Presentatie thema-avond HCC Joomla! Heerenveen
6 oktober 2015

Configureren .htaccess met .htaccessmaker in Akeeba Admin Tools Pro

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Veel websites worden gehost op een Apache webserver:

- Met een .htaccess bestand kun je een scala aan extra opdrachten aan de Apache webserver meegeven tijdens het opvragen van een webpagina. Opdrachten betreffende bijv. veiligheid, SEF, performance, redirects etc.
- .htaccessbestanden werken niet met IIS (gebruik web.config.txt) of NginX (gebruik nginx.conf) webservers.
- mod_rewrite module moet aanstaan in de Apache configuratie in httpd.conf (webhost). Bij een WAMP-server staat dit vaak niet aan. Haal de # weg voor 'LoadModule mod_rewrite' in httpd.conf.

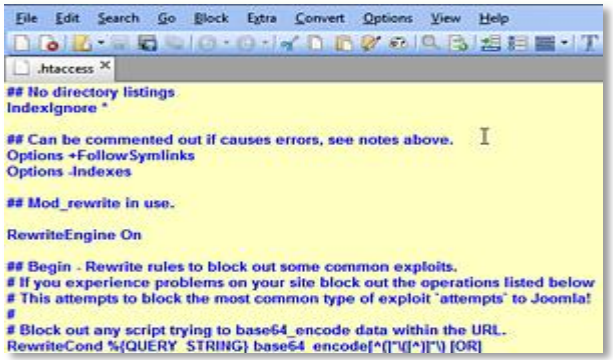
Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Webhost

- Let op: niet iedere webhost staat het gebruik van custom .htaccess bestanden toe. Is dat bij jou het geval? Verhuis zo snel mogelijk naar een fatsoenlijke webhost!

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

.htaccess editen als tekstbestand



Editen in teksteditor

- Een .htaccess bestand is een tekstbestand, dat je gewoon kunt editen met een code-editor als WeBuilder of Notepad++ of een teksteditor als Editpad Lite. Let op: Gebruik nooit Windows kladblok of MS Word om een .htaccess te editen.

- De naam van het .htaccess bestand bestaat uit 'een punt' + 'htaccess'. Op Linux en Unix servers worden bestanden voorafgegaan door een punt als verborgen bestanden gezien. Om ze zichtbaar te maken in je FTP-programma moet je de optie 'Toon verborgen bestanden' (Show hidden files) activeren.

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

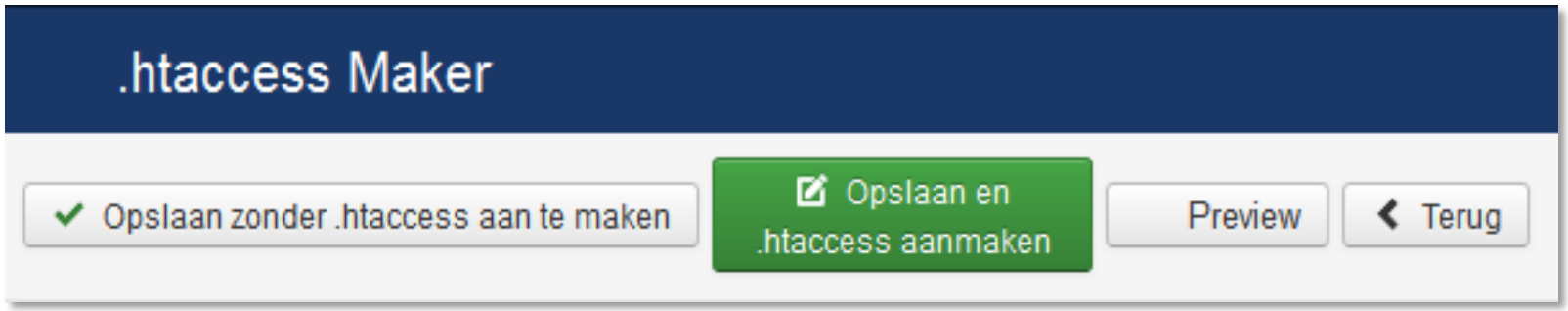
Joomla's htaccess.txt

- In Joomla wordt bij installatie (of update) in de websiteroot het bestand htaccess.txt meegeleverd. Je kunt dit htaccess.txt bestand hernoemen naar .htaccess. Het is dan direct functioneel. Maak vooraf wel een backup (kopie) van het tekstbestand.

- Dit is een .htaccess bestand dat je website al redelijk beveiligt en je URL-en kan herschrijven, zodat je geen 'index.php' meer aantreft in je URL-en. Wel zo SEF friendly (zoekmachinevriendelijk).

- Tegenwoordig (sinds Joomla 3.4) is er de opdracht IndexIgnore * in opgenomen. Die zorgt er automatisch voor dat de webserver geen indexen van een directory meer naar een browser verstuurt. Daarom is het nu dus ook niet meer noodzakelijk om in elke Joomlamap een lege 'index.html' te plaatsen.

