Fall 2013 CDC Web Crash Course

Ben Holland

bholland@iastate.edu

www.ben-holland.com/slides

Its OK to Fail…

- This is probably the:
  - Largest web app
  - Weirdest web app
  - Most complex web app
- Time is really crunched this year…
- This is closer to something you might find in industry
  - Difficult to just rewrite the whole thing before the competition
- Everyone is struggling…but that's ok.
- Just learn something and have fun!
- Ask lots of questions!

Full Disclosure

- I’m not a professional “web” developer
  - But I’m not too shabby at it either
- I probably messed things up accidently
  - Also messed up some things intentionally…
- Most of this is new to me too!
  - I picked new things so I get to learn too
- I do my best but I get things wrong too
  - So sorry if I explain something to you wrong!

Why Scala (programming language)?

- Scala is considered one of the hot new languages to learn right now
- Scala is used in industry
  - Twitter switched large portions of the backend from Ruby to Scala
  - Foursquare is written in Scala
  - LinkedIn wrote many of its API's in Scala
- It's not PHP (I'm sick of PHP)
- I wanted to learn something new…

Why Play2 (Web Framework)?

- It’s a framework used by industry
  - Heroku and Google App Engine both support Play
- Introduces some important web concepts
  - MVC (Model-View-Controller)
  - RESTful services
  - View templates, JSON, routes, etc
- Has full support for Java JRE
- I wanted to learn something new…
  - Just be glad I decided against Scala/Lift framework

Why PostgreSQL

- It’s not MySQL (most of you should be bored of MySQL by now…)
- PostgreSQL and MySQL are very similar
- Both are widely used

I hate you…

- Good. I don’t care.
  - Actually I do care…but I’m not sorry.

Some Stats

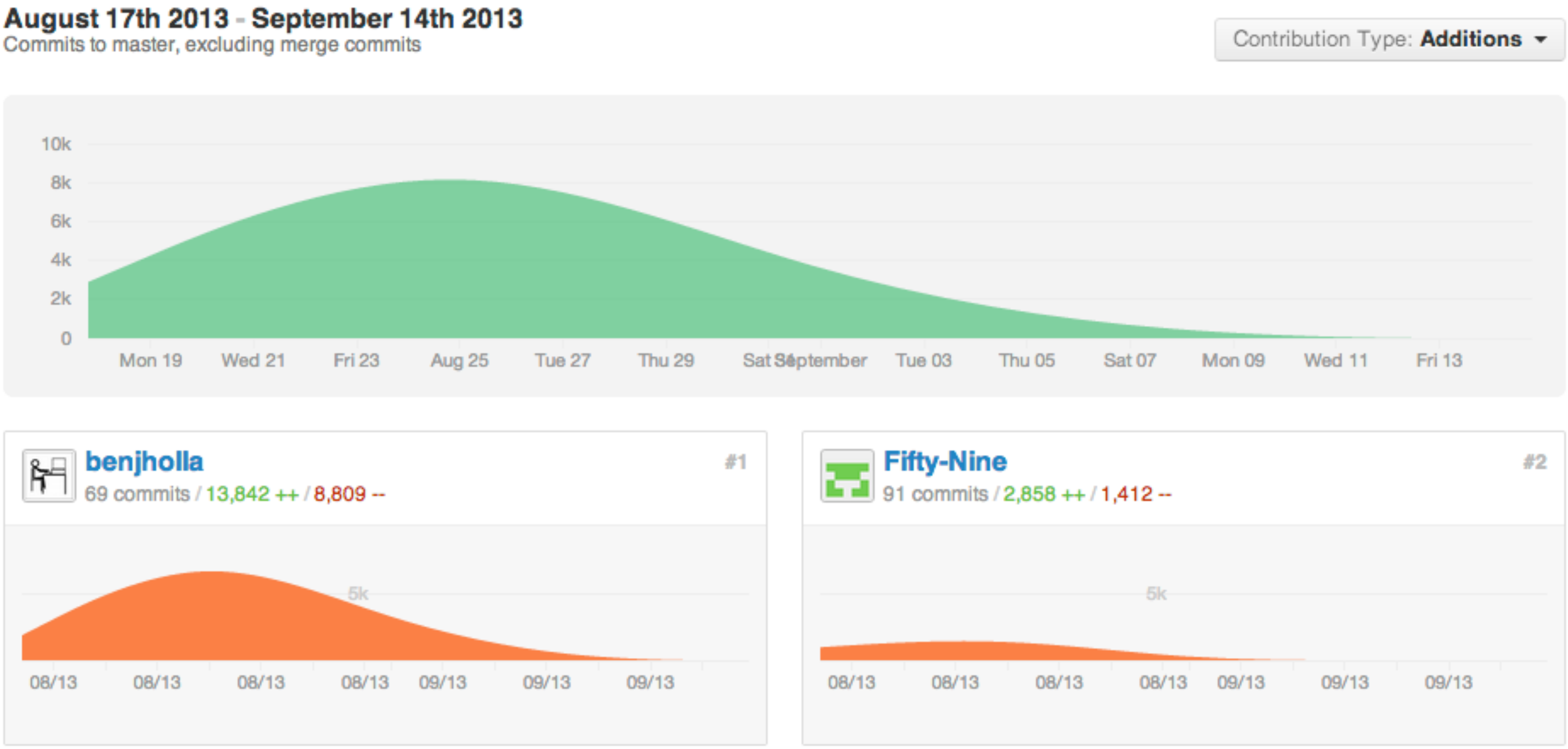
```
Desktop$ ./cloc-1.60.pl Blackbook-master.zip
      89 text files.
      89 unique files.
      14 files ignored.

http://cloc.sourceforge.net v 1.60  T=0.39 s (190.0 files/s, 15384.8 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
CSS                              7            114            111           1910
HTML                            25            253              0           1715
Scala                           30            284             46           1369
SQL                              9             52              0            143
Javascript                       3              3             11             35
Java                             1              7              0             20
-------------------------------------------------------------------------------
SUM:                            75            713            168           5192
-------------------------------------------------------------------------------
```

