

```
# .htaccess for tt-pds
Options All -Indexes
ErrorDocument 403 /template/error.php
ErrorDocument 404 /template/error.php

# deny direct access to all files except index.php, error.php and filetypes *.css, *.js
and *.png
order allow,deny
<FilesMatch "^(index|error)\.php)?$">
    allow from all
</FilesMatch>
<FilesMatch "\.(css|png|js)$">
    Order Deny,Allow
    Allow from all
</FilesMatch>
# Prevent viewing .htaccess and config files
<FilesMatch ".htaccess|config">
    order allow,deny
    deny from all
</FilesMatch>

# Prevent code injection: http://blogs.interdose.com/dominik/2008/03/20/sicherer-php-code-
php-code-injection-verhindern/
RewriteEngine on
RewriteCond %{QUERY_STRING} https?[:%] [NC]
RewriteRule .* /--http-- [F,NC]
RewriteRule http: /--http-- [F,NC]
```