

# Froscon

Free and Open Source Conf.  
St. Augustin 2010

# The cake is a lie

- Sebastian Bergmann

# Doctrine 2

- Benjamin Eberlei
- Neuentwicklung des ORM
- kein Active Record Implementierung
- evtl. in Zukunft in Zend Framework
- Teile von MDB2 “abgeschaut”
- Kompatibilitätsmodus wird evtl. ausgebaut
- Teilweise nicht performant (evtl. mit PECL)

# Hip Hop

- Scott MacVigar

# IPv6 Workshop

- Jens Link
- Guter Talk, aber genug um einen ganzen Vortrag darüber zu halten (würde ich gerne hören :-)

# PHP Unconference

Hamburg 2010

# Warum PHP sich rechnet

- Johann Hartmann Mayflower CTO
- 70% der Top 10 .de nutzen PHP
- Platz 4 in Toibe-Ranking
- Gartner: 2009 80:20 in 2013 50:50  
Amateure:Pros
- Markt wird volatiler, NYSE nutzt Optionen

# Cucumber

- Behavior Driven Design
- Testing mit Python
- Testschreiben für Dummies (Non-Developer)
- Jan Brauer

# Webinstaller

- Kore Nordmann Qafoo
- Zielgruppe: Shared Hosting Kunden
- angetrieben durch arbit (mehr Info???)
- großes Interesse von phpBB
- Anforderungen sehr sehr unterschiedlich
- I&I + Parallels bereits ohne großen Erfolg

# Hudson

- Continuous Integration
- Alternative zu Cruise Control
- plugins: git, svn, ant, phing, xunit, jsunit, checkstyle, pmd, email, irc, twitter, ...
- merkt wenn php mit fatal aussteigt!
- Gunnar Wrobel

# Top Ten Irrtümer und Fehler von PDO

- PDO ist TOT!
- Viele Designfehler (limit, in, prepare, ...), viele Bugs (Oracle, ...)
- Seit Jahren keine Weiterentwicklung
- Anlauf in 2007 für PDO2 gescheitert
- Johannes Schlüter

# PHP.next

- Johannes Schlüter, PHP5.3 Release Manager
- Ebenfalls bitter, weil Features nicht klar
- Vielleicht neues Release-Modell

# Softwarearchitektur für PHP Entwickler

- Architecture Tradeoff Analysis Method (ATAM by Berkeley Uni.)
- FURPS (functionality, usability, reliability, performance, security)
- Entscheidungsvalidierung/-dokumentierung
- Johann Hartmann

