web2py - Web-Framework mit didaktischem Hintergrund

Nik Klever
Hochschule Augsburg

web2py

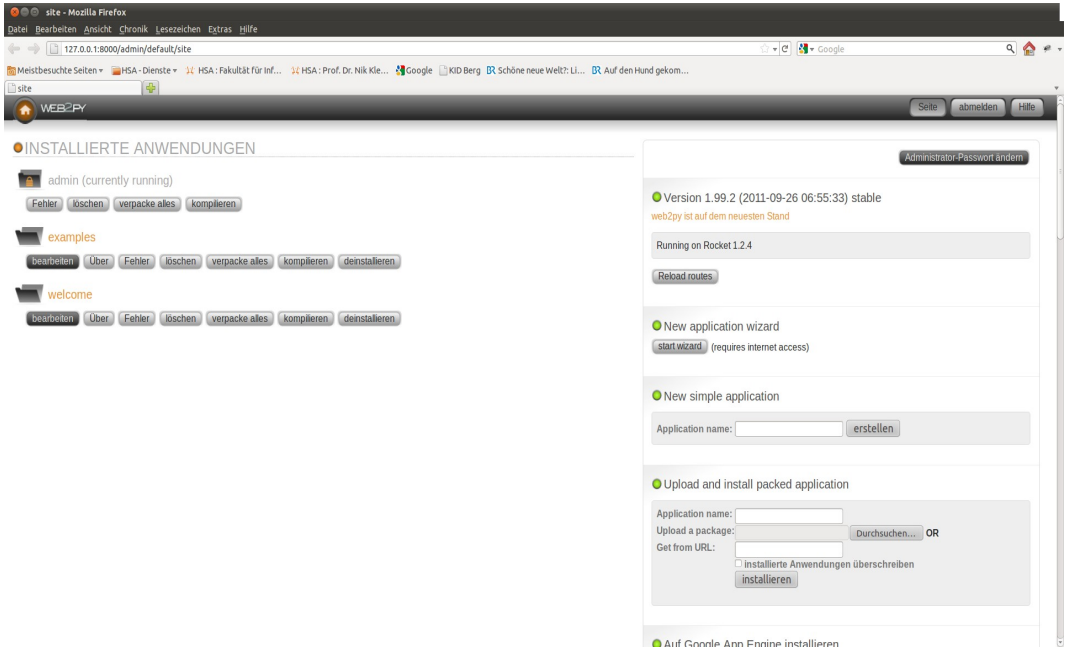
- ein modernes Python-Application-Framework,
- dessen Ausrichtung ursprünglich auf die Ausbildung von Studierenden abzielte,
- sich jedoch inzwischen generell als interessante Alternative für Python-basierte Web-Application-Frameworks entwickelt hat.

Grundlage

- Web-Application-Framework auf der Basis von Python
- SQLite 3 integriert
- Rocket Webserver integriert
- jQuery integriert
- trotzdem modular und einfach anbindbar an alle gängigen Datenbanken und Webserver

