Gebruikers van je website dwingen om Authenticatie in twee stappen te gebruiken

In deze tutorial beschrijf ik hoe je met behulp van drie Regular Labs Pro extensies een procedure kunt implemeteren om bezoekers van je website te dwingen om 'Authenticatie in twee stappen' (2FA) in te schakelen in hun gebruikersprofiel. Door 2FA af te dwingen verbeter je de veiligheid van je website en van de gebruikers. Nadat 2FA is ingesteld kan men alleen nog inloggen door Gebruikersnaam, Wachtwoord en de Beveiligingscode in te vullen.

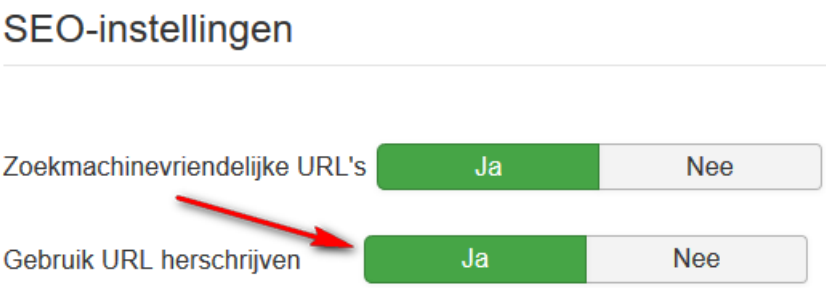
Ik ben voor deze tutorial gestart met een vers geïnstalleerde website, maar in principe is implementatie op elke Joomla 3.5+ website mogelijk. Waar nodig zal ik instructies verduidelijken met screenshots van instellingen.

1.) Installeer de laatste Joomla versie (ik heb Joomla 3.7 beta 3 gebruikt).

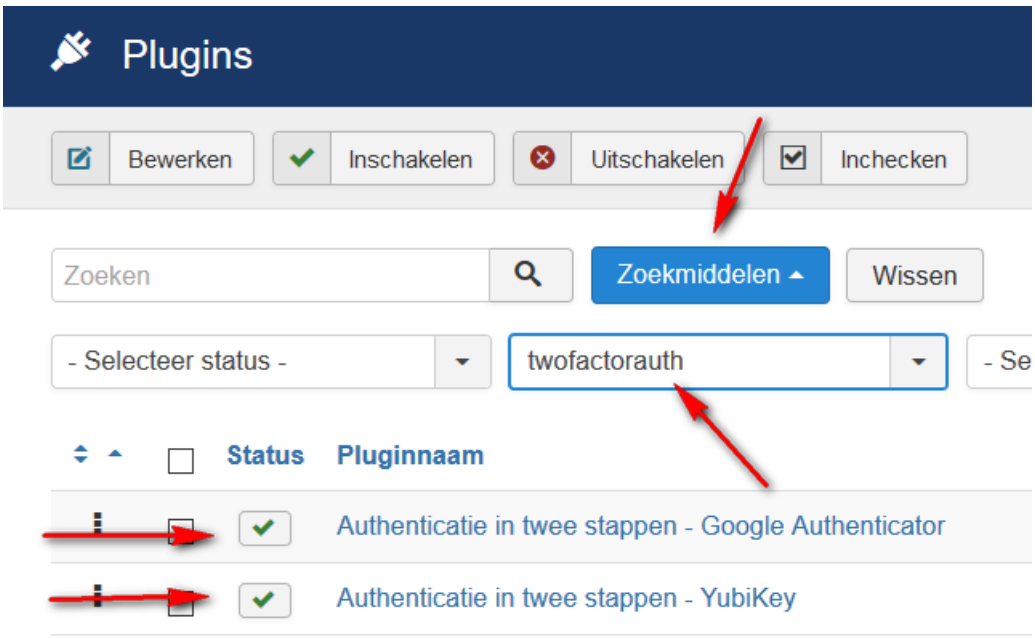
2.) Installeer de Nederlandse taalbestanden en stel deze in als standaard.

3.) Kopieer htaccess.txt naar .htaccess of installeer Akeeba Admin Tools en maak .htaccess aan met de .htaccessmaker.

4.) Stel de 'Algemene instellingen' in en stel 'Gebruik URL herschrijven' in op 'Ja'.