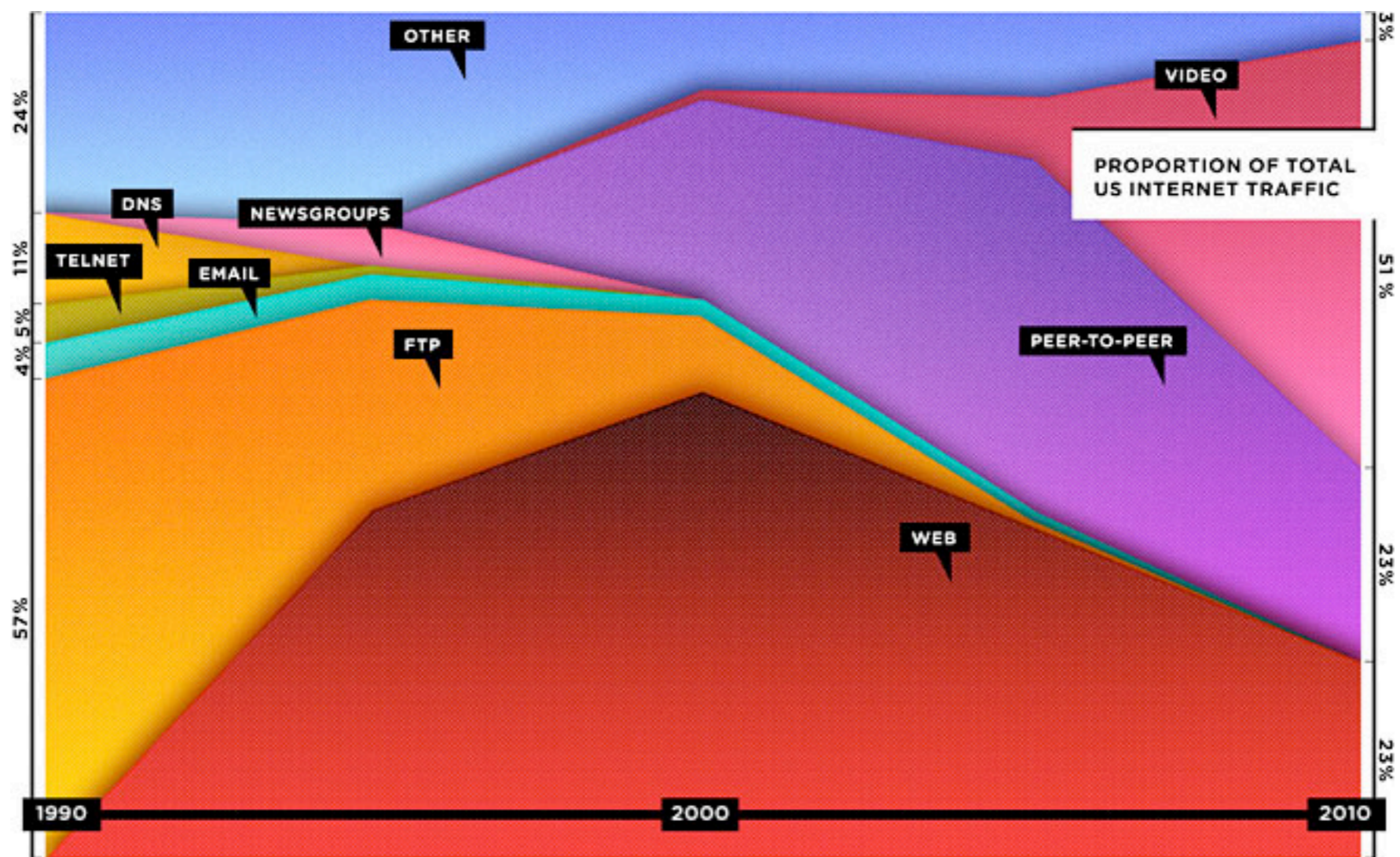
# IPC Mainz

10th IPC since 2001

# IPC Keynote

- “The web is dead”

[[http://www.wired.com/magazine/2010/08/ff\\_webrip/all/1](http://www.wired.com/magazine/2010/08/ff_webrip/all/1)]



# Apache Traffic Server

- Tom Melendez Yahoo!
- efficient caching proxy (30k rps per quad-core at Yahoo! (internal up to 300k))
- delivers 400 TB per day at Yahoo!
- multi-threaded, event driven
- Opensource (core committers from Yahoo!, Google, Akamai, ...), own Yahoo! team to only develop/test/maintain ATS
- compile yourself (docs available also for Amazon EC2)
- replaces more and more squid at Yahoo!
- Yahoo! uses localized DNS from Akamai and try to get away from it
- [trafficserver.apache.org](http://trafficserver.apache.org)

# Your tests are lying

- Sebastian Bergermann thePHP.cc
- is it money worth to test simple setter/getters?
  - use `assertAttributeEquals(...)`
  - or ignore setter/getter in code coverage
  - or test them during other tests
- PHP 3.5 with better code coverage restrictions (test can only generate coverage in same named classes using naming conventions)

- No asserts means no tests (only coverage!!!  $\geq 3.4$  also counts assertions therefore, 3.5 shows as incomplete with naming conventions activated)
- Do not directly output information to avoid corrupting PHPUnit output
- Be careful with output buffering to avoid catching all PHPUnit output also
- Test could be buggy: false negatives (pass when shouldn't) / false positives (fail when shouldn't)
- “Test Smell”
  - Fragile Tests: SUT (system under test) is changed but tests wasn't (interface/behaviour/data/context sensitivity)
  - Obscure Tests: Too difficult to understand test itself (not 2nd class code, not too much asserts in one test)
  - Hard-to-Test Code (Global vars, long methods, highly coupled)

# AtomPub Webservice

- Ben Ramsey Moontoast
- Atom Publishing Protocol for publishen and editing web resources using HTTP and XML (Atom itself is read only)
- how to use ... rtfm

