```
# Allow access to web fonts from all domains.
<IfModule mod_headers.c>
    <FilesMatch "\.(eot|otf|tt[cf]|woff)$">
        Header set Access-Control-Allow-Origin "*"
    </FilesMatch>
</IfModule>

# Prevent Apache from returning a 404 error as the result of a rewrite
# when the directory with the same name does not exist.
Options -MultiViews

# Customize what Apache returns to the client in case of an error.
ErrorDocument 404 /resources/404.html
ErrorDocument 403 /resources/403.html

# Use UTF-8 encoding for anything served as text/html or text/plain.
AddDefaultCharset utf-8

# Turn on the rewrite engine and enable the FollowSymLinks option
<IfModule mod_rewrite.c>
    Options +FollowSymlinks
  # Options +SymLinksIfOwnerMatch
    RewriteEngine On
  # RewriteBase /
</IfModule>

# Rewrite http://www.example.com -> https://example.com
<IfModule mod_rewrite.c>
    RewriteCond %{HTTPS} off
    RewriteRule .* https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
    RewriteCond %{HTTP_HOST} ^www\.(.+)$ [NC]
    RewriteRule ^ http://%1%{REQUEST_URI} [L,R=301]
</IfModule>

# Block access to directories without a default document.
<IfModule mod_autoindex.c>
    Options -Indexes
</IfModule>

# Block access to hidden files and directories.
<IfModule mod_rewrite.c>
```

```
<IfModule mod_rewrite.c>
    RewriteCond %{SCRIPT_FILENAME} -d [OR]
    RewriteCond %{SCRIPT_FILENAME} -f
    RewriteRule "(^|/)\." - [F]
</IfModule>

# Block access to files that can expose sensitive information.
<FilesMatch "(^#.*#|\.(bak|config|dist|fla|in[ci]|log|psd|sh|sql|sw[op])|~)$">

    # Apache < 2.3
    <IfModule !mod_authz_core.c>
        Order allow,deny
        Deny from all
        Satisfy All
    </IfModule>

    # Apache ≥ 2.3
    <IfModule mod_authz_core.c>
        Require all denied
    </IfModule>

</FilesMatch>
```