Een whitepaper door DWB Internet / Holland Webgroep
www.dwb-internet.nl - www.hollandwebgroep.nl
Neem voor meer informatie contact op met
sales@dwb-internet.nl

Security in Drupal

De veiligheid van Drupal als Web CMS en applicatie platform nader bekeken

Elke webproject neemt veiligheidsrisico's met zich mee

Bijvoorbeeld:

1. Website worden gehacked waardoor derden deze kunnen aanpassen, offline stellen etc..
2. Dataverkeer kan worden 'afgeluisterd' tussen de webserver en de browser van de bezoeker
3. Diefstal van persoonsgegevens en andere gevoelige informatie van bezoekers
4. Kwaadwillenden kunnen de werking en stabiliteit van de server in gevaar brengen

Hoe?

Om enkele voorbeelden te noemen:

5. Door het exploiteren van zwakheden in de website software
6. Door het toepassen van hack-technieken zoals cross-site scripting, cross-domain forgery, SQL injection
7. Door onzorgvuldig gebruik van inloggegevens door gebruikers

Het goede nieuws:

Drupal is een zeer veilig CMS / applicatie platform.

Drupal is een zeer veilig CMS / applicatie platform

Als platform voor honderduizenden websites is Drupal voortdurend onderwerp van onderzoek en analyse naar security issues en kwetsbaarheden. Zo heeft Drupal kunnen uitgroeien tot een zeer veilig web platform. Om maar wat te noemen:

1. Drupal is ‘secure by design’
2. Het plukt de (security)vruchten van de Open Source cultuur
3. Het heeft een full-committed Security Team
4. Drupal kent goed-gedocumenteerde *Best Practices* en aanbevelingen voor developers
5. Er bestaan een groot aantal security-ondersteunende modules

1. Drupal is Secure by Design

Drupal wordt wel *Secure by design* genoemd, wat zoveel wil zeggen als: ‘ontworpen met de veiligheid van het systeem voorop gesteld’. Of zoals Acquia, één van de grootste internationale Drupal consultancies het zegt: *Drupal is designed to prevent critical security vulnerabilities, including the Top 10 security risks identified by the Open Web Application Security Project (OWASP).*

Een voorbeeld hiervan is de versleuteling van de wachtwoorden in de database (sinds versie 7: SHA512 versleuteling met een per-user salt toepassing) en de manier waarop Drupal user input verwerkt (een fijnmazig, configureerbaar en lang-bewezen systeem van in- en output filtering).

Open Source

De beste open source projecten (en daar mogen we Drupal toe rekenen) hebben op het vlak van security een aantal pluspunten in vergelijking met proprietary software. Drupal, platform van miljoenen websites, met een zeer grote user base en een actieve community van meer dan 32.000 developers, biedt op gebied van security een aantal typische open-source-voordelen:

- De (PHP) code waaruit Drupal is opgebouwd is voor iedereen in te zien, te analyseren en te testen. Iedereen kan voorstellen doen voor verbetering. Zwaktes in de code blijven niet verborgen.
- De grote en actieve user base fungeert als levensgroot testpanel; bugs en veiligheidsproblemen worden in de praktijk doorgaans snel opgemerkt en gemeld.
- Bij (veiligheids)problemen staan in potentie 32.000 developers klaar om deze snel op te lossen.

Bij de tegenhanger van open source software, *proprietary software*, wordt, ook als het om de veiligheid van het systeem gaat, soms het tegenovergestelde aangetroffen: veiligheidsproblemen worden soms lange tijd ‘onder de pet’ gehouden en niet bekend gemaakt, patches komen traag van de grond. De geslotenheid van proprietary software maakt dit mogelijk; de transparantie die open source software uit haar aard meebrengt, is één van haar sterkste garanties voor een veilig softwaresysteem.

Security Team

De Drupal Association kent een Security Team, bestaande uit ongeveer 40 personen die zich continue bezig houden met het auditen en verbeteren van de veiligheid van Drupal core en de contributed modules.

De werkzaamheden van het Security Team verlopen volgens vaste, bewezen protocollen, waarbij de core- en module-auteurs nauw worden betrokken.
Naast het praktisch opsporen en verhelpen van security issues houdt het team zich bezig met het publiceren van best practices en aanbevelingen voor module ontwikkelaars.

Het Drupal Security Team publiceert gemiddeld ongeveer 15 advisories per maand, met betrekking tot zowel Drupal core als contrib.

Best Practices en aanbevelingen voor developers en beheerders

De online Drupal documentatie verschaft een grote hoeveelheid *Best Practices* en aanbevelingen, niet alleen voor Drupal developers maar ook voor website beheerders. Deze documentatie bevat niet alleen zaken die je pro-actief zou moeten doen, maar ook de zaken die je *niet* zou moeten doen.

Voor Drupal's documentatie geldt wat al werd genoemd toen het ging over Drupal's source code: *de documentatie is voor iedereen in te zien, te analyseren en te testen. Iedereen kan voorstellen doen voor verbetering. Zwaktes in de documentatie blijven niet verborgen*.

Security-ondersteunende modules

Naast Drupal's policy ten aanzien van veiligheid kan ook the *community effort* niet over het hoofd gezien worden. Drupal kent een groot aantal contributed modules die kunnen helpen bij het veilig maken en houden van je Drupal webproject. Een greep uit het aanbod:

- File integrity check
- Securitydoq
- PHPIDS
- Security Report
- Paranoia
- Auto Log Out
- Session Limit
- Security review
- Update manager
- Login security

Naast een veelheid aan security gerelateerde modules kent drupal.org een grote hoeveelheid community documentation over alle mogelijke facetten van dit onderwerp.

Tips voor een veilige Drupal installatie

1. Zorg ervoor dat Drupal core en modules regelmatig worden ge-update; een verouderde installatie is in potentie een veiligheidsrisico.

2. Gebruik modules die zichzelf hebben bewezen: let voor installatie op het aantal gebruikers en/of de tijd dat de module al bestaat.

3. Volg de periodiek verschijnende Security Advisors van het Security Team.

4. Gebruik ondersteunende modules zoals bijvoorbeeld de Security Review module.

5. Host je website op een betrouwbare hosting-omgeving (niet elk shared-hosting account van € 7,- per maand biedt per sé alle veiligheid die nodig is…)

6. Besteed de ontwikkeling van uw Drupal site en custom modules uit aan een bureau dat bewezen heeft veilig en verantwoord te werken.

Drupal security links

Drupal Security Report

Hoe voldoet Drupal –steeds meer een social publishing platform- aan haar belangrijke taak om de veiligheid hoog te houden in webprojecten die zijn bedoeld en ontwikkeld om input uit allerlei verschillende bronnen te verwerken.

Drupal Security Advisories

Actuele Security Advisories van het Drupal Security Team.

Writing Secure Code

Een uitgebreide verzameling user generated documentatie voor Drupal ontwikkelaars waarin een veelheid aan security-gerelateerde zaken de revue passeren.

Security Team

Alle informatie over Drupal's Security Team, waaronder de doelstellingen, structuur en verantwoordelijkheden, vragen als *hoe rapporteer ik een issue aan het Security Team?*, *hoe publiceert het team zijn bevindingen*, en nog veel meer.

Drupal Security Team op Twitter

Blijf op de hoogte van alle mededelingen van het Sencurity Team!