TRALIOS
Linux Server Management

PHP sicher, performant und skalierbar betreiben

Update zum PHP Usergroup Vortrag 2012

Dominik Vallendor ■ 22.05.2018

Über mich

TRALIOS
Linux Server Management

- Dominik Vallendor
- Studium der Informatik in Karlsruhe
- Seit 1995: Internet / Linux
- Seit 1999: PHP-Entwicklung
- Seit 2002: Selbständig
- Seit 2010: Tralios IT GmbH: Betrieb von Linux-basierten Web/Mailservern

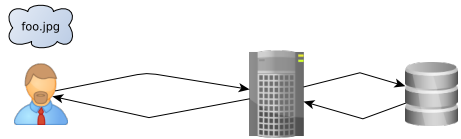
Übersicht

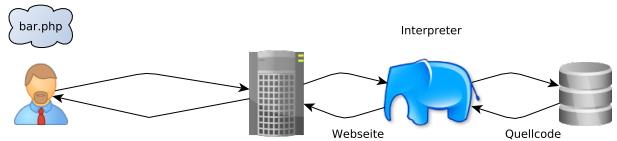
TRALIOS
Linux Server Management

- Der Webseiten-Aufruf
- Verschiedene Möglichkeiten PHP aufzurufen
- PHP Sicherheit
- Fragen & Diskussion

Webseiten-Aufruf

TRALIOS
Linux Server Management





PHP-Aufruf

TRALIOS
Linux Server Management

Der Aufruf von PHP kann auf verschiedenen Wegen erfolgen:

- **Apache-Modul mod_php**
- Apache-Modul mod_SuPHP
- Aufruf als CGI-Skript
- FastCGI
- **FastCGI Process Manager (FPM)**

Außerdem: PHP-Kommandozeileninterpreter

PHP-Aufruf

TRALIOS
Linux Server Management

Aufrufe von PHP unterscheiden sich u.a.

- im Konfigurationsaufwand / Komplexität des Betriebs
- in der Geschwindigkeit
- im Kontext/Rechten, in denen der Prozess ausgeführt wird
- in der Möglichkeit, PHP-Einstellungen vorzunehmen
- in der Möglichkeit, Timeouts und Prozessanzahlen festzulegen

mod_php

TRALIOS
Linux Server Management

- Aufruf erfolgt durch Apache-Modul
- Einfache Konfiguration
- PHP läuft immer im Kontext und mit den Rechten des Webservers
  (typischerweise User *apache* oder *httpd*)
- Gemeinsame PHP.INI
  Einzelne Einstellungen über VirtualHost-Einträge oder .htaccess änderbar

Über CGI und FastCGI zu PHP-FPM

TRALIOS
Linux Server Management

- Programm-Aufruf, wie für jede andere Skriptsprache (insb. Perl)
- FastCGI, PHP-FPM: PHP läuft dauerhaft, dadurch schneller als CGI

- Ausführung mit Rechten eines anderen Benutzers möglich
- Verschiedene PHP-Einstellungen für jeden Prozess möglich
- Prozessanzahl, Timeouts, etc. lassen sich feingranular steuern

Vergleich

TRALIOS
Linux Server Management

Welche PHP-Aufrufvariante eignet sich für welchen Zweck?

- **mod_php:** wenn nur eine Webseite pro Server & keine besonderen Zugriffsbeschränkungen von Nöten
- **PHP-FPM:** Shared Hosting-Umgebungen & aus Sicherheitsgründen immer zu empfehlen

Empfehlung: nach Möglichkeit immer PHP-FPM einsetzen

Verhalten bei zu vielen Anfragen

TRALIOS
Linux Server Management

MOD_PHP:

- Apache reicht alle Anfragen an PHP durch
- Server überlastet → sehr lange Antwortzeiten - Server ist scheinbar tot
- Theoretisch werden alle Seiten ausgeliefert, aber User warten nicht so lange

