**20180502**

**第1章 Flask安装**

[Flask](http://flask.pocoo.org/)是小型框架，其有两个主要依赖：路由、调试和Web服务器网关接口(WSGI, Web Server Gateway Interface)子系统由[Werkzeug](http://werkzeug.pocoo.org/)提供；模板系统由[Jinja2](http://werkzeug.pocoo.org/)提供。Werkzeug和Jinjia2 都是由 Flask的核心开发者开发而成。

Flask并不原生支持数据库访问、Web 表单验证和用户认证等高级功能，需要以扩展的形式实现，然后再与核心包集成。

* 虚拟环境virtualenv

① 安装virtualenv包：$ pip install virtualenv

② 创建虚拟环境venv：$ virtualenv venv

当前目录(比如hello目录)生成一个venv子目录，虚拟环境名字为venv

③ 激活虚拟环境venv：$ venv\Scripts\activate

虚拟环境被激活后，命令提示符变为：(venv) $

其中Python 解释器临时添加到PATH

④ 退出虚拟环境：$ deactivate

以后就在虚拟环境venv安装Python第三方模块，如：

|  |
| --- |
| (venv) $ pip install flask  (venv) $ pip freeze  click==6.7  Flask==1.0.1  itsdangerous==0.24  Jinja2==2.10  MarkupSafe==1.0  Werkzeug==0.14.1 |

**第2章 程序的基本结构**

* 2.1 初始化

所有Flask程序必须创建一个程序实例。Web 服务器使用WSGI协议把接收自客户端的所有请求转交给这个对象处理。

Flask 类的构造函数只有一个必须指定的参数，即程序主模块或包的名字：

|  |
| --- |
| from flask import Flask  app = Flask(\_\_name\_\_) |

* 2.2 路由(route)和视图函数(view)

客户端把请求发给Web 服务器，Web 服务器再把请求发给Flask程序实例。程序实例需要知道对每个URL请求运行哪些代码，所以保存了一个URL到Python 函数的映射关系。处理URL和函数之间关系的程序称为路由。

定义路由最简便方式，是使用程序实例提供的app.route 装饰器，把函数注册为路由。

|  |
| --- |
| @app.route('/')  def index():  return '<h1 style=color:red>hello world!</h1>' |

动态路由：URL地址中可以包含可变部分，如/user/<name>，尖括号内容就是动态部分，Flask将动态部分作为参数传入视图函数：

|  |
| --- |
| @app.route('/user/<name>') *# 动态路由*  def user(name):  return '<h1>hello, {}!</h1>'.format(name) |

Flask支持在路由中使用int、float和path类型。path类型也是字符串，但不把斜线视作分隔符，而作为动态的一部分。

|  |
| --- |
| dct = {5: 'rin', 6: 'maki', 7: 'nozomi'}  @app.route('/user/<int:id>')  def user1(id):  return '<h1>hello, {}!</h1>'.format(dct.get(id, 'world')) |

* 2.3 启动服务器

|  |
| --- |
| if \_\_name\_\_ == '\_\_main\_\_':  *# 默认端口5000, 可以修改*  app.run(debug=True, port=8888) |

① 公认端口(Well Known Ports)：0~1023，紧密绑定于一些服务。通常这些端口的通讯明确表明了某种服务协议。80端口实际上总是HTTP通讯。

② 注册端口(Registered Ports)：1024~49151，松散地绑定于一些服务。这些端口同样用于许多其它目的。如许多系统处理动态端口从1024左右开始。

③ 动态和/或私有端口(Dynamic and/or Private Ports)：49152~65535。理论上不应为服务分配这些端口。实际上机器通常从1024起分配动态端口。

服务器启动后，会进入轮询，等待并处理请求。轮询一直运行，直到程序停止。

* 2.4 请求-响应循环

请求对象封装了客户端发送的HTTP 请求。要让视图函数能够访问请求对象，可以将其作为参数传入视图函数，但会导致每个视图函数都增加一个参数。

为了避免传入大量参数使得视图函数变得乱七八糟，Flask使用上下文临时把某些对象变为全局可访问。

|  |
| --- |
| from flask import request  @app.route('/')  def index():  user\_agent = request.headers.get('User-Agent')  return '<h1 style=color:red>hello world!</h1><br><p>{}</p>'.format(user\_agent) |

此视图函数把request当全局变量使用。但事实上request不可能是全局变量。比如多线程处理不同客户端不同请求时，每个线程的request对象一定不同

Flask上下文全局变量：程序上下文和请求上下文

|  |  |  |
| --- | --- | --- |
| **变量名** | **上下文** | **说明** |
| current\_app | 程序上下文 | 当前激活程序的程序实例 |
| g | 程序上下文 | 处理请求时用作临时存储的对象。每次请求都会重设此变量 |
| request | 请求上下文 | 请求对象，封装了客户端发出的HTTP 请求内容 |
| session | 请求上下文 | 用户会话，用于存储请求之间需要记住值的词典 |

Flask在分发请求之前激活(或推送)程序和请求上下文，请求处理完成后再将其删除。程序上下文被推送后，可以在线程中使用current\_app 和g 变量；请求上下文被推送后，可以使用request 和session 变量。如果使用这些变量时没有激活上下文，就会导致错误。

* 2.5 URL映射

生成映射除了用app.route装饰器，还可以用app.add\_url\_rule()方法

使用app.url\_map可以查看URL映射(用shell或另一个py文件)

同目录的test.py：

|  |
| --- |
| from hello import app  print(app.url\_map) |

结果：

|  |
| --- |
| Map([<Rule '/' (GET, OPTIONS, HEAD) -> index>,  <Rule '/static/<filename>' (GET, OPTIONS, HEAD) -> static>,  <Rule '/user/<id>' (GET, OPTIONS, HEAD) -> user1>,  <Rule '/user/<name>' (GET, OPTIONS, HEAD) -> user>]) |

/static/<*filename*>是Flask添加的特殊路由，用于访问静态文件。

URL映射中的HEAD、Options、GET是请求方法，由路由处理。Flask为每个路由指定了请求方法，不同的请求方法发送到相同的URL上时，使用不同的视图函数处理。HEAD和OPTIONS方法由Flask自动处理。