# Gearman

- Frank Ruske Mayflower
- Skalierbarer Opensource Job Dispatcher
- Linux daemon (gibts auch als ubuntu package, kann aber mit pecl probleme machen)
- PECL-Extension (aktuell gearman-0.7.0, auch in die cli php.ini hinzufügen, wird oft vergessen)
- GM-Server verteilt, Clients können Aufgaben beim Server anfragen, Worker arbeiten Aufgaben ab.
- Binärpakete über TCP-Sockets (12 byte overhead)
- Server bietet Telnet-Schnittstelle um Textbefehle abzusetzen (z.B. "workers", "status", ...)
- synchron/asynchron nutzbar (MySQL-Extension um Ergebnisse in DB zu schreiben)
- Jobs/Server können TTL haben
- MySQL Client (UDF) implementierung als User defined functions (Aufgaben von MySQL über Gearman in anderes MySQL auslagern)
- Gearman Manager nutzt POSIX um PHP-Prozesse zu forken (starten/stoppen/überwachen/neu laden bei Code Änderungen)  
(<http://github.com/brianlmoon/GearmanManager>)
- <http://gearman.org>

# Web Workers

- Sebastian Bauer, Nero
- HTML5 Feature
- kein echtes Multitasking (Opera innerhalb eines Threads weil singlethreaded, Chrome echtes threading, ...)
- pseudo Parallellisierung loswerden (setTimeout(...))
- Shared Worker über mehrere Seiten, endet erst mit der letzten Seite (Verbindung dann über Ports)
- Einschränkungen:
  - kein Zugriff auf DOM, alert(), getElementBy...
  - kein Zugriff auf Elternseite (window object, global scope)

- Was geht denn überhaupt:
  - navigator, location (read only) object
  - XMLHttpRequest, setTimeout(), setInterval()
  - Object, Array, String, Date, Math  
canvas kann z.B. berechnet und als json zurückgegeben werden
  - ApplicationCache API, mehr Worker
- Best Practice
  - Worker spezialisieren
  - Keine riesigen Objekte rumschieben (je nach Browsersecurity dauert prüfen der Objekte lange)
  - addEventListener() nutzen (direkt über self gehen funktioniert in manchen Browsern nicht)
- Interessant für
  - Spiele-Engines / -Entwicklung
  - Desktopanwendungen (AIR)
  - Graphenberechnungen
- Kompatibilität
  - GEHT: Opera, Chrome, Safari, Firefox (Shared nur in Chrome und Opera, Firefox evtl. 4.0)
  - GEHT NICHT: bis einschl. IE8, IE9 ???

# PHP inside embedded

- Derick Rethans Freelancer / Core Developer
- PHP with GTK+ on OpenMocko Neo Phone
- compiles in  $\approx$  3h
- App starts slow, runs unstable, not for a long time, running faster than suggested, be careful with data handling, GTK styles not made for touch devices...
- DBUS required to talk to phone services (not very easy due to permission issues)
- just an experience... (Android/WebOS/Meego next?)

# PhoneGap

# SenchaTouch

- Christian Otto Freelancer/crosscan GmbH
- eine Sprache für alle Plattformen
- PhoneGap
  - Crosscompiler nutzt HTML/CSS/Javascript
  - benötigt Xcode
  - Apple Developer Account notwendig für Device-Tests und AppStore
  - Apple akzeptiert PhoneGap Kompilate
  - jslint hilft beim Entwickeln

- Sencha Touch
  - HTML5/CSS/Javascript für Browser
  - multitouch support
  - GPLv3 (oder FLOSS exception: BSD, MIT, PHP-License, ...)
  - OOP / komponentenbasiert / plugins
  - unterstützt YQL (Yahoo! Query Language)
  - iOS & Android (Blackberry6 & WebOS später)
  - Animationen auf Android noch Software gerendert
  - ExtJs <> Sencha Touch
  - noch Beta
  - bis 27.10 Ausschreibung für beste TouchApp (50k \$)

# JQuery Plugins

- Jakob Westhoff
- JQuery ist dokumentenbasiert (Selectoren und Setter und Fluent interface)
- verschiedene Möglichkeiten um Plugins zu entwickeln (Set Methods ist die meist genutzte und erweitert Standard-Sets)
- Plugin sollte mit `jQuery.noConflict()` funktionieren (fixed `$`-Verlinkung, z.B. `$j = $.noConflict()`)
- immer Event-Namespaces nutzen
- Plugin-Repository mit Vorsicht genießen (wenn schon nicht an die Namenskonventionen gehalten, dann eher schlecht)
- Gibts bald auch als Buch...

