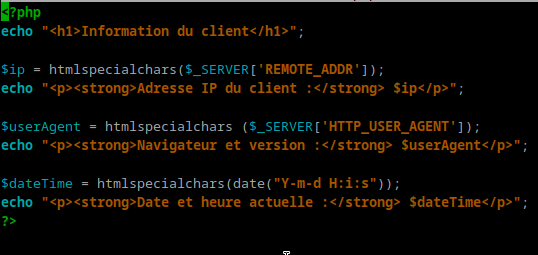
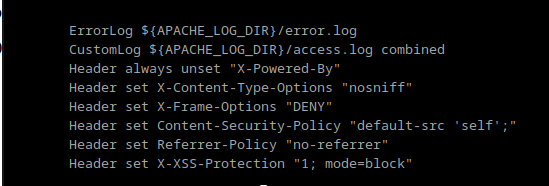
Jalon 20 - INETSRV HTTP

Pour mettre en place le service HTTP, il faut installer apache2 puis php, la version 8.2 pour ce serveur. Le but de ce site web est de récupérer les informations du client qui se connecte comme @IP, le navigateur utilisé, sa version et enfin, l’heure et la date actuelle. Pour cela, il faut créer un script afin de récupérer ses informations. Voici le script index.php créé dans /var/www/html :



Après avoir créé le script, lorsque l’on accéder au site via l’ip du serveur, on obtient les informations du client :



Enfin, il fallait sécuriser le site afin qu’il n’y ait pas d’informations sensibles dans les headers et footers du serveur. Pour cela il faut ajouter des paramètres dans le fichier /etc/apache2/sites-available/000-default.conf : 

**ErrorLog** : Enregistre les erreurs du serveur Apache.

**CustomLog** : Enregistre les accès HTTP en format détaillé.

**X-Powered-By** : Supprime l'en-tête exposant la technologie utilisée (ex : PHP).

**X-Content-Type-Options** : Empêche le navigateur de deviner le type de contenu (évite le MIME sniffing).

**X-Frame-Options** : Empêche l'affichage du site dans une iframe (protège contre le clickjacking).

**Content-Security-Policy** : Limite le chargement de contenu externe (protège contre le XSS).

**Referrer-Policy** : Ne transmet pas l'origine de la requête (renforce la confidentialité).

**X-XSS-Protection** : Active la protection contre le XSS dans le navigateur.

Mise en place de HTTPS :

Génération d'une clé privée et d'une demande de certificat (CSR)

* Objectif : Obtenir un certificat SSL/TLS valide pour sécuriser les échanges.

Commande :  
openssl req -new -newkey rsa:2048 -nodes -keyout monsite.key -out monsite.csr

* + -newkey rsa:2048 : Crée une nouvelle clé RSA de 2048 bits.
  + -keyout : Génère le fichier de clé privée.
  + -out : Génère le fichier CSR (Certificate Signing Request).

**Envoi de la demande CSR à une autorité de certification (CA)**

* Théorie :
  + Le fichier CSR est envoyé à une autorité de certification (CA) reconnue (ex : Let's Encrypt, Sectigo, GlobalSign).
  + La CA vérifie l'identité du domaine (via un challenge DNS, HTTP ou validation manuelle).
* Résultat : La CA délivre un certificat signé (monsite.crt).

Installation du certificat sur le serveur Apache

* Place les fichiers générés (clé privée, certificat signé et certificat intermédiaire) dans un répertoire sécurisé, par exemple /etc/ssl/.

**Configure le fichier VirtualHost Apache pour activer HTTPS :**  
  
<VirtualHost \*:443>

ServerName monsite.com

SSLEngine on

SSLCertificateFile /etc/ssl/monsite.crt

SSLCertificateKeyFile /etc/ssl/monsite.key

SSLCertificateChainFile /etc/ssl/intermediate.crt

DocumentRoot /var/www/html

</VirtualHost>

* + SSLCertificateFile : Chemin du certificat signé.
  + SSLCertificateKeyFile : Chemin de la clé privée.
  + SSLCertificateChainFile : Chaîne de confiance (certificat intermédiaire)