* 2.6 请求钩子

有时在处理请求之前或之后执行相同函数，为了避免每个视图函数都使用重复代码，Flask提供注册通用函数的功能。

请求钩子通过装饰器实现：

① before\_first\_request：在处理第一个请求之前运行；

② before\_request：在每次请求之前运行；

③ after\_request：如果没有未处理的异常抛出，在每次请求之后运行；

④ teardown\_request：即使有未处理的异常抛出，也在每次请求之后运行。

在请求钩子函数和视图函数之间共享数据一般使用上下文全局变量g。

如before\_request处理程序可从数据库中加载已登录用户，并将其保存到g.user中。之后调用视图函数再使用g.user获取用户。

* 2.7 响应

视图函数返回值作为响应内容，可以是一个简单的字符串，作为HTML页面返回客户端。

① 状态码是HTTP响应的重要部分，Flask默认200，表示成功处理请求。

状态码可以作为视图函数第2个返回值：

|  |
| --- |
| @app.route('/user/<int:id>')  def user1(id):  name = dct.get(id)  if name:  return '<h1>hello, {}!</h1>'.format(name)  return '<h1>Bad Request</h1>', 400 |

make\_response()函数(参数和视图的返回值一样)可以返回一个Response对象，返回一个Response对象。可以在响应对象上调用各种方法，比如设置cookie：

|  |
| --- |
| from flask import make\_response  @app.route('/')  def index():  res = make\_response('<h1>F12查看cookie</h1>') *# 创建Response对象*  res.set\_cookie('name', 'hikari') *# 设置cookie*  return res |

② 重定向，通常使用302状态码，通常在Web表单中使用

Flask提供redirect()辅助函数生成重定向响应

|  |
| --- |
| from flask import redirect  @app.route('/')  def index():  return redirect('https://www.baidu.com') |

③ abort()函数用于处理错误，生成特殊的响应

|  |
| --- |
| from flask import abort  @app.route('/user/<int:id>')  def user1(id):  name = dct.get(id)  if name is None:  abort(404)  return '<h1>hello, {}!</h1>'.format(name) |

如果URL动态参数id对应用户不存在就返回404。

abort不会把控制权交还给调用的函数，而是抛出异常把控制权交给Web服务器。

* 2.8 Flask扩展

Flask设计为可扩展，没有提供一些重要的功能(如数据库和用户认证)，所以可以自由选择最适合的包，或者按需求自行开发。

**使用Flask-Script支持命令行选项**

Flask支持很多启动设置选项，但只能在脚本中作为参数传给app.run()，不方便，传递设置选项的理想方式是使用命令行参数。

// 为什么在下认为命令行反而不友好...

Flask-Script是一个Flask扩展，为Flask程序添加一个命令行解析器。Flask-Script自带一组常用选项，而且支持自定义命令。

|  |
| --- |
| from flask\_script import Manager  app = Flask(\_\_name\_\_)  manager = Manager(app)  *# 视图与之前一样*  if \_\_name\_\_ == '\_\_main\_\_':  manager.run() |

运行hello.py：

|  |
| --- |
| $ (venv) python hello.py  usage: hello.py [-?] {shell,runserver} ...  positional arguments:  {shell,runserver}  shell Runs a Python shell inside Flask application context.  runserver Runs the Flask development server i.e. app.run()  optional arguments:  -?, --help show this help message and exit |

① shell命令用于在程序上下文启动Python Shell会话，可以测试或维护；

② runserver命令启动Web服务器：

python hello.py runserver --help可以查看用法：

|  |
| --- |
| (venv) $ python hello.py runserver --help  usage: hello.py runserver [-?] [-h HOST] [-p PORT] [--threaded]  [--processes PROCESSES] [--passthrough-errors] [-d]  [-D] [-r] [-R] [--ssl-crt SSL\_CRT]  [--ssl-key SSL\_KEY]  ... |

-h或--host，默认指定服务器监听localhost的连接，所以只接受来自服务器所在计算机发起的连接。要允许同网其他计算机连接服务器指定--host 0.0.0.0：

|  |
| --- |
| (venv) $ python hello.py runserver --host 0.0.0.0  \* Serving Flask app "hello" (lazy loading)  \* Environment: production  WARNING: Do not use the development server in a production environment.  Use a production WSGI server instead.  \* Debug mode: off  \* Running on http://0.0.0.0:5000/ (Press CTRL+C to quit) |

这样，Web服务器可使用http://a.b.c.d:5000/网络中的任一台电脑访问，其中a.b.c.d是服务器所在计算机的外网IP地址。

**第3章 模板**

例如用户注册，视图函数需要访问数据库，添加新用户，此为业务逻辑；注册完将响应返回浏览器，此为表现逻辑。如果两者耦合太大，使代码难以理解和维护。

把表现逻辑移到模板中能降低耦合，提高可维护性。

* 3.1 Jinja2模板引擎

模板是一个包含响应文本的文件，其中包含用占位变量{{ variable }}表示的动态部分，其具体值只在请求上下文中才知道。

渲染：使用真实值替换变量，再返回最终得到的响应字符串。

① 渲染模板

默认Flask在程序根目录的templates子目录寻找模板。

hello.py：

|  |
| --- |
| from flask import Flask, render\_template  app = Flask(\_\_name\_\_)  @app.route('/')  def index():  return render\_template('index.html')  @app.route('/user/<name>')  def user(name):  return render\_template('user.html', name=name)  if \_\_name\_\_ == '\_\_main\_\_':  app.run(debug=True, port=8000) |

index.html：

|  |
| --- |
| h1 {font: 36px/36px "Microsoft YaHei"; color: red;}  <h1>welcome to hikari's website!!!</h1> |

user.html：

|  |
| --- |
| h1 {font: 36px/36px "Microsoft YaHei";}  .user {color: #ff00ff;}  <h1>hello,<span class="user">{{ name }}</span>!</h1> |

② Jinja2变量

类似于{{ name }}结构表示变量，是特殊的占位符，告诉模板引擎这个位置的值从渲染模板使用的数据中获取。

|  |
| --- |
| {{ dct['key'] }} *{# 字典根据键获取值 #}*  {{ lst[0] }} *{# 列表指定索引 #}*  {{ lst[i] }} *{# 列表索引是变量 #}*  {{ obj.func() }} *{# 对象的方法 #}* |

③ 过滤器

可以使用过滤器修改变量，格式：{{ variable|filter }}

如：{{ name|capitalize }}

Jinja2常用过滤器

|  |  |
| --- | --- |
| **常用过滤器** | **说明** |
| safe | 渲染值时不转义 |
| capitalize | 首字母转大写，其他字母小写 |
| lower | 转换成小写 |
| upper | 转换成大写 |
| title | 每个单词的首字母转换成大写 |
| trim | 去除首尾空格 |
| striptags | 渲染之前删除变量所有HTML标签 |

默认出于安全考虑，Jinja2会转义变量。如果一个变量的值为'<h1>maki</h1>'，Jinja2 会将其渲染成'&lt;h1&gt;maki&lt;/h1&gt;'，浏览器显示<h1>maki</h1>，没有解析成h1标签。但很多情况需要显示变量中存储的HTML代码，就可使用 safe过滤器：{{ name|safe }}，浏览器显示**maki**，将其作为h1标签解析。

**注意**：千万别在不可信的值上使用safe过滤器，例如用户在表单中输入的文本。

④ Jinja2控制结构

1) if语句：

|  |
| --- |
| {% if user %}  Hello, {{ user }}!  {% else %}  Hello, Stranger!  {% endif %} |

