





Konzept eines Datenbankprototypen

Inhalt (1)

- 
- Projektvorstellung & Projektzeitplan
 - Softwarekomponenten
 - Detaillierte Beschreibung der System Bausteine

 - MySQL & Rechtesystem
 - Was ist eine Session?
 - Session \Rightarrow MySQL DB
 - Datenbank Demonstration
 - Ausblick
 - Fragen & Diskussion

Projektvorstellung

- 
- Realisierung eines Datenbank Prototypen
 - System muss sicher sein, soll den Benutzer aber nicht einschränken
 - System soll in höchstem Maße automatisiert sein
 - Gesamtkosten müssen so niedrig wie möglich gehalten werden ⇒ es dürfen nur Hardwarekosten entstehen
 - Bis Juni 2003 (in Verbindung mit Projekt 2) soll ein ansprechendes webbasiertes Ergebnis stehen

Softwarekomponenten

- Betriebssystem: Linux (Redhat 7.3)
- Secure WEB Server: Apache HTTPS
- Datenbank Management System: MySQL
- Middleware: PHP
- Häufige Verwendung dieser Kombination von Grundkomponenten \Rightarrow LAMP

- FTP Server: ProFTPD
- Firewall mit Iptables
- Zusätzliche Computersprachen: HTML, CSS, JavaScript
- Software ist kostenlos \Rightarrow Open Source, General Public License

Building a Firewall

- Auf iptables basierende Firewall (gShield-current release 2.8)
[<http://muse.linuxmafia.org/gshield.html> | 270603]
- Kann durch Konfigurationsdateien gesteuert werden:
Individuelle: `client_hosts`, `client_services`, `closed_ports`, ...
Globale: `gShield.conf`
- Kann durch ein graphisches FrontEnd gesteuert werden
- Test der Firewall durch `nessus` und `nmap`
[<http://www.nessus.org> | 270603]
[<http://www.nmap.org> | 270603]

Apache HTTPS Server(1/2)

• Aufbau

– Module

- *Einbindung beim Kompilieren*
- *Einbindung als DLL (flexibelste Methode)*
- *Erweiterbarkeit des Servers (mod_ssl)*