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

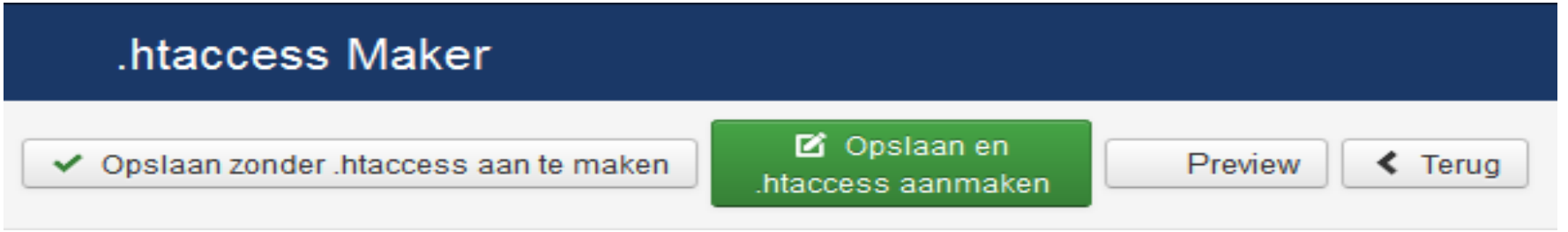


Editen met behulp van .htaccess Maker

- Een meer overzichtelijke manier om een .htaccess bestand aan te maken en te verfijnen is met de .htaccess Maker van Akeeba's Admin Tools Pro. Immers, het handmatig configureren van een .htaccess bestand vereist een behoorlijk goede kennis van de uitgebreide opdrachten (regular expressions bijvoorbeeld) en opties binnen een .htaccess. Zomaar wat uitproberen leidt vrijwel zeker tot een niet (meer) werkende site.

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

.htaccess Maker: Backup - Opslaan - Errors



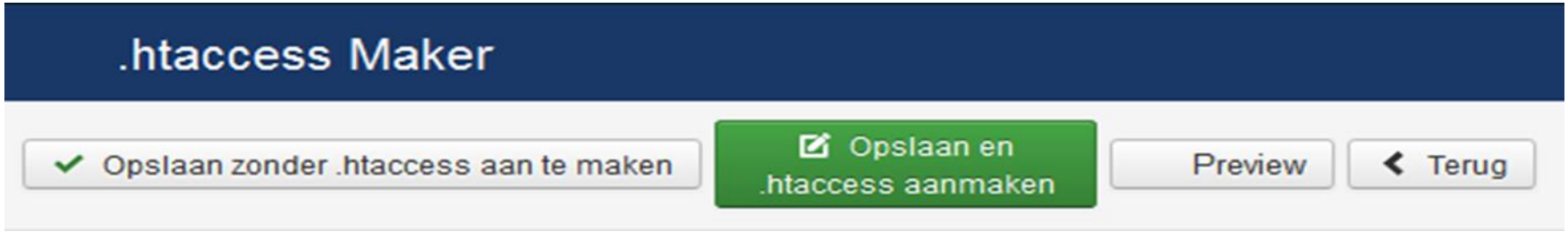
.htaccess Maker (onderdeel van Akeeba Admin Tools Pro)

- Backup: zorg dat je altijd een backup van de laatst werkende .htaccess hebt voordat je met de .htaccess Maker gaat stoeien! Gaat er wat fout, dan kun je de foutieve door .htaccess Maker gegenereerde .htaccess overschrijven met jouw gebackupte, en werkende .htaccess (via FTP).

- Opslaan: Wanneer je een .htaccess opslaat (Groene knop) dan wordt eerst de huidige .htaccess hernoemd naar .htaccess.admintools (=backup), en de nieuwe .htaccess wordt geschreven en is direct actief.

- Errors: Gaat er iets fout, bijv. een 'Internal Server Error 500 error' pagina of een witte pagina, verwijder dan de .htaccess en hernoem .htaccess.admintools naar .htaccess.

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

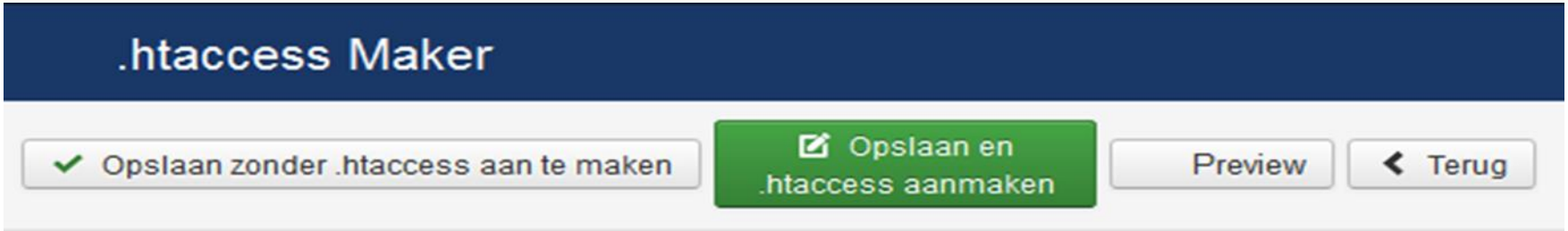


Indeling instellingen in .htaccess Maker

In de .htaccess Maker vinden we de volgende verdeling in hoofdgroepen:

1. Basisbeveiliging (Basic security)
2. Serverbeveiliging (Server protection)
3. Aangepaste .htaccess regels (Custom .htaccess rules)
4. Optimalisatie en hulpprogramma (Optimisation and utility)
5. Systeeminstellingen (System configuration)

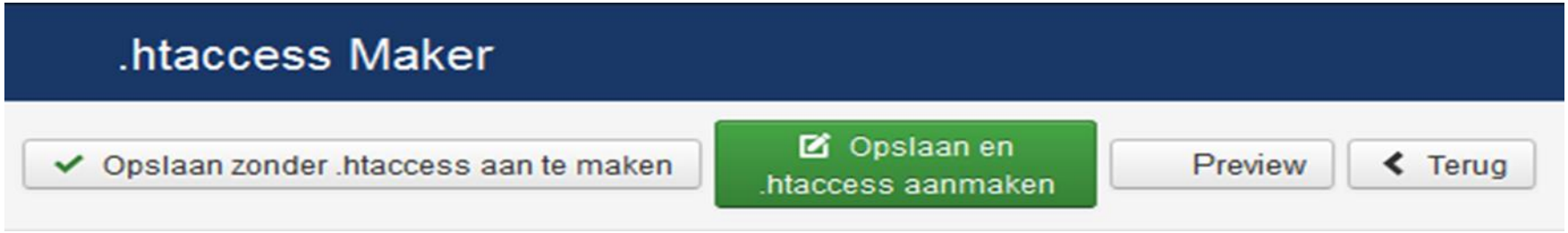
Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.