Usability

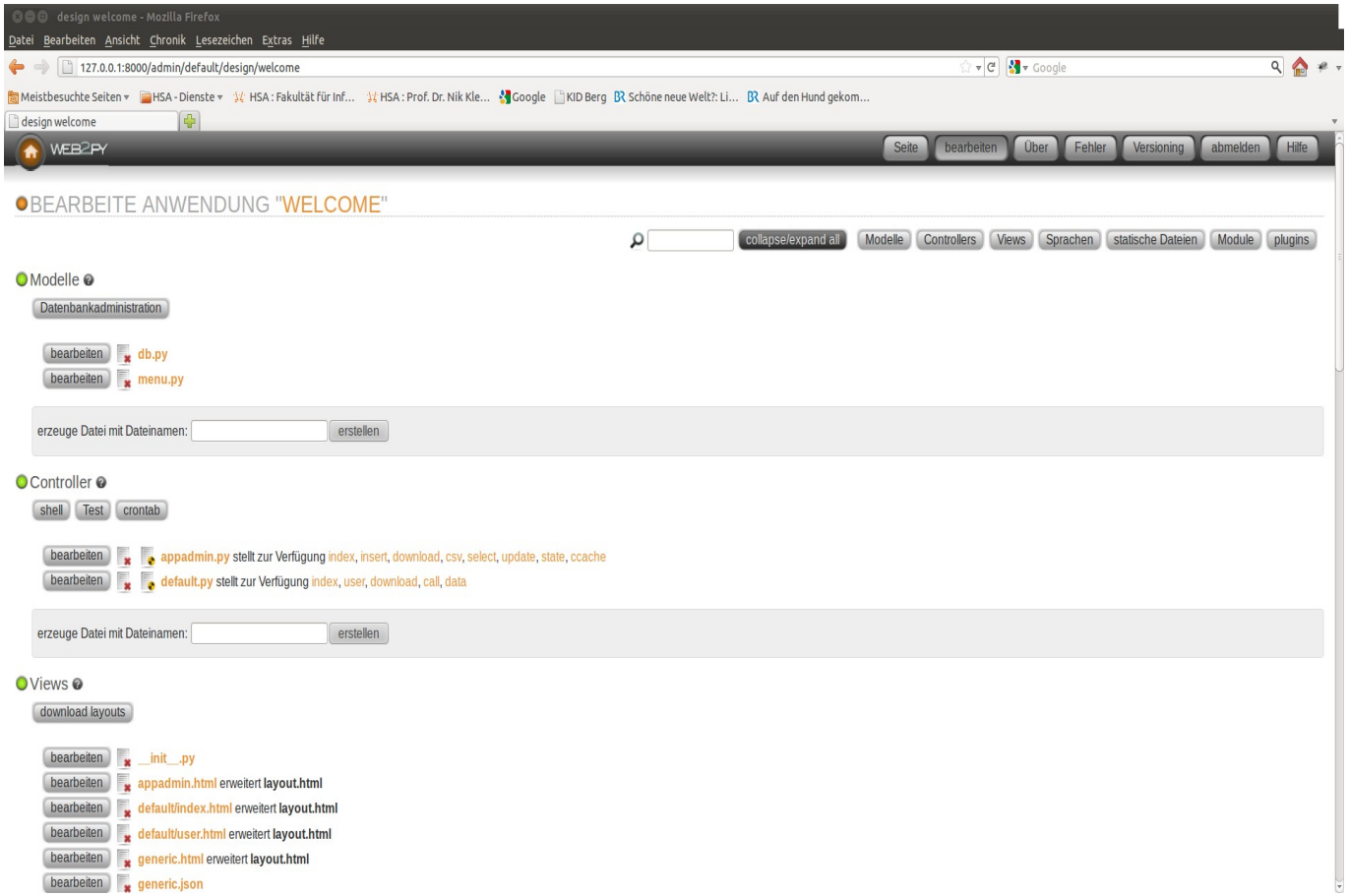
- Lauffähig auf allen gängigen Betriebssystemen und auf der Google Application Engine (GAE)
- Einfach zu installieren
  - exe (Windows), zip (Linux, Mac),
  - ein einziges Kommando: python web2py.py
- Einfach zu bedienen
  - Web-Schnittstelle
- Rückwärts kompatibel