- ~5,000 Lines of Code

Some Stats

- 2 developers for ~1 month to build



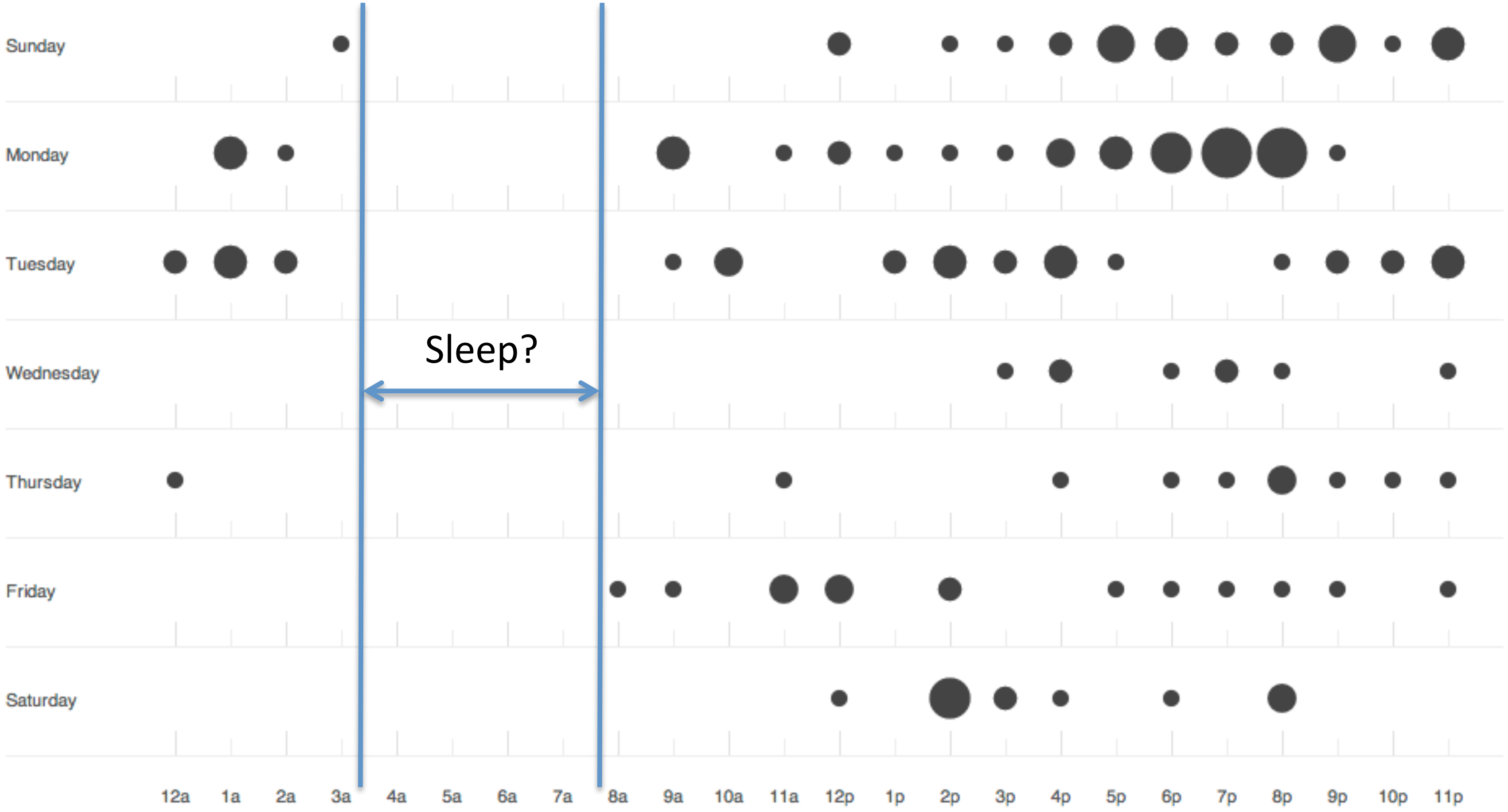
August 17th 2013 - September 14th 2013
Commits to master, excluding merge commits

Contribution Type: **Additions**

benjholla #1
69 commits / 13,842 ++ / 8,809 --

Fifty-Nine #2
91 commits / 2,858 ++ / 1,412 --

Some Stats



Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sleep?
12a
1a
2a
3a
4a
5a
6a
7a
8a
9a
10a
11a
12p
1p
2p
3p
4p
5p
6p
7p
8p
9p
10p
11p

Production Vs. Development

- You are a security group hired to protect the business
  - So don't go messing up the company website!
  - You don't see Max debugging the live version of IScore by trying insert XSS attacks…
  - Use the dev environment for that, then push changes to production AFTER you test them
- Development Environment
  - http://download.iseage.org/web_dev.zip (local)
  - Also clonable in VSphere

Go go gadget Dev Machine!

- Overview of the Blackbook web app

- cd ~/Desktop/Blackbook
- play run
- Open your web browser to:
  http://127.0.0.1:9000

Note: Play if you find play command is missing on the path..

