

# 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>  
DOSHashTableSize 3097  
DOSPageCount 10  
DOSSiteCount 150  
DOSPageInterval 1  
DOSSiteInterval 1  
DOSBlockingPeriod 3600  
DOSLogDir /var/log/mod_evasive  
DOSEmailNotify hostname@domain.tld  
DOSWhitelist 127.0.0.1  
</IfModule>
```

et pour finir activer le mod et redémarrer apache2

```
# a2enmod evasive  
# /etc/init.d/apache2 restart
```

plus d'info [ici](#)

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

Permanent link:  
[https://wiki.virtit.fr/doku.php/kb:linux:apache2:securiser\\_apache2?rev=1526589166](https://wiki.virtit.fr/doku.php/kb:linux:apache2:securiser_apache2?rev=1526589166)

Last update: **2018/05/17 20:32**