Didaktik

- Architektur-Vorgabe
  Model – View – Controller

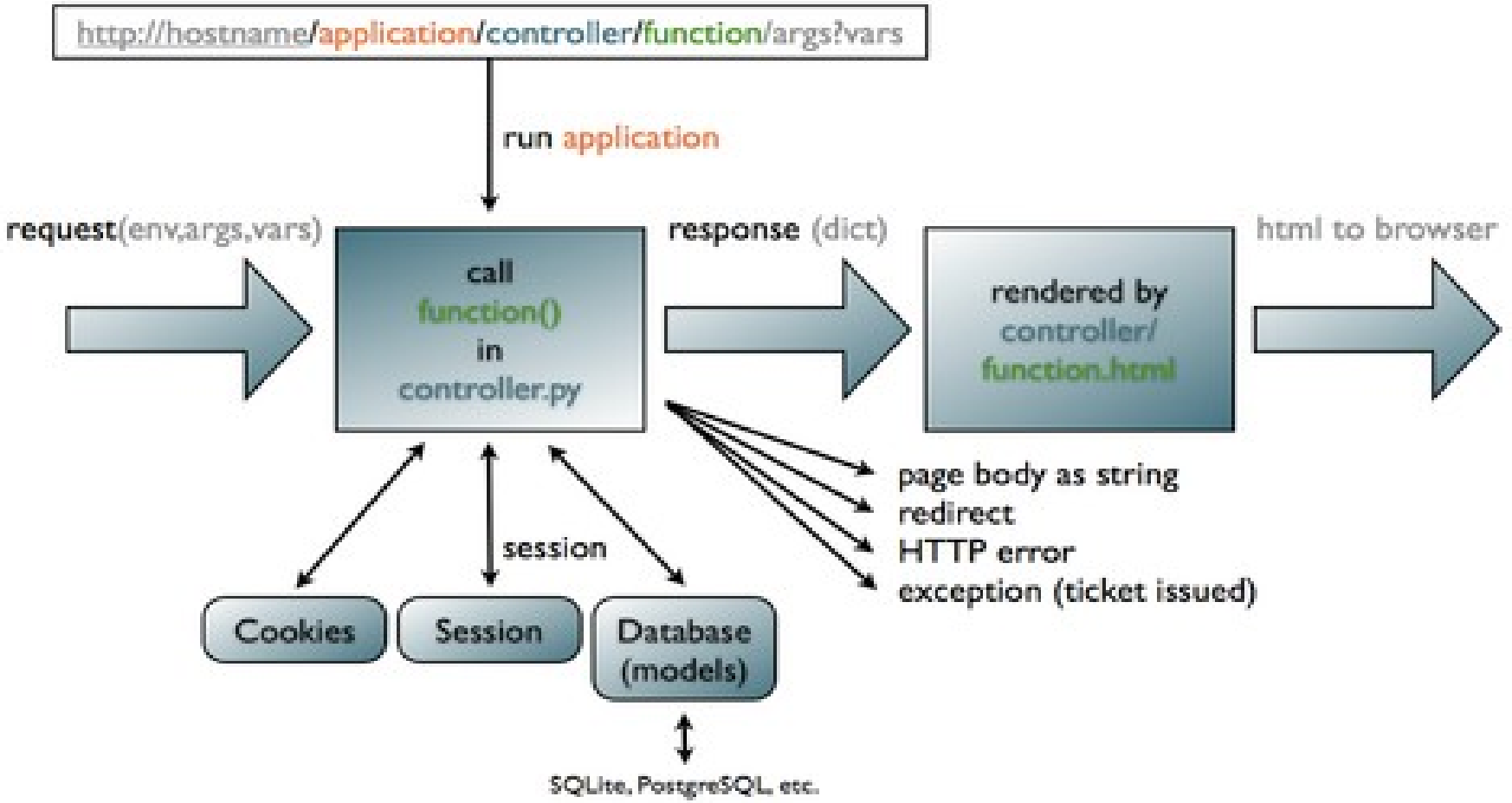
- einfache Installation und Bedienung
  - Web-Schnittstelle (Web-Editor)
  - Datenbank-schnittstelle (ohne SQL)
- gute Dokumentation
  - u.a. Online-Book



Apps - Applications - Anwendungen

- Jede Anwendung wird standardmäßig aus der Anwendung *welcome* kopiert und enthält bereits
  - ein Basis-Modell in model/db.py
  - Standard-Views im Ordner views/default/
  - Basis-Controller-Funktionen in controller/default.py
  - Standard-Übersetzungs-Tabellen im Ordner languages/
  - sowie weitere Ordner und Dateien …
- automatischer Import aller Framework-Komponenten
- Entwicklung und Einbindung eigener Module