Quick Fix: *export PATH="$PATH:/usr/local/lib/play2”*

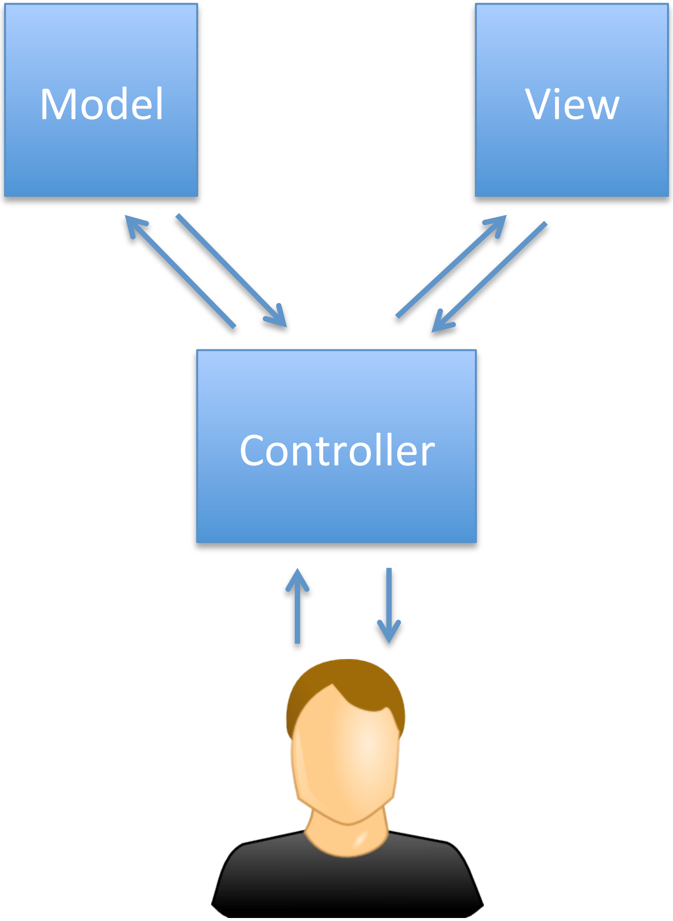
Permanent Fix: *sudo vi /etc/environment*

Change: *PATH="/usr/local/..../usr/games:/usr/local/lib/play”*

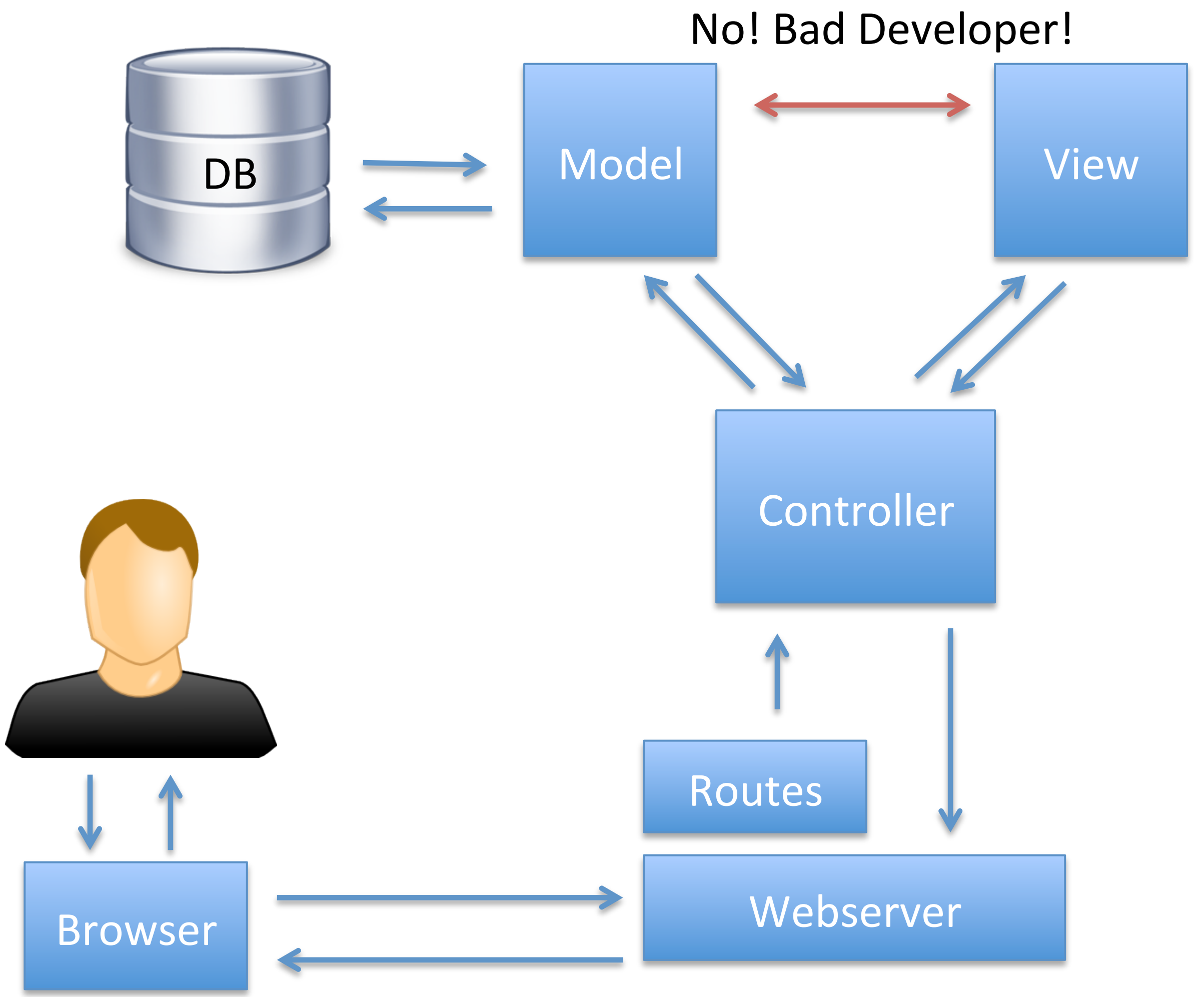
To: *PATH="/usr/local/..../usr/games:/usr/local/lib/play**2**”*