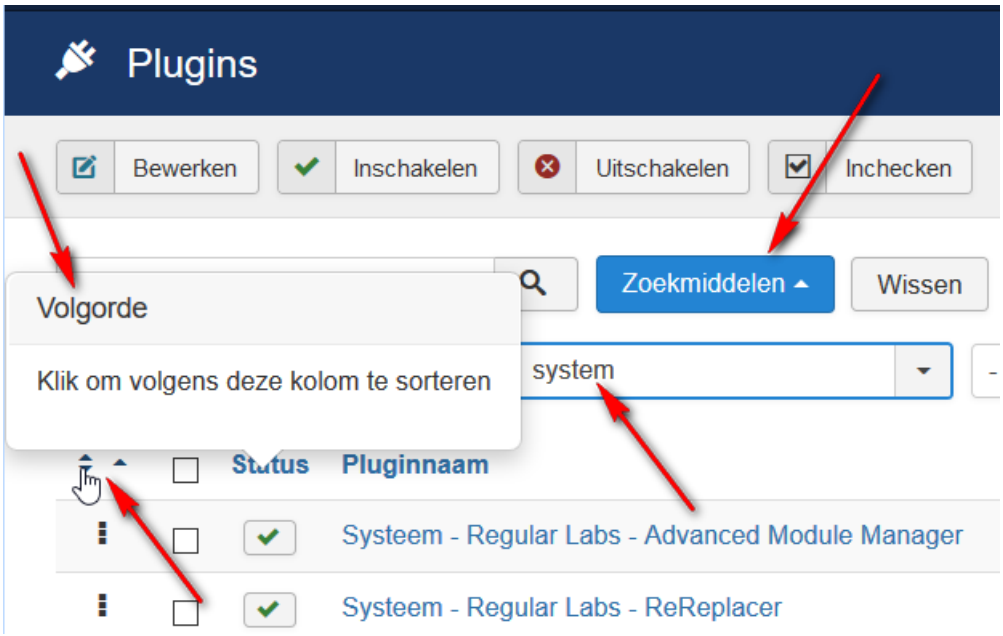


5.) Activeer 2FA via post-installatieberichten of via het inschakelen van Extensies/Plugins/'Authenticatie in twee stappen - Google Authenticator' en 'Authenticatie in twee stappen - YubiKey'.

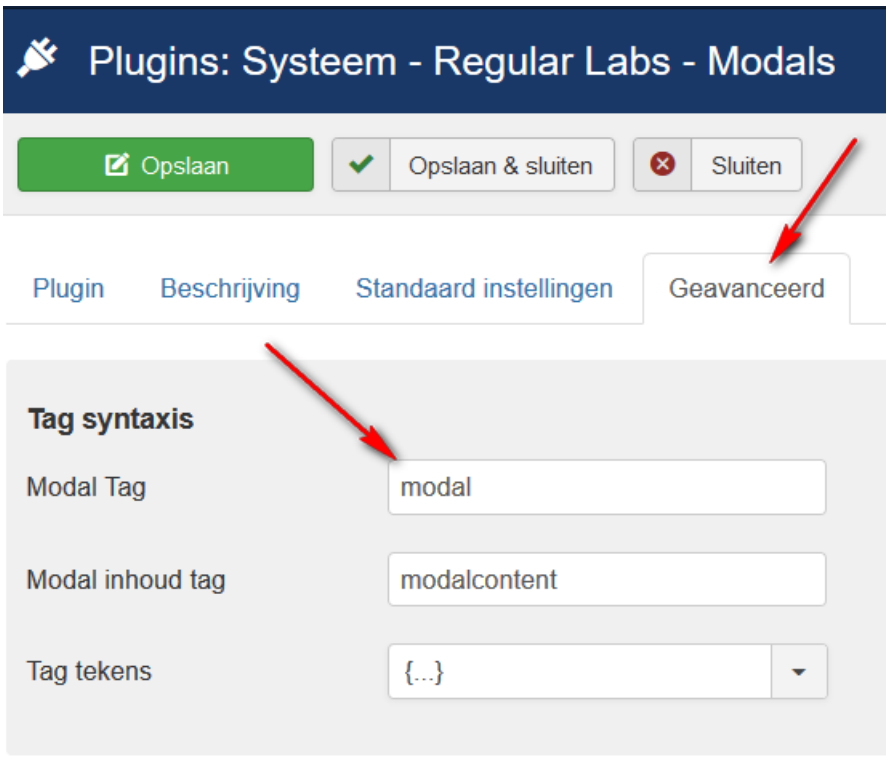


6.) Installeer: Regular Labs Extension Manager, voer de downloadcode in en installeer daarna de volgende drie Pro extensies: Advanced Module Manager, Modals, en ReReplacer.

7.) Ga naar Pluginbeheer, kies 'Zoekmiddelen' en selecteer type 'Systeem'. Klik op 'Volgorde' (pijltje omhoog en omlaag bovenaan eerste kolom) en sleep 'Systeem - Regular Labs - Modals' een heel eind naar onderen (dus later in de pluginvolgorde).