1.Basisbeveiliging (a)

- Schakel map listings uit (aanbevolen): Ja
  Niet tonen van Indexlijsten indien geen index.html of index.php aanwezig in directory.
- Bescherm tegen gemeenschappelijke bestandsinjectie-aanvallen: Ja
  Dit gebeurt door elke URL te blokkeren waarbij in de query string http:// or https:// voorkomt (uitzonderingen: zie Admin Tools User's Guide (PDF)).
- PHP easter eggs uitschakelen: Ja
  Blokkeert Easter Egg die de PHP-versie verraadt. Php-versie is interessante info voor hackers.
- Blokkeer de toegang tot configuration.php-dist en htaccess.txt: Ja
  Blokkeert toegang tot deze bestanden in de websiteroot (geven info over Joomlaversie).
- Protect against clickjacking: Ja
  Voorkomt het laden van je webpagina's in een, Frame, I-Frame of Object tag, behalve binnen een pagina van je eigen site.

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.



1. Basisbeveiliging (b)

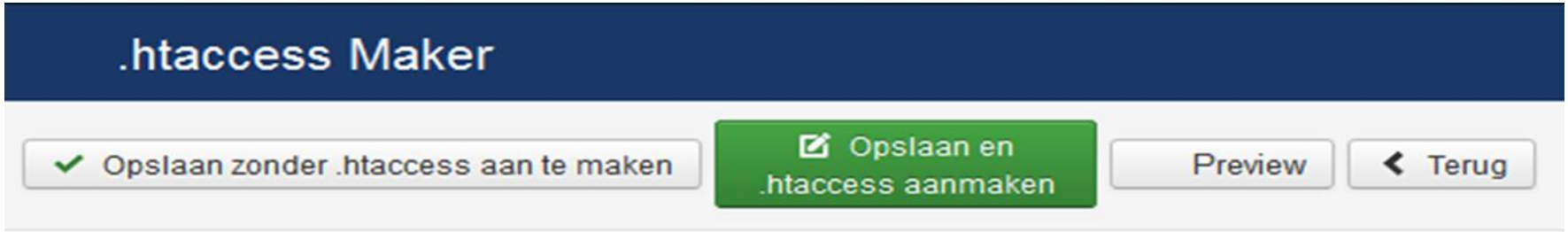
- Reduce MIME type security risks: Ja
  IE9+ en Chrome negeren de mimetype van de HTTP-header en leiden het soort bestand af van de extensie. Bijvoorbeeld een .exe vermomd als .jpg. Deze instelling dwingt de browser om de HTTP Mimetype header te respecteren.

- Reflected XSS prevention: Ja
  Voorkomt XSS aanvallen (Cross Site Scripting) via speciaal geprepareerde URL's met Javascript code. (Alleen IE8, Chrome, Webkit browsers)

- Remove Apache and PHP version signature: Ja
  Blokkeert tonen van het versienummer van Apache webserver en PHP.

  Prevent content transformation: Ja
  Voorkomt wijziging van content (afbeeldingen, CSS etc.) door proxyservers.

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

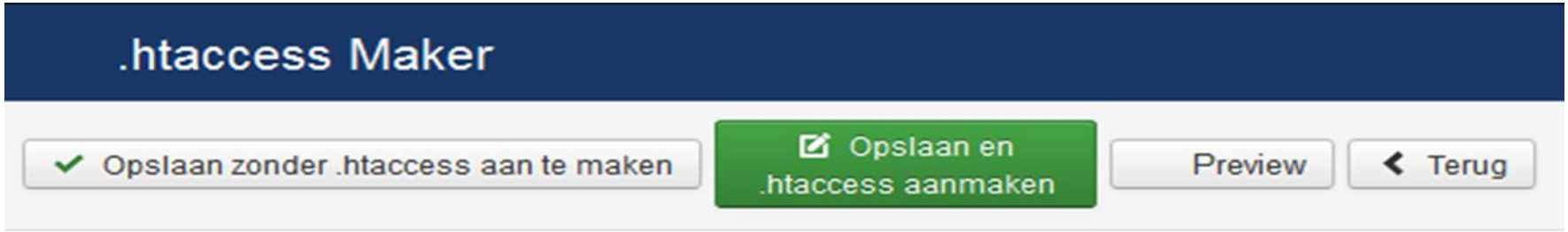


1. Basisbeveiliging (c)

- Blokkeer de toegang van specifieke user agents: Ja
  Blokkeert alle Useragents (Bots, downloaders) uit de lijst eronder.

- Te blokkeren user agents, één per regel: Lijst
  Je hoeft niet de gehele User Agent (UA) string in te voeren, alleen een deel ervan is voldoende.
  Een uitgebreide lijst vind je in de Admin Tools User's Guide onder de alinea: Default list of user agents to block. Je kunt deze user guide downloaden van de website van Akeeba:
  https://www.akeebabackup.com/download/admintools/3-6-2/admin-tools-pdf-zip-36.raw

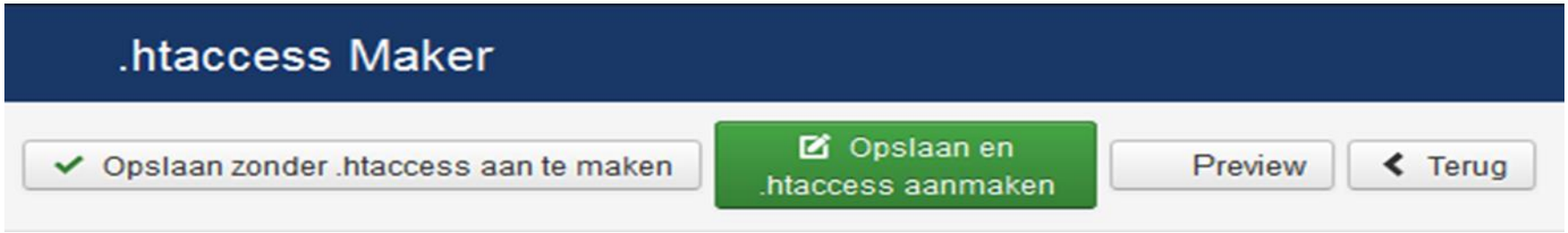
Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.