# arbit issue tracker

- Kore Nordmann Qafoo
- still alpha version
- Goals/Why: extensible clean PHP code, multi-project support, modularized, won't suck
- Features planned: continuous integration, wiki, issue tracker, source browsing, notifications, ...
- requires CouchDB yet (Doctrine2 or other RD in future)
- wiki/issue uses Restructured Text currently for editing entries

# Clean Code with Aspect Oriented Programming

- Robert Lemke Typo3 Assoc.
- AOP wird verwendet in Typo3 Phoenix / Flow3
- Funktionalität (Aspekte) laufen im Hintergrund (Logging, Security, ...)
- nutzt Annotations
- Model/Controller-Code kann unverändert bleiben und wird befreit von solchen Aspekten
- erschwert Debugging
- Proxy-Subclasses um line numbers zu erhalten, kein code-rewriting
- kein scaffolding
- Beim ersten Klick wird analysiert und gecached

# Lesser known Security Issues in PHP Apps

- Stefan Esser SektionEins
- https is still vulnerable to MITM without cert verification (file\_get\_contents('https://...',false,\$ctx) requires a configured stream context)
- PDO\_MySQL with multi-queries allows SQL-Injection within prepared statements using: ORDER BY, user supplied table/field names, IN() statements
- Prepared statements allows now SQL evaluation wich allows hiding injections
- saving user object within session could be dangerous if temporarily session object is changed to admin and script fails after user object could be written back

- unserialize() is very dangerous if it's exposed to user input (many internal vulnerabilities in the past). supports most PHP data types also objects. \_\_wakeup()/\_\_destruct() is called and all properties could be controlled => **POP exploits** (Property Oriented Programming). Autoload will help a lot.
- md5/sha1 prepending secrets is easily breakable (appending will be ok, better is using hash\_hmac())  
e.g. flickr used it the wrong way in the past
- using long encryption keys for CBC encryption could be broken with "padding oracle"  
(all .net sites are attackable at the moment!)
- SektionsEins opens a Security Blog next week starting with this

# Debugging Rules and Tools

- [www.debuggingrules.com](http://www.debuggingrules.com)
- jmeter from apache
- macgdbp
- debugger in eclipse conditional breakpoints
- git bisect good/bad

# Why MVC is not an application architecture

- SPLObserver - subject:attach,detach,notify  
observer:update
- MVC is based on observer
- separate presentation is good
- view is not observing controller nor model
- view is full html page
- no events from view
- no sync with view

# Designing HTTP URLs and REST Interfaces

- good URL `www/products/`
- good URL `www/products/?filter=cats&sort=desc`
- good URL `www/products/1234`
- good URL `www/products/1234/photos`
- no session, logins or cookies to maintain state

# Web Single Sign-on und IAM mit SAML

- top 10 problem:
  1. rollen nicht klar verteilt
  2. Zugangskontrolle zu Applikation sind unsicher
  3. Zuganskontrolle zu DB sind unsicher
  4. Entwickler haben zugriff auf Produktion
  5. Zuviele Admins
  6. ausgeschiedene Mitarbeiter haben Zugriff
- diese ersten 6 sind SAML Probleme

# From eZ to Zeta Components

- Migration from EZ to Zeta into Apache
- ...

# Continuous Improvement

- kaizen (kai change, zen good)
- Code is aging
- XP and Scrum are very compatible
- Technical debt (you need to pay interest)
- Improve code base
- use PHP\_CodeBrowser
- use phpmd

# Ran an den Klienten - ein Cache-Plugin für mysqlnd

- Performance increase:
  - ByteCodeCache => 161%
  - 5.2 auf 5.3 => 173%
  - mysqlnd => 180% (Zufall) mysqli und mysqlnd fast gleich schnell
  - mysqlnd plugins (in C) moeglich: load balancing, monitoring, performance
  - mysqlnd-uh => 168%
  - mysqlnd-qc/mysqlnd-qc-apc => 167%
  - anschalten vom cache mysqlnd\_qc.cache\_by\_default=1 => 188%
  - anschalten von table cache mysqlnd\_qc.cache\_no\_table = 1 => 194%
  - PHP 5.3.99-dev 249%

# HTML5 Security

- viel neue Tags und Attr
- viele neue und schlimmere XSS-Angriffe
- Information Exposure (Geolocation)
- Canvas (Remote Information Transport)
- Web Messaging (XSS)
- Web storage (XSS)
- Web SQL DB (XSS, SQL Injection)
- CORS