ranges: bytes

<html>
  <head>
    <title>Hello! Accessing this file is allowed.</title>
  </head>
</html>
zengallierroot@ubuntu22: ~/Desktop/nspj_hw2/Task_2$ curl -i http://localhost:8080/unsafe_index.html
HTTP/1.1 403 Forbidden
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 14 Apr 2024 08:46:17 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>
zengallierroot@ubuntu22: ~/Desktop/nspj_hw2/Task_2$
```

## Task2.1

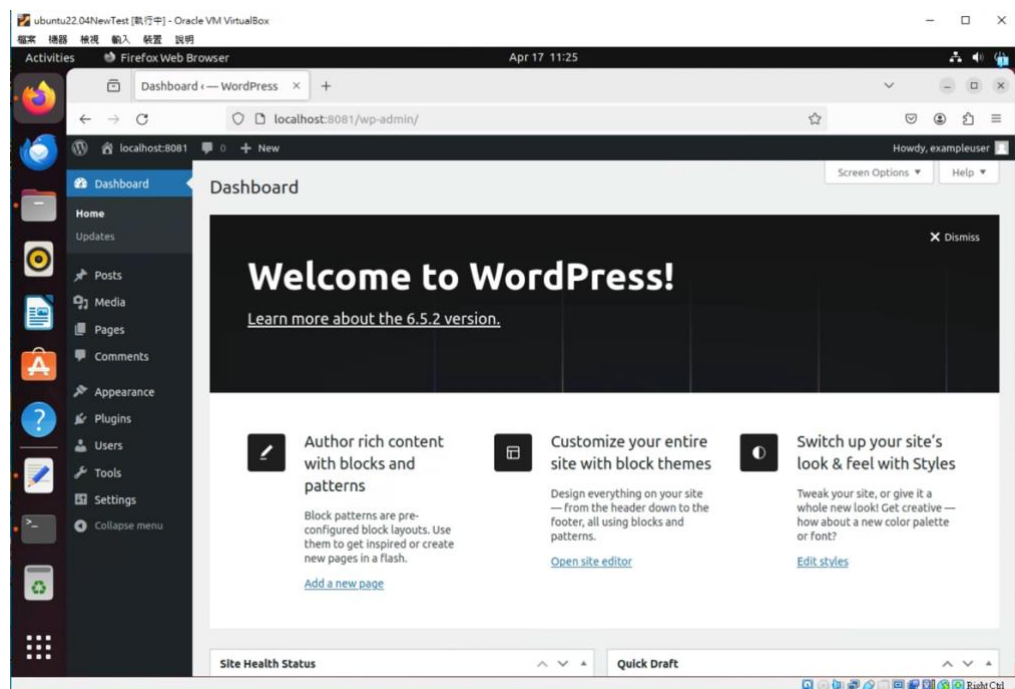
在 Task\_2 文件夾中

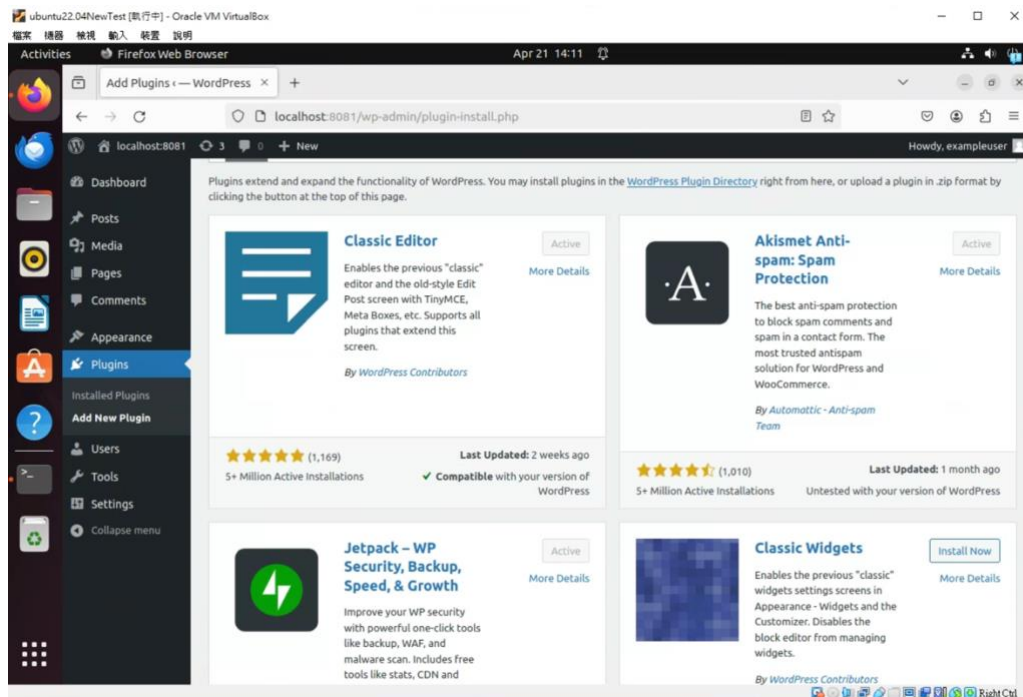
```
$sudo apt-get update && apt-get install docker-compose
```

```
$sudo docker build -t nspj:latest .
