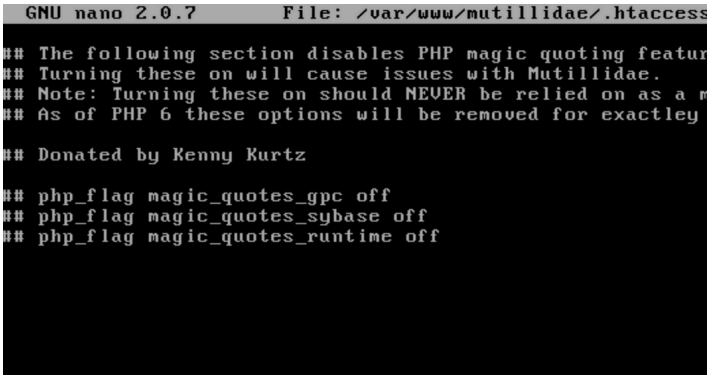
Mettre en place des contre-mesures

DOCUMENT CREATED
BY ERICSSON

CYBERSÉCURITÉ

Étape 1 : Metasploitable, configure un VirtualHost HTTPS pour Mutillidae.



Modifie le fichier **.htaccess :**

nano /var/www/mutillidae/.htaccess

Mets en commentaire les lignes commençant par php_flag.

Étape 2 : Configurer un VirtualHost HTTPS

```
  GNU nano 2.0.7            File: default-ssl                      Modif

<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin admin@mutillidae.local
                ServerName mutillidae.local
                DocumentRoot /var/www/mutillidae

                SSLEngine on
                SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoi.pem
                SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                        SSLOptions +StdEnvVars
                </FilesMatch>

                <Directory /usr/lib/cgi-bin>
                        SSLOptions +StdEnvVars
                </Directory>

                BrowserMatch "MSIE [2-6]" \
                        nokeepalive ssl-unclean-shutdown \
```

```
  GNU nano 2.0.7            File: default-ssl

                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                        SSLOptions +StdEnvVars
                </FilesMatch>

                <Directory /usr/lib/cgi-bin>
                        SSLOptions +StdEnvVars
                </Directory>

                BrowserMatch "MSIE [2-6]" \
                        nokeepalive ssl-unclean-shutdown \
                        downgrade-1.0 force-response-1.0

                BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
        </VirtualHost>
</IfModule>
```

Va dans le répertoire où sont stockés les fichiers de configuration d'Apache :

cd /etc/apache2/sites-enabled

Crée un nouveau fichier nommé default-ssl :

nano default-ssl

Étape 3 : Activer SSL dans Apache

```
Usage: apache2 [-D name] [-d directory] [-f file]
               [-C "directive"] [-c "directive"]
               [-k start|restart|graceful|graceful-stop|stop]
               [-v] [-V] [-h] [-l] [-L] [-t] [-S] [-X]
Options:
  -D name             : define a name for use in <IfDefine name> directi
  -d directory        : specify an alternate initial ServerRoot
  -f file             : specify an alternate ServerConfigFile
  -C "directive"      : process directive before reading config files
  -c "directive"      : process directive after reading config files
  -e level            : show startup errors of level (see LogLevel)
  -E file             : log startup errors to file
  -v                  : show version number
  -V                  : show compile settings
  -h                  : list available command line options (this page)
  -l                  : list compiled in modules
  -L                  : list available configuration directives
  -t -D DUMP_VHOSTS   : show parsed settings (currently only vhost setti
  -S                  : a synonym for -t -D DUMP_VHOSTS
  -t -D DUMP_MODULES  : show all loaded modules
  -M                  : a synonym for -t -D DUMP_MODULES
  -t                  : run syntax check for config files
  -X                  : debug mode (only one worker, do not detach)
msfadmin@metasploitable:/etc/apache2/sites-enabled$ _
```

Active le module SSL dans Apache :

a2enmod ssl

Active le site par défaut SSL :

a2ensite default-ssl

Redémarre le service Apache pour appliquer les modifications :

service apache2 restart