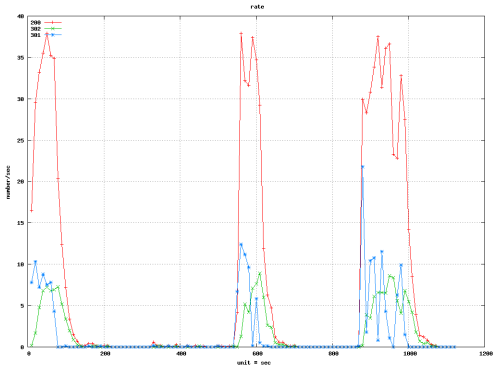
PHP-FPM:

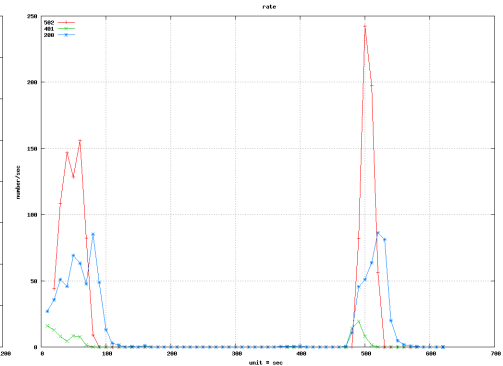
- Apache reicht nur beschränkte Anzahl Anfragen an PHP durch
- User erhält sehr schnell eine Antwort: entweder Webseite oder Fehlermeldung
- Für User besser nachvollziehbar, Fehlermeldung kann “hübsch“ gestaltet werden

Verhalten bei zu vielen Anfragen

TRALIOS
Linux Server Management

MOD_PHP vs. FastCGI/FPM:





PHP Sicherheit

TRALIOS
Linux Server Management

Wogegen absichern?

- Angriffe durch “Hacker“
- Erschleichen von Ressourcen durch eigene Kunden
- Absicherung gegen amok laufende Skripte

Angriffe und Probleme verhindern

TRALIOS
Linux Server Management

- PHP richtig in Apache einbinden, korrekter Handler Aufruf
- Sinnvolle/sichere PHP-Einstellungen
- PHP aktuell halten

Korrekter Aufruf des PHP-Handlers

TRALIOS
Linux Server Management

- Falsch:

  AddType application/x-httpd-php5 .php

  Ermöglicht die Ausführung von datei123**.php**.jpg

  Problematisch z.B. beim Upload von Dateien durch Webseitenbesucher

- Korrekt:

  <FilesMatch "\.php$" >

  SetHandler application/x-httpd-php5

  </FilesMatch>

Wichtige PHP-Einstellungen

TRALIOS
Linux Server Management

Ehemalige Problemkinder, inzwischen entfernt:

- magic_quotes_gpc
- safe_mode
- register_globals

Weiterhin wichtig:

- **open_basedir**: Pfad, auf den ein Skript zugreifen darf
- **memory_limit**: Maximaler RAM-Vebrauch pro Skript
- **allow_url_fopen** / **allow_url_include**: Laden/Einbinden von Code von fremden Servern

Die PHP.INI

TRALIOS
Linux Server Management

- Alle PHP-Einstellungen in einer einzigen Datei
- Nur manche Variablen lassen sich durch den Nutzer oder das Skript überschreiben
  .htaccess bei mod_php bzw. Aufruf von ini_set()
- Der Benutzer sollte **keine** Möglichkeit haben, eine eigene PHP.INI zu verwenden
  falls doch: Absicherung durch weitere Maßnahmen, z.B. *ulimit* notwendig
- Achtung: viele Einstellungen lassen sich umgehen; weitere Absicherung notwendig

