# 环境搭建

Ubuntu

sudo apt-get install python-virtualenv

**Windows**

pip install virtualenv

c:\python27\Scripts\pip install virtualenv

cd e:\projects\tutorial-flask

c:\python27\Scripts\virtualenv venv

激活虚拟环境

venv\Scripts\activate

deactivate

安装flask

pip install flask

# Python 语法

装饰器

类变量 类方法

属性函数

@property 内置装饰器，把一个方法变成属性调用

class Student(object):

@property

def score(self):

return self.\_score

@scroe.setter

def score(self,value):

self.\_score = value

**Q: @staticmethod 和 @classmethod区别 ？**

A: 区别如下：

@staticmethod不需要表示自身对象的self和自身类的cls参数，就跟使用函数一样。

@classmethod也不需要self参数，但第一个参数需要是表示自身类的cls参数。

# 社交博客程序

## 用户认证

Flask-Login 管理已登录用户的用户会话

pip install flask-login

**Flask-Login要求实现的用户方法**

is\_authenticated() 如果用户已经登录，必须返回True，否则返回False

is\_active() 如果允许用户登录，必须返回True，否则返回False。如果要禁用账户，可以返回False

is\_anonymous() 对普通用户必须返回False

get\_id() 必须返回用户的唯一标识符，使用Unicode 编码字符串

Werkzeug 计算密码散列值并进行核对

generate\_password(password,method=pbkdf2:sha1,salt\_length=8)

check\_password\_hash(hash,password)

Q:即使u1和u2两个用户使用相同的密码，散列值也不一样？

A:加密时混入一段“随机”字符串（盐值）再进行哈希加密。即使 密码相同，如果盐值不同，那么哈希值也是不一样的。

itsdangerous:生成并核对加密安全令牌

**对于不同的程序功能，使用不同的蓝本，是保持代码整齐有序的方法。**

1

认证用户

注册用户

确认用户

管理用户

## 用户角色

## 用户资料

用户头像

<https://secure.gravatar.com/avatar/aa3acadb60d47c8115913339d6d59366>

https://secure.gravatar.com/avatar/ d4c74594d841139328695756648b6bd6

# 大型程序结构

多文件Flask程序基本结构

Flask(project name)

|-app 主要代码包含在这个app包中

|-templates/

|-static/

|-main/

|-\_\_init\_\_.py

|-errors.py

|-forms.py

|-views.py

|-\_\_init\_\_.py

|-email.py

|-models.py

|-migrations/ 数据库迁移脚本

|-tests/ 单元测试

|-\_\_init\_\_.py

|-test\*.py

|-venv/ 虚拟环境

|-requirements.txt 列出所有依赖包，便于重新生成相同的虚拟环境

|-config.py 配置

|-mange.py 用于启动程序及其他的程序任务

需求文件如何产生？

pip freeze > requirements.txt

pip install -r requirements.txt

# 电子邮件-邮箱

测试邮箱

[pythonflaskytest@gmail.com](mailto:pythonflaskytest@gmail.com)

pip install flask-mail

**Flask-Mail SMTP 服务器配置**

MAIL\_SERVER localhost 电子邮件服务器的主机名或IP 地址

MAIL\_PORT 25 电子邮件服务器的端口

MAIL\_USE\_TLS False 启用传输层安全（Transport Layer Security，TLS）协议

MAIL\_USE\_SSL False 启用安全套接层（Secure Sockets Layer，SSL）协议

MAIL\_USERNAME None 邮件账户的用户名

MAIL\_PASSWORD None 邮件账户的密码

Ubuntu

(venv) $ export MAIL\_USERNAME=<Gmail username>

(venv) $ export MAIL\_PASSWORD=<Gmail password>

Windows

(venv) $ set MAIL\_USERNAME=<Gmail username>

(venv) $ set MAIL\_PASSWORD=<Gmail password>

发送电子邮件

同步

异步：启动一个线程发送电子邮件

如果程序需要发送大量电子邮件时，使用专门发送电子邮件的作业要比给每封邮件都新建一个线程更合适。Celery任务队列（http://www.celeryproject.org/）

# 数据库

pip install flask-sqlalchemy

## MySQL For Python 安装

安装mysql-python 的步骤

pip install mysql-python

Windows下可能需要安装离线安装包

<https://download.microsoft.com/download/7/9/6/796EF2E4-801B-4FC4-AB28-B59FBF6D907B/VCForPython27.msi>