Must log out and then log in again for changes to take effect

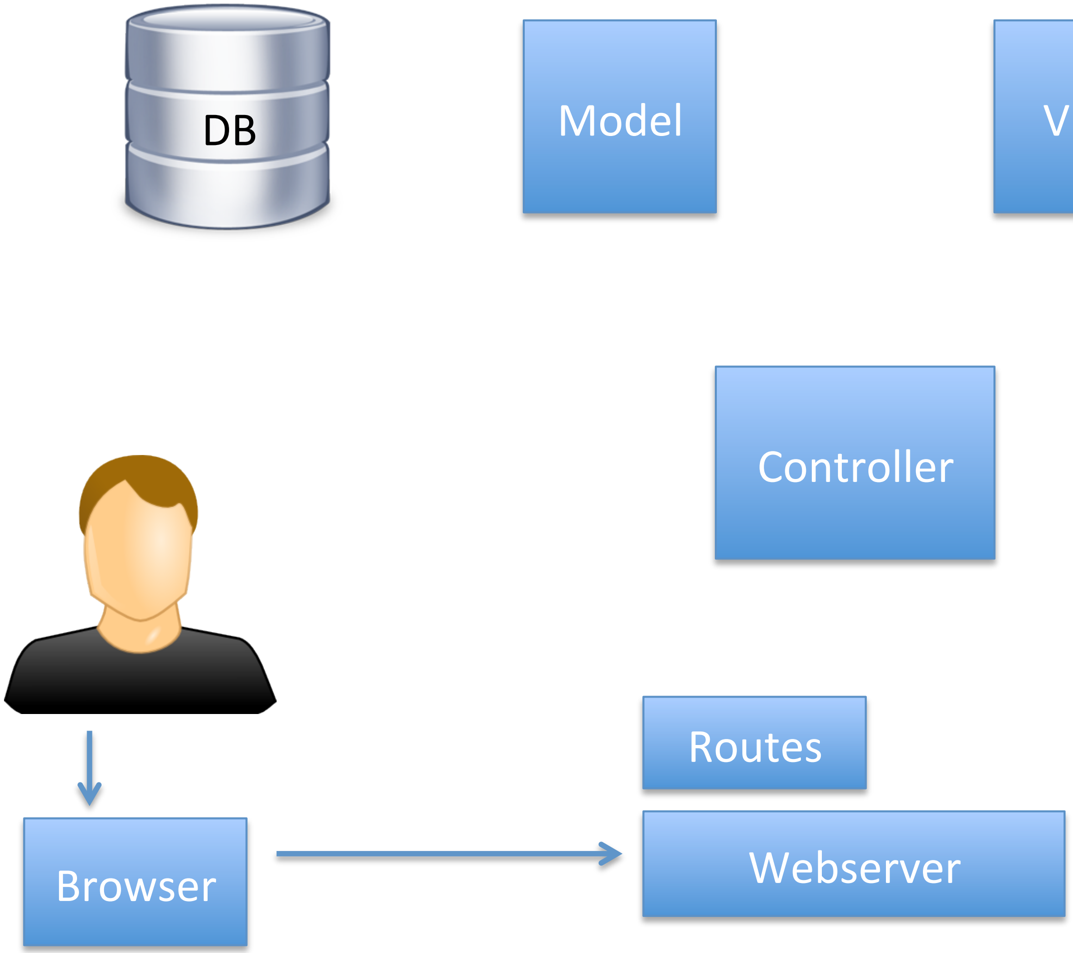
Model-View-Controller



Model-View-Controller (detailed)



Model-View-Controller (example)