Probleme

TRALIOS
Linux Server Management

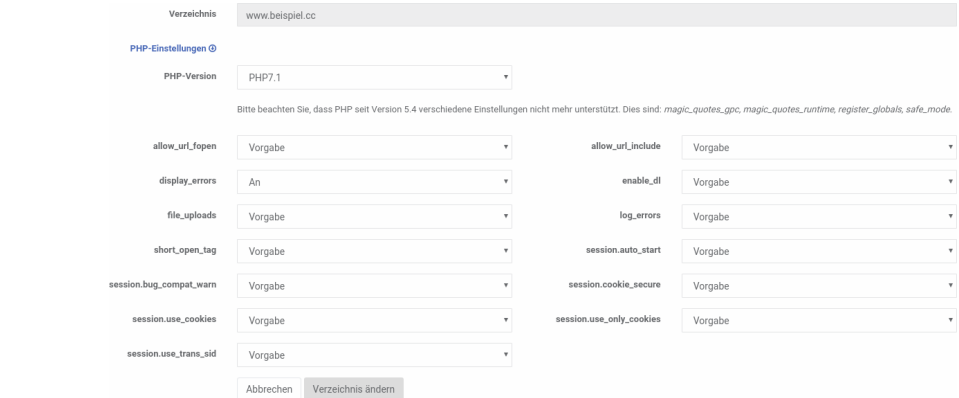
- Einschränkungen lassen sich umgehen (z.B. open_basedir durch Verwendung von *exec()*)
- Sicherheitskritische Befehle in PHP vorhanden, insb. *eval()*
- Viele Einstellungen lassen sich überschreiben, dadurch wirkungslos

→ Kritische Funktionen ausschalten mit *disable_functions*

→ Durch Frontend konfigurierbare PHP-Einstellungen

Konfigurierbare PHP-Einstellungen

TRALIOS
Linux Server Management



PHP absichern

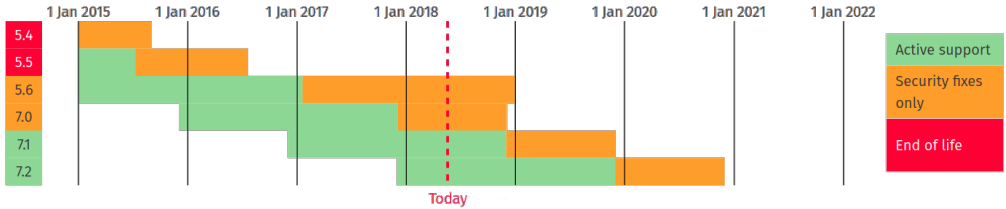
TRALIOS
Linux Server Management

- Auf Apache-Einbindung achten
- Kritische Funktionen ausschalten mit *disable_functions*
- Nutzung von SUHOSIN
- Getrennte Systembenutzer
- eventuell PHP einsperren (chroot, Docker)
- System absichern, Betriebssystem
- Dienste drumherum ebenfalls absichern:
  Apache-Prozesslimit, aktueller Kernel, Firewall, etc.

PHP Versionen aktuell halten

TRALIOS
Linux Server Management

(noch) unterstützte Versionen:



Siehe http://php.net/supported-versions.php

PHP Versionen aktuell halten

TRALIOS
Linux Server Management

Vorgehen zum Update:

- Veraltete Versionen rechtzeitig außer Betrieb nehmen
- Deaktivierung alter Versionen frühzeitig ankündigen
- Frühzeitig umschalten mit Möglichkeit, nochmal Version zu wechseln

Fazit

TRALIOS
Linux Server Management

- Verschiedene Möglichkeiten, PHP zu nutzen
  PHP-FPM empfohlen, da sicher und flexibel
- PHP absichern, z.B. durch SUHOSIN, disable_functions
- Bestimmte Werte in PHP.INI sind sicherheitskritisch
  $\rightarrow$dürfen nicht durch Benutzer editiert werden
- PHP aktuell halten

Fragen & Diskussion

TRALIOS
Linux Server Management

???

Kontakt

TRALIOS
Linux Server Management

- Dipl.-Inform. Dominik Vallendor

- Tralios IT GmbH
  Douglasstr. 24-26
  76133 Karlsruhe
  Telefon: 0721 - 94269660
  Telefax: 0721 - 94269666
  E-Mail: vallendor@tralios.de