2. Serverbeveiliging (a): Schakel de beveiliging in of uit

- Back-end bescherming (Administrator): Ja
- Front-end bescherming (Website): Ja
  Bescherming tegen de meest voorkomende bedreigingen van een Joomlasite.
  Het credo is: Niets wordt er op je site uitgevoerd, tenzij je het zelf toestaat.

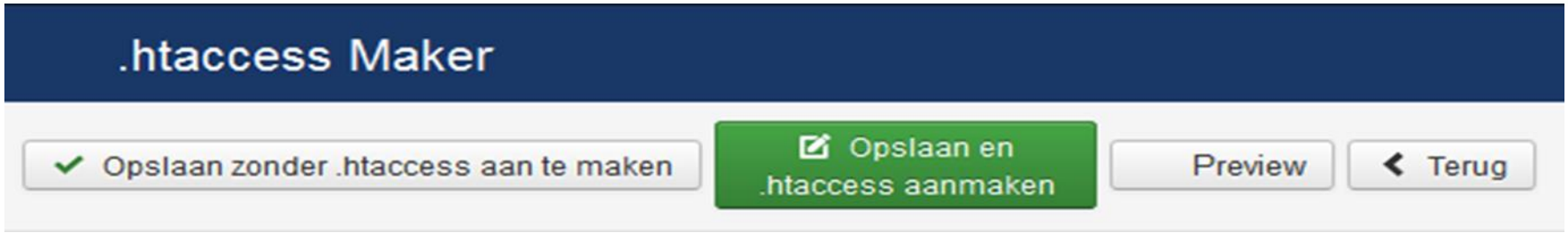
Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.



2. Serverbeveiliging (b): Fijnafstemming

- Back-end mappen waar bestandstype-uitzonderingen zijn toegestaan:
  (standaard: components, modules, templates, images, plugins) maar natuurlijk aanpasbaar.
- Back-end bestandstype toegestaan in de geselecteerde mappen:
  (standaard: jpe, jpg, jpeg, jp2, jpe2, png, gif, bmp, css, js, swf, html, mpg, mp3, mpeg, mp4, avi, wav, ogg, ogv, xls, xlsx, doc, docx, ppt, pptx, zip, rar, pdf, xps, txt, 7z, svg, odt, ods, odp, flv, mov, htm, ttf, woff, woff2, eot, JPG, JPEG, PNG, GIF, CSS, JS, TTF, WOFF, WOFF2, EOT)
- Front-end mappen waar bestandstype-uitzonderingen zijn toegestaan:
  (standaard: components, modules, templates, images, plugins, media, libraries, media/jui/fonts)
- Front-end bestandstype toegestaan in de geselecteerde mappen:
  (standaard: jpe, jpg, jpeg, jp2, jpe2, png, gif, bmp, css, js, swf, html, mpg, mp3, mpeg, mp4, avi, wav, ogg, ogv, xls, xlsx, doc, docx, ppt, pptx, zip, rar, pdf, xps, txt, 7z, svg, odt, ods, odp, flv, mov, htm, ttf, woff, woff2, eot, JPG, JPEG, PNG, GIF, CSS, JS, TTF, WOFF, WOFF2, EOT)

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.



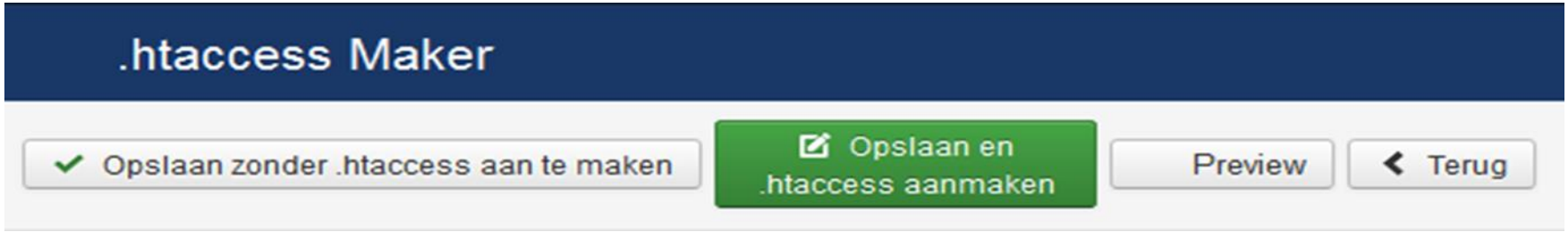
2. Serverbeveiliging (c): Uitzonderingen

- Sta directe toegang tot deze bestanden toe:
  (standaard:
  administrator/components/com_akeeba/restore.php,
  administrator/components/com_admintools/restore.php,
  administrator/components/com_joomlaupdate/restore.php,
  administrator/components/com_cmsupdate/restore.php)

- Sta directe toegang, met uitzondering van .php bestanden, in deze mappen toe:
  (bijvoorbeeld: media/jui/less) nodig wanneer je zelf templates maakt waarbij je de core bootstrap less bestanden opnieuw compiled.