2) for语句：

|  |
| --- |
| <ul>  {% for i in data %}  <li>{{ i }}</li>  {% endfor %}  </ul> |

3) 宏，类似于函数

|  |
| --- |
| {% macro show(name) %}  <li>{{ name }}</li>  {% endmacro %}  <ul>  {% for i in data %} {{ show(i) }} {% endfor %}  </ul> |

为了重复使用宏，可以将其保存到单独文件如macros.html；

需要使用时导入：

|  |
| --- |
| {% import 'macros.html' as macros %}  <ul>  {% for i in data %}  {{ macros.show(i) }}  {% endfor %}  </ul> |

需要多处重复使用的模板代码片段可以写入单独文件，再包含在所有模板中， 以避免重复：{% include 'common.html' %}

另一种重复使用代码的强大方式是模板继承，类似于Python 中的类继承。

⑤ 模板继承

base.html父模板：

|  |
| --- |
| <!DOCTYPE html>  <html lang="en">  <head>  {% block head %}  <meta charset="UTF-8">  <meta name="viewport" content="width=device-width, initial-scale=1.0">  <meta http-equiv="X-UA-Compatible" content="ie=edge">  <title>{% block title %}{% endblock %} - hikari app</title>  {% endblock %}  </head>  <body>  {% block body %} {% endblock %}  </body>  </html> |

block标签在父模板中挖坑，比如上面定义了head, title, body 3个坑。

index.html：

|  |
| --- |
| {% extends "base.html" %} *{# 继承于base.html模板 #}*  {% block head %} {{super()}}*{# 父模板中内容非空,使用super()获取原来的内容 #}*  <style> h1 {font: 36px/36px "Microsoft YaHei"; color: red;}</style>  {% endblock %}  {% block title %}index{% endblock%}  {% block body %}<h1>hello world!</h1>{% endblock %} |

index.html继承于base.html，在其中填坑。

* 3.2 Flask-Bootstrap

Bootstrap 是客户端框架，因此不会直接涉及服务器。服务器需要做的只是提供引用了Bootstrap CSS和JavaScript文件的HTML响应，并在HTML、CSS和JavaScript代码中实例化所需组件。这些操作最理想的执行场所就是模板。

要在程序中集成Bootstrap，可以使用Flask-Bootstrap扩展。

初始化Flask-Bootstrap后，在程序中可以使用其提供的父模板bootstrap/base.html。利用Jinja2的模板继承机制，子模板就引入了Bootstrap元素。

示例：使用Flask-Bootstrap修改user.html

hello.py：

|  |
| --- |
| from flask import Flask, render\_template  from flask\_bootstrap import Bootstrap  app = Flask(\_\_name\_\_)  bootstrap = Bootstrap(app)  @app.route('/')  def index():  return render\_template('index.html')  @app.route('/user/<name>')  def user(name):  return render\_template('user.html', name=name)  if \_\_name\_\_ == '\_\_main\_\_':  app.run(debug=True, port=8000) |

user.html：

|  |
| --- |
| {% extends "bootstrap/base.html" %}  *{# 提供网页框架, 引入Bootstrap所有CSS和JS文件 #}*  {% block title %}User{% endblock%}  {% block styles%}  {{super()}}  <style>  h1 {font: 36px/36px "Microsoft YaHei";}  .user {color: #ff00ff;}  </style>  {% endblock %}  {% block navbar %}*{# 导航条, 直接复制吧, 太难记了 #}*  <div class="navbar navbar-inverse navbar-static-top" role="navigation">  <div class="container">  <div class="navbar-header">  *{# 当设备宽度小, 菜单内容折叠时出现此按钮, 点击出现data-target指向collapse #}*  <button type="button" class="navbar-toggle" data-toggle="collapse" data-target=".navbar-collapse">  <span class="sr-only">Toggle navigation</span>  <span class="icon-bar"></span>  <span class="icon-bar"></span>  <span class="icon-bar"></span></button>  *{# logo区域#}*  <a class="navbar-brand" href="/">Flasky</a></div>  <div class="navbar-collapse collapse">  *{# nav navbar-nav:导航条菜单 #}*  <ul class="nav navbar-nav"><li><a href="/">Home</a></li></ul>  </div></div></div>  {% endblock %}  {% block content %}  <div class="container">  <div class="page-header">  <h1>hello, <span class="user">{{ name }}</span>!</h1></div></div>  {% endblock %} |

效果：



Flask-Bootstrap父模板中定义的block：

|  |  |  |  |
| --- | --- | --- | --- |
| **块名** | **说明** | **块名** | **说明** |
| doc | 整个HTML文档 | styles | css样式 |
| html\_attribs | <html>标签的属性 | body\_attribs | <body>标签的属性 |
| html | <html>标签的内容 | body | <body>标签的内容 |
| head | <head>标签的内容 | navbar | 用户定义的导航条 |
| title | <title>标签的内容 | content | 用户定义的页面内容 |
| metas | 一组<meta>标签 | scripts | 文档底部的JS声明 |

其中很多块都是Flask-Bootstrap自用，如果直接重定义可能会导致问题。

如Bootstrap所需的css和js文件在styles和scripts块中声明。如果程序需要在已经有内容的块中添加新内容，必须使用Jinja2提供的super()函数。

* 3.3 自定义错误页面

在浏览器输入没有配置的url，会显示一个404错误页面，然而这个页面太丑了！

Flask可以基于模板自定义错误页面。

常见错误代码：404：客户端请求未知页面；500：有未处理的异常。

① hello.py自定义错误页面的视图

|  |
| --- |
| @app.errorhandler(404)  def page\_not\_found(e):  return render\_template('404.html'), 404  @app.errorhandler(500)  def internal\_server\_error(e):  return render\_template('500.html'), 500 |

需要创建404.html和500.html，可以复制user.html内容，但是太麻烦；可以使用模板继承，templates/base.html 继承于bootstrap/base.html，然后user.html、404.html和500.html都继承此父模板。

② templates/base.html：

|  |
| --- |
| {% extends "bootstrap/base.html" %}  {% block title %}hikari app{% endblock%}  {% block styles %}  {{ super() }}  <style>  h1 {font: 36px/36px "Microsoft YaHei";}  .user {color: #ff00ff;}</style>  {% endblock %}  {% block navbar %}*{# 导航条,直接复制吧,太难记了 #}*  <div class="navbar navbar-inverse navbar-static-top" role="navigation">  <div class="container">  <div class="navbar-header">  <button type="button" class="navbar-toggle" data-toggle="collapse" data-target=".navbar-collapse">  <span class="sr-only">Toggle navigation</span>  <span class="icon-bar"></span>  <span class="icon-bar"></span>  <span class="icon-bar"></span></button>  <a class="navbar-brand" href="/">Flasky</a></div>  <div class="navbar-collapse collapse">  <ul class="nav navbar-nav">  <li><a href="/">Home</a></li></ul>  </div></div></div>  {% endblock %} {% block content %}  <div class="container">  {% block page\_content %}{% endblock %}</div>  {% endblock %} |

