**Project: Sitting up a Secure Apache Web Server on Ubuntu with Virtual Host and SSL**

**Step 1:** System Update & Apache Installation

sudo apt update

Updates your package list.

sudo apt install apache2

Installs Apache web server.

**Step 2:** Create Web Root Directory and Test HTML Page

sudo mkdir -p /var/www/diunextdoor

Creates the folder where your website files will be stored.

sudo chown -R $USER:$USER /var/www/diunextdoor

Gives you ownership of the directory.

echo "<h1>Welcome to DIUNextdoor</h1>" | sudo tee /var/www/diunextdoor/index.html

Creates a simple test HTML page.

**Step 3:** Create Apache Virtual Host Configuration File (HTTP)

sudo nano /etc/apache2/sites-available/diunextdoor.com.conf

Opens a new virtual host config file.

Paste this config:

apache

<VirtualHost \*:80>

ServerAdmin shifat@diunextdoor.com

ServerName diunextdoor.com

ServerAlias www.diunextdoor.com

DocumentRoot /var/www/diunextdoor

ErrorLog ${APACHE\_LOG\_DIR}/diu\_error.log

CustomLog ${APACHE\_LOG\_DIR}/diu\_access.log combined

</VirtualHost>

**Step 4:** Enable the Site & Reload Apache

sudo a2ensite diunextdoor.com.conf

Enables your new site.

sudo systemctl reload apache2

Reloads Apache to apply changes.

**Step 5:** Map Local Domain in `/etc/hosts`

sudo nano /etc/hosts

Adds the domain mapping locally.

Add this line at the bottom:

127.0.0.1 diunextdoor.com www.diunextdoor.com

**Step 6**: Generate Self-Signed SSL Certificate

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \

keyout /etc/ssl/private/diunextdoor.key \

out /etc/ssl/certs/diunextdoor.crt

Creates a private key and SSL certificate valid for 1 year.

**Step 7**: Enable Apache SSL Module

sudo a2enmod ssl

Activates SSL support in Apache.

**Step 8:** Create Apache Virtual Host Configuration File (HTTPS)

sudo nano /etc/apache2/sites-available/diunextdoor-ssl.conf

Paste this config:

apache

<IfModule mod\_ssl.c>

<VirtualHost \*:443>

ServerAdmin shifat@diunextdoor.com

ServerName diunextdoor.com

DocumentRoot /var/www/diunextdoor

SSLEngine on

SSLCertificateFile /etc/ssl/certs/diunextdoor.crt

SSLCertificateKeyFile /etc/ssl/private/diunextdoor.key

ErrorLog ${APACHE\_LOG\_DIR}/error.log

CustomLog ${APACHE\_LOG\_DIR}/access.log combined

</VirtualHost>

</IfModule>

**Step 9:** Enable SSL Site & Restart Apache

sudo a2ensite diunextdoor-ssl.conf

Enables the HTTPS site.

sudo systemctl restart apache2

Restarts Apache to load both HTTP & HTTPS sites.

**Step 10:** (Optional) Test Apache Configuration

sudo apache2ctl configtest

Checks if Apache configuration is valid.

**Step 11:** (Optional) Allow Apache Through Firewall

sudo ufw allow 'Apache Full'

Opens HTTP and HTTPS ports (80 and 443).

**Step 12:** (Optional) Redirect HTTP to HTTPS

Edit the HTTP virtual host config:

sudo nano /etc/apache2/sites-available/diunextdoor.com.conf

Add this inside `<VirtualHost \*:80>`:

apache

Redirect permanent / https://diunextdoor.com/

Then restart Apache:

sudo systemctl restart apache2

**Final Test:**

Open browser:

http://diunextdoor.com` → Redirects to HTTPS (if added)

https://diunextdoor.com` → Secure version (with warning for self-signed SSL)