```

```
$sudo docker-compose up
```

完成後登入帳號並安裝 Classic Editor、Akismet、Jetpack



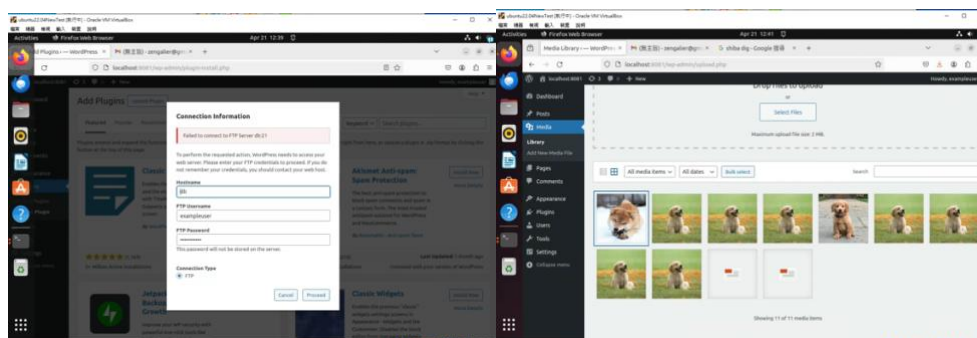


## Task2.2

1. 在 apparmor.d 文件夾中創建 nspj-docker\_312706026，內容為空，在 docker-compose.yml 中的 security\_opt 項加入- apparmor:nspj-docker\_312706026

```
# TODO: attach the apparmor profile into this section
security_opt:
  - apparmor:nspj-docker_312706026
```

2. 重複\$ sudo systemctl restart docker 和\$ sudo docker-compose up 和\$ sudo aa-logprof 完成 nspj-docker\_312706026 基本配置。
3. 根據要求修改 nspj-docker\_312706026 配置內容，使在安裝 plugins 時連接 FTP 失敗，能夠讀取 uploads 文件夾使在上傳圖片時可以成功。



在 nspj-docker\_312706026 中主要完成這個功能的部分為（需注意順序）：



```
zengallerroot@ubuntu22: /etc/apparmor.d

profile nspj-docker_312706026 {
    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/** rwx,
    /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/zengallerroot/** rw,
    /dev/tty rw,
```

最終完整的 nspj-docker\_312706026 內容為：

```
# 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_312706026 {
    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/** rwx,
    /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/zengallerroot/** rw,
    /dev/tty rw,
    /etc/ImageMagick-6/coder.xml r,
    /etc/ImageMagick-6/magic.xml r,
    /etc/apache2/* r,
    /etc/apache2/envvars r,
    /etc/gai.conf r,
    /etc/group r,
    /etc/host.conf r,
    /etc/hosts r,
    /etc/issue.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 grx,
    /usr/bin/diffname lx,
    /usr/bin/diffname lx,
    /usr/bin/docker f,
    /usr/bin/docker-proxy f,
    /usr/bin/dockerd f,
    /usr/bin/id lx,
    /usr/bin/id rw,
    /usr/bin/mkdir lx,
    /usr/bin/mkdir f,
    /usr/bin/rm lx,
    /usr/bin/rm f,
    /usr/local/bin/apache2-foreground lx,
    /usr/local/bin/apache2-foreground f,
    /usr/local/bin/docker-entrypoint.sh rw,
    /usr/sbin/apache2 lx,
    /usr/sbin/apache2 f,
    /var/log/apache2/* log w,
    #/var/www/html/wp-content/uploads/** rw,
    owner /etc/ImageMagick-6/log.xml r,
    owner /etc/ImageMagick-6/policy.xml r,
    owner /etc/host.conf r,
    owner /proc/*/*/* w,
    owner /run/apache2/apache2.pid.0PnXgK w,
    owner /run/apache2/apache2.pid.0mZeYk w,
    owner /run/apache2/apache2.pid.2dXsX5 w,
    owner /run/apache2/apache2.pid.3prRm w,
    owner /run/apache2/apache2.pid.4H1Zt w,
    owner /run/apache2/apache2.pid.4VtV9M w,
    owner /run/apache2/apache2.pid.4uF6m w,
    owner /run/apache2/apache2.pid.5K17d w,
    owner /run/apache2/apache2.pid.5LwN1 w,