和上面templates/user.html 基本一样，主要最后在content 坑里挖了一个page\_content的坑。

③ templates/404.html：使用模板继承自定义404错误页面

|  |
| --- |
| {% extends "base.html" %} *{# 继承于自定义的base.html模板#}*  {% block title %}hikari app - Page Not Found{% endblock %} *{# 覆盖父模板的title#}*  {% block page\_content %}  <div class="page-header"><h1>Not Found</h1></div>  {% endblock %} |

④ templates/500.html：使用模板继承自定义500错误页面

|  |
| --- |
| {% extends "base.html" %}  {% block title %}hikari app - Internal Server Error{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>Internal Server Error</h1></div>  {% endblock %} |

⑤ 简化templates/user.html：

|  |
| --- |
| {% extends "base.html" %}  {% block title %}User{% endblock %}  {% block page\_content %}  <div class="page-header">  <h1>hello,<span class="user">{{ name }}</span>!</h1></div>  {% endblock %} |

* 3.4 链接

任何具有多路由的程序都需要可以链接到不同页面，例如导航条。

url\_for()函数可以使用URL映射中保存的信息生成URL。

最简单用法是以视图函数名作为参数：

如{{ url\_for('index') }}返回/；

{{ url\_for('index', \_external=True) }}返回http://localhost:5000/；

\_external=True表示绝对地址。

使用url\_for()生成动态地址时，将动态部分作为关键字参数传入。

如<a *href*="{{ url\_for('user', name='hikari' , \_external=True) }}">hikari</a>

链接地址是http://localhost:5000/user/hikari

还可以添加查询字符串：{{ url\_for('index', page=2) }}结果是/?page=2

* 3.5 静态文件

对静态文件的引用作为特殊路由：/*static*/<*filename*>

如{{ url\_for('static', filename='css/main.css', \_external=True) }}

结果是：http://localhost:5000/static/css/main.css

Flask默认在程序根目录的static子目录寻找静态文件。

示例：定义收藏夹图标

templates/base.html：

|  |
| --- |
| {% block head %}  {{ super() }}  <link rel="shortcut icon" href="{{ url\_for('static', filename = 'shortcuticon.png') }}" type="image/png">  <link rel="icon" href="{{ url\_for('static', filename = 'shortcuticon.png') }}" type="image/png">  {% endblock %} |

左上角的小图标：



* 3.6 Flask-Moment本地化日期和时间

服务器需要统一时间，一般使用协调世界时(Coordinated Universal Time，UTC)

但用户更希望看到当地时间，而且采用当地惯用的格式。

一个优雅的解决方案：把时间单位发送给Web浏览器，转换成当地时间，然后渲染。因为浏览器能获取用户计算机的时区和区域设置。

[moment.js](http://momentjs.com/)是使用JavaScript开发的优秀客户端开源代码库，可以在浏览器中渲染日期和时间。Flask-Moment是一个Flask程序扩展，把moment.js集成到Jinja2模板中。

示例：

① hello.py：初始化Flask-Moment

|  |
| --- |
| from flask\_moment import Moment  moment = Moment(app) |

② templates/base.html：在底部引入moment.js库

|  |
| --- |
| {% block scripts %}  {{ super() }}  {{ moment.include\_moment() }}  {{ moment.lang('zh-CN') }} *{# 指定时间戳本地化语言 #}*  {% endblock %} |

为了处理时间戳，Flask-Moment向模板开放了moment类

③ hello.py：index视图添加一个now变量：

|  |
| --- |
| from datetime import datetime  @app.route('/')  def index():  return render\_template('index.html', now=datetime.utcnow()) |

④ templates/index.html：使用Flask-Moment渲染时间戳

|  |
| --- |
| {% block page\_content %}  <div class="page-header">  <h3>时间：{{ moment(now).format('YYYY年MM月DD日 ddd HH:mm:ss') }}</h3>  *{# 根据电脑的时区和区域设置渲染日期和时间 #}*  <h3>时间：{{ moment(now).format('LLLL') }}</h3>  <h3>那是{{ moment(now).fromNow(refresh=True) }}。</h3>  </div>  {% endblock %} |

结果：



fromNow()渲染相对时间戳，会随着时间的推移自动刷新显示的时间。最开始显示几秒前；但指定refresh参数后，会随着时间的推移而更新，比如1分钟前、2 分钟前等。

Flask-Moment实现了moment.js中的format()、fromNow()、fromTime()、 calendar()、

valueOf()和unix()方法。查阅[文档](http://momentjs.com/docs/#/displaying/)学习全部格式化选项。

**第4章 Web表单**

[Flask-WTF](http://pythonhosted.org/Flask-WTF/)扩展把处理Web表单的过程变成一种愉悦的体验。它对独立的[WTForms](http://wtforms.simplecodes.com)包进行了包装，方便集成到Flask程序中。

* 4.1 跨站请求伪造保护

默认Flask-WTF能保护所有表单免受跨站请求伪造(Cross-Site Request Forgery，CSRF)的攻击。恶意网站把请求发送到被攻击者已登录的其他网站时就会引发 CSRF攻击。

为了实现CSRF保护，Flask-WTF需要程序设置一个密钥。Flask-WTF使用这个密钥生成加密令牌，再用令牌验证请求中表单数据的真伪。

示例：hello.py：设置Flask-WTF密钥：

|  |
| --- |
| app = Flask(\_\_name\_\_)  app.config['SECRET\_KEY'] = 'hoshizora rin' *# csrf保护* |

app.config字典可用来存储框架、扩展和程序本身的配置变量；还提供了一些方法，可以从文件或环境中导入配置值。

SECRET\_KEY配置变量是通用密钥，可在Flask和多个第三方扩展中使用。加密的强度取决于变量值的机密程度。不同的程序要使用不同的密钥，而且要保证其他人不知道所用的字符串。

**注意**：为了增强安全性，密钥不应该直接写入代码，而要保存在环境变量中。

**20180503**

* 4.2 表单类

每个表单都由一个继承自FlaskForm的类表示。这个类定义表单中的一组字段，每个字段都用对象表示。字段对象可附属一个或多个验证函数。验证函数用来验证用户提交的输入值是否符合要求。

示例：包含一个文本字段和一个提交按钮的简单表单

|  |
| --- |
| from flask\_wtf import FlaskForm  from wtforms import StringField, SubmitField  from wtforms.validators import DataRequired  class NameForm(FlaskForm): *# 一个文本字段和一个提交按钮*  name = StringField('你的名字是？', validators=[DataRequired()])  submit = SubmitField('提交') |

StringField类表示属性为type="text"的<input>元素。SubmitField类表示属性为 type="submit"的<input>元素。字段构造函数的第一个参数是把表单渲染成 HTML时使用的标号。

