```
<IfModule mod_rewrite.c>
    ## Start activating mod_rewrite
    Options +FollowSymLinks
    RewriteEngine On

    ## Begin - Rewrite rules to block out some common exploits.
    # Block out any script trying to base64_encode data within the URL.
    RewriteCond %{QUERY_STRING} base64_encode[^(]*\([^)]*\) [OR]
    # Block out any script that includes a <script> tag in URL.
    RewriteCond %{QUERY_STRING} (<|%3C)([^s]*s)+cript.*(>|%3E) [NC,OR]
    # Block out any script trying to set a PHP GLOBALS variable via URL.
    RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]
    # Block out any script trying to modify a _REQUEST variable via URL.
    RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
    # Return 403 Forbidden header and show the content of the root homepage
    RewriteRule .* index.php [F]
    ## End - Rewrite rules to block out some common exploits.

    ## Begin - SEF Section
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
    # If the requested path and file is not /index.php and the request
    # has not already been internally rewritten to the index.php script
    RewriteCond %{REQUEST_URI} !^/index\.php
    # and the request is for something within the component folder,
    # or for the site root, or for an extensionless URL, or the
    # requested URL ends with one of the listed extensions
    #RewriteCond %{REQUEST_URI} (/[^.]*|\.(php|html?|feed|pdf|vcf|raw))$ [NC]
    # and the requested path and file doesn't directly match a physical file or folder
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteCond %{REQUEST_FILENAME} !-d
    # internally rewrite the request to the index.php script
    RewriteRule .* index.php [L]
    ## End - SEF Section.
</IfModule>

<IfModule !mod_rewrite.c>
    # If we don't have mod_rewrite installed, all 404's
    # can be sent to index.php, and everything works as normal.
    ErrorDocument 404 /index.php
</IfModule>
```