- Sta directe toegang, inclusief .php bestanden, in deze mappen toe:
  (In ieder geval je templatemap: bijvoorbeeld: templates/mijntemplatemap)

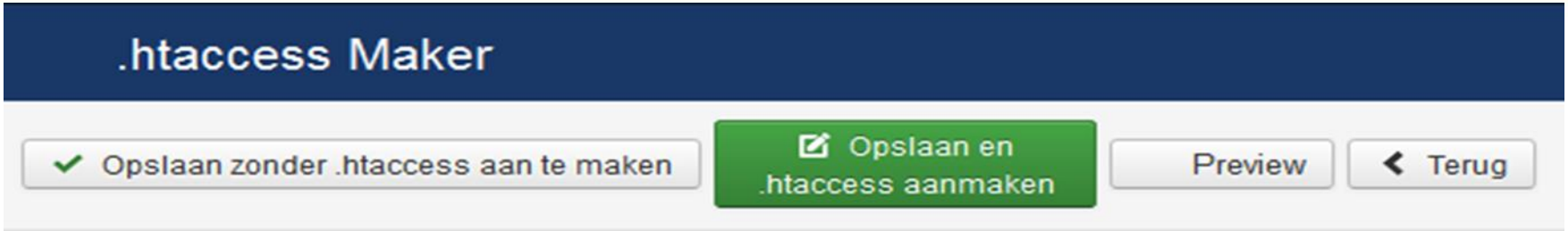
Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.



3. Aangepaste .htaccess regels (a)

- Aangepaste .htaccess regels bovenaan in het bestand:
  (Bijvoorbeeld: AddHandler application/x-httpd-php56 .php)
  De AddHandler-opdracht hier zegt tegen de server dat hij PHPversie 5.6* moet gebruiken om de browserrequests voor deze site af te handelen.

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

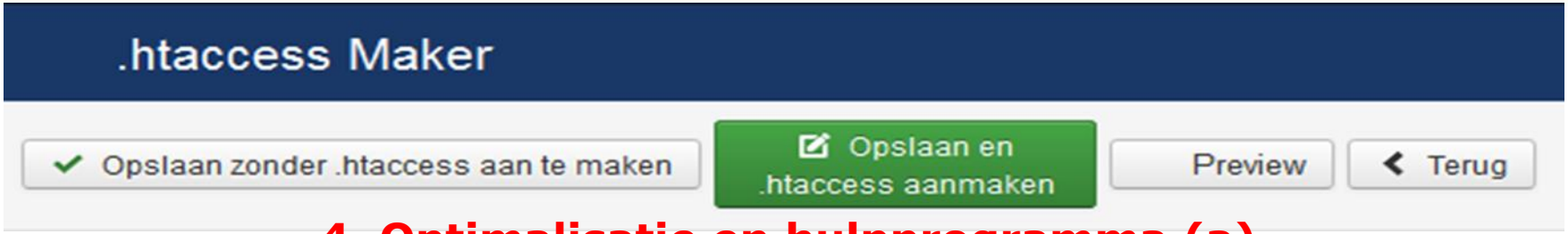


3. Aangepaste .htaccess regels (b)

- Aangepaste .htaccess regels onderaan in het bestand:
  (Bijvoorbeeld instructie voor Leverage Browser Cache:

```
<IfModule mod_expires.c>
   ExpiresActive On
   ExpiresByType image/jpg "access plus 1 year"
   ExpiresByType image/jpeg "access plus 1 year"
   ExpiresByType image/gif "access plus 1 year"
   ExpiresByType image/png "access plus 1 year"
   ExpiresByType text/css "access plus 1 month"
   ExpiresByType application/font-woff "access plus 1 year"
   ExpiresByType application/x-font-woff "access plus 1 year"
   ExpiresByType application/pdf "access plus 1 month"
   ExpiresByType text/js "access plus 1 years"
   ExpiresByType text/javascript "access plus 1 years"
   ExpiresByType application/javascript "access plus 1 years"
   ExpiresByType application/x-javascript "access plus 1 years"
   ExpiresByType application/x-shockwave-flash "access plus 1 month"
   ExpiresByType image/x-icon "access plus 1 year"
   ExpiresDefault "access plus 2 days"
</IfModule>)
```

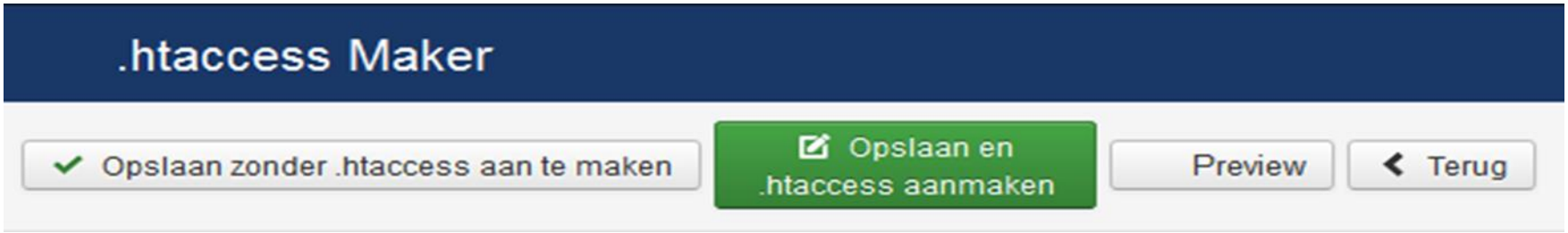
Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.



4. Optimalisatie en hulpprogramma (a)

- Forceer uitvoeren van index.php voor index.html: Ja
  Geeft index.php altijd voorrang op index.html
- Stel standaard verlooptijd in op 1 uur: Nee
  Is een soort van Leverage Browser Cache. Wanneer je die hierboven al gebruikt deze op Nee zetten.
- Automatisch comprimeren statische bronnen: Ja
  Minder bandbreedte gebruik door Gzip: snellere site en lief voor je phone's data-abonnement.
- Force GZip compression for mangled Accept-Encoding headers: Ja
  Forceert 'Automatisch comprimeren statische bronnen' indien de browser verminkte Accept headers voor compressed content verstuurt. 'Automatisch comprimeren statische bronnen' moet hierbij wel aan staan.
- index.php omleiden naar de Root van de site: Ja
  Verwijst http://mijndomein.nl/index.php naar http://mijndomein.nl/ Dit is goed om 'duplicated content' te voorkomen. Google ziet het als 2 afzonderlijke pagina's met dezelfde inhoud. En dat is niet handig voor je SEO ranking.