可选参数validators指定一个由验证函数组成的列表，在接受用户提交的数据之前验证数据。验证函数DataRequired()确保提交的字段不为空。

注：FlaskForm基类由Flask-WTF扩展定义；字段和验证函数却可以直接从WTForms包中导入。

WTForms支持的HTML标准字段有：StringField、TextAreaField、PasswordField、HiddenField、IntegerField等。

WTForms验证函数有：Email、Length、Regexp、EqualTo等。

具体查狗书P35。

* 4.3 表单渲染成HTML

Flask-Bootstrap提供一个非常高端的辅助函数，可以使用Bootstrap中预先定义好的表单样式渲染整个Flask-WTF表单。

|  |
| --- |
| {% import "bootstrap/wtf.html" as wtf %}  {{ wtf.quick\_form(form) }} |

wtf.quick\_form()函数的参数为Flask-WTF表单对象，使用Bootstrap默认样式渲染传入的表单。

示例：使用Flask-WTF和Flask-Bootstrap渲染表单

templates/index.html：

|  |
| --- |
| {% extends "base.html"%}  {% import "bootstrap/wtf.html" as wtf %}  {% block title %}index{% endblock%}  {% block page\_content %}  <div class="page-header">  <h1>Hello, {% if name %}{{ name }}{% else %}Stranger{% endif %}!</h1></div>  {{ wtf.quick\_form(form) }} *{# 使用Bootstrap默认样式渲染表单 #}*  {% endblock %} |

* 4.4 在视图函数处理表单

index视图：

|  |
| --- |
| @app.route('/', methods=['GET', 'POST']) *# 支持GET和POST*  def index():  name = None  form = NameForm()  if form.validate\_on\_submit(): *# 提交表单,数据被验证函数接受*  name = form.name.data *# 获取字段data属性*  form.name.data = '' *# 清空字段*  return render\_template('index.html', form=form, name=name) |

index视图可以GET和POST请求。第1次访问，服务器收到没有表单数据的GET请求，validate\_on\_submit()返回 False，name为None；模板执行else语句，显示Stranger；输入名字后name获取数据，传给模板显示：

不输入直接提交，提示：



* 4.5 重定向和用户会话

上面表单，提交之后刷新会出现警告，要求再次提交表单之前进行确认。



因为刷新页面，浏览器会重新发送之前已经发送过的最后一个请求。如果是包含表单数据的POST请求，刷新页面会再次提交表单。

最好不要让POST请求成为浏览器发送的最后一个请求。

可以使用重定向作为POST请求的响应。重定向是特殊的响应，响应内容是URL，而不是HTML代码的字符串，浏览器收到重定向响应后，向重定向的URL发送GET请求。称为Post/重定向/Get模式。

但是处理POST请求时，使用form.name.data获取用户输入，但请求结束，数据随之丢失，所以需要程序能保存输入数据。这样重定向后的请求也可以获得这个数据，从而构建真正的响应。

程序可以把数据存储在用户会话中，在请求之间记住数据。用户会话是私有存储，存在每个连接到服务器的客户端中。用户会话是请求上下文中的变量session，类似于字典。

**注**：默认用户会话保存在客户端cookie中，使用设置的SECRET\_KEY进行加密签名。如果篡改了cookie的内容，签名就会失效，会话也随之失效。

示例：修改index()，实现重定向和用户会话：

|  |
| --- |
| from flask import Flask, redirect, render\_template, session, url\_for  @app.route('/', methods=['GET', 'POST']) *# 支持GET和POST*  def index():  form = NameForm()  if form.validate\_on\_submit(): *# 提交表单,数据被验证函数接受*  session['name'] = form.name.data *# 获取字段data属性存入session*  return redirect(url\_for('index')) *# 重定向,GET方式请求index*  return render\_template('index.html', form=form, name=session.get('name')) |

第1次GET请求，session没有name字段，显示stranger；输入名字POST提交表单后，name被存入session中，随即重定向再次GET请求，显示name；下次再刷新，仍然是同一个name。浏览器的cookies保存有session字段。

session在不同请求之间共享数据。

* 4.6 Flash消息

flash()函数实现请求完成后告诉用户状态发生了变化，比如用户提交错误登录表单后，服务器发回响应重新渲染表单，显示消息提示用户名或密码错误。

示例：

① index视图，Flash消息：

|  |
| --- |
| from flask import Flask, redirect, render\_template, session, url\_for, flash  @app.route('/', methods=['GET', 'POST']) *# 支持GET和POST*  def index():  form = NameForm()  if form.validate\_on\_submit(): *# 提交表单,数据被验证函数接受*  old\_name = session.get('name') *# 获取session已有name*  if old\_name and old\_name != form.name.data: *# 旧名字与获取名字不同*  flash('你似乎改名字了！')  session['name'] = form.name.data *# 获取字段data属性存入session*  return redirect(url\_for('index')) *# 重定向,GET方式请求index*  return render\_template('index.html', form=form, name=session.get('name')) |

每次提交名字都会和之前存储在session的名字比较，如果不一样就调用flash()函数，发给客户端下一个响应中显示消息。

仅调用flash()函数不能显示消息，需要在模板渲染才能显示消息。最好在父模板templates/base.html中渲染flash消息，这样所有页面都能显示。

② templates/base.html渲染Flash消息：

修改content坑位：

|  |
| --- |
| {% block content %}  <div class="container">  {% for message in get\_flashed\_messages() %}  <div class="alert alert-warning">  <button type="button" class="close" data-dismiss="alert">&times;</button>  {{ message }}  </div>  {% endfor %}  {% block page\_content %}{% endblock %}  </div>  {% endblock %} |



Flask把get\_flashed\_messages()函数开放给模板，用来获取并渲染消息。

在模板中使用循环是因为在之前的请求循环中每次调用flash()函数都会生成一个消息，可能有多个消息在排队等待显示。

**第5章 数据库**

数据库按照一定规则保存数据，程序发起查询取回所需的数据。Web程序最常用基于关系模型的数据库，也称为SQL数据库，因为它们使用结构化查询语言。不过最近几年文档数据库和键值对数据库成了流行的替代选择，这两种合称NoSQL数据库。

* 5.1 SQL数据库

关系型数据库把数据存储在表中，表的列是固定的，行数是可变的。表中有个特殊的列称为主键，是各行唯一标识符。表中还可以有称为外键的列，引用同一个或不同表某行的主键。

如下图两个表：



roles表可用的用户角色，每种角色都有唯一id；users表是用户列表，每个用户也都有唯一id，还有一个外键role\_id引用roles表的id，指定每个用户角色。

关系型数据库存储数据高效，避免重复。重命名角色很简单，只要修改roles表的角色名，users表不需要修改，通过role\_id立刻能看到更新。但数据分别存储在不同表中，需要连接查询，使用复杂。

