

```
#-----
# Proteção do arquivo .htaccess
#-----
<Files .htaccess>
order allow,deny
deny from all
</Files>

#-----
# Páginas de error personalizadas
#-----
ErrorDocument 400 http://exemplo.com.br/index.php
ErrorDocument 401 http://exemplo.com.br/index.php
ErrorDocument 403 http://exemplo.com.br/index.php
ErrorDocument 404 http://exemplo.com.br/index.php
ErrorDocument 500 http://exemplo.com.br/index.php

#-----
# Use codificação UTF-8 para qualquer coisa como text/plain ou text/html
#-----
AddDefaultCharset utf-8

#-----
# Força UTF-8 para um número de formatos de arquivo
#-----
AddCharset utf-8 .atom .css .js .json .rss .vtt .xml

#-----
# Desativar pesquisa nos diretórios dos sites
#-----
Options All -Indexes

#-----
# Ativa mod_rewrite usado em filtros contra certos robôs piratas
#-----
RewriteEngine On

#-----
# Exceção de tipos de arquivos que robôs podem acessar
#-----
RewriteCond %{REQUEST_URI} !^/robots.txt
```

```

RewriteCond %{REQUEST_URI} ! /robots.txt
RewriteCond %{REQUEST_URI} ! ^/sitemap.xml

#-----
# Bloqueio contra softwares que baixam páginas do site para navegação off-line
#-----
RewriteCond %{HTTP_USER_AGENT} ^-?$ [OR]

#-----
# Bloqueio contra tipos de requisição gerados por robôs
#-----
RewriteCond %{HTTP_USER_AGENT} ^curl|^Fetch|^API|^Request|^GT|^\\:|^WWW|^HTTP|^\\:|^Lite|^http|^lib|^
RewriteRule (.*) - [F]

#-----
# O arquivo index.php vai ser o padrão do diretório raiz
#-----
DirectoryIndex index.php

#-----
# Proíbe que outros tipos de arquivos sejam utilizados como index
#-----
<Files ~ "^(index)\\. (p?s?x?htm?|txt|asp|x?|cfm|?|cgi|pl|php[3-9]|js|xml)$">
order allow,deny
deny from all
</Files>

#-----
# Arquivos permitidos a serem executados no servidor e proibidos pela web
#-----
<Files ~ "\.(incl|class|sql|ini|conf|exel|dll|bin|tpl|bkp|dat|cl|hl|py|spdl|themel|module)$">
deny from all
</Files>

#-----
# Proíbe a exibição de certos arquivos de configuração como login, config, adm
#-----
<Files ~ "^(install?|admin|(wp-)?config(\\.inc)?|configure|configuration|login|logging|option
9.|pl|php|shell|ssh|root|cmd|[0-9]{1,6}|test|data)\\. (p?s?x?htm?|?|txt|asp|x?|cfm|?|cgi|pl|php[
order allow,deny
deny from all

```

</Files>

#-----
Código para neutralizar URLs falsas
#-----

```
RedirectMatch gone ^/_vti.*
RedirectMatch gone ^/MSOffice.*
RedirectMatch gone ^[-_a-z0-9/\.]*/.*
RedirectMatch gone ^.*etc/passwd.*
```

#-----
Filtro contra XSS, redirecionamento HTTP, base64_encode, injeção sql simples
#-----

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} (GET|POST) [NC]
RewriteCond %{QUERY_STRING} ^(.*)(<|>)?script(.*)$ [NC,OR]
RewriteCond %{QUERY_STRING} ^(.*)(<|>)?javascript(%3A|:)(.*)$ [NC,OR]
RewriteCond %{QUERY_STRING} ^(.*)document\.location\.href(.*)$ [OR]
RewriteCond %{QUERY_STRING} ^(.*)(<|>)?http(%3A|:)(/|/ %2F)(2)(.*)$ [NC,OR]
```

#-----
Cuidado e atenção com essa regra pois ela pode quebrar redirecionamentos
#-----

```
RewriteCond %{QUERY_STRING} ^(.*)base64_encode(.*)$ [OR]
RewriteCond %{QUERY_STRING} ^(.*)GLOBALS(=[| |%[0-9A-Z]{0,2}))(.*)$ [OR]
RewriteCond %{QUERY_STRING} ^(.*)_REQUEST(=[| |%[0-9A-Z]{0,2}))(.*)$ [OR]
RewriteCond %{QUERY_STRING} ^(.*)(<|>)?(SELECT(%20| |)+| UNION(%20| |)+ ALL| INSERT(%20| |)+| DELETE(%20| |)+| )$ [OR]
RewriteRule (.*) - [F]
```

#-----
Filtro contra phpshell.php, RemoteView, C99.php, r57.php, etc
#-----

```
RewriteEngine On
RewriteCond %{REQUEST_URI} .*((php|my)?shell|remview.*|phpremoteview.*|sshphp.*|pcom|nstview
RewriteCond %{REQUEST_METHOD} (GET|POST) [NC]
RewriteCond %{QUERY_STRING} ^(.*)=/home/wwwindus/public_html/(.*)$ [OR]
RewriteCond %{QUERY_STRING} ^work_dir=. *$ [OR]
RewriteCond %{QUERY_STRING} ^command=. *&output.*$ [OR]
RewriteCond %{QUERY_STRING} ^nts_[a-z0-9_]{0,10}=. *$ [OR]
RewriteCond %{QUERY_STRING} ^(.*)cmd=. *$ [OR]
```