<https://cdn.mysql.com//Downloads/Connector-C/mysql-connector-c-6.0.2-win32.msi>

1. VCForPython27.msi
2. mysql-connector-c-6.0.2-win32.msi

**可能连接不上数据库**

**<2003,”Can’t connect to MySQL server on ‘localhost’(10061)”>**

mysql://root:123456@localhost:3306/dbname

需要将localhost 修改为 127.0.0.1

## SQLAlchemy 列类型

**类型名 Python类型 说明**

Integer int 普通整数，一般是32 位

SmallInteger int 取值范围小的整数，一般是16 位

BigInteger int 或long 不限制精度的整数

Float float 浮点数

Numeric decimal.Decimal 定点数

String str 变长字符串

Text str 变长字符串，对较长或不限长度的字符串做了优化

Unicode unicode 变长Unicode 字符串

UnicodeText unicode 变长Unicode 字符串，对较长或不限长度的字符串做了优化

Boolean bool 布尔值

Date datetime.date 日期

Time datetime.time 时间

DateTime datetime.datetime 日期和时间

Interval datetime.timedelta 时间间隔

Enum str 一组字符串

PickleType 任何Python 对象自动使用Pickle 序列化

LargeBinary str 二进制文件

## SQLAlchemy 列选项

选项名 说明

primary\_key 如果设为True，这列就是表的主键

unique 如果设为True，这列不允许出现重复的值

index 如果设为True，为这列创建索引，提升查询效率

nullable 如果设为True，这列允许使用空值；如果设为False，这列不允许使用空值

default 为这列定义默认值

## 查询过滤器

filter() 把过滤器添加到原查询上，返回一个新查询

filter\_by() 把等值过滤器添加到原查询上，返回一个新查询

limit() 使用指定的值限制原查询返回的结果数量，返回一个新查询

offset() 偏移原查询返回的结果，返回一个新查询

order\_by() 根据指定条件对原查询结果进行排序，返回一个新查询

group\_by() 根据指定条件对原查询结果进行分组，返回一个新查询

## 常用查询执行函数

all() 以列表形式返回查询的所有结果

first() 返回查询的第一个结果，如果没有结果，则返回None

first\_or\_404() 返回查询的第一个结果，如果没有结果，则终止请求，返回404 错误响应

get() 返回指定主键对应的行，如果没有对应的行，则返回None

get\_or\_404() 返回指定主键对应的行，如果没找到指定的主键，则终止请求，返回404 错误响应

count() 返回查询结果的数量

paginate() 返回一个Paginate 对象，它包含指定范围内的结果

## 关系

SQLAlchemy 关系选项

backref 在关系的另一个模型中添加反向引用

primaryjoin 明确指定两个模型之间使用的联结条件。只在模棱两可的关系中需要指定

lazy 指定如何加载相关记录。可选值有select（首次访问时按需加载）、immediate（源对象加

载后就加载）、joined（加载记录，但使用联结）、subquery（立即加载，但使用子查询），

noload（永不加载）和dynamic（不加载记录，但提供加载记录的查询）

**dynamic 禁止自动执行查询**，一对多关系，可以返回一个未执行的查询

user\_role.users.order\_by(User.username).all()

按名字排序，可以执行过滤器

uselist 如果设为Fales，不使用列表，而使用标量值

order\_by 指定关系中记录的排序方式

secondary 指定多对多关系中关系表的名字

secondaryjoin SQLAlchemy 无法自行决定时，指定多对多关系中的二级联结条件

### 一对多关系

多对多关系

## 模型变更 – 数据库迁移 Migrate

pip install flask-migrate

1. 创建迁移仓库

python hello.py db init

2）创建迁移脚本

python hello.py db migrate -m “initial migration”

3) 更新数据库

python hello.py db upgrade

对于第一次迁移来说，相当于create\_all()函数

# HTML

## 转义字符



&times; 乘号，叉 关闭含义

# Bootstrap

## button

<button type=”button” class=”close” data-dismiss=”alert”>&times;</button>

button 为HTML的一个TAG。

class=”close” 为button设置关闭按钮样式，是一个CSS　class

data-dismiss=”alert” 为警告框添加关闭功能

## 警告Alerts

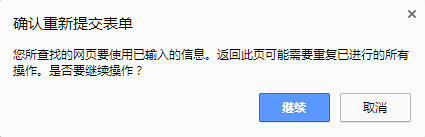
<div class=”alert alert-success alert-dismissable”>