* 5.2 NoSQL数据库

NoSQL数据库一般用集合代替表，使用文档代替记录。大多数NoSQL数据库不支持联结操作。

对于上面users和roles表，改写成NoSQL，结构应该是：



每个用户都存储一个具体的角色，重命名操作将会非常耗时。

但NoSQL不用联结，虽数据重复量增加，但查询速度快，操作简单。

* 5.3 SQL or NoSQL

SQL数据库擅于用高效且紧凑的形式存储结构化数据，需花费大量精力保证数据的一致性。NoSQL数据库放宽了要求，性能上有优势。

对中小型程序，SQL和NoSQL都是很好的选择，性能相当。

* 5.4 Python数据库框架

选择数据库框架时要考虑的因素：

① 易用性

如果直接比较数据库引擎和数据库抽象层，显然后者取胜。抽象层，也称为对象关系映射(Object-Relational Mapper，ORM)或对象文档映射(Object-Document Mapper，ODM)，在用户不知觉的情况下把高层的面向对象操作转换成低层的数据库指令。

② 性能

ORM和ODM把对象业务转换成数据库业务会有一定的损耗。大多数情况下，ORM和ODM对生产率的提升远远超过性能的损耗。关键在于如何选择一个能直接操作低层数据库的抽象层，以防特定的操作需要直接使用数据库原生指令优化。

③ 可移植性

④ Flask集成度

不一定非得选择已经集成了Flask的框架，但选择这些框架可以节省编写集成代码的时间，简化配置和操作。

狗书推荐使用[Flask-SQLAlchemy](http://pythonhosted.org/Flask-SQLAlchemy/)，其集成了[SQLAlchemy](http://www.sqlalchemy.org/)框架。

* 5.5 Flask-SQLAlchemy管理数据库

Flask-SQLAlchemy简化了在Flask程序中使用SQLAlchemy的操作。

SQLAlchemy是一个强大的关系型数据库框架，支持多种数据库后台。

其提供了高层ORM和原生SQL的低层功能。

在Flask-SQLAlchemy中，数据库使用URL指定。

**常用FLask-SQLAlchemy数据库URL**

|  |  |
| --- | --- |
| **数据库引擎** | **URL** |
| MySQL | *mysql://username:password@hostname/database* |
| Postgres | *postgresql://username:password@hostname/database* |
| SQLite(Unix) | *sqlite:////absolute/path/to/database* |
| SQLite(Windows) | *sqlite:///c:/absolute/path/to/database* |

**注**：SQLite数据库不需要使用服务器，因此不用指定hostname、username和password。URL中的database是硬盘上文件的文件名。

程序使用的数据库URL必须保存到Flask配置对象的 SQLALCHEMY\_DATABASE\_URI键中。配置对象中还有一个很有用的选项，即SQLALCHEMY\_COMMIT\_ON\_TEARDOWN键，设为True时，每次请求结束后都会自动提交数据库中的变动。

示例：配置数据库

|  |
| --- |
| from flask\_sqlalchemy import SQLAlchemy  import os  basedir = os.path.abspath(os.path.dirname(\_\_file\_\_)) *# flask程序根目录*  app = Flask(\_\_name\_\_)  *# 配置sqlite数据库*  app.config['SQLALCHEMY\_DATABASE\_URI'] = 'sqlite:///' + \  os.path.join(basedir, 'data.sqlite') *# 数据库名字为data.sqlite*  app.config['SQLALCHEMY\_COMMIT\_ON\_TEARDOWN'] = True *# 自动提交修改*  db = SQLAlchemy(app) |

db对象是SQLAlchemy类的实例，表示程序使用的数据库，同时还获得了Flask-SQLAlchemy提供的所有功能。

* 5.6 定义模型

模型表示程序使用的持久化实体。在ORM中模型一般是一个类，类的属性对应数据库表中的列。

Flask-SQLAlchemy创建的数据库实例为模型提供了一个父类以及一系列辅助类和辅助函数，可用于定义模型的结构。

示例：定义Role和User模型

|  |
| --- |
| class Role(db.Model):  \_\_tablename\_\_ = 'roles' *# 表名*  id = db.Column(db.Integer, primary\_key=True) *# 主键*  name = db.Column(db.String(64), unique=True)  def \_\_repr\_\_(self):  return '<Role %r>' % self.name    class User(db.Model):  \_\_tablename\_\_ = 'users'  id = db.Column(db.Integer, primary\_key=True) *# 主键*  username = db.Column(db.String(64), unique=True, index=True)  def \_\_repr\_\_(self):  return '<User %r>' % self.username |

自定义模型继承于db.Model类，一个模型对应一张表，模型的属性对应表中的列，是db.Column类的实例。

\_\_repr()\_\_返回一个具有可读性的字符串表示模型，可在调试和测试时使用。

常见SQLAlchemy列(字段)类型有String、Integer、Text、Date等，见狗书P48

常见SQLAlchemy列选项(约束)有：

|  |  |
| --- | --- |
| **选项名** | **说明** |
| primary\_key | 设为True表示主键 |
| unique | 设为True不允许出现重复的值 |
| index | 设为True为这列创建索引，提升查询效率 |
| nullable | 设为True，允许使用空值；设为False，不允许使用空值 |
| default | 为这列设置默认值 |

* 5.7 关系

关系型数据库使用关系把不同表中的行联系起来。roles表示用户角色，有主键id和name字段；users表示用户信息，有主键id、username、password字段，还有一个外键role\_id表示用户角色。显然1个角色对应n个用户，1个用户只能有1个角色，是一对多的关系。

示例：Role和User关系

|  |
| --- |
| class Role(db.Model):  \_\_tablename\_\_ = 'roles' *# 表名*  id = db.Column(db.Integer, primary\_key=True) *# 主键*  name = db.Column(db.String(64), unique=True)  users = db.relationship('User', backref='role')  class User(db.Model):  \_\_tablename\_\_ = 'users'  id = db.Column(db.Integer, primary\_key=True) *# 主键*  username = db.Column(db.String(64), unique=True, index=True)  role\_id = db.Column(db.Integer, db.ForeignKey('roles.id')) *# 外键* |

添加到User模型的role\_id为外键，db.ForeignKey()参数'role.id'表示这列值是roles表的id值。

添加到Role模型的users属性代表这个关系的面向对象视角。对于Role类的一个实例，其users属性将返回与角色相关联的用户组成的列表。

db.relationship()的第一个参数表示关系的另一端是哪个模型。如果模型类尚未定义，可使用字符串形式指定。

backref参数向User模型中添加一个role属性，从而定义反向关系。这一属性可替代role\_id访问Role模型，获取的是模型对象，而不是外键的值。

**常用SQLAlchemy关系选项**

|  |  |
| --- | --- |
| **选项名** | **说明** |
| 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) |
| uselist | 如果设为 False，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 |

一对一关系可以用一对多关系表示，但调用db.relationship()时要把uselist 设为False，把多变成一。

多对多关系很复杂，需要用到第三张表，称为关系表。

* 5.8 数据库操作

学习使用模型最好方法是在Python shell中实际操作。

要使用shell用Flask-Script支持命令行：

|  |
| --- |
| from flask\_script import Manager  manager = Manager(app)  if \_\_name\_\_ == '\_\_main\_\_':  manager.run() |