8.) Alleen indien de JCE Mediabox is geïnstalleerd: open Extensies/Plugins/Systeem - Regular Labs - Modals en wijzig op tabblad 'Geavanceerd' bij 'Tag syntax' 'modal' naar bijv. 'modalbox' gebruik vervolgens alleen nog {modalbox) in plaats van {modal}.



9.) Maak een nieuw artikel aan met als titel bijvoorbeeld 'Authenticatie in twee stappen', kies een categorie, bijvoorbeeld 'Uncategorised', en stel de toegang in op 'Registered'. Stel onder tabblad Opties de gewenste opties in (bijna alles verbergen).

10.) Klik 'Schakelen tekstverwerker' button (dus weg van TinyMCE of JCE), plak onderstaande voorbeeldcode in de basic editor en sla daarna op:

<h1 style="font-size: 22px; color: #0d6dab; margin-bottom: 10px;">Authenticatie in twee stappen</h1>

<h2 class="btn btn-warning" style="display: block; margin-bottom: 10px;">Je hebt de 'Authenticatie in twee stappen' (2FA) in je gebruikersprofiel nog niet ingeschakeld!</h2>

Om op deze website veilig in te kunnen loggen maken wij gebruik van Authenticatie in twee stappen. (Two factor authentication of 2FA in het Engels.) Dit houdt in dat je, om in te loggen, niet alleen je gebruikersnaam en wachtwoord moet invoeren, maar ook een extra beveiligingscode (2FA-code). Je stelt dit in in je gebruikersprofiel. Hierbij kun je uit twee verschillende authenticatiesystemen kiezen: OTP (One Time Password) en Yubikey.

Voor 2FA kun je gebruik maken van de 'Google Authenticator' OTP app (gratis te downloaden voor Android en IOS) op je smartphone of van een zogenaamde Yubikey (aanbevolen). Zo'n Yubikey moet je wel zelf aanschaffen wanneer je daarvan gebruik wilt gaan maken. De Yubikey is op vele websites en programma's voor 2FA te gebruiken (bijv. Google, Facebook, Dropbox, Lastpass, Keepass, MacOS, Windows etc.) en is handiger en veiliger in gebruik dan de OTP apps.
Tip: Indien je kiest voor de Yubikey, koop dan gelijk de Neo versie. Deze bevat ook een NFC chip waardoor je de Yubikey ook kunt gebruiken op tablets en smartphones (met NFC) om in te loggen op websites met 2FA.

Voor degene die niet over een smartphone beschikken en geen Yubikey willen aanschaffen is het mogelijk om toch vanaf een Windows pc of een Mac met 2FA in te loggen. Op Windows kun je hiervoor 'WinAuth' gebruiken (ook portable vanaf USB stick te gebruiken) en op de Mac 'OTP Manager'.

<h2 class="btn btn-info" style="display: block; margin-bottom: 10px;">Instellen van de Authenticatie in twee stappen:</h2>

Klik hieronder op de groene knop: 'Stel Authenticatie in twee stappen in'. Scroll, wanneer het formulier van je gebruikersprofiel is geladen, naar 'Authenticatie in twee stappen'.

Kies bij Authenticatiemethode voor 'Google Authenticator' (OTP) of Yubikey. ('WinAuth' en 'OTP manger' zijn dus alternatieven voor 'Google Authenticator'.) Hier kun je eventueel ook kiezen om een eerder ingestelde 'Authenticatie in twee stappen' weer uit te schakelen, bijvoorbeeld omdat je deze opnieuw wilt instellen bij verlies van de Yubikey of bij een nieuwe smartphone etc.

Lees de instructies goed en voer deze uit.

Belangrijk: Scroll na het opslaan van je profiel naar de onderkant van het opgeslagen, en herlade formulier om de 'Eénmalige noodwachtwoorden' te kopiëren (10 stuks). Sla die op een veilige plek op. Deze noodwachtwoorden zijn dus elk maar éénmalig te gebruiken, en kunnen gebruikt worden wanneer bijvoorbeeld je Yubikey of je Smartphone niet beschikbaar is.

