

Apache

Toujours s'assurer d'avoir la dernière mise à jour du logiciel

Prevoir un page pour les erreurs 404

`htpasswd` Permet de créer et de maintenir les fichiers textes où sont stockés les noms d'utilisateurs et mots de passe pour l'authentification de base des utilisateurs HTTP

`htaccess` Fichier qui permet d'appliquer sa configuration http aux répertoires et sous répertoires d'où il se trouve

`mod-security` Parefeu applicatif dont le rôle est de filtrer les requêtes entrant sur un serveur HTTP Apache

Mise en place de sauvegardes du site web sur un support séparé et idéalement dans un autre lieu

`/var/log/apache2/error.log` Fichier des journaux d'erreur d'Apache

`/var/log/apache2/access.log` Fichier des journaux des demandes entrantes et traitées d'Apache.

`/etc/apache2/conf.d/security` Contient les informations fournis par Apache

`/etc/php5/apache2/php.ini` Fichier de configuration de PHP sur Apache

PHP

Utiliser les framework adaptés au langages

Toujours maintenir PHP à jour

Never Trust User Input

Effectuer une vérification des formulaire coté serveur en plus du coté client

apache2.conf

`ServerTokens Prod` & `ServerSignature` Options à entrer dans le fichier `security` pour limiter les informations fournies par Apache

`expose_php off` Rajouter dans `php.ini` pour désactiver php

apache2.conf (cont)

`Order deny, allow` & `Deny from all` Tout interdire par défaut (dans le fichier `apache2.conf`)

`Allow From IP` Limiter l'accès au répertoire seulement à l'IP souhaitée

`Options -Indexes` Empêche le parcours des répertoires (à ajouter dans le fichier `apache2.conf`)

`Options -ExecCGI` Permet de désactiver la possibilité d'exécuter des scripts CGI

`Options -FollowSymLinks` Permet d'empêcher Apache de suivre les liens symboliques

`MaxClients` Permet de limiter le *nombre* de connexions simultanées

`MaxKeepAliveRequests` Permet de limiter le *nombre* de connexions persistantes

php.ini

`register_globals` off Les variables EGPCS (Environment, GET, POST, Cookie, Server) ne seront pas enregistrées comme des variables globales

`safe_mode` 1 Empêche un script d'accéder à des fichiers situés en dehors du dossier où se trouve le site

`display_errors` off Désactiver l'affichage des erreurs pour éviter d'afficher des informations aux utilisateurs

`magic_quotes_gpc` on Ajoute le caractère `"\"` devant les apostrophes, les guillemets et le caractère nul. Empêche le système d'interpréter une requête saisie dans un formulaire HTML

`session.save_path` Répertoire dans lequel sont enregistrés les identifiants temporairement (mettre un *répertoire* non accessible depuis le site web)

`session.use_only_cookies` Le système lit les informations d'identifiant uniquement à partir des cookies

`= 1`