    owner /run/apache2/apache2.pid.5ZkPPy w,
    owner /run/apache2/apache2.pid.6Uv9f w,
    owner /run/apache2/apache2.pid.7JOSYA w,
    owner /run/apache2/apache2.pid.7dhrRk w,
    owner /run/apache2/apache2.pid.7rnf1 w,
    owner /run/apache2/apache2.pid.8Fw62H w,
    owner /run/apache2/apache2.pid.8SpRd w,
    owner /run/apache2/apache2.pid.8yHfF w,
    owner /run/apache2/apache2.pid.94G713 w,
    owner /run/apache2/apache2.pid.96E8B2 w,
    owner /run/apache2/apache2.pid.93BRK w,
    owner /run/apache2/apache2.pid.AkXNB2 w,
    owner /run/apache2/apache2.pid.BB1qxt w,
    owner /run/apache2/apache2.pid.BX1tK w,
    owner /run/apache2/apache2.pid.CmCvV w,
    owner /run/apache2/apache2.pid.DmCqj w,
    owner /run/apache2/apache2.pid.DqtUd3 w,
    owner /run/apache2/apache2.pid.Ehy41w w,
    owner /run/apache2/apache2.pid.G6g9g w,
    owner /run/apache2/apache2.pid.G78V3L w,
    owner /run/apache2/apache2.pid.GelUti w,
    owner /run/apache2/apache2.pid.H2PAPY w,
    owner /run/apache2/apache2.pid.HDQ6b7 w,
    owner /run/apache2/apache2.pid.lbpPL1 w,
    owner /run/apache2/apache2.pid.156cgb w,
    owner /run/apache2/apache2.pid.1YbC8a w,
    owner /run/apache2/apache2.pid.1mX2C w,
    owner /run/apache2/apache2.pid.1yZ5Dl w,
    owner /run/apache2/apache2.pid.K6hceX w,
    owner /run/apache2/apache2.pid.L66cC0 w,
    owner /run/apache2/apache2.pid.Lx1Y15 w,
    owner /run/apache2/apache2.pid.NB1YK w,
    owner /run/apache2/apache2.pid.M5lgX3 w,
    owner /run/apache2/apache2.pid.NEYoY w,
    owner /run/apache2/apache2.pid.NZgqd3 w,
    owner /run/apache2/apache2.pid.OjCMA w,
    owner /run/apache2/apache2.pid.0M6C30 w,
    owner /run/apache2/apache2.pid.0nYgX w,
    owner /run/apache2/apache2.pid.0pksAt w,
    owner /run/apache2/apache2.pid.Pchgn w,
    owner /run/apache2/apache2.pid.PkXRP w,
    owner /run/apache2/apache2.pid.PrUD13 w,
    owner /run/apache2/apache2.pid.Q74ru w,
    owner /run/apache2/apache2.pid.088IH9 w,
    owner /run/apache2/apache2.pid.0EWH2 w,
    owner /run/apache2/apache2.pid.R0P14 w,
    owner /run/apache2/apache2.pid.Se3W7w w,
    owner /run/apache2/apache2.pid.T8y18u w,
    owner /run/apache2/apache2.pid.T0dP8 w,
    owner /run/apache2/apache2.pid.TYX001 w,
    owner /run/apache2/apache2.pid.Tr1a3D w,
    owner /run/apache2/apache2.pid.TV8R6 w,
```

```
owner /run/apache2/apache2.pid.PIKORF w,
owner /run/apache2/apache2.pid.PR0d13 W,
owner /run/apache2/apache2.pid.Q2GZwz W,