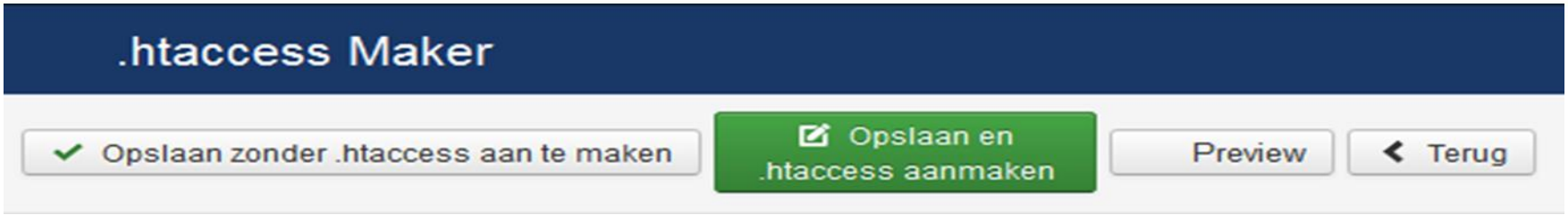
Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.



4. Optimalisatie en hulpprogramma (b)

- Leid www en niet www adressen om: Redirect www to non-www
  Ook hier beter om wel te gebruiken i.v.m. 'duplicated content'. En 'www' is zo 1995...
- Deze (oude) domeinnaam omleiden naar de nieuwe:
  Bij siteverhuizingen, en ook om 'duplicated content' te voorkomen. Syntax: http://mijnoudesite.nl , http://mijnnieuwesite.nl Dus gescheiden door een komma!
- Forceer HTTPS voor deze URL's (domeinnamen uitsluiten) :
  Redirect http link naar https link. (Zie Admin Tools User's Guide (pdf))
- HSTS Header (alleen voor HTTPS-sites): Nee / Ja
  Dwingt de browser om voortaan de hele site via https te benaderen.
- Verbied weergeven in FRAME (voor HTTPS-only sites): Nee / Ja
  Zelfde als Protect against clickjacking, maar dan voor https.

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.



4. Optimalisatie en hulpprogramma (c)

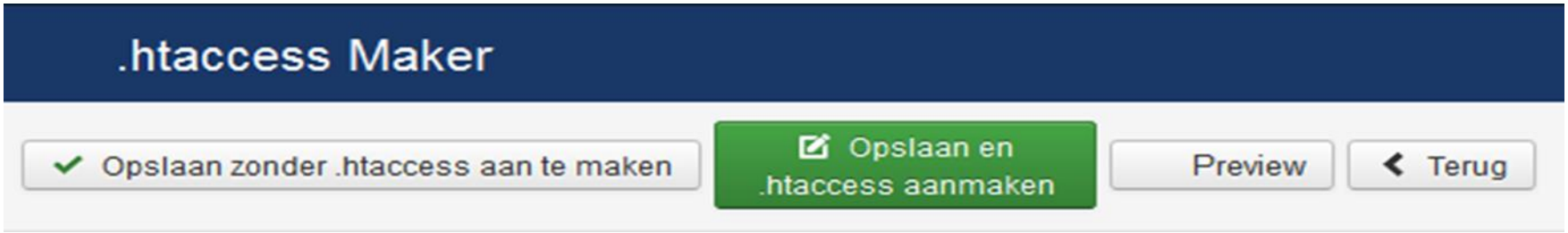
- Schakel de HTTP methodes TRACE en TRACK uit : Nee
  Hiermee voorkom je dat 'remote clients' de HTTP methodes 'TRACE' en 'TRACK' gebruiken om te connecten met je site. Dit kan door hackers gebruikt worden voor 'Cross Site Tracing (XST)' aanvallen (https://www.owasp.org/index.php/Cross_Site_Tracing). Volgens Akeeba kun je dit zonder problemen uitzetten, maar zowel bij Siteground als bij PCextreme levert dit een witte pagina in je browser op.

- Enable Cross-Origin Resource Sharing (CORS): Nee
  Toestemming voor derde partijen, om via AJAX content van jouw website op te halen. Alleen op Ja zetten wanneer je hierover expliciete afspraken hebt gemaakt met een derde partij.

- Set the UTF-8 character set as the default: Ja
  Joomla werkt standaard met UTF-8, maar dat weet Apache op oudere servers niet. Die gebruiken soms nog: ISO-8859-1.

- Send Etag: Server default
  Code in HTTP-header, berekend uit bestandsgrootte, inodenummer en laatst gewijzigde tijd. Code is bedoeld om te controleren of een bestand op de server is gewijzigd. Zo niet, dan gebruikt de browser het bestand uit de browsercache. Werkt niet op CDN's en loadbalanced serverparken.

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.