URL Ablauf



Quelle: The Official web2py Book

View bzw. web2py Templates

- web2py benutzt {{ ... }} um Python Code in HTML einzubetten
- Der Vorteil von geschweiften Klammern anstelle von eckigen Klammern ist deren Transparenz in allen gängigen HTML Editoren, die somit von allen Entwicklern benutzt werden können, um web2py views zu erstellen
- Bei diesem Vorgang wird also Python Code in HTML eingebettet, also sollte notwendige Einrückungen entsprechend den HTML-Regeln erfolgen und nicht den Regeln von Python. Daher wird nicht eingerückter Python Code innerhalb der {{ ... }} Tags erlaubt. Da Python normalerweise Einrückungen zur Abgrenzung von Code Blöcken verwendet, ist eine andere Methode notwendig, um die Code Blöcke abzugrenzen. Deshalb verwendet die web2py Template Sprache hierfür das Python Schlüsselwort **pass**
- Ein Code Block beginnt mit einer Zeile wo am Ende der Zeile ein Doppelpunkt steht und endet mit einer Zeile die mit pass beginnt. Das Schlüsselwort pass ist nicht notwendig, wenn das Ende des Blocks aus dem Kontext heraus ersichtlich ist

Database Abstraction Layer

- **DAL – Database Abstraction Layer**
  - Einbindung der objektorientierten Konzepte von Python für die Datenbank-Anbindung
  - standardmäßig wird Web2py mit SQLite ausgeliefert
  - alle gängigen Datenbanken sind über die umfangreichen Python-Bibliotheken und DB-Schnittstellen eingebunden
  - die Google Application Engine ist ebenfalls in das DAL-Konzept eingebunden

Sicherheit - 1

Cross Site Scripting: web2py verändert standardmäßig alle Veriablen die in der View dargestellt werden

Injection Flaws (SQL Injection): web2py enthält einen Database Abstraction Layer, der SQL Injection unmöglich macht

Malicious File Execution*:* web2py erlaubt nur exponierten Funktionen die Ausführung von Code um Malicious File Execution zu verhindern. Importierte Funktionen sind niemals exponiert. Nur Aktionen können exponiert sein. web2py benutzt eine Web-basierte Administration Schnittstelle, die einem die Unterscheidung zwischen exponiert und nicht exponiert sehr leicht macht

Insecure Direct Object Reference: web2py gibt keine internen Objekte nach außen. web2py überprüft alle URLs, verhindert dadurch directory traversal attacks. web2py stellt auch einen einfachen Mechanismus zur Erstellung von Formularen zur Verfügung, die automatisch jede Eingabe überprüfen

Cross Site Request Forgery (CSRF): web2py verhindert CSRF genauso wie die zufällige doppelte Abgabe von Formularen über ein einmaliges Zufalls-generiertes Token, welches jedem Formular mitgegeben wird. Zudem benutzt web2py UUIDs für Session Cookies

Information Leakage and Improper Error Handling: web2py enthält ein Ticketing System. Kein Fehler kann in Code resultieren, die normale Benutzer zu Gesicht bekommen. Alle Fehler werden mitgeloggt und ein Ticket wird dem Benutzer ausgestellt, damit die Fehlerverfolgung durchgeführt werden kann. Fehler und Quellcode sind jedoch nur für den Administrator zugänglich

Sicherheit - 2

Broken Authentication and Session Management: web2py stellt einen eingebauten Mechanismus für die Administrator Authentifizierung zur Verfügung und es steuert Sessions für jede Anwendung unabhängig. Die Administrations Schnittstelle zwingt zur Nutzung sicherer Session Cookies, wenn der Client ist nicht „localhost“. Für Anwendungen enthält web2py eine leistungsfähige rollen-basierte Zugangs-Kontroll-API

Insecure Cryptographic Storage: web2py benutzt den MD5 oder den HMAC+SHA-512 Hash Algorithmus um abgespeicherte Passwörter zu schützen