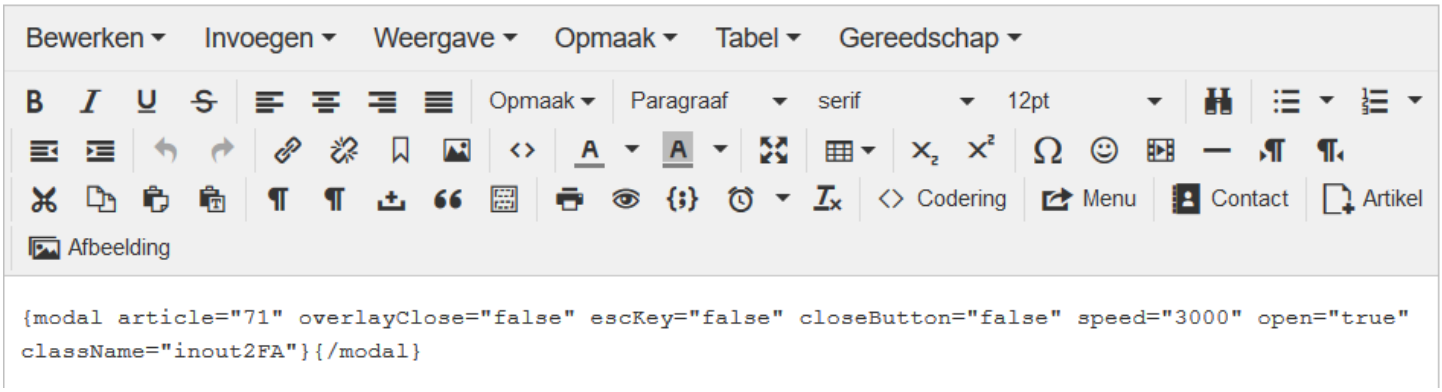
Indien je je smartphone of Yubikey definitief niet meer kunt gebruiken, log dan in met een noodwachtwoord en schakel de 'Authenticatie in twee stappen' uit in je profiel. Log uit, log opnieuw in en stel uw 'Authenticatie in twee stappen' opnieuw in.

Stel Authenticatie in twee stappen in

11.) Maak twee menu-items aan in het User Menu: 1.) Titel: 'Edit profile', Menu-itemtype: 'Bewerk gebruikersprofiel', en Toegang: 'Registered' en 2.) Titel: 'Log out', Menu-itemtype: 'Uitloggen' .

12.) Maak in Modulebeheer een nieuwe 'Aangepast' module aan: Titel: '2FA-warning', Toon titel: 'Verberg', Toegang: 'registered' en Positie: 'position-3' (mag elke actieve positie zijn).

13.) Voer in deze nieuwe '2FA-warning' module in de editor (TinyMCE of JCE de volgende code in: {modal article="71" overlayClose="false" escKey="false" closeButton="false" speed="3000" open="true" className="inout2FA"}{/modal}



14.) Let op: article="71" is het article id van het hierboven aangemaakte artikel 'Authenticatie in twee stappen' en className="inout2FA" is een CSS classnaam (de naam 'inout2FA' is hier zelf verzonnen classnaam) die aan de HTML van de modal wordt toegevoegd zodat je een aanknopingspunt hebt om je modal verder vorm te geven met CSS indien gewenst. Let ook in de laatste regel op de 'modal' tag. Indien je bij stap 09 de tag {modal} hebt gewijzigd naar bijvoorbeeld {modalbox} dan moet je dat in deze laatste code regel hierboven ook wijzigen.

15.) Bij tabblad 'Toewijzingen' invoeren bij URL ==> Uitsluiten (iedere url op nieuwe regel):

```
index.php?option=com_users&view=profile&layout=edit
/bewerk-profiel
/edit-profile
```

16.) Bij tabblad 'Toewijzingen' PHP invoeren van de volgende PHP code:

```
if ($user->guest)  {
        return false;
}
$query = $db->getQuery(true)
        ->select($db->quoteName('otpKey'))
        ->from($db->quoteName('#__users'))
        ->where($db->quoteName('id') . ' = ' . (int) $user->id);
$db->setQuery($query);
$otpkey = $db->loadResult();

return empty($otpkey) ? true : false;
```

17.) Sla de module op.

18.) Ga naar de front-end en log in met een gebruikersaccount (testaccount) waarbij nog geen 2FA is ingesteld. Het aangemaakte artikel 'Authenticatie in twee stappen' (id=71) zal in een modal worden getoond, waarbij het **niet** mogelijk is om de modal af te sluiten behalve via de link onderaan (button): 'Stel Authenticatie in twee stappen in'. Deze link verwijst rechtstreeks naar het profielformulier waarin onderaan de 2FA kan worden ingesteld. Zolang 2FA niet is ingesteld en men is ingelogd, zal iedere pagina de modal genereren en is verder navigeren op de site niet mogelijk.