DB

Model

View

Controller

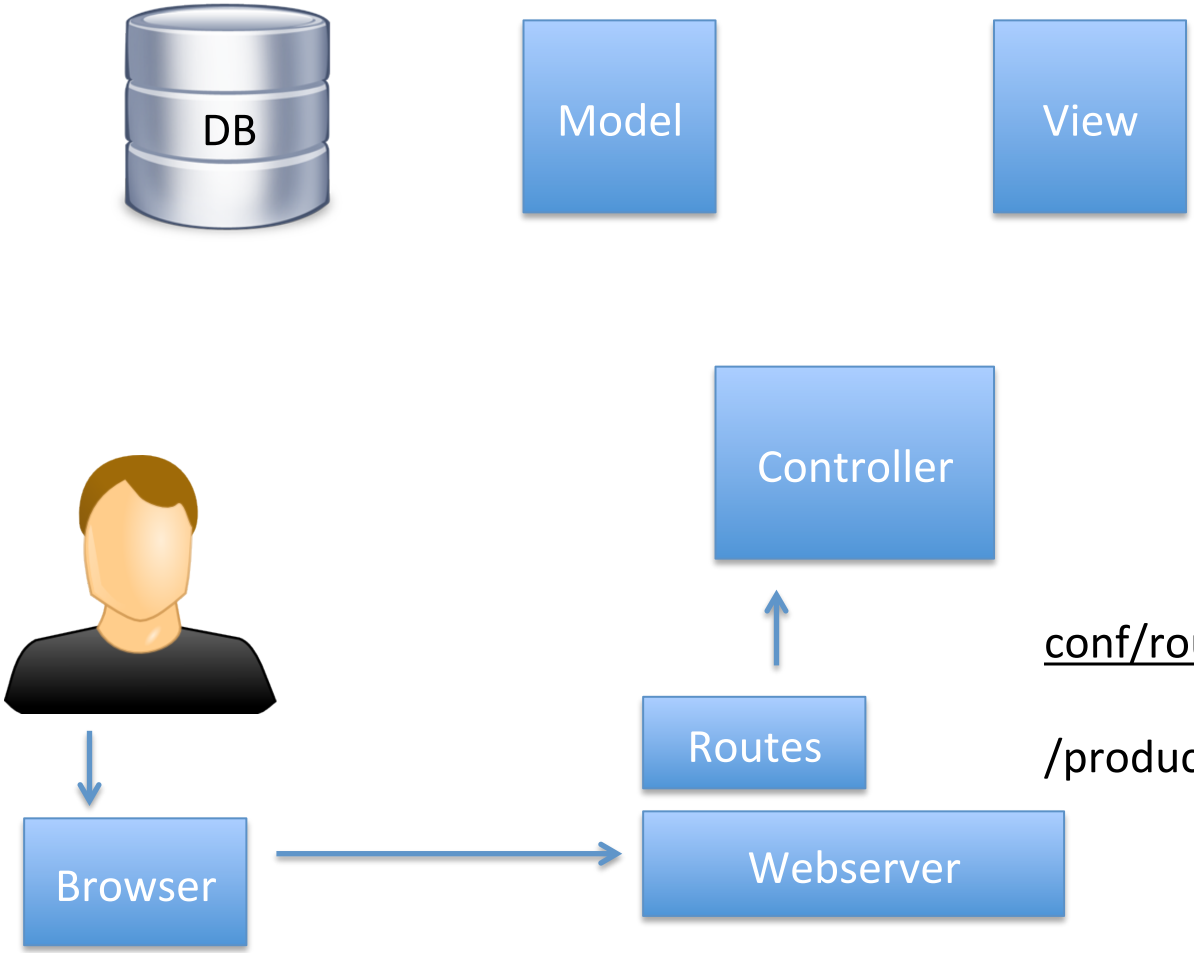
Routes

Webserver

Browser

http://127.0.0.1:9000/products

Model-View-Controller (example)



