

CTP : R4.Cyber.11 HTTP (nginx)

Ce TP vise à sécuriser un service web basé sur le serveur web Nginx en utilisant le protocole TLS/SSL pour chiffrer les données transmises. Les étudiants apprendront à configurer Nginx pour utiliser des certificats SSL, à rediriger le trafic HTTP vers HTTPS et à appliquer des en-têtes de sécurité pour améliorer la protection du site web.

Étapes du travail pratique :

1. Installation et configuration de base de Nginx :

- Installation de Nginx sur un système Linux.
- Configuration d'un site web simple avec Nginx, accessible via HTTP.

2. Sécurisation de Nginx avec SSL/TLS :

- Génération d'un certificat SSL auto-signé ou obtention d'un certificat d'une autorité de certification (comme Let's Encrypt).
- Configuration de Nginx pour utiliser le certificat SSL et activer HTTPS.
- Test de la configuration SSL/TLS.

3. Redirection de HTTP vers HTTPS :

- Configuration de Nginx pour rediriger automatiquement toutes les requêtes HTTP vers HTTPS.
- Test de la redirection.

4. Configuration des en-têtes de sécurité :