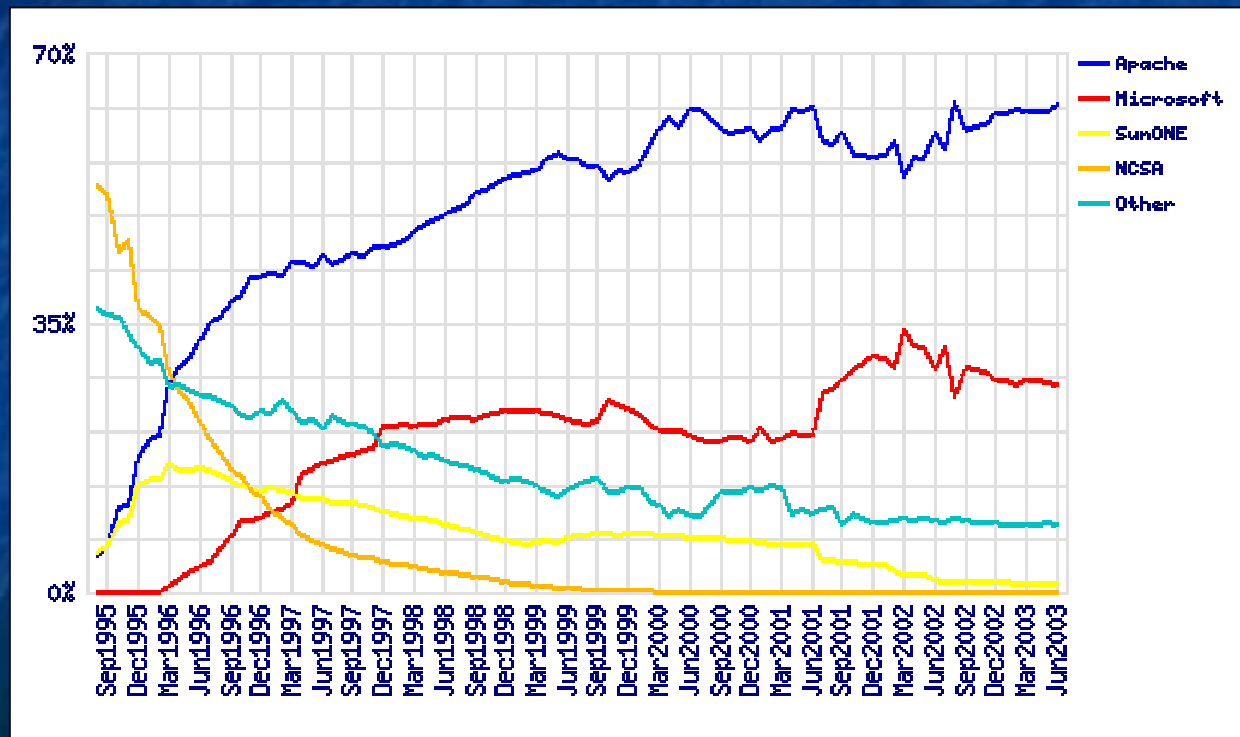
– Direktiven

- *in httpd.conf einstellbar*
- *Steuerung von Aktionen (deny in einem Directory)*
- *Umfang der Direktiven > 150*

Apache HTTPS Server(2/2)

- Verbreitung des Servers

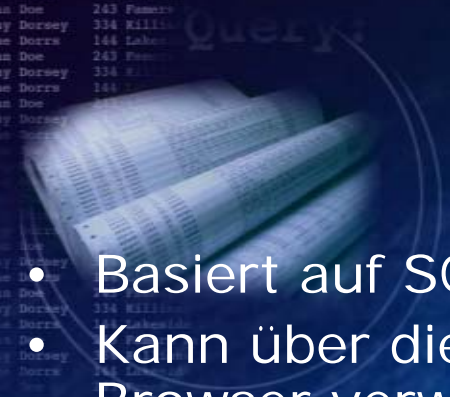
— [http://news.netcraft.com/archives/2003/06/12/_june_2003_web_server_survey.html | 270603]



PHP (PHP Hypertext Preprocessor)

- Scriptsprache zur Erstellung dynamischer Webseiten
- Einfach in HTML einzubetten
- Script wird am Server vom PHP-Interpreter ausgeführt (serverseitig)
- Besondere Stärke ist Verwendung von PHP mit Datenbanken
- MySQL wird direkt unterstützt

MySQL

- 
- Basiert auf SQL (Structured Query Language)
 - Kann über die Konsole aber auch graphisch z.B. über den Browser verwaltet werden ⇒ phpmyadmin [<http://www.phpmyadmin.net/> | 270603]
 - MySQL verwaltet:
 - beliebig viele Datenbanken mit...
 - beliebig vielen Tabellen welche...
 - beliebig viele Spalten und Zeilen haben können
 - Ausgeklügeltes Benutzer- und Rechtesystem
 - Zugriff auf MySQL mittels Benutzer/Passwort
 - Einschränkungen der Benutzer
 - *Datenbanken*
 - *Tabellen*
 - *Einzelne Spalten*
 - *Ausführbare Befehle*
 - *Lese/Schreibzugriff*

Client

URL, 1
Formulardaten



6

Server

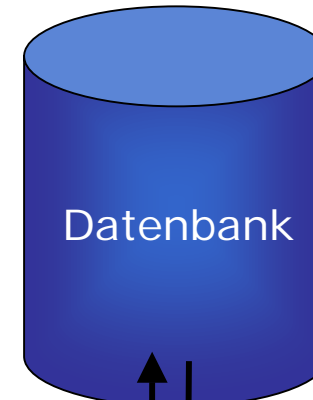
Webserver

```
<html>
<head>
<title>
<?php echo $seitentitel; ?>
</titel>
<h1>
<?php $news_header ?>
</h1>
```

PHP-Skript

```
<html>
<head>
<title>
Willkommen bei PHP!
</titel>
<h1>
HEUTE: Neue Release 4.0.18
</h1>
```

Webserver-Output

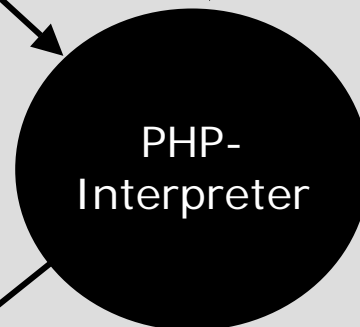


Datenbank

3
4


2

5



PHP-Interpreter

Inhalt (2)

- 
- MySQL & Rechtssystem
 - Was ist eine Session?
 - Session \Rightarrow MySQL DB
 - Datenbank Demonstration
 - Ausblick
 - Fragen & Diskussion

MySQL & Rechtesystem (1)