Insecure Communications: web2py enthält den SSL-freigegebenen Rocket WSGI Webserver, aber es kann ebenso Apache oder Lighttpd und mod_ssl benutzen, um die Kommunikation mittels SSL Kodierung sicher zu machen

Failure to Restrict URL Access: web2py bildet URL Requests auf Python Module und Funktionen ab. web2py stellt einen Mechanismus zur Verfügung um Funktionen öffentlich oder über Authentifizierung und Authorisierung zugangsbeschränkt zu deklarieren. Die in web2py enthaltene rollen-basierte Zugangskontroll-API erlaubt Entwicklern den Zugang auf jede Funktion basierend auf login, Gruppenmitgliedschaft oder Gruppenbasierte Bewilligungen zu beschränken.

Weitere Aspekte

- Internationalisierung
- unterschiedliche und anpassbare Authentifizierungsmethoden
- rollen-basierte Zugangskontrolle
- Fehlerprotokollierung und Ticketsystem
- jQuery-Einbindung
- Anbindung unterschiedlichster Protokolle (HTML, XML, JSON, RSS, CSV, …)
- Mercurial-Versionierung für die Anwendungen
- Social-Media Integration (Google, Twitter, Facebook, ...)

Plugins und Komponenten

- Komponenten:
  - Konzept von modularen Anwendungen, jedoch mit minimaler Server Auslastung und maximaler Wiederbenutzung von Code
  - Eine Komponente ist ein funktional autonomer Teil einer Webseite
- Plugins:
  - Ein Plugin ist eine beliebige Untermenge von Dateien einer Anwendung
  - Ein Plugin stellt einen Mechanismus zur Verfügung, eine Untermenge einer Anwendung so zusammenzupacken, dass diese für andere Anwendung entsprechend ausgepackt und dort wiederverwendet werden kann
    - Ein Plugin muss nicht funktional autonom sein und es kann von anderen plugins oder irgendeinem anderen Code abhängig sein
    - Ein Plugin ist nicht Teil eines Plugin-Systems und muss sich aus diesem Grund weder registrieren noch muss es isoliert werden, obwohl Regel vorgegeben sind, um eine gewisse Isolierung zu erreichen

Community

- wachsende und agile Community
  http://groups.google.com/group/web2py/
- rasante Entwicklung
  - 09/2011: 1.99
  - 09/2010: 1.85
  - 09/2009: 1.66
  - 09/2008: 1.49
  - 09/2007: Gluon 1.0

Web2py Mobile

- Einbindung als Client via
  jQuery mobile
- Einbindung als Server via
  SL4A – Scripting Layer for Android
  - Notwendige Anpassung:
    das Standard-Python Module shelve läuft infolge des Rückfalls von anydbm auf dumbdbm unter Android nicht korrekt
  - Nachteil:
    Probleme mit der Disk-Cache-Funktionalität

Bossie Awards 2011
for Best Open Source Development Software

Als Massimo Di Pierro, Professor für Computerwissenschaften an der DePaul University, web2py plante, hatte er als Ziel vor Augen, ein Python-basiertes Web-Framework zu entwickeln, das sowohl leistungsstark als auch einfach zu bedienen ist. Es ist ihm gelungen. Web2py ist ein intelligent konzipiertes, gut gemachtes Framework von kleinem Umfang, einer übersichtlichen API, einer hervorragenden Dokumentation und einem allumfassenden Web-basierten Administrations-Tool sowie einer kompletten integrierten Entwicklungs-umgebung. Die Installation ist einfach, Assistenten helfen dabei, neue Anwendungen sehr schnell zu erzeugen und die Komplexität ist herausgenommen. Web2py ist ein starkes und umfangreiches Framework mit vielen angenehmen Überraschungen - ein herausragendes unter allen Python-Frameworks.

http://www.infoworld.com/d/open-source-software/bossie-awards-2011-the-best-open-source-application-development-software-171759-0

Quellen

- www.web2py.com
- Massimo di Pierro: The Official web2py Book (3rd ed.), 2010
- Infoworld.com: BOSSIE Awards - Best of Open Source Software