</div>

# 浏览器警告

## 刷新表单重新提交

* **问题描述：**用户提交表单后，点击浏览器的刷新按钮，会看到一个警告，要求再次提交表单之前进行确认。



* **问题原因：**刷新会导致浏览器重新发送之前已经发送过的最后一个请求，如果最后一个请求是一个包含表单数据的POST请求，那么浏览器会再次提交表单，这并非理想的处理方式。
* **解决方法：**Post/重定向/Get 模式解决。不要把Post请求作为浏览器的最后一个请求，响应POST请求的是一个重定向URL，这个URL会发出Get请求，那么始终可以保证最后一个请求不是Post请求。

# 扩展

pip install flask-script

pip install flask-bootstrap

本地化日期和时间

pip install flask-moment

<http://momentjs.com/docs/#/displaying/>

## Web表单 WTForms

pip install flask-wtf

**支持HTML标准字段**

StringField 文本字段

TextAreaField 多行文本字段

PasswordField 密码文本字段

HiddenField 隐藏文本字段

DateField 文本字段，值为datetime.date 格式

DateTimeField 文本字段，值为datetime.datetime 格式

IntegerField 文本字段，值为整数

DecimalField 文本字段，值为decimal.Decimal

FloatField 文本字段，值为浮点数

BooleanField 复选框，值为True 和False

RadioField 一组单选框

SelectField 下拉列表

SelectMultipleField 下拉列表，可选择多个值

FileField 文件上传字段

SubmitField 表单提交按钮

FormField 把表单作为字段嵌入另一个表单

FieldList 一组指定类型的字段

**内建的校验函数**

Email 验证电子邮件地址

EqualTo 比较两个字段的值；常用于要求输入两次密码进行确认的情况

IPAddress 验证IPv4 网络地址

Length 验证输入字符串的长度

NumberRange 验证输入的值在数字范围内

Optional 无输入值时跳过其他验证函数

Required 确保字段中有数据

Regexp 使用正则表达式验证输入值

URL 验证URL

AnyOf 确保输入值在可选值列表中

NoneOf 确保输入值不在可选值列表中

# JinJa2 模板引擎

**变量过滤器**

safe 渲染值时不转义

capitalize 把值的首字母转换成大写，其他字母转换成小写

lower 把值转换成小写形式

upper 把值转换成大写形式

title 把值中每个单词的首字母都转换成大写

trim 把值的首尾空格去掉

striptags 渲染之前把值中所有的HTML 标签都删掉

完整的过滤器列表

<http://jinja.pocoo.org/docs/templates/#builtin-filters>

Flask-Bootstrap 模板定义

Flask-Bootstrap基模板中定义的块

块　　名说　　明

doc 整个HTML 文档

html\_attribs <html> 标签的属性

html <html> 标签中的内容

head <head> 标签中的内容

**title** <title> 标签中的内容

metas 一组<meta> 标签

styles 层叠样式表定义

body\_attribs <body> 标签的属性

body <body> 标签中的内容

**navbar** 用户定义的导航条

**content** 用户定义的页面内容

scripts 文档底部的JavaScript 声明

# CSRF 跨站请求伪造

攻击者盗用了你的身份，以你的名义发送恶意请求。CSRF能够做的事情包括：以你名义发送邮件，发消息，盗取你的账号，甚至于购买商品，虚拟货币转账......造成的问题包括：个人隐私泄露以及财产安全。



从上图可以看出，要完成一次CSRF攻击，受害者必须依次完成两个步骤：

　　1.登录受信任网站A，并在本地生成Cookie。

　　2.在不登出A的情况下，访问危险网站B。

　　看到这里，你也许会说：“如果我不满足以上两个条件中的一个，我就不会受到CSRF的攻击”。是的，确实如此，但你不能保证以下情况不会发生：

　　1.你不能保证你登录了一个网站后，不再打开一个tab页面并访问另外的网站。

　　2.你不能保证你关闭浏览器了后，你本地的Cookie立刻过期，你上次的会话已经结束。（事实上，关闭浏览器不能结束一个会话，但大多数人都会错误的认为关闭浏览器就等于退出登录/结束会话了......）

　　3.上图中所谓的攻击网站，可能是一个存在其他漏洞的可信任的经常被人访问的网站。