DB

Model

View

Controller

Routes

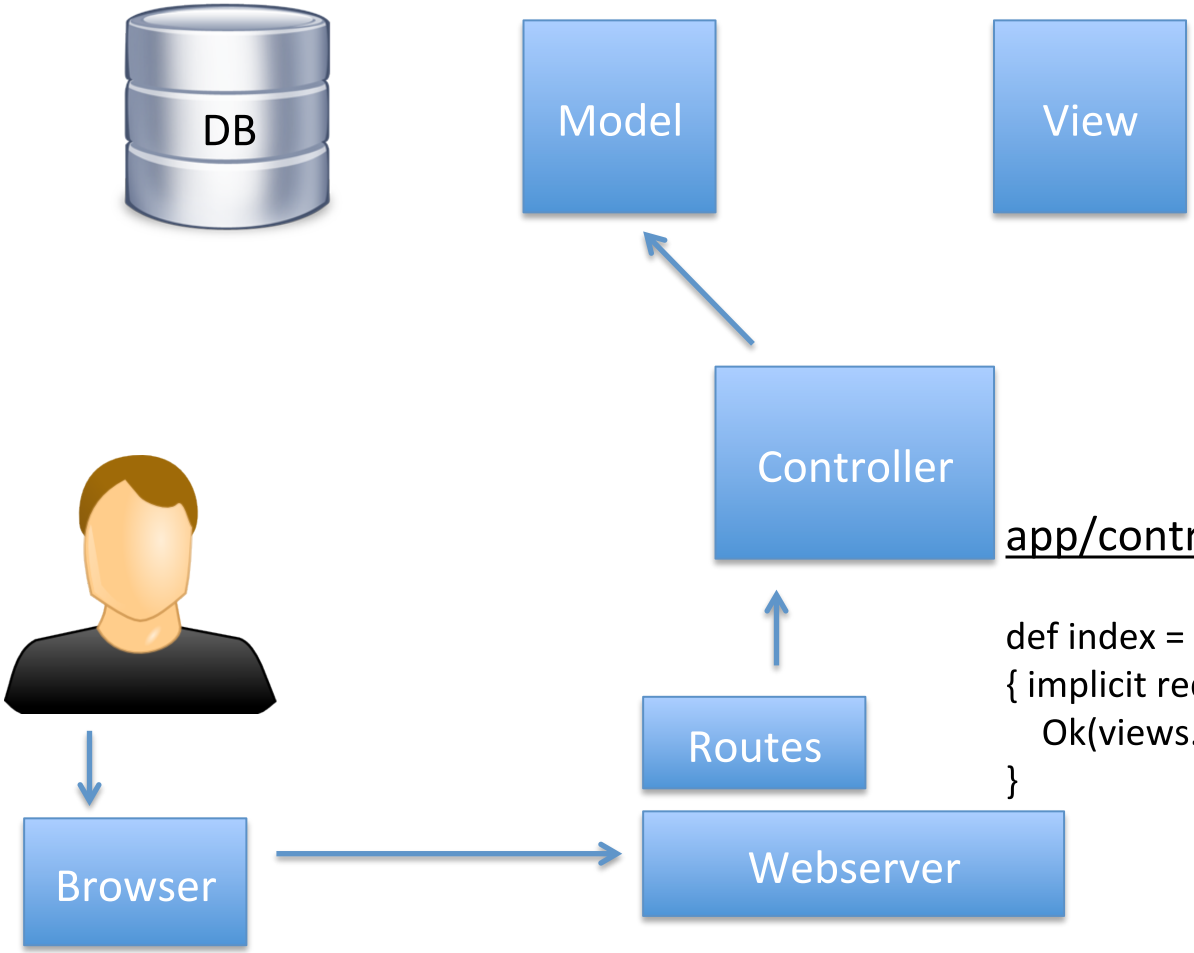
Webserver

Browser

<u>conf/routes.scala</u>

/products   controllers.Products.index

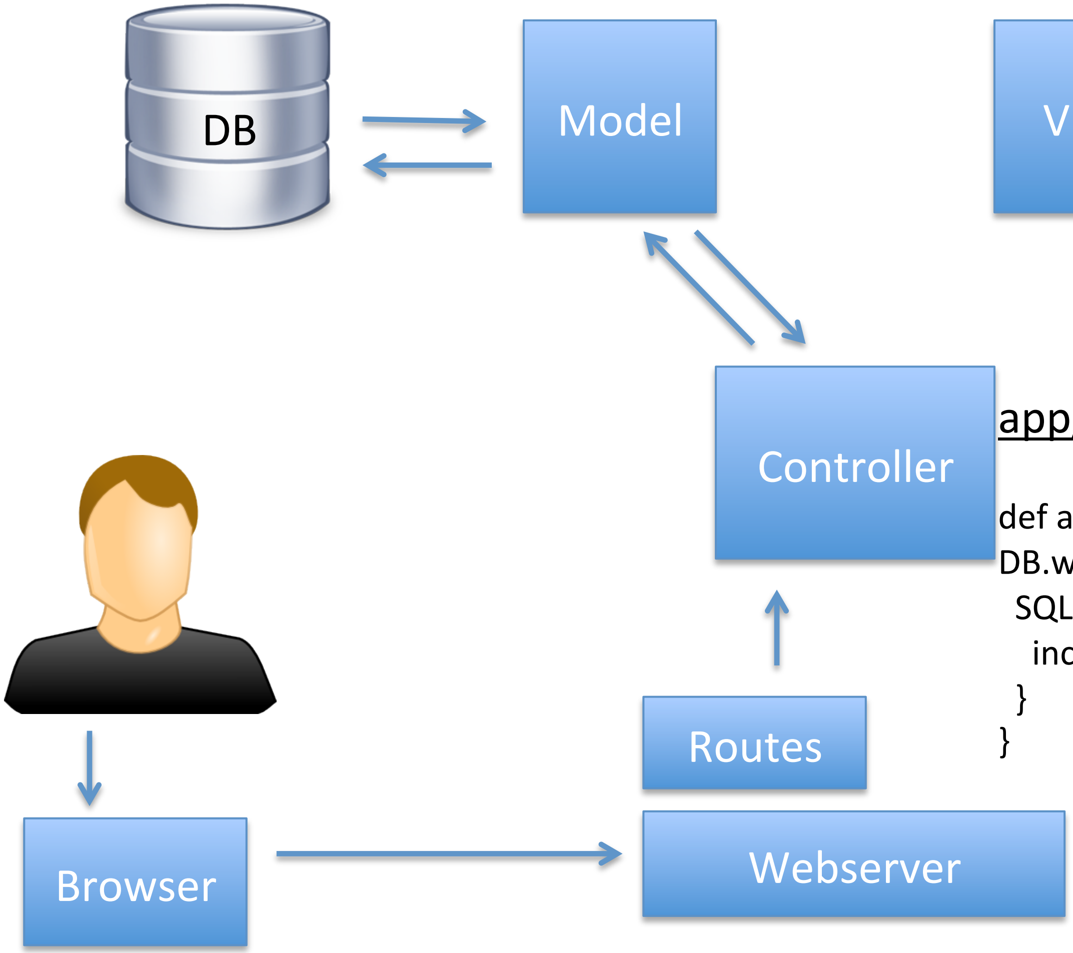
Model-View-Controller (example)



app/controllers/Products.scala

```
def index = WithPermissions(Perm.ViewProducts)
{ implicit request =>
   Ok(views.html.products.index(Product.all()))
}
```

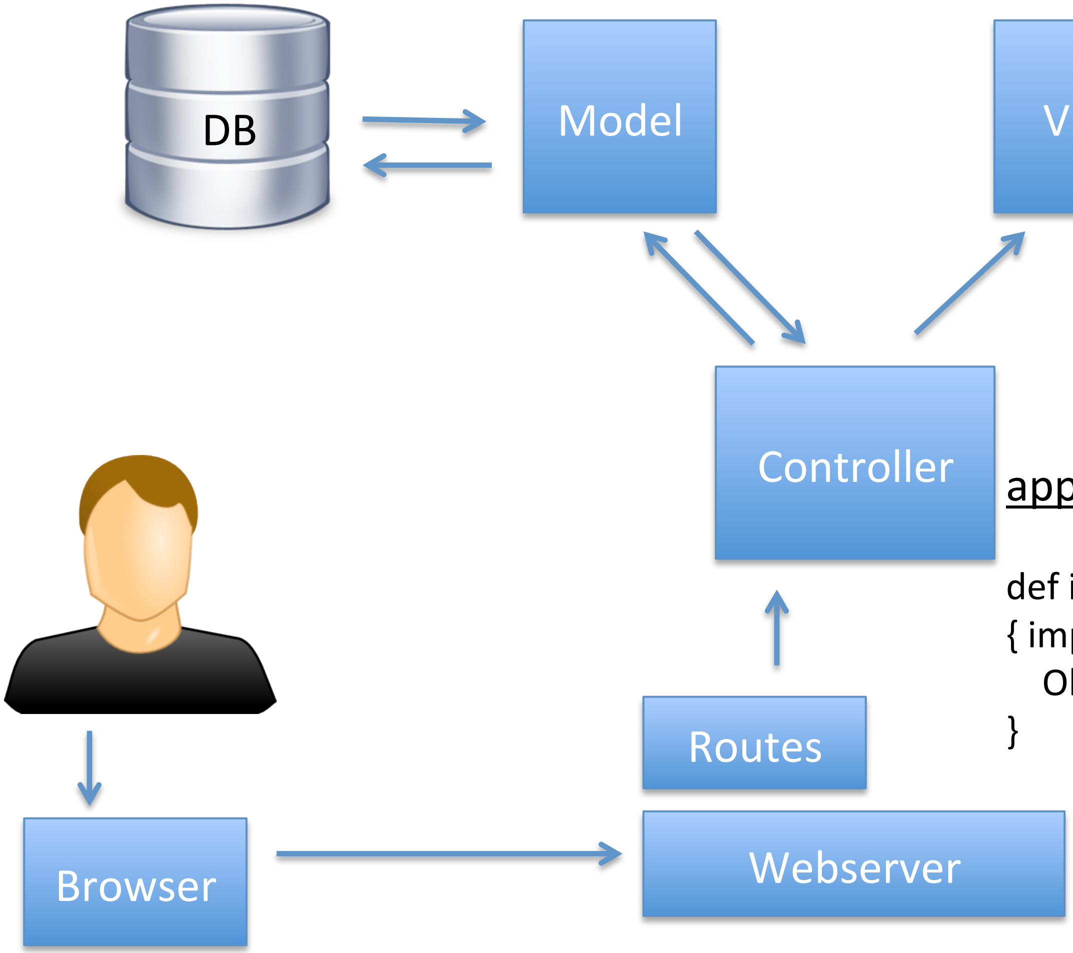
Model-View-Controller (example)