- Rechte sind in Datenbank „mysql“ gespeichert
- Besteht defaultmäßig aus 5 Tabellen
- Rangmäßig folgende Reihenfolge:
 - „user“
 - „host“
 - „db“
 - „tables_priv“
 - „columns_priv“

| Tabelle | Einträge | Typ | Größe |
|-------------------|----------|-----------|---------------|
| columns_priv | 0 | MyISAM | 1,0 KB |
| db | 1 | MyISAM | 3,1 KB |
| host | 0 | MyISAM | 1,0 KB |
| tables_priv | 0 | MyISAM | 1,0 KB |
| user | 2 | MyISAM | 2,5 KB |
| 5 Tabellen | 3 | -- | 8,7 KB |

| | Bearbeiten | Bearbeiten |
|------------------------|------------|------------------|
| | Löschen | Löschen |
| Host | % | 193.171.243.33 |
| User | | daniel |
| Password | | 521752a513424cf9 |
| Select_priv | N | Y |
| Insert_priv | N | Y |
| Update_priv | N | Y |
| Delete_priv | N | Y |
| Create_priv | N | Y |
| Drop_priv | N | Y |
| Reload_priv | N | Y |
| Shutdown_priv | N | Y |
| Process_priv | N | Y |
| File_priv | N | Y |
| Grant_priv | N | Y |
| References_priv | N | Y |
| Index_priv | N | Y |
| Alter_priv | N | Y |

MySQL & Rechtesystem (2)

- „user“ Tabelle enthält globale Rechte
 - Sind alle auf „Y“ darf Benutzer jeden Befehl in jeder Datenbank ausführen
 - Mit „N“ wird das Recht genommen
- Benutzer kann Zugriff bis auf Spaltenebene verwehrt/gestattet werden
 - Tabelle „host“ kontrolliert von welchen Hosts der Benutzer auf Datenbanken zugreifen kann
 - Tabelle „db“ verwehrt/gestattet Rechte auf Datenbanken
 - Tabelle „tables_priv“ verwehrt/gestattet Rechte auf Tabellen in Datenbanken
 - Tabelle „columns_priv“ verwehrt/gestattet Rechte auf Spalten in Tabellen
- Online Demonstration
 - <https://fmgeolx05.tu-graz.ac.at/phpMyAdmin-2.4.0/index.php>

| | Bearbeiten | Bearbeiten |
|-----------------|------------|------------------|
| | Löschen | Löschen |
| Host | % | 193.171.243.33 |
| User | | daniel |
| Password | | 521752a513424cf9 |
| Select_priv | N | Y |
| Insert_priv | N | Y |
| Update_priv | N | Y |
| Delete_priv | N | Y |
| Create_priv | N | Y |
| Drop_priv | N | Y |
| Reload_priv | N | Y |
| Shutdown_priv | N | Y |
| Process_priv | N | Y |
| File_priv | N | Y |
| Grant_priv | N | Y |
| References_priv | N | Y |
| Index_priv | N | Y |
| Alter_priv | N | Y |

Session

- Möglichkeit bestimmte Daten während einer Folge von Aufrufen der Website serverseitig festzuhalten
- Client wird mit „session_start()“ eine eindeutige ID zugewiesen ⇒ Session-ID
- Beliebige Anzahl von Variablen können in der Session gespeichert werden

Session & Sicherheit


- Session kann Sicherheitslücke darstellen
- Wenn Session-ID bekannt ist können Dritte auf Daten der Session zugreifen
- Maßnahmen dass Dritte nicht Informationen der Session lesen können:
 - Schutz der Session ID, keine Übertragung der Session ID über ungeschützte Netze ⇒ SSL
 - Session ID in der URL unsichtbar
- Zusätzliche Maßnahme im Projekt:
 - Session wird direkt in MySQL Datenbank gespeichert und obliegt somit wiederum dessen Rechtssystem
- Online Demonstration
 - <https://fmgeolx05.tu-graz.ac.at/search/database.php>
 - <https://fmgeolx05.tu-graz.ac.at/phpMyAdmin-2.4.0/index.php>

Datenbank Demonstration

- Login
- Such Algorithmus
- FTP Download
- FTP Upload
- Onlinedemonstration

– <https://fmgeolx05.tu-graz.ac.at/search/database.php>

Ausblick

- 
- FTP Server auf SFTP umstellen und Verbesserung des PHP-FTP Clients
 - Automatisierung der Benutzeranlegung (Script Unterstützung)
 - Verbesserung des Layouts
 - Abfangen und Unterdrücken von Fehlermeldungen (z.B. bei Ausfall einer Systemkomponente, PHP...)
 - Optimierung des Source-Codes
 - Überlegungen bzgl. Datenbackup (System, Database...)
 - Hardwareüberlegungen zur physischen Sicherheit (RAID...)
 - Detaillierte Dokumentation (Report)