```

RewriteCond %{QUERY_STRING} union\([\^s]*s)+select \[NC,OR]
RewriteCond %{QUERY_STRING} union\([\^a]*a)+11\([\^s]*s)+select \[NC,OR]
RewriteCond %{QUERY_STRING} (;|<|>|'|\"|\)|%0A|%0D| %22| %27| %3C| %3E| %00).*(\/\*| union| select| ir
RewriteCond %{QUERY_STRING} (sp_executesql) \[NC]
RewriteRule ^(.*)$ - [F,L]

```

```

#-----
# Proteção dedicada exclusivamente a SQL Injection
#-----

```

```

RewriteRule ^.*EXEC\(@.*$ - [R=404,L,NC]
RewriteRule ^.*CAST\(.*$ - [R=404,L,NC]
RewriteRule ^.*DECLARE.*$ - [R=404,L,NC]
RewriteRule ^.*DECLARE%20.*$ - [R=404,L,NC]
RewriteRule ^.*NVARCHAR.*$ - [R=404,L,NC]
RewriteRule ^.*sp_password.*$ - [R=404,L,NC]
RewriteRule ^.*%20xp_.*$ - [R=404,L,NC]

```

```

#-----
# Protege contra ataque DOS, limitando o tamanho de upload de arquivos
#-----

```

```

LimitRequestBody 10240000

```

```

#-----
# Força a compressão de arquivos a serem enviados para o navegador
#-----

```

```

<IfModule mod_deflate.c>

```

```

    # Force compression for mangled headers.
    # http://developer.yahoo.com/blogs/ymn/posts/2010/12/pushing-beyond-gzipping

```

```

    <IfModule mod_setenvif.c>
        <IfModule mod_headers.c>
            SetEnvIfNoCase ^(\Accept-Encoding|X-cept-Encoding|X(15)|^(15)|-(15))$ ^((gzip|deflate|
            RequestHeader append Accept-Encoding "gzip, deflate" env=HAVE_Accept-Encoding
        </IfModule>
    </IfModule>

```

```

    # Compress all output labeled with one of the following MIME-types
    # (for Apache versions below 2.3.7, you don't need to enable 'mod_filter'
    # and can remove the '<IfModule mod_filter.c>' and '</IfModule>' lines
    # as 'AddOutputFilterByType' is still in the core directives).

```

```

    <IfModule mod_filter.c>

```

```
AddOutputFilterByType DEFLATE application/atom+xml \
                                application/javascript \
                                application/json \
                                application/rss+xml \
                                application/vnd.ms-fontobject \
                                application/x-font-ttf \
                                application/x-web-app-manifest+json \
                                application/xhtml+xml \
                                application/xml \
                                font/opentype \
                                image/svg+xml \
                                image/x-icon \
                                text/css \
                                text/html \
                                text/plain \
                                text/x-component \
                                text/xml
```

```
</IfModule>
```

```
</IfModule>
```

```
#-----
# Controle do Cache-Control e Expires Header no navegador
#-----
```

```
<ifModule mod_headers.c>
    <filesMatch "\.(ico|jpe?g|png|gif|swf)$">
        Header set Cache-Control "public"
    </filesMatch>
    <filesMatch "\.(css)$">
        Header set Cache-Control "public"
    </filesMatch>
    <filesMatch "\.(js)$">
        Header set Cache-Control "private"
    </filesMatch>
    <filesMatch "\.(x?html?|php)$">
        Header set Cache-Control "private, must-revalidate"
    </filesMatch>
</ifModule>
```

```
#-----
# Força a utilização do Cache-Control e Expires Header no navegador
```

```

#-----
<IfModule mod_headers.c>
    Header unset ETag
</IfModule>
FileETag None

<IfModule mod_expires.c>
    ExpiresActive on
    ExpiresDefault "access plus 1 month"

# CSS
    ExpiresByType text/css "access plus 4 hour"

# Data interchange
    ExpiresByType application/json "access plus 0 seconds"
    ExpiresByType application/xml "access plus 0 seconds"
    ExpiresByType text/xml "access plus 0 seconds"

# Favicon (cannot be renamed!)
    ExpiresByType image/x-icon "access plus 1 week"

# HTML components (HTCs)
    ExpiresByType text/x-component "access plus 1 month"

# HTML
    ExpiresByType text/html "access plus 0 seconds"

# JavaScript
    ExpiresByType application/javascript "access plus 1 year"

# Manifest files
    ExpiresByType application/x-web-app-manifest+json "access plus 0 seconds"
    ExpiresByType text/cache-manifest "access plus 0 seconds"

# Media
    ExpiresByType audio/ogg "access plus 1 month"
    ExpiresByType image/gif "access plus 4 hour"
    ExpiresByType image/jpeg "access plus 4 hour"
    ExpiresByType image/png "access plus 4 hour"
    ExpiresByType video/mp4 "access plus 1 month"
    ExpiresByType video/ogg "access plus 1 month"

```

```
ExpiresByType video/webm "access plus 1 month"

# Web feeds
ExpiresByType application/atom+xml "access plus 1 hour"
ExpiresByType application/rss+xml "access plus 1 hour"

# Web fonts
ExpiresByType application/font-woff2 "access plus 1 month"
ExpiresByType application/font-woff "access plus 1 month"
ExpiresByType application/vnd.ms-fontobject "access plus 1 month"
ExpiresByType application/x-font-ttf "access plus 1 month"
ExpiresByType font/opentype "access plus 1 month"
ExpiresByType image/svg+xml "access plus 1 month"
</IfModule>
```