configuración apache

directivas para securizar

- evitar listado directorios `Options -Indexes`
- permitir .htaccess: (/etc/apache/sites-available/default)`AllowOverride All`
- evitar información del servidor (/etc/apache/conf.d/security):
  - `ServerSignature Off`
  - `ServerTokens Prod`
- securizar galletas (via https) para evitar XSS
  - en `/etc/php5/apache2/php.ini`, cambiar estas dos variables a true:
    - `session.cookie_httponly = True session.cookie_secure = True`
  - modificar `/etc/apache2/mods-enabled/headers.load`:
    - `Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure`

módulos para securizar

- mod_security
- mod_qos
- http://www.juliojosesanz.com/dos-modulos-de-seguridad-esenciales-para-apache-mod_security-y-mos_qos/
- mod_status
- `$ sudo apt-get install libapache2-mod-security $ sudo a2enmod mod-security $ sudo /etc/init.d/apache2 force-reload`
  - /vía: https://www.modsecurity.org/
  - modsecurity console: http://waf-fle.org/
- http://yuniervp.bligoo.es/mejorar-la-seguridad-de-apache

httpd.conf, trucos

- se pueden utilizar variables de entorno de BASH para configurar el apache, permitiendo tener una «plantilla» para usar en varios servidores (o ficheros INCLUDE)
  - dentro del httpd.conf, usar:

```
User = ${VARIABLE}
```

  - en el bash:

```
VARIABLE="apache"
```