提示SQLALCHEMY\_TRACK\_MODIFICATIONS要设为True或False…

|  |
| --- |
| app.config['SQLALCHEMY\_TRACK\_MODIFICATIONS'] = False |

① 创建表：create\_all()

|  |
| --- |
| (venv) $ python hello.py shell  >>> from hello import \*  >>> db.create\_all() |

程序根目录多了一个data.sqlite的文件。

如果数据库表已经存在于数据库，db.create\_all()不会重新创建或者更新这个表。如果修改模型后要应用到数据库，粗暴的方式是先删除再创建：

|  |
| --- |
| >>> db.drop\_all()  >>> db.create\_all() |

但是这将数据库原来的数据删除了。

② 插入行

|  |
| --- |
| >>> admin\_role = Role(name='Admin')  >>> mod\_role = Role(name='Moderator')  >>> user\_role = Role(name='User')  >>> hikari = User(username='hikari',role=admin\_role)  >>> maki = User(username='maki',role=user\_role)  >>> rin = User(username='rin',role=user\_role) |

id没有明确指定，因为主键由Flask-SQLAlchemy管理。

这些对象只存在于Python中，还未写入数据库。

|  |
| --- |
| >>> print(admin\_role.id)  None |

id没有被赋值，说明数据的确未写入数据库。

通过数据库会话(也称事务)db.session管理对数据库所做的改动

|  |
| --- |
| >>> db.session.add(admin\_role)  >>> db.session.add(mod\_role)  >>> db.session.add(user\_role)  >>> db.session.add(hikari)  >>> db.session.add(maki)  >>> db.session.add(rin) |

可以简写为：

|  |
| --- |
| >>> db.session.add\_all([admin\_role, mod\_role, user\_role, hikari, maki, rin]) |

调用commit()方法提交会话，将对象写入数据库：

|  |
| --- |
| >>> db.session.commit()  >>> print(admin\_role.id)  1 |

说明id已经被赋值了，数据存入了数据库。

数据库会话能保证数据库的一致性。提交操作使用原子方式把会话中的对象全部写入数据库。如果在写入过程中发生了错误，整个会话都会失效。

db.session.rollback()：数据库会话回滚

③ 修改行

数据库会话使用add()方法也可以更新模型。

比如将'Admin'角色重命名为'Administrator'：

|  |
| --- |
| >>> admin\_role.name='Administrator'  >>> db.session.add(admin\_role)  >>> db.session.commit() |

④ 删除行

数据库会话使用delete()方法删除行。

比如将"Moderator"字段从数据库删除：

|  |
| --- |
| >>> db.session.delete(mod\_role)  >>> db.session.commit() |

⑤ 查询行

每个模型类都有query对象，查询字段所有行使用all()方法：

|  |
| --- |
| >>> Role.query.all()  [<Role 'Administrator'>, <Role 'User'>]  >>> User.query.all()  [<User 'hikari'>, <User 'maki'>, <User 'rin'>] |

使用过滤器可以对query对象进行更精确的数据库查询。  
如查询User中所有角色是user\_role的用户：

|  |
| --- |
| >>> User.query.filter\_by(role=user\_role).all()  [<User 'maki'>, <User 'rin'>] |

将query对象转换成字符串可以查看SQLAlchemy生成的原生SQL查询语句：

|  |
| --- |
| >>> str(User.query.filter\_by(role=user\_role))  'SELECT users.id AS users\_id, users.username AS users\_username, users.role\_id AS users\_role\_id \nFROM users \nWHERE ? = users.role\_id' |

如果退出shell会话后，再打开新的shell会话，此时没有Python对象，需要从数据库读取行，再重新创建Python对象。

|  |
| --- |
| >>> from hello import \*  >>> user\_role = Role.query.filter\_by(name='User').first()  >>> user\_role.users  [<User 'maki'>, <User 'rin'>] |

**常用的SQLAlchemy查询过滤器**

|  |  |
| --- | --- |
| **过滤器** | **说明** |
| 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 |

在查询上应用指定的过滤器后，通过调用all()执行查询，以列表的形式返回结果。还有其他方法能触发查询执行。

**常用的SQLAlchemy查询执行函数**

|  |  |
| --- | --- |
| **方法** | **说明** |
| 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；没有返回None |
| first\_or\_404() | 返回查询的第一个结果；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，没有则返回None |
| get\_or\_404() | 返回指定主键对应的行，没有则终止请求，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，包含指定范围内的结果 |

关系和查询的处理方式类似。

示例：分别从关系的两端查询角色和用户之间的一对多关系：

|  |
| --- |
| >>> users = user\_role.users  >>> users  [<User 'maki'>, <User 'rin'>]  >>> users[0].role  <Role 'User'> |

但是此时执行user\_role.users表达式，隐含的查询会调用all()返回一个用户列表。 query对象是隐藏的，无法指定更精确的查询过滤器。

示例：修改Role模型的动态关系

|  |
| --- |
| class Role(db.Model):  \_\_tablename\_\_ = 'roles' *# 表名*  id = db.Column(db.Integer, primary\_key=True) *# 主键*  name = db.Column(db.String(64), unique=True)  users = db.relationship('User', backref='role', lazy='dynamic') |

加入了lazy = 'dynamic'参数，禁止自动执行查询，可以添加过滤器：

|  |
| --- |
| >>> users = user\_role.users  >>> users  <sqlalchemy.orm.dynamic.AppenderBaseQuery object at 0x055DC210>  >>> users.order\_by(User.username.desc()).all()  [<User 'rin'>, <User 'maki'>]  >>> users.count()  2 |

* 5.9 在视图函数中操作数据库

① index视图

|  |
| --- |
| @app.route('/', methods=['GET', 'POST']) *# 支持GET和POST*  def index():  form = NameForm()  if form.validate\_on\_submit(): *# 提交表单,数据被验证函数接受*  user = User.query.filter\_by(username=form.name.data).first() *# 数据库查询*  if user is None: *# 数据库不存在用户则添加*  user = User(username=form.name.data)  db.session.add(user)  session['known'] = False  else:  session['known'] = True  session['name'] = form.name.data *# 获取字段data属性存入session*  form.name.data = '' *# 清空文本框*  return redirect(url\_for('index')) *# 重定向, GET方式请求index*  return render\_template('index.html', form=form, name=session.get('name'), known=session.get('known', False)) |

② templates.index.html：

|  |
| --- |
| {% extends "base.html"%} *{# 继承于base.html模板 #}*  {% import "bootstrap/wtf.html" as wtf %}  {% block title %}index{% endblock%}  {% block page\_content %}  <div class="page-header">  <h1>hello, {% if name %}{{ name }}{% else %}Stranger{% endif %}!</h1>  {% if not known %}  <p>很高兴见到你！</p> *{# 新用户 #}*  {% else %}  <p>非常高兴再次见到你！</p> *{# 数据库已知用户 #}*  {% endif %}  </div>  {{ wtf.quick\_form(form) }} *{# 使用Bootstrap默认样式渲染表单 #}*  {% endblock %} |