Bonus 1:

Iedere browser heeft wel de mogelijkheid om de inloggegevens gebruikersnaam en wachtwoord van een site op te slaan. Zodra er voor de eerste keer wordt ingelogd zal de browser vragen of de inloggegevens moeten worden opgeslagen. Daarbij wordt het vaak ingestelde HTML atribuut: autocomplete="off" genegeerd. Wanneer een gebruiker er voor kiest om de inloggegevens op te slaan, zal bij elke nieuwe inlog op die website de gebruikersnaam en wachtwoord automatisch worden ingevuld. Bij het profiel-formulier van Joomla om 2FA in te stellen levert dat echter een probleem op: er staan twee wachtwoordvelden boven in dat formulier. De browser vult echter maar één wachtwoordveld met het huidige wachtwoord in, indien dit bewaard is. Wanneer je dat niet in de gaten hebt en je hebt onderaan de 2FA ingesteld en opgeslagen dan zal het opslaan mislukken. De twee wachtwoordvelden zijn immers niet identiek.

De eenvoudigste remedie is dan of in het tweede veld ook het juiste wachtwoord in te vullen, ofwel beide velden leeg te maken. Dan zal het opslaan wel lukken.

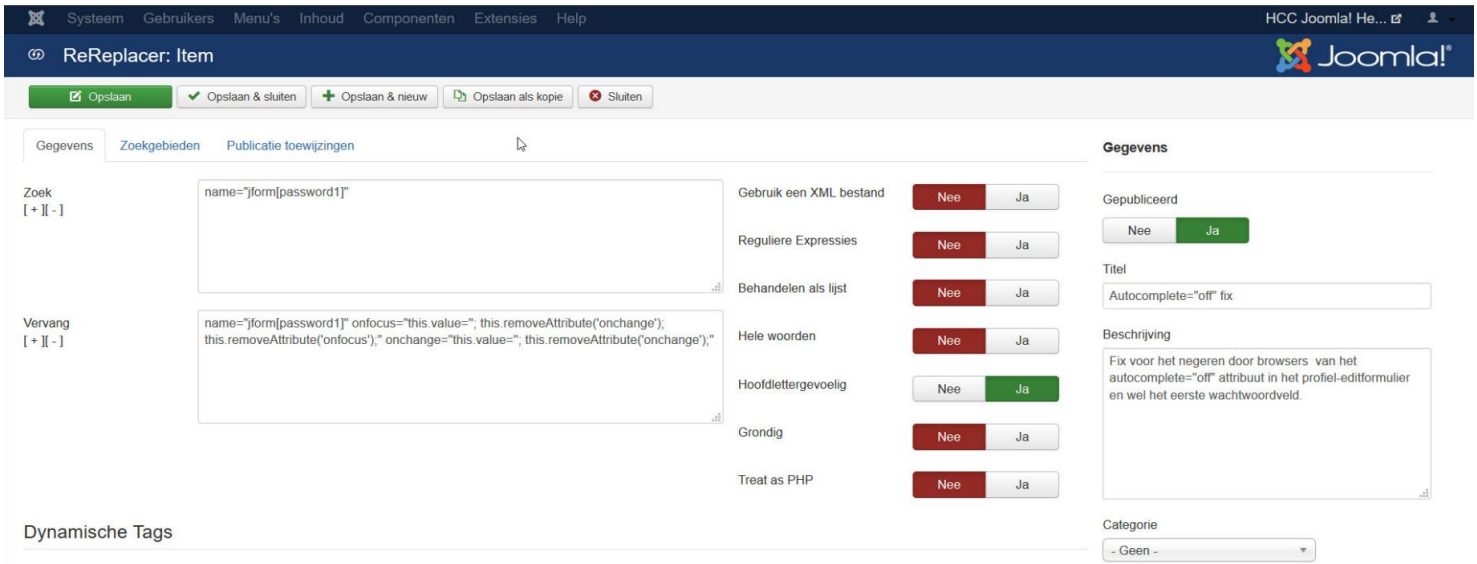
Om verwarring hiermee te voorkomen kun je met ReReplacer de HTMLcode van het eerste wachtwoordveld iets veranderen door een onChange en een onFocus event toe te voegen (zie screenshots). Hiermee verwijder je automatisch het door de browser ingevulde wachtwoord in het eerste wachtwoordveld van het edit-profiel formulier. Hieronder de zoek en vervang tekst. Neem de andere instellingen over van de screenshots daaronder.