5. Systeeminstellingen

- Hostnaam voor HTTPS verzoeken (zonder https://): Domeinnaam
  Domeinnaam voor https requests (secure) Bijvoorbeeld: mijndomein.nl
- Hostnaam voor HTTP verzoeken (zonder http://) : Domeinnaam
  Domeinnaam voor http requests (standaard) Bijvoorbeeld: mijndomein.nl
- Volg symlinks (kan leiden tot een lege pagina of een 500 Internal Server Error): Alleen als eigenaar overeenkomt
  Joomla maakt normaliter geen symlinks aan en heeft geen symlinks nodig. Tegelijkertijd kunnen hackers die een site zijn binnengedrongen symlinks gebruiken om toegang te krijgen tot bestanden die normaal buiten het bereik van de website, die ze hebben gehackt, zijn opgeslagen.
  (Zie ook de Admin Tools User's Guide. (pdf))
- Basismap van uw website (/ voor de root van de domeinnaam): /
  Meestal: / Op localhost (Xamp bijv.) Voorbeeld: /mijnmap/backuptestsite

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

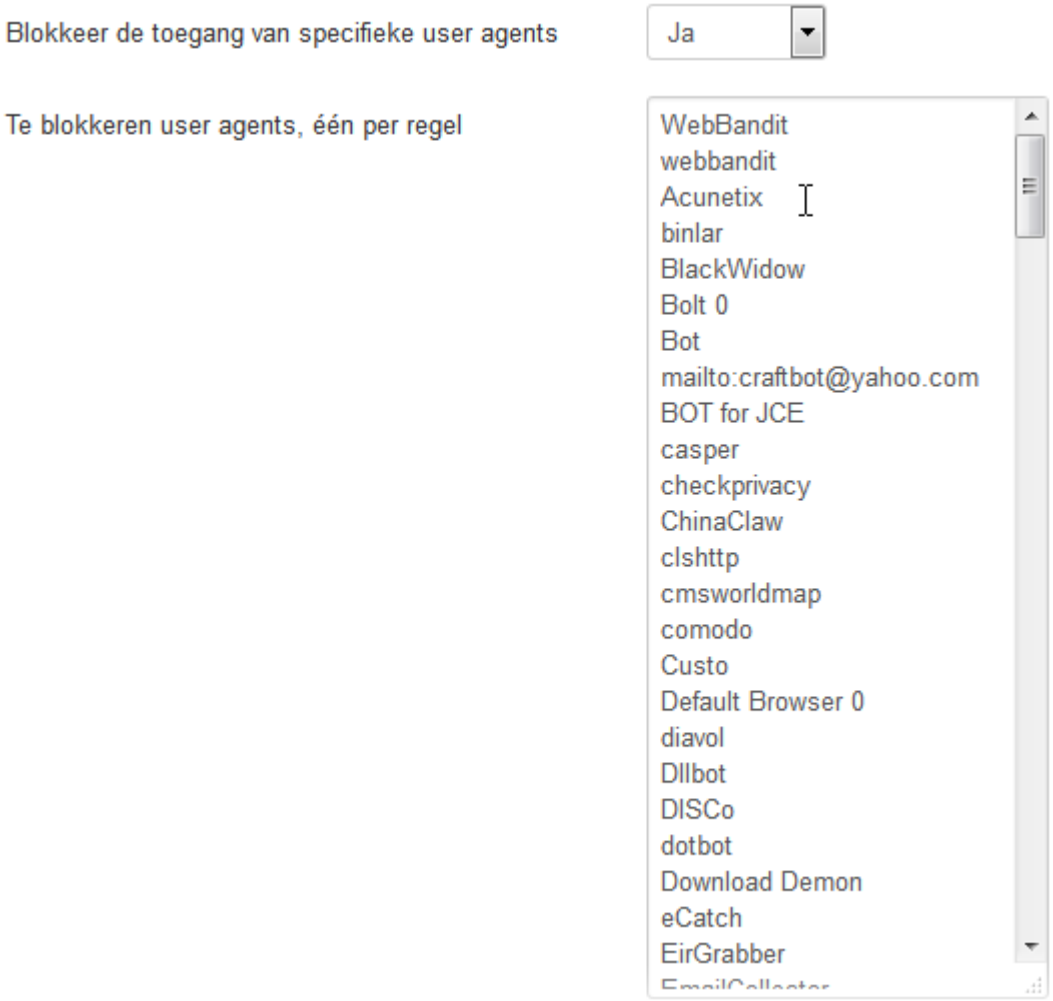
Voorbeeld .htaccess

Basisbeveiliging

Schakel map listings uit (aanbevolen)	Ja
Bescherm tegen gemeenschappelijke bestandsinjectie aanvallen	Ja
PHP easter eggs uitschakelen	Ja
Blokkeer de toegang tot configuration.php-dist en htaccess.txt	Ja
Protect against clickjacking	Ja
Reduce MIME type security risks	Ja
Reflected XSS prevention	Ja
Remove Apache and PHP version signature	Ja
Prevent content transformation	Ja

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Voorbeeld .htaccess



Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Voorbeeld .htaccess

Serverbeveiliging

Schakelt de beveiliging in en uit

Back-end bescherming: Ja

Front-end bescherming: Ja

Fijnafstemming

Back-end mappen waar bestandstype uitzonderingen zijn toegestaan:
components
modules
templates
images
plugins

Back-end bestandstype toegestaan in de geselecteerde mappen:
jpe
jpg
jpeg
jp2
jpe2
png
gif
bmp

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Voorbeeld .htaccess

Front-end mappen waar bestandstype uitzonderingen zijn toegestaan

- components
- modules
- templates
- images
- plugins
- media
- libraries
- media/jui/fonts

Front-end bestandstype toegestaan in de geselecteerde mappen

- jpe
- jpg
- jpeg
- jp2
- jpe2
- png
- gif
- bmp
- css
- js
- swf
- html
- mpg
- mp3
- mpeg
- mp4
- avi

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Voorbeeld .htaccess

Uitzonderingen

Sta directe toegang tot deze bestanden toe	administrator/components/com_akeeba/restore.php administrator/components/com_admintools/restore.php administrator/components/com_joomlaupdate/restore.php administrator/components/com_cmsupdate/restore.php
Sta directe toegang, met uitzondering van .php bestanden, in deze mappen toe	media/jui/less
Sta directe toegang, inclusief .php bestanden, in deze mappen toe	templates/mijntemplatemap