owner /run/apache2/apache2.pid.088Ht W,
owner /run/apache2/apache2.pid.0EWHK w,
owner /run/apache2/apache2.pid.R0P9J r,
owner /run/apache2/apache2.pid.Sc3kT,
TrnB8r /run/apache2/apache2.pid.T8y18a W,
owner /run/apache2/apache2.pid.T0m28 W,
owner /run/apache2/apache2.pid.TV00D W,
TrnW3o /run/apache2/apache2.pid.TrIeJ3 W,
owner /run/apache2/apache2.pid.Tv9AP6 W,
owner /run/apache2/apache2.pid.Ted6L W,
owner /run/apache2/apache2.pid.U4LTsp W,
owner /run/apache2/apache2.pid.UVRU4 w,
owner /run/apache2/apache2.pid.UZ4Wf W,
owner /run/apache2/apache2.pid.UZM4N w,
owner /run/apache2/apache2.pid.Uj1Q8T W,
owner /run/apache2/apache2.pid.uqgW08 W,
owner /run/apache2/apache2.pid.VdR7C W,
owner /run/apache2/apache2.pid.Vs3Z5D W,
owner /run/apache2/apache2.pid.XP3rY W,
owner /run/apache2/apache2.pid.XoL7R W,
owner /run/apache2/apache2.pid.qXg1U9 W,
owner /run/apache2/apache2.pid.z00t1P W,
owner /run/apache2/apache2.pid.af30og W,
owner /run/apache2/apache2.pid.ar0K4E W,
owner /run/apache2/apache2.pid.atZ0WT W,
owner /run/apache2/apache2.pid.bS1vbD W,
owner /run/apache2/apache2.pid.b9u1Lz W,
owner /run/apache2/apache2.pid.BNkX6z W,
owner /run/apache2/apache2.pid.bc3UX3 W,
owner /run/apache2/apache2.pid.cK5Nz W,
owner /run/apache2/apache2.pid.dZ578x W,
owner /run/apache2/apache2.pid.e4e24D W,
owner /run/apache2/apache2.pid.f21l9k W,
owner /run/apache2/apache2.pid.fj8R3J W,
owner /run/apache2/apache2.pid.hRC03R W,
owner /run/apache2/apache2.pid.h18Rr W,
owner /run/apache2/apache2.pid.hCRGT W,
owner /run/apache2/apache2.pid.IACFV0 W,
owner /run/apache2/apache2.pid.iET6D W,
owner /run/apache2/apache2.pid.JML6p W,
owner /run/apache2/apache2.pid.l4070E W,
owner /run/apache2/apache2.pid.K5rtvY W,
owner /run/apache2/apache2.pid.mYtW7 W,
owner /run/apache2/apache2.pid.o9EFK W,
owner /run/apache2/apache2.pid.oE131J W,
owner /run/apache2/apache2.pid.oF8W3 W,
owner /run/apache2/apache2.pid.oF8W3 W,
owner /run/apache2/apache2.pid.pN1Y75 W,
owner /run/apache2/apache2.pid.pc1c39A W,
owner /run/apache2/apache2.pid.pr1L3P W,
owner /run/apache2/apache2.pid.pj0F4D W,
owner /run/apache2/apache2.pid.psoZ0D W,
owner /run/apache2/apache2.pid.q1LEP W,
owner /run/apache2/apache2.pid.q1h8H W,
owner /run/apache2/apache2.pid.r3HB8W W,
owner /run/apache2/apache2.pid.rHm9d W,
owner /run/apache2/apache2.pid.sCE1z W,
owner /run/apache2/apache2.pid.sh29vZ W,
owner /run/apache2/apache2.pid.s1jW78 W,
owner /run/apache2/apache2.pid.t51Z1r W,