app/models/Product.scala

```
def all(includeDisabled: Boolean = false): List[Product] =
DB.withConnection { implicit c =>
  SQL("SELECT * FROM Products").as(product *).filter { p =>
    includeDisabled || p.isEnabled
  }
}
```

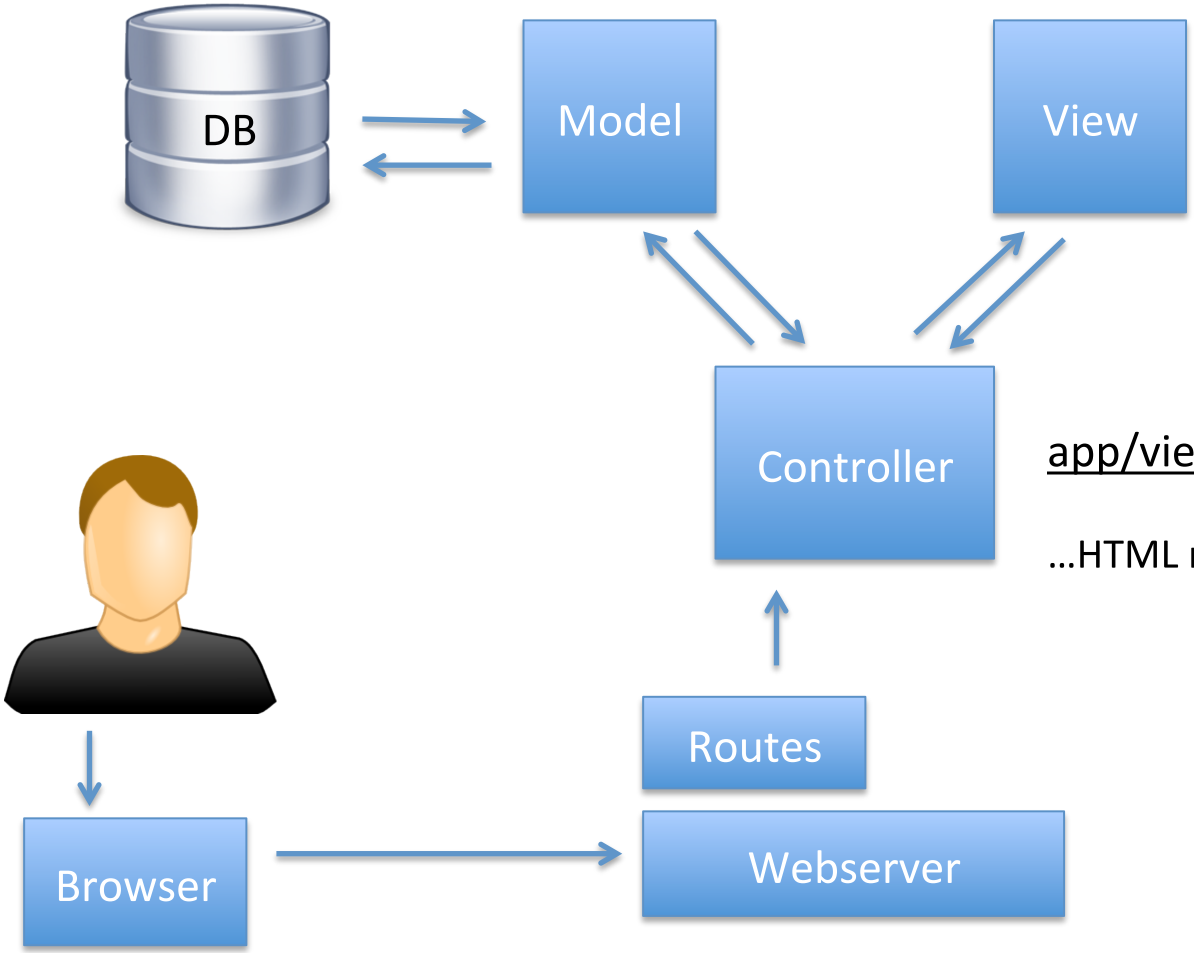
Model-View-Controller (example)



app/controllers/Products.scala

```
def index = WithPermissions(Perm.ViewProducts)
{ implicit request =>
   Ok(views.html.products.index(Product.all()))
}
```

