

# Installation de dokuwiki

## Liste des plugins:

- Pour le wysiwyg [Prosemirror](#) a évaluer.
- Ou encore CGK editor

# Installation de wallabag



Au 08/2020 wallabag n'est pas compatible PHP 7.4 (je crois sur wallabag 2.3 et il faut attendre la 2.4.

Un petit bug qui traîne : <https://github.com/wallabag/wallabag/issues/2768>

## Et la solution

```
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
```

# Hardening TLS Apache2

Hardening de base : <https://wiki.debian.org/Apache/Hardening>

Evaluation de base :

<https://www.ssllabs.com/ssltest/analyze.html?d=alban.montaigu.io&s=163.172.180.167>

La partie hardening TLS : [https://httpd.apache.org/docs/trunk/ssl/ssl\\_howto.html](https://httpd.apache.org/docs/trunk/ssl/ssl_howto.html)

```
SSLProtocol    all -SSLv3 -TLSv1 -TLSv1.1
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-
ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-
SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
SHA256
SSLHonorCipherOrder on
SSLCompression off
SSLSessionTickets off
```

Activation DNS CAA :

<https://blog.qualys.com/product-tech/2017/03/13/caa-mandated-by-cabrowser-forum>

Autre tuto intéressant :

<https://community.bitnami.com/t/howto-a-on-all-tests-at-ssllabs-com-with-apache-2-4-xx/67885> mais a priori trop violent pour les vieux matériels

Activation hsts aussi :

<https://www.justegeek.fr/activer-len-tete-hsts-sur-apache-pour-proteger-son-site-web/?cn-reloaded=1>

```
nano /etc/apache2/conf-enabled/security.com
```

```
ServerTokens Prod
ServerSignature Off
```

```
Header set X-Content-Type-Options: "nosniff"
```

```
Header set X-Frame-Options: "sameorigin"
```

Aller plus loin dans les resultats SSLabs :

<https://community.bitnami.com/t/howto-a-on-all-tests-at-ssllabs-com-with-apache-2-4-xx/67885>

Une piste pour améliorer la compliance :

[https://developer.mozilla.org/fr/docs/Web/Security/Public\\_Key\\_Pinning](https://developer.mozilla.org/fr/docs/Web/Security/Public_Key_Pinning)

Une autre poste encore : <https://gist.github.com/GAS85/42a5469b32659a0aecc60fa2d4990308>

```
openssl dhparam -out /etc/ssl/certs/dhparam.pem 4096
```

Pinning : <https://gist.github.com/GAS85/a668b941f84c621a15ff581ae968e4cb>

```
cat /etc/letsencrypt/live/alban.montaigu.io/cert.pem | openssl x509 -pubkey
| openssl pkey -pubin -outform der | openssl dgst -sha256 -binary | base64
```

Aussi a voir ca :

- <https://community.letsencrypt.org/t/how-to-get-100-on-ssllabs-com-with-nginx/114196>
- <https://community.letsencrypt.org/t/howto-a-with-all-100-s-on-ssl-labs-test-using-nginx-mainline-stable/55033>
- <https://serverfault.com/questions/877774/trying-to-get-100-in-ssllabs-com-key-exchange/877784>
- <https://itigloo.com/2017/02/21/how-to-get-an-a-rating-with-100-score-on-the-ssllabs-test-with-apache/>
- <https://security.stackexchange.com/questions/166484/how-to-disable-cbc-mode-ciphers>
- [https://wiki.csnu.org/index.php/S%C3%A9curisation\\_SSL\\_TLS\\_de\\_apache](https://wiki.csnu.org/index.php/S%C3%A9curisation_SSL_TLS_de_apache)

Pas mal mas de weak et une compatibilité générale pas trop moche :

```
SSLCipherSuite
ALL:!RSA:!CAMELLIA:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4:!S
HA1:!SHA256:!SHA384
```

```
# HSTS Header always set Strict-Transport-Security "max-age=31536000;  
includeSubDomains; preload"
```

La référence :

<https://ssl-config.mozilla.org/#server=apache&version=2.4.41&config=intermediate&openssl=1.1.1d&guideline=5.6>

Le fichier complet (avec quelques spécificités moches dues au template ispcnfig):

```
<IfModule mod_ssl.c>  
SSLEngine on  
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1  
SSLOpenSSLConfCmd ECDHParameters secp384r1  
SSLOpenSSLConfCmd Curves secp521r1:secp384r1  
SSLOpenSSLConfCmd DHParameters "/etc/ssl/certs/dhparam.pem"  
SSLCipherSuite ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-  
GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-  
ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-  
SHA256:DHE-RSA-AES256-GCM-SHA384  
SSLHonorCipherOrder off  
SSLCompression off  
SSLSessionTickets off  
SSLCertificateFile  
/var/www/clients/client1/web2/ssl/alban.montaigu.io-le.crt  
SSLCertificateKeyFile  
/var/www/clients/client1/web2/ssl/alban.montaigu.io-le.key  
SSLUseStapling on  
SSLStaplingResponderTimeout 5  
SSLStaplingReturnResponderErrors off  
  
# Enhance header configuration  
<IfModule mod_headers.c>  
Header always set Content-Security-Policy "upgrade-insecure-  
requests;"  
Header always set Strict-Transport-Security "max-age=31536000;  
includeSubDomains; preload"  
# Rewrite any session cookies to make them more secure  
# Make ALL cookies created by this server are HttpOnly and Secure  
Header always edit Set-Cookie (.*) "$1;HttpOnly;Secure"  
Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure  
</IfModule>
```

```
<IfModule mod_ssl.c>  
SSLStaplingCache shmcb:/var/run/ocsp(128000)  
</IfModule>
```

Intéressant a voir en spécifique ISPCONFIG : <https://git.ispconfig.org/ispconfig/ispconfig3/-/issues/5368>

Pour permettre l'utilisation de certificats sur plusieurs domaines avec nameservers

```
SSLOpenSSLConfCmd Curves X25519:secp521r1:secp384r1
```



La partie **X25519** est particulièrement importante sinon les autres domaines ne fonctionneront pas.

From:  
<https://wiki.montaigu.io/> - **Alban's Wiki**

Permanent link:  
[https://wiki.montaigu.io/doku.php?id=guide:installation\\_serveur\\_2020&rev=1599944610](https://wiki.montaigu.io/doku.php?id=guide:installation_serveur_2020&rev=1599944610)

Last update: **2021/04/18 20:24**