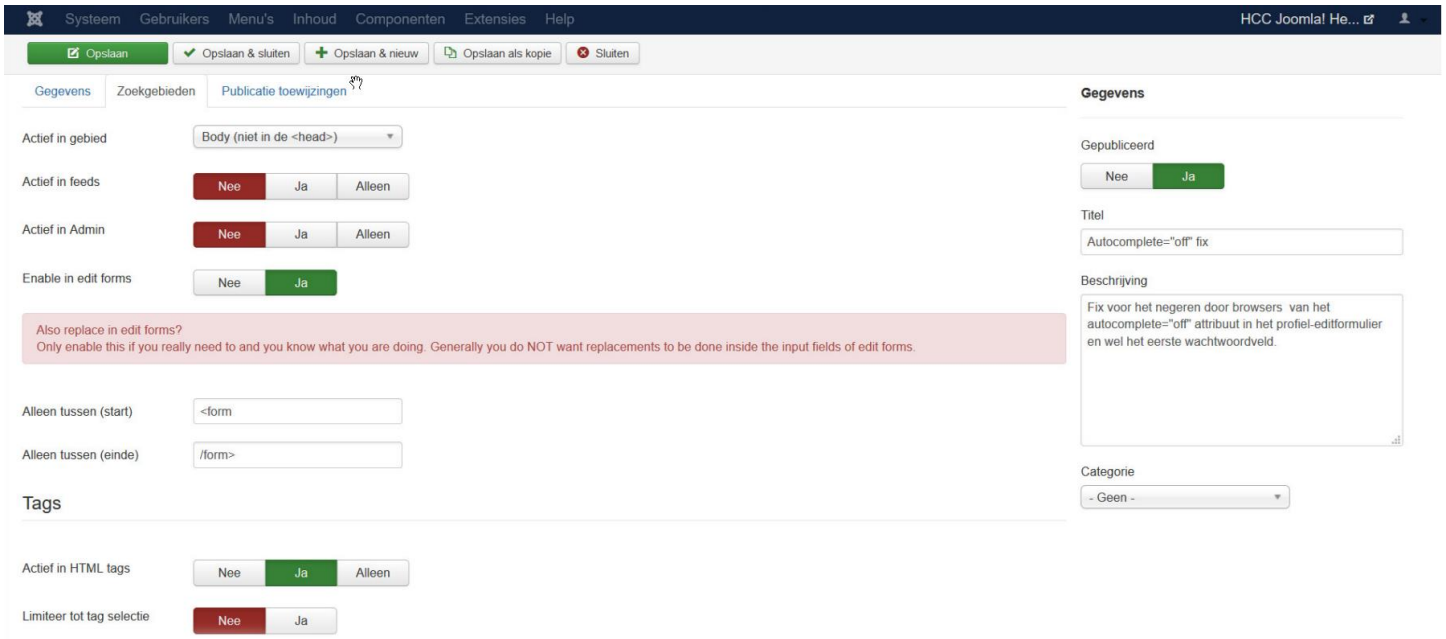
Laat ReReplacer zoeken naar de volgende tekststring:

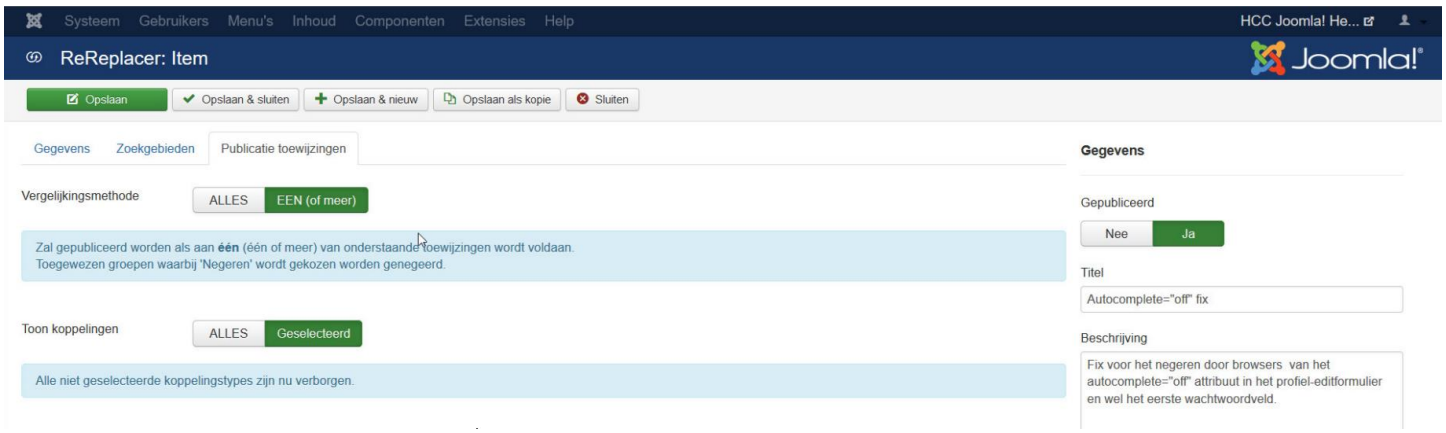
```
name="jform[password1]"
```

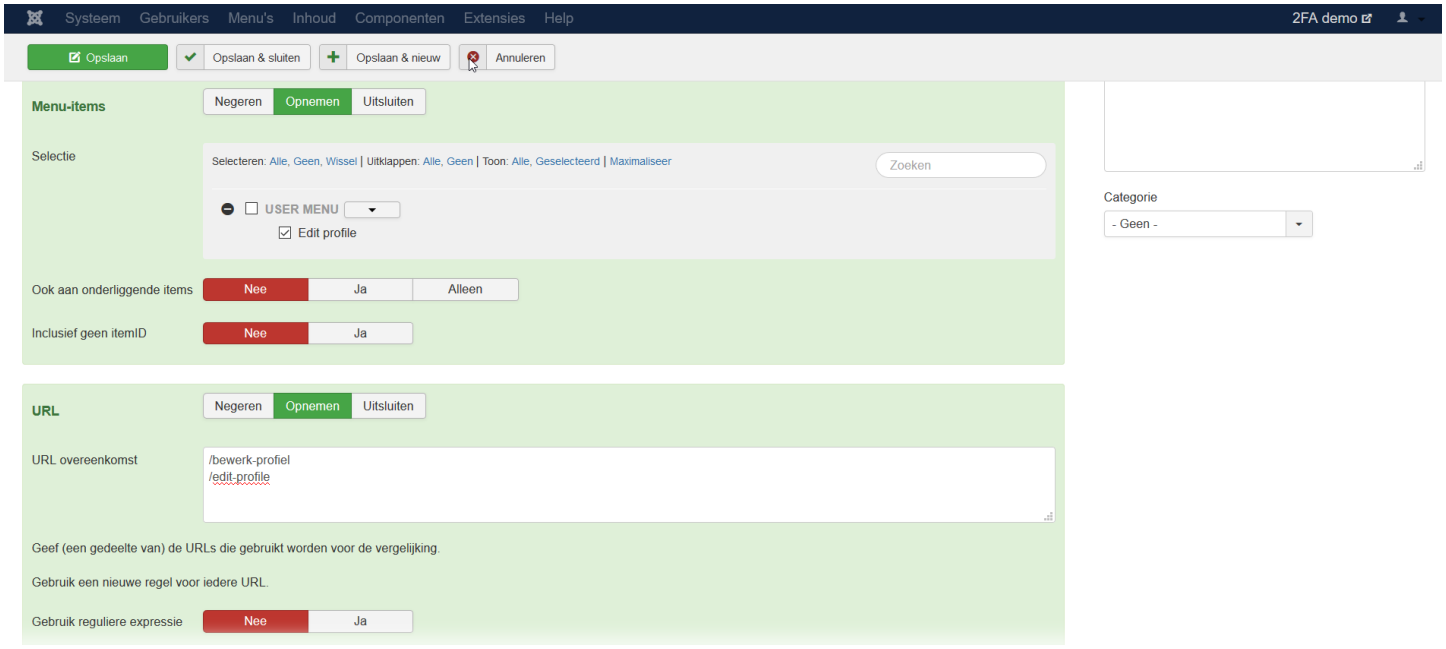
En vervang die met:

```
name="jform[password1]" onfocus="this.value=''; this.removeAttribute('onchange'); this.removeAttribute('onfocus');" onchange="this.value=''; this.removeAttribute('onchange');"
```





