✅ 1. Proprietario e gruppo consigliati

Su Debian, Apache gira normalmente come **utente** `www-data` e gruppo `www-data`. Puoi verificarlo con:

```
ps aux | grep apache
# o
ps aux | grep www-data
```

Quindi, la regola generale è:

```
sudo chown -R www-data:www-data /var/www/html
```

Ma attenzione:

- Se sviluppi manualmente (es. carichi file via SSH/SFTP), può essere comodo mantenere **il tuo utente come proprietario** e **www-data come gruppo**:

  ```
  sudo chown -R tuo_utente:www-data /var/www/html
  ```

  Così puoi modificare i file senza `sudo`, e Apache può comunque leggerli ed eseguirli.

✅ 2. Permessi raccomandati

📁 Cartelle

Le directory devono essere **eseguibili** (`x`) per poterci accedere:

```
sudo find /var/www/html -type d -exec chmod 755 {} \;
```

👉 Permessi `755` = `rwxr-xr-x`

- Proprietario: può leggere/scrivere/eseguire
- Gruppo e altri: possono leggere ed entrare nella cartella

📄 File

I file devono essere **leggibili** ma non **eseguibili**:

```
sudo find /var/www/html -type f -exec chmod 644 {} \;
```

👉 Permessi `644` = `rw-r--r--`

- Proprietario: può leggere e scrivere
- Gruppo e altri: possono solo leggere

⚙️ 3. Eccezioni (solo se servono)

- Se usi **upload di file** o **cache scrivibili dal webserver** (es. WordPress `wp-content/uploads`, `cache`, `logs`, ecc.), allora:

```
sudo chown -R www-data:www-data /var/www/html/cartella_scrivibile
sudo chmod -R 775 /var/www/html/cartella_scrivibile
```

👉 Permette ad Apache di scrivere nella cartella.

🚫 4. Cose da **non fare**

× Non usare permessi 777 — chiunque potrebbe scrivere nel sito (rischio gravissimo). × Non dare la proprietà completa al tuo utente se Apache deve scrivere. × Non impostare eseguibili su file PHP o HTML.

🧩 5. Riassunto finale

Tipo	Proprietario	Gruppo	Permessi	Note
Tutto il sito	`tuo_utente` (o `www-data`)	`www-data`	—	Proprietà corretta per Apache
Cartelle	`755`		Accesso in lettura/esecuzione	
File	`644`		Solo lettura per Apache	
Cartelle scrivibili (cache/upload)	`www-data:www-data`	`775`	Solo dove serve scrittura	

🖥️ 6. Script per impostare automaticamente i permessi

```
#!/bin/bash
# ========================================================
# Script: set_www_permissions.sh
# Scopo: Impostare permessi e proprietari corretti per /var/www/html
# Sistema: Debian/Ubuntu con Apache
# Autore: ChatGPT
# ========================================================
```

```
# === CONFIGURAZIONE ===
WEB_DIR="/var/www/html"        # directory del sito
USER_DEV="tuo_utente"          # <-- Sostituisci con il tuo utente Linux
GROUP_WEB="www-data"           # gruppo usato da Apache

echo "Configurazione permessi per $WEB_DIR..."
echo "Utente sviluppatore: $USER_DEV"
echo "Gruppo webserver: $GROUP_WEB"
echo "-----------------------------------"

# 1️⃣ Imposta proprietario e gruppo
echo "[1/4] Imposto proprietari..."
sudo chown -R "$USER_DEV":"$GROUP_WEB" "$WEB_DIR"

# 2️⃣ Imposta permessi sulle cartelle
echo "[2/4] Imposto permessi sulle cartelle (755)..."
sudo find "$WEB_DIR" -type d -exec chmod 755 {} \;

# 3️⃣ Imposta permessi sui file
echo "[3/4] Imposto permessi sui file (644)..."
sudo find "$WEB_DIR" -type f -exec chmod 644 {} \;

# 4️⃣ Opzionale: cartelle scrivibili da Apache
# Aggiungi qui le directory dove Apache deve poter scrivere:
WRITABLE_DIRS=(
    "$WEB_DIR/wp-content/uploads"
    "$WEB_DIR/cache"
    "$WEB_DIR/logs"
)

echo "[4/4] Imposto permessi speciali su cartelle scrivibili..."
for DIR in "${WRITABLE_DIRS[@]}"; do
    if [ -d "$DIR" ]; then
        echo " - Configuro $DIR"
        sudo chown -R "$GROUP_WEB":"$GROUP_WEB" "$DIR"
        sudo chmod -R 775 "$DIR"
    fi
done

echo "-----------------------------------"
echo "✅ Permessi e proprietari configurati correttamente!"
echo "Consiglio: verifica con 'ls -l $WEB_DIR'"
```