

Sécuriser Apache2

Attention, ce n'est pas exhaustif



Cacher la version d'Apache2

Permet de cacher la version d'Apache.
A mettre dans `/etc/apache2/apache2.conf`

```
ServerSignature Off  
ServerTokens Prod
```

Protéger les fichiers d'Apache2

Cela va empêcher la navigation dans les fichiers des sites.
Normalement, il n'y aura aucun effet de bord.

Modifier **apache2.conf** comme ceci :

```
156. <Directory />  
157.     Options None  
158.     Order deny,allow  
159.     Deny from all  
160. </Directory>  
161.  
162. <Directory /var/www/>  
163.     Options -Indexes +FollowSymLinks  
164.     AllowOverride None  
165.     Require all granted  
166. </Directory>
```

Puis dans chaque VirtualHosts comme ceci :

```
20. <Directory "/var/www/XXX">  
21.     Order allow,deny  
22.     Allow from all  
23. </Directory>
```

Protéger le Brute Force

Cela BAN les IP (avec IPTABLES) des personnes effectuant trop de requêtes sur un même site.

Cela utilise un mod qu'il faut installer :

```
# apt install libapache2-mod-evasive
```

puis créer l'emplacement des logs :

```
# mkdir /var/log/mod_evasive && chown www-data:www-data  
/var/log/mod_evasive/
```

puis configurer le fichier de conf */etc/apache2/mods-available/evasive.conf* :

[evasive.conf](#)

```
<IfModule mod_evasive20.c>  
    D0SHashTableSize 3097  
    D0SPageCount 10  
    D0SSiteCount 150  
    D0SPageInterval 1  
    D0SSiteInterval 1  
    D0SBlockingPeriod 3600  
    D0SLogDir /var/log/mod_evasive  
    D0SEmailNotify hostname@domain.tld  
    D0SWhitelist 127.0.0.1  
</IfModule>
```

et pour finir activer le mod et redémarrer apache2

```
# a2enmod evasive && systemctl restart apache2
```

plus d'info [ici](#)

From:
<https://wiki.virtit.fr/> - **VirtIT**

Permanent link:
https://wiki.virtit.fr/doku.php/kb:linux:apache2:securiser_apache2

Last update: **2018/05/17 21:19**

