**SSL Practice**

**What is SSL?**

**SSL (Secure Sockets Layer)** is a **security protocol** that encrypts the data sent between a user's browser and a web server, ensuring confidentiality and integrity. It's used to protect sensitive data like:

* Login credentials
* Payment information
* Personal details

SSL has been officially replaced by **TLS (Transport Layer Security)**, but people still commonly refer to it as SSL.

### How SSL Works (Simplified)

1. **Browser connects to a secure website** (<https://example.com>).
2. The **server sends its SSL certificate** to the browser.
3. The browser checks:
   * Is the certificate valid?
   * Is it signed by a trusted authority?
4. If valid, the browser and server:
   * **Exchange encryption keys** using asymmetric encryption.
   * Establish a **secure session** using symmetric encryption.
5. All further communication is **encrypted**.

### What is an SSL Certificate?

An **SSL Certificate** is a digital certificate that:

* Authenticates a website's identity.
* Enables encryption via HTTPS.
* Is issued by a **Certificate Authority (CA)** (e.g., DigiCert, Let's Encrypt).

#### Common certificate details:

* Domain name
* Certificate issuer
* Expiry date
* Public key

### How to Identify SSL in Use

* URL starts with https://
* Padlock icon in the browser's address bar
* Clicking the padlock shows certificate details

### Practice by creating the SSL

### Step 1: Create a Self-Signed SSL Certificate

sudo openssl req -x509 -nodes -days 365 \

-newkey rsa:2048 \

-keyout /etc/ssl/private/nginx-selfsigned.key \

-out /etc/ssl/certs/nginx-selfsigned.crt

#### When prompted, enter:

* Country, state, etc.
* Common Name: use localhost or your domain

### Step 2: Create a Strong Diffie-Hellman Group (Optional but Recommended)

sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048

### Step 3: Configure NGINX for SSL

Edit your default server block:

sudo nano /etc/nginx/sites-available/default

Replace everything with this minimal SSL config:

nginx

server {

listen 80;

listen [::]:80;

server\_name localhost;

return 301 https://$host$request\_uri;

}

server {

listen 443 ssl;

listen [::]:443 ssl;

server\_name localhost;

ssl\_certificate /etc/ssl/certs/nginx-selfsigned.crt;

ssl\_certificate\_key /etc/ssl/private/nginx-selfsigned.key;

ssl\_dhparam /etc/ssl/certs/dhparam.pem;

ssl\_protocols TLSv1.2 TLSv1.3;

ssl\_ciphers HIGH:!aNULL:!MD5;

root /var/www/html;

index index.html index.htm;

}

### Step 4: Restart NGINX

sudo nginx -t

sudo systemctl reload nginx

### Step 5: Test in Browser

Open your browser and go to:

https://localhost

There will be a warning like **"Your connection is not private"** — this is expected because it's a **self-signed** certificate. Click **Advanced > Proceed**.