Systeem-, veiligheidsaudit Drupal

Datum: 22-01-2013
Auteur: HC de Raad (HaLeNaS v.o.f.)

Inleiding

De website [WEBSITE] wordt door leverancier [LEVERANCIER] gemigreerd naar een Drupal CMS oplossing.
Dit project verkeerd inmiddels nabij opleveringsfase en er dienen diverse (acceptatie)tests plaats te vinden.
Een van deze acceptatietests betreft een systeem-, en veiligheidsaudit van de Programmatuur zoals deze in de productie-omgeving is geinstalleerd door [LEVERANCIER].
Dit is nadrukkelijk een moment opname en biedt geen lange termijn garantie voor een onverstoord functioneren.

Voor de samenstelling van deze checklist is gebruik gemaakt van de security-gerelateerde best practises zoals deze door het Nationaal Cyber Secutiry Centrum, de PHP community, de MySQL community, en de Drupal community zijn gespecificeerd in hun documentatie, tevens is gebruik gemaakt van enkele standaardhulpmiddelen van PHP en het Drupal.

Niet alle richtlijnen zijn volledig overgenomen voor deze acceptatietest aangezien een groot gedeelte van de gesuggereerde maatregelen door de standaard Drupal Programmatuur reeds wordt geïmplementeerd/geboden, wel wordt gecontroleerd in hoeverre deze standaardprogrammatuur ook daadwerkelijk in onaangepaste vorm wordt uitgevoerd, wanneer hieraan namelijk in het ontwikkeltraject inhoudelijke aanpassingen (patches) zijn gedaan kan dit aanvullende beveiligingsrisico's openen. Dit geldt tevens voor het gebruik van inhuis-ontwikkelde, alsmede het gebruik van third-party modules vanuit het Drupal ecosysteem (drupal.org).

Als bijlages wordt een export van de PHP installatieconfiguratie (phpinfo) en een export van de geinstalleerde Drupal modules opgenomen.

Verhouding [LEVERANCIER] / hostingpartij

Door [LEVERANCIER] is de feitelijke hosting van de [DOMEIN] website uitbesteed aan [HOSTINGPROVIDER].
Indien deze hostingprovider beschikt over een (actuele) ISO27001 certificering zijn een aantal van de onderdelen uit deze audit niet nader onderzocht aangezien deze worden afgedekt door deze certificering. Deze punten betreffen met name de infrastructuur van de server (security updates/patches) en de netwerkconnectiviteit.

Checklist

Algemene maatregelen

Maatregel / controle onderdeel	**Beoogd resultaat**	**Daadwerkelijk resultaat / aanbevelingen**
De webserver verstuurt alleen HTTP headers die voor het functioneren van HTTP van belang zijn	Systeemdetails zoals gebruikte software (Apache, PHP) en hun versie worden niet in de HTTP headers meegezonden.	
De webserver beperkt de informatie bij het optreden van een fout, aan de gebruiker, tot een minimum	Enkel in HTTP responsecodes, of door een standaard fout-pagina, wordt een fout aan de gebruiker kenbaar gemaakt.	
De webserver maakt alleen gebruik van de hoogst noodzakelijke HTTP-methoden	Voor Drupal dient alleen het gebruik van GET, POST (en eventueel HEAD) toegestaan te worden.	
Directory listings zijn uitgeschakeld	Wanneer een directory in het filesysteem vanuit de webserver via een directe url/link wordt aangeroepen wordt geen lijst van bestanden/mappen in die directory weergegeven.	
Voor het benaderen beheersfunctionaliteiten zijn aanvullende beveiligingsmaatregelen getroffen	Zoals het beveiligen van de loginprocedure middels HTTPS, en/of het moeten invullen van een CAPTCHA bij inloggen, en/of 2 factor authenticatie, en/of het beperken van de toegestane IP adressen (bijv via htaccess) dat de loginpagina mag benaderen.	
De componenten van de hosting infrastructuur zijn opgenomen in een Intrusion Detection, en Monitoring Systeem en worden actief bewaakt	Het besturingssysteem van de server(s) wordt actief gemonitord op belasting, de database-, en webserver worden actief gemonitord op fouten/afwijkingen. In geval van dergelijke situaties liggen vooraf gedefinieerde scenario's klaar om maatregelen te treffen, of in ultimo naar een uitwijklocatie te migreren.	

Webserver (Apache/PHP)

Maatregel / controle onderdeel	**Beoogd resultaat**	**Daadwerkelijk resultaat / aanbevelingen**
Cookieconfiguratie is ingesteld op HTTPOnly	In de PHP.ini is de standaard setting voor session cookies als session.cookie_httponly = 1 – NB Dit is standaard Drupal 7 gedrag, echter kan uitgeschakeld worden waardoor javascript toegang tot cookies mogelijk is en CSS en CSRF aanvallen mogelijk worden.	
Server sofware is up to date	Laatste versies zijn: Apache [RECENT 2.0] of [RECENT 2.2]. PHP [RECENT 5.4] of [RECENT5.3], wanneer [RECENT5.3]wordt toegepast dient tevens de Suhosin patch geinstalleerd te zijn.	
PHP wordt niet uitgevoerd als CGI binary	PHP wordt uitgevoerd als Apache module of middels FastCGI.	
De webserverinstance / service wordt met beperkte rechten uitgevoerd.	De standaard “nobody” gebruiker wordt niet gebruikt voor de webserver. De webserver draait niet als “root”. PHP is geconfigureerd met open_basedir directive.	
De volgende PHP ini instellingen zijn geconfigureerd	max_execution_time = serverafhankelijk (default 30) max_input_time = serverafhankelijk (default -1, advies max 10) max_input_nesting_level = serverafhankelijk (default 64) max_input_vars = max 1000 (default 1000) magic_quotes_gpc = 0 magic_quotes_runtime = 0 open_basedir = serverafhankelijk display_errors = off log_errors = on (serverafhankelijk naar welk type log) register_globals = off expose_php = off	