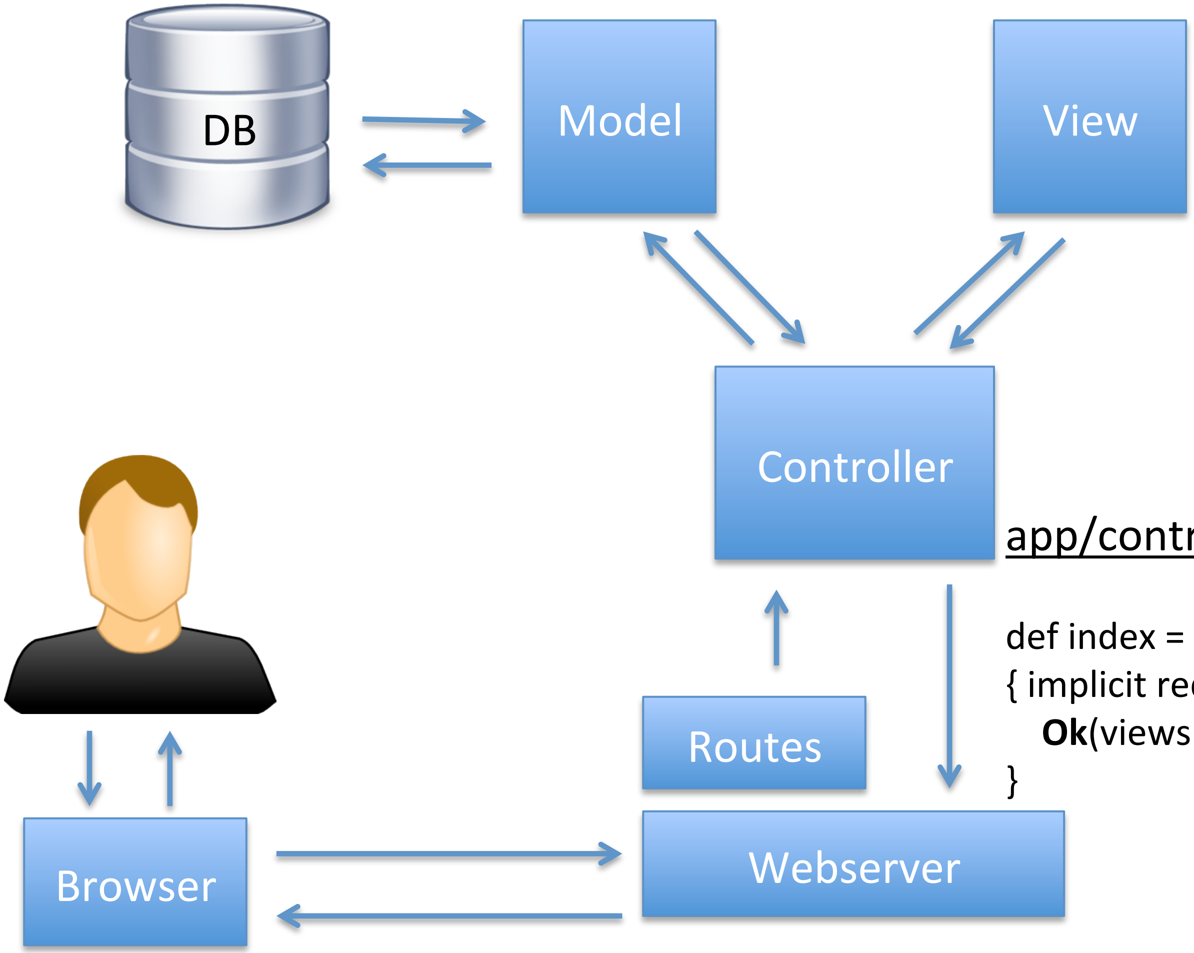
Model-View-Controller (example)



app/views/products/index.scala.html

…HTML rendering code….

Model-View-Controller (example)



app/controllers/Products.scala

```
def index = WithPermissions(Perm.ViewProducts)
{ implicit request =>
   Ok(views.html.products.index(Product.all()))
}
```

Database Security

- PostgreSQL database name is “blackbook”
- Relevant Files:
  - /etc/postgresql/9.1/main/postgresql.conf
  - /etc/postgresql/9.1/main/pg_hba.conf
- Restart service for changes to take effect
  - sudo service postgresql restart

- PostgreSQL can restrict access to various IP addresses and users
- Is your Database doing that?
- Does your database need to be accessed outside of your network?
  - Does it need to be accessed from anywhere except the Web box?

Major Hints

- Default Logins
  - Developers are lazy…
  - How do you add the first user?
- Stored XSS
  - Try entering <script>alert(42);</script> into forms..
- User Access Issues
  - Do all users have appropriate permissions?
  - Are user sessions handled properly?
  - Are controllers asking for the right permissions?
  - Are controllers actually enforcing permissions?

Major Hints

- Views do not protect controllers they only display
  - Are all controllers properly protected?
    - Use: WithPermissions method, not WithSomePermission
    - WithSomePermission basically equals isUserLoggedIn
  - What about controllers for the JSON API?
- Are your user passwords hashed?
  - For extra security you can salt them too
- How does your app handle errors?
  - Debug pages are not good in production environments

Super Duper MAJOR Hints

- We "generally" wrote the web app to be secure.
  - The last few days of development I mixed in some bug fixes and vulnerabilities…
  - Web app was developed with Git on Github
  - https://github.com/benjholla/Blackbook
  - Version Control is a wonderful thing…
- Developers:
  - Make mistakes, may be malicious, may not understand what they are doing…
  - Comments are not always to be trusted…

How do I deploy to Production?

- Use Git!
  - Make a git patch
  - Fork the repo online and push changes there
    - Github has 5 free private repos for students
      - https://github.com/edu
    - git clone <your repo url here>
  - Upload somewhere then download it to web
- On web box recompile the new source
  - In /var/www/webapp run "play clean compile stage"
  - Output startup script gets placed in:
    var/www/webapp/target/start
  - http://www.playframework.com/documentation/2.0/Production
  - sudo service webapp stop
  - sudo service webapp start

What questions do you have?

- Come to Lab Jam and we can fix stuff together!