owner /run/apache2/apache2.pid.tARNA8 W,
owner /run/apache2/apache2.pid.tEtBC8 W,
owner /run/apache2/apache2.pid.tYtelC W,
owner /run/apache2/apache2.pid.tg6hzr W,
owner /run/apache2/apache2.pid.tvP306 W,
owner /run/apache2/apache2.pid.u6U8U W,
owner /run/apache2/apache2.pid.v6W6yy W,
owner /run/apache2/apache2.pid.vGNH14 W,
owner /run/apache2/apache2.pid.w6L1Lz W,
owner /run/apache2/apache2.pid.vVwX0k W,
owner /run/apache2/apache2.pid.wIC0C W,
owner /run/apache2/apache2.pid.wfM8T W,
owner /run/apache2/apache2.pid.wXMDU W,
owner /run/apache2/apache2.pid.wXB11W W,
owner /run/apache2/apache2.pid.xCN2tO W,
owner /run/apache2/apache2.pid.xSH1Lz W,
owner /run/apache2/apache2.pid.ylvbE4 W,
owner /run/apache2/apache2.pid.y53ZH7 W,
owner /run/apache2/apache2.pid.yo3RHp W,
owner /usr/local/etc/php/conf.d/r,
owner /usr/local/etc/php/conf.d/docker-php-ext-bcmath.ini r,
owner /usr/local/etc/php/conf.d/docker-php-ext-xmlrpc.ini r,
owner /usr/local/etc/php/conf.d/docker-php-ext-gd.ini r,
owner /usr/local/etc/php/conf.d/docker-php-ext-imaplib.ini r,
owner /usr/local/etc/php/conf.d/docker-php-ext-mysql.ini r,
owner /usr/local/etc/php/conf.d/docker-php-ext-opcache.ini r,
owner /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini r,
owner /usr/local/etc/php/conf.d/docker-php-ext-zip.ini r,
owner /usr/local/etc/php/conf.d/error-logging.ini r,
owner /usr/local/etc/php/conf.d/opcache-recommended.ini r,
owner /usr/local/lib/php/extensions/no-debug-non-zts-20220829/bcmath.so mr,
owner /usr/local/lib/php/extensions/no-debug-non-zts-20220829/exif.so mr,
owner /usr/local/lib/php/extensions/no-debug-non-zts-20220829/gd.so mr,
owner /usr/local/lib/php/extensions/no-debug-non-zts-20220829/imaplib.so mr,
owner /usr/local/lib/php/extensions/no-debug-non-zts-20220829/intl.so mr,
owner /usr/local/lib/php/extensions/no-debug-non-zts-20220829/mysqli.so mr,
owner /usr/local/lib/php/extensions/no-debug-non-zts-20220829/sodium.so mr,
owner /usr/local/lib/php/extensions/no-debug-non-zts-20220829/sqlite3.so mr,
/var/www/html/index.nginx-debian.html rw,
/var/www/html/index.php rw,
/var/www/html/LICENSE.txt,
$deny /var/www/html/_app-content/index.php w,
$deny /var/www/html/_app-content/plugins/* rw,
$deny /var/www/html/_app-content/themes/* rw,
/var/www/html/* = rf,
```

遇到的困難：

1. 在 Task2 中，由於 apparmor 配置檔的內容有順序問題，因此在順序上面研究了一段時間，後來通過不同的嘗試，找到正確的寫法。
2. 在 Task1，一開始執行 nginx 時會出現各種文件 permission denied，最初以為是因為 ubuntu 系統的問題，後來仔細研究 apparmor 後，通過使用 aa-logprof 來修改配置檔內容解決這個問題。