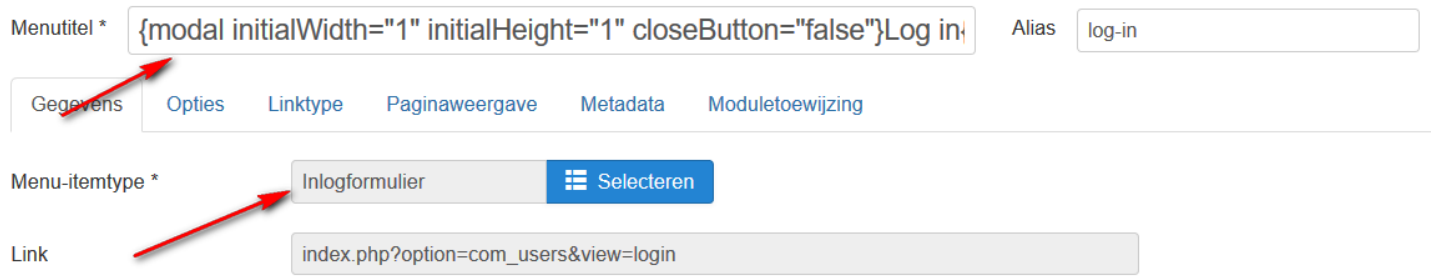




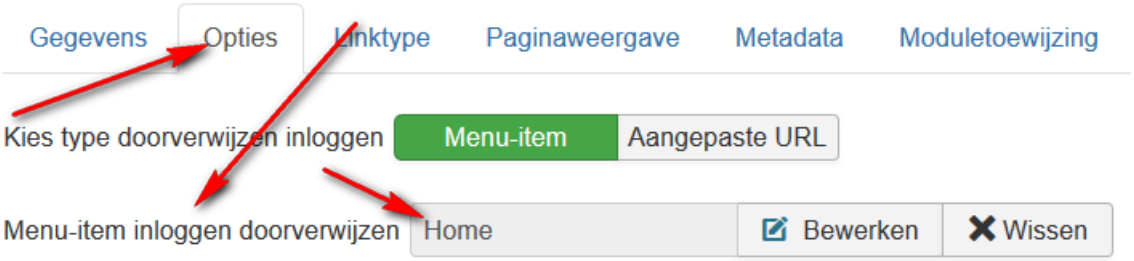
Bonus 2:

Bij stap 11 in deze tutorial heb je een 'Log out' menu-item aangemaakt in het User Menu. Je kunt in plaats hiervan het inlogscherm en uitlogscherm ook via een modal aan de gebruiker tonen. In dit voorbeeld maak ik in het topmenu een inlog- en uitloglink aan, die het inlogscherm en het uitlogscherm tonen in een modal.

1.) Maak een nieuw menu-item aan in het menu 'Top' van het type Gebruikers – Inlogformulier. Stel de toegang in op 'Guest' en geef bij alias de waarde log-in in. De menutitel 'Log in' wordt omgeven door de modal tags: {modal initialWidth="1" initialHeight="1" closeButton="false"}Log in{/modal}.

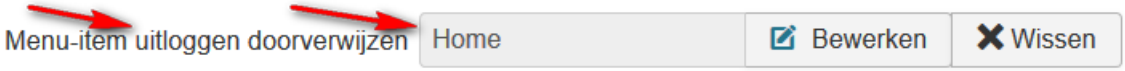


Selecteer op tabblad opties waarheen na inloggen de gebruiker doorgestuurd moet worden (bijvoorbeeld 'Home').



2.) Maak nog een nieuw menu-item aan in het menu 'Top' van het type Gebruikers – Inlogformulier. Stel de toegang in op 'Registered' en geef bij alias de waarde log-out in. De menutitel 'Log out' wordt omgeven door de modal tags: {modal initialWidth="1" initialHeight="1" closeButton="false"}Log out{/modal}.

Selecteer ook hier op tabblad opties waarheen na uitloggen de gebruiker doorgestuurd moet worden. Bijv. 'Home'



3.) Het 'Log in' menu-item wordt nu alleen getoond wanneer er nog niet is ingelogd en omgekeerd wordt het 'Log out' menu-item alleen getoond wanneer er wel is ingelogd. Beide acties worden nu in een modal getoond.

Tot zover deze tutorial. Ik hoop dat steeds meer mensen de waarde van 'Authenticatie in twee stappen' gaan inzien. Het inloggen op je website wordt weliswaar iets minder makkelijk door de extra handeling om de veiligheidscode in te vullen, maar de veiligheid van je website wordt hierdoor enorm verbeterd. De vrijblijvendheid om uit gemakszucht maar geen 2FA te gebruiken is met deze methode verleden tijd, en hackers kunnen veel moeilijker de standaard inloggegevens misbruiken.

Tot slot: ik heb deze tutorial gemaakt voor mijn presentatie op de thema-avond van HCC Joomla! Heerenveen. Nadat het programma voor deze avond al bekend was gemaakt en de PR al was verzorgd kwam het bericht dat Akeeba ook bezig is met het maken van een gratis plugin 'LoginGuard' om het instellen van 2FA af te dwingen en dat er een beta versie van de plugin op Github te downloaden was. Ik heb deze beta plugin getest en mijn conclusie was dat deze plugin nog absoluut niet stabiel is en nog niet bruikbaar is op een productiewebsite. De in deze tutorial beschreven methode is dat natuurlijk wel.

Vragen over deze tutorial kun je stellen in de Telegram groeps-chat Joomlacafé Heerenveen, of via het forum van Joomla Heerenveen.

Succes met implementeren!

Benno Stulemeijer (Klipper)