Databaseserver (MySQL)

Maatregel / controle onderdeel	**Beoogd resultaat**	**Daadwerkelijk resultaat / aanbevelingen**
MySQL versie is up to date	Meest recente versie [RECENT 5.5](of andere relevante versie uit de 5.x serie) is geinstalleerd en operationeel	

Maatregel / controle onderdeel	Beoogd resultaat	Daadwerkelijk resultaat / aanbevelingen
De databaseserverinstance / service wordt met beperkte rechten uitgevoerd.	De standaard “nobody” gebruiker wordt niet gebruikt voor de databaseserver. De databaseserver draait niet als “root”.	
Enkel root gebruiker heeft schrijfrechten tot de user tabel in de mysql database	Enkel de root (administrator) user van de database mag wijzigingen doorvoeren aan de databaserechten.	
Drupal webserver databaseuser heeft beperkte rechten	De databaseuser waarmee de Drupal website draait heeft geen schema-wijzigingsrechten. De drush user wel.	
Database is enkel benaderbaar vanaf beperkte hosts/ips	De databaseserver mag enkel direct benadert worden door de webserver of een administrator werkstation, filtering op basis van host/ip-adres.	
Er zijn geen databaseusers zonder password	Alle mysql users maken gebruik van een username/password login combinatie. Er wordt nooit enkel op host/ip authenticatie een useraccount toegang verleend tot de database(server).	
Systeemmappen zijn niet beschrijfbaar voor webserveruser	De systeemmappen van de database (bijv voor plugins, log-, of databestanden) zijn nooit direct beschrijfbaar door de webserveruser.	
Backups van de database worden automatisch uitgevoerd	Er is een geautomatiseerd backuprooster voor de database actief.	

Applicatie (Drupal)

Maatregel / controle onderdeel	Beoogd resultaat	Daadwerkelijk resultaat / aanbeveling
Drupal versie is up to date	Versie [RECENT7] is geinstalleerd.	
Drupal Status pagina	Drupal Status pagina geeft geen afwijkingen.	
De webapplicatie valideert / filtert alle invoer, gegevens die aan de webapplicatie worden aangeboden aan de serverzijde.	Er zijn in de Drupal instance restrictieve text formats geimplementeerd (zoals het standaard Filtered HTML) en deze worden standaard gebruikt. “Full HTML” is niet toegestaan, of enkel door een daartoe geautoriseerde beheerder.	
Toegangsprofielen zijn	De Drupal user profiles zijn voor de	

Maatregel / controle onderdeel	**Beoogd resultaat**	**Daadwerkelijk resultaat / aanbeveling**
geconfigureerd op minimaal benodigde toegang	redacteuren, en functioneel beheerders, geconfigureerd op minimaal benodigde toegang.	
Beheer van toegangsprofielen is uitgeschakeld	Het is voor gebruikers met een beheerdersautorisatie niet mogelijk inhoudelijke wijzigingen door te voeren aan de toegangsprofielen (bijv dmv de Secure Permissions module)	
Onderhoud aan de Drupal installatie vind plaats via command line	De Drupal installatie wordt bijgewerkt via drush commanline tool om online administrator toegang te minimaliseren.	
Drupal user met id 1 is uitgeschakeld/vergrendelt	De user met id 1 kan in Drupal altijd met alle permissies werken, deze user dient in een live omgeving danook niet ingeschakeld te zijn.	
De Security Review module geeft geen foutmeldingen weer	De Security Review module geeft op geen enkel punt een foutmelding weer.	
De bestanden install.php en update.php, en andere systeembestanden, zijn niet publiekelijk benaderbaar	De bestanden/scripts waarmee een Drupal installatie of upgrade kan worden uitgevoerd, of andere systeem bestanden, zoals README en CHANGELOG, zijn niet publiekelijk benaderbaar of zijn verwijdert en worden enkel in geval van noodzaak beschikbaar gemaakt.	
De module Secure Pages is geinstalleerd en operationeel wanneer HTTPS gebruik mogelijk is	Voor gebruikersacties (zoals inloggen/edit/etc) wordt gebruik gemaakt van beveiligd HTTPS verkeer.	
De Flood control module is geinstalleerd en geconfigureerd	Er zijn diverse restricties geimplementeerd inzake failed logins met automatische bans/restricties voor IP adressen en usernames.	
Toekenning van mogelijk risicovolle permissies is niet van toepassing of zeer beperkt	Toekenning van een, of meerdere, van de volgende permissies is niet van toepassing, of geminimaliseerd: • Administer filters • Administer users • Administer permissions • Administer content types • Administer site configuration • Administer views	

Bijlage: Bronvermeldingen

Voor het samenstellen van deze checklist is gebruik gemaakt van:

1. ICT Beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum, deel 1 en 2, met name de onderdelen Applicatiebeveiliging:
    1. https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
2. Het onderdeel Security uit het PHP Manual
    1. http://php.net/manual/en/security.php
3. Drupal best practises voor Securing your site
    1. http://drupal.org/security/secure-configuration
4. Het onderdeel Security van het MySQL Manual
    1. http://dev.mysql.com/doc/refman/5.5/en/security.html

Bijlage: PHP Runtime Informatie

[INVOEGEN PHPINFO INFORMATIE]

Bijlage: Drupal Modules

Pakket	***Naam***	***Versie***