

```
DirectoryIndex index.php
AddDefaultCharset UTF-8
DefaultLanguage en-US
SetEnv TZ Europe/Rome
```

```
# MIXED #####
```

```
ServerSignature Off
FileETag MTime Size
```

```
# PROTECT FROM FLOOD
```

```
LimitRequestBody 10485760
```

```
# MISPELLING #####
```

```
<IfModule mod_speling.c>
    CheckSpelling On
</IfModule>
```

```
# .HTACCESS #####
```

```
<Files .htaccess>
    Order Allow,Deny
    Deny from all
</Files>
```

```
# REWRITE #####
```

```
<IfModule mod_rewrite.c>
    RewriteEngine On

    RewriteCond %{REQUEST_FILENAME} -s [OR]
    RewriteCond %{REQUEST_FILENAME} -l [OR]
    RewriteCond %{REQUEST_FILENAME} -d
    RewriteRule ^.+ $ - [NC,L]

    RewriteRule ^(.*)\.(css|js)$ /minify/index.php?f=$1.$2 [L]
    RewriteRule ^css/font/(.+)$ /fonts/font-awesome/$1 [L]
    RewriteRule .* /index.php [QSA,L]
</IfModule>
```

```
# SECURITY #####
```

```
<IfModule mod_security.c>
    SecFilterEngine On
    SecFilterEngine On
```

```
SecAuditEngine RelevantOnly
```

```
SecFilterCheckURLEncoding On
```

```
SecFilterCheckCookieFormat On
```

```
SecAuditLog /path/to/silex/tmp/logs/audit.log
```

```
SecFilterDefaultAction "deny,log,auditlog,status:406"
```

```
Include /path/to/silex/src/modsecurity_crs_10_config.conf
```

```
Include /path/to/silex/lib/OWASP-
```

```
CRS/base_rules/modsecurity_crs_20_protocol_violations.conf
```

```
Include /path/to/silex/lib/OWASP-
```

```
CRS/base_rules/modsecurity_crs_21_protocol_anomalies.conf
```

```
Include /path/to/silex/lib/OWASP-
```

```
CRS/base_rules/modsecurity_crs_40_generic_attacks.conf
```

```
Include /path/to/silex/lib/OWASP-CRS/base_rules/modsecurity_crs_42_tight_security.conf
```

```
Include /path/to/silex/lib/OWASP-CRS/base_rules/modsecurity_crs_41_sql_injection.conf
```

```
Include /path/to/silex/lib/OWASP-CRS/base_rules/modsecurity_crs_41_xss.conf
```

```
Include /path/to/silex/lib/OWASP-
```

```
CRS/base_rules/modsecurity_crs_41_phpids_converter.conf
```

```
Include /path/to/silex/lib/OWASP-CRS/base_rules/modsecurity_crs_41_phpids_filters.conf
```

```
Include /path/to/silex/lib/OWASP-CRS/base_rules/modsecurity_crs_45_trojans.conf
```

```
</IfModule>
```

```
# EXPIRES #####
```

```
<IfModule mod_expires.c>
```

```
ExpiresActive On
```

```
ExpiresByType image/x-icon "access plus 1 month"
```

```
ExpiresByType image/gif "access plus 1 month"
```

```
ExpiresByType image/jpeg "access plus 1 month"
```

```
ExpiresByType image/png "access plus 1 month"
```

```
ExpiresByType application/javascript "access plus 2 week"
```

```
ExpiresByType application/x-javascript "access plus 2 week"
```

```
ExpiresByType text/css "access plus 2 week"
```

```
</IfModule>
```

```
# PHP #####
```

```
<IfModule mod_php5.c>
```

```
php_value zlib.output_compression 16386
```

```
.....
```

```
php_value allow_url_fopen      off
php_value allow_url_include    off
php_value display_errors       off
php_value log_errors           on
php_value expose_php           off
php_value file_uploads         off
php_value magic_quotes_gpc     off
php_value memory_limit         128M
php_value post_max_size        256K
php_value register_globals     off
php_value session.save_path    /path/to/silex/tmp/sessions
php_value upload_max_filesize  256K
php_value upload_tmp_dir       /path/to/silex/tmp/sessions
php_value session.use_trans_sid off
php_value xhprof.output_dir    /path/to/silex/tmp/profiling
```

```
</IfModule>
```