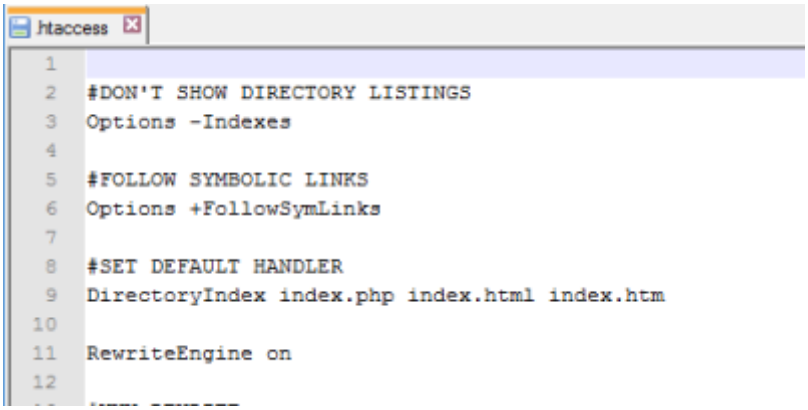
Le fichier ".htaccess"



Le **.htaccess** (Hypertext Access) est un fichier de **configuration** qui permet de modifier les paramètres du serveur **Apache** sans avoir à modifier directement ses fichiers de configuration principaux. Il agit sur le **répertoire** où il est placé ainsi que sur tous ses sous-**répertoires**.

Le fichier **.htaccess** n'est pas l'unique moyen de configurer son serveur WEB, néanmoins c'est la solution si la configuration d'**Apache** n'est pas accessible par exemple pour les hébergements **VPS**.

Créer le fichier .htaccess

Il s'uffit de créer un fichier nommée “.htaccess” sans extension à la racine du site web.

Le fichier peut-etre créer dans un autre répertoire mais la configuration ne prendra effet que sur le repertoire courant et ces sous répertoires et non les dossiers précèdents.

Interdire l'accès au fichier

Le fichier doit etre impérativement sécuriser car il contient des règles et configurations importantes qui contrôlent le comportement et l'accès à votre site web. Si un pirate informatique y accède, il pourrait:

- Modifier les règles d'accès et d'autorisations, compromettant ainsi la sécurité globale du site.
- Injecter du code malveillant pour rediriger les visiteurs vers des sites malveillants.

- Désactiver des mesures de sécurité existantes, rendant le site vulnérable aux attaques.

Même si le fichier n'est pas disponible en écriture il falicitera le travail de Forensic.

Pour le protéger il faut rajouter ces lignes dans le fichier :

```
<Files .htaccess>
Order Allow,Deny
Deny from all
</Files>
```

N'importe quels autres fichiers comme par exemple le info.php peuvent être interdits.

```
<Files info.php>
Order Allow,Deny
Deny from all
</Files>
```

Interdire l'affichage du contenu des répertoires

“Options -Indexes” est une mesure de sécurité simple mais efficace qui aide à protéger votre site web contre divers risques tout en améliorant son professionnalisme et son optimisation pour les moteurs de recherche.

```
Options -Indexes
```

Configurer l'en-tête HSTS (Autoriser uniquement HTTPS)

Le HSTS (HTTP Strict Transport Security) est un mécanisme de sécurité web qui sert à plusieurs fins importantes :

- Il oblige les navigateurs à utiliser uniquement des connexions HTTPS sécurisées pour accéder au site web.
- Toutes les requêtes HTTP sont automatiquement converties en HTTPS par le navigateur.

Il peut être configurer dans le fichier .htaccess

```
<IfModule mod_headers.c>
    Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload"
</IfModule>
```

- Active HSTS pour votre domaine

- Définit une durée de 1 an (31536000 secondes)
- Inclut les sous-domaines
- Ajoute l'option “preload” pour une sécurité maximale

Configurer redirection de pages

Il est possible de configurer les redirection WEB par exemple la redirection suite à une erreur 404.

```
ErrorDocument 404 /404.html
```

D'autres redirections sont configurables comme par exemple lors d'un changement de nom de domaine il est possible de rediriger les requêtes de l'ancien domaine vers le nouveau.

```
RewriteEngine On
RewriteCond %{HTTP_HOST} ^anciendomaine.com$ [OR]
RewriteCond %{HTTP_HOST} ^www.anciendomaine.com$
RewriteRule (.*)$ https://www.nouveaudomaine.com/$1 [R=301,L]
```

Outils pour créer un .htaccess

Des outils existe pour aider a générer une base d'un fichier .htaccess.

https://websitesetup.org/tools/htaccess-generator/

https://www.seoptimer.com/fr/htaccess-generator