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Voorbeeld .htaccess

Aangepaste .htaccess regels

Aangepaste .htaccess regels bovenaan in het bestand

```
AddHandler application/x-httpd-php56 .php
```

Aangepaste .htaccess regels onderaan in het bestand

```
<IfModule mod_expires.c>
ExpiresActive On
ExpiresByType image/jpg "access plus 1 year"
ExpiresByType image/jpeg "access plus 1 year"
ExpiresByType image/gif "access plus 1 year"
ExpiresByType image/png "access plus 1 year"
ExpiresByType text/css "access plus 1 month"
ExpiresByType application/font-woff "access plus 1 year"
ExpiresByType application/x-font-woff "access plus 1 year"
ExpiresByType application/pdf "access plus 1 month"
ExpiresByType text/js "access plus 1 years"
ExpiresByType text/javascript "access plus 1 years"
ExpiresByType application/javascript "access plus 1 years"
ExpiresByType application/x-javascript "access plus 1 years"
ExpiresByType application/x-shockwave-flash "access plus 1 month"
ExpiresByType image/x-icon "access plus 1 year"
ExpiresDefault "access plus 2 days"
</IfModule>
```

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Voorbeeld .htaccess

Optimalisatie en hulpprogramma

Forceer uitvoeren van index.php voor index.html	Ja
Stel standaard verlooptijd in op 1 uur	Nee
Automatisch comprimeren statische bronnen	Ja
Force GZip compression for mangled Accept-Encoding headers	Ja
index.php omleiden naar de Root van de site	Ja
Leid www en niet www adressen om	Leid www om naar niet www
Deze (oude) domeinnaam omleiden naar de nieuwe	
Forceer HTTPS voor deze URL's (domeinnamen uitsluiten)	

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Voorbeeld .htaccess

HSTS Header (alleen voor HTTPS sites)	Nee
Verbied weergeven in FRAME (voor HTTPS-only sites)	Nee
Schakel de HTTP methodes TRACE en TRACK uit (bescherming tegen XST)	Nee
Enable Cross-Origin Resource Sharing (CORS)	Nee
Set the UTF-8 character set as the default	Ja
Send ETag	Server default

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Voorbeeld .htaccess

Systeem instellingen

Hostnaam voor HTTPS verzoeken (zonder https://)	mijndomein.nl
Hostnaam voor HTTP verzoeken (zonder http://)	mijndomein.nl
Volg symlinks (kan leiden tot een lege pagina of een 500 Internal Server Error)	Alleen alle eigenaar
Basis map van uw website (/ voor de root van de domeinnaam)	/

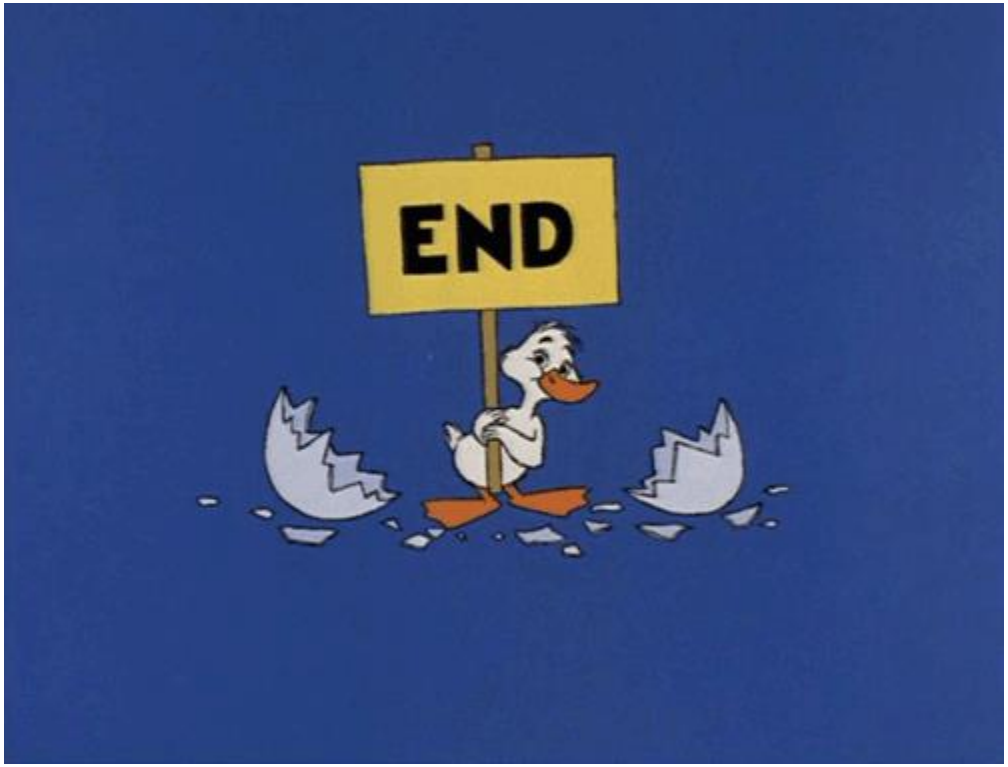
Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Bonus: Directory beveiligen met .htaccess en .htpasswd

- Surf naar tools.aharef.nl, en scroll naar .htpasswd-generator
  Met een .htaccess en een .htpasswd bestand kun je iedere directory beveiligen met een gebruikersnaam / wachtwoord combinatie.
- Voer gewenste username en password in en het serverpad maar .htpasswd
  Het .htpasswd bestand hoeft dus niet in de te beveiligen directory opgeslagen te worden. Het serverpad is dus niet een http(s) pad, maar bijv: /home/account/public_html/administrator/.htpasswd
- Klik Go button en volg de instructies op.
  Tip: Hover met je muis over de rode driehoekjes om de instructies te lezen.

Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.

Einde presentatie



Copyright © 2015 HCC-Joomla! Heerenveen, Benno Stulemeijer.
Alle rechten voorbehouden.