* 5.10 集成Python shell

shell练习用尚可，但每次都要重复导入模型和实例，枯燥、不友善。可以做些配置，让Flask-Script的shell命令自动导入特定的对象。

想把对象添加到导入列表中，要为shell命令注册一个make\_context回调函数

|  |
| --- |
| from flask\_script import Shell  *# 注册了应用app、数据库实例db、模型User和Role*  def make\_shell\_context():  return dict(app=app, db=db, User=User, Role=Role)  manager.add\_command("shell", Shell(make\_context=make\_shell\_context)) |

该函数注册了app、db、User、Role，因此可以直接导入shell

|  |
| --- |
| (venv) $ python hello.py shell  >>> app  <Flask 'hello'>  >>> db  <SQLAlchemy engine=sqlite:///D:\hello\data.sqlite>  >>> User  <class '\_\_main\_\_.User'>  >>> User.query.all()  [<User 'hikari'>, <User 'rin'>, <User 'maki'>, <User 'haha'>, <User 'nozomi'>] |

* 5.11 Flask-Migrate实现数据库迁移

开发过程中，有时需要修改数据库模型，修改之后还需要更新数据库。

仅当数据库表不存在时，Flask-SQLAlchemy才会创建表。因此，更新表的唯一方式就是先删除旧表，不过会丢失数据库中的所有数据。

更好的方法是使用数据库迁移框架。数据库迁移框架能跟踪数据库模式的变化，然后增量式的把变化应用到数据库中。

SQLAlchemy的主力开发人员编写了一个迁移框架[Alembic](https://alembic.readthedocs.org/en/latest/index.html)；[Flask-Migrate](http://flask-migrate.readthedocs.org/en/latest/)扩展对Alembic做了轻量级包装，并集成到Flask-Script中。

① 创建迁移仓库

示例：配置Flask-Migrate

|  |
| --- |
| from flask\_migrate import Migrate, MigrateCommand  migrate = Migrate(app, db)  manager.add\_command('db', MigrateCommand) |

为了导出数据库迁移命令，Flask-Migrate提供了一个MigrateCommand类，可附加到Flask-Script的manager 对象上。

此处，MigrateCommand类使用db命令附加。

在维护数据库迁移之前，要使用init子命令创建迁移仓库：

|  |
| --- |
| (venv) $ python hello.py db init |

然后生成migrations文件夹，所有迁移脚本都存放其中。

**注**：数据库迁移仓库中的文件要和程序其他文件一起纳入版本控制。

② 创建迁移脚本

在Alembic中，数据库迁移用迁移脚本表示。脚本有两个函数：upgrade()把迁移中的改动应用到数据库中；downgrade()将改动删除。

Alembic可以添加和删除改动，数据库可重设到历史的任意一点。

可以使用revision命令手动创建迁移，也可使用migrate命令自动创建。

手动创建的迁移只是一个骨架，upgrade()和downgrade()函数都是空的，要使用Alembic提供的Operations对象指令实现具体操作。自动创建的迁移会根据模型定义和数据库当前状态之间的差异生成upgrade()和downgrade()函数的内容。

**注意**：自动创建的迁移不一定正确，有可能会漏掉一些细节。自动生成迁移脚本后一定要进行检查。

migrate子命令自动创建迁移脚本：

|  |
| --- |
| (venv) $ python hello.py db migrate -m "initial migration" |

③ 更新数据库

使用db upgrade命令把迁移应用到数据库：

|  |
| --- |
| (venv) $ python hello.py db upgrade |

对第一个迁移，其作用和调用db.create\_all()方法一样。但后续迁移中，upgrade 命令能把改动应用到数据库中，且不影响其中保存的数据。

**第6章 电子邮件**

很多应用都需要在特定事件发生时提醒用户，比如注册成功、异地登录等，常用的通信方式是电子邮件。虽然Python标准库的smtplib包可用在Flask程序中发送电子邮件；但包装了smtplib的Flask-Mail扩展能更好地和Flask集成。

* 6.1 使用Flask-Mail 提供电子邮件支持

Flask-Mail连接到SMTP (Simple Mail Transfer Protocol，简单邮件传输协议)服务器，并把邮件交给这个服务器发送。如果不进行配置，Flask-Mail会连接*localhost* 上的端口25，无需验证即可发送电子邮件。

**Flask-Mail SMTP服务器的配置**

|  |  |  |
| --- | --- | --- |
| **配置** | **默认值** | **说明** |
| 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TLS(Transport Layer Security，传输层安全)协议 |
| MAIL\_USE\_SSL | False | 启用SSL(Secure Sockets Layer，安全套接层)协议 |
| MAIL\_USERNAME | None | 邮件账户的用户名 |
| MAIL\_PASSWORD | None | 邮件账户的密码 |

示例：配置Flask-Mail使用163邮箱：

|  |
| --- |
| from flask\_mail import Mail  app.config['MAIL\_SERVER'] = 'smtp.163.com'  app.config['MAIL\_PORT'] = 465 *# SMTP的加密SSL端口*  app.config['MAIL\_USE\_SSL'] = True  app.config['MAIL\_USE\_TLS'] = False  app.config['MAIL\_USERNAME'] = os.environ.get('MAIL\_USERNAME') *# xxx@163.com*  app.config['MAIL\_PASSWORD'] = os.environ.get('MAIL\_PASSWORD') *# 授权码, 不是密码*  mail = Mail(app) |

注意：邮箱需要手动开启SMTP发信功能。

千万不要把账户密码直接写入脚本，特别是要把源码传递GitHub或博客时。

为了保护账户信息，需要让脚本从环境变量中导入敏感信息。

设置环境变量：

Linux：

|  |
| --- |
| (venv) $ export MAIL\_USERNAME=abc@163.com |

Windows：

|  |
| --- |
| (venv) $ set MAIL\_USERNAME=abc@163.com |

**20180504**

* 6.2 在程序中集成发送电子邮件

// 用163邮箱按照例子发送邮件总是失败，换QQ邮箱了...

QQ邮箱-->设置-->账户-->开启服务-->POP3/SMTP服务-->手机发短信-->得到16位授权码

① 发送邮件函数send\_mail()：

|  |
| --- |
| from flask\_mail import Mail, Message  app.config['MAIL\_SERVER'] = 'smtp.qq.com'  app.config['MAIL\_PORT'] = 465 *# SMTP的加密SSL端口*  app.config['MAIL\_USE\_SSL'] = True  with open('mail.hikari') as f:  data = eval(f.read()) *# 不想用环境变量...*  my\_mail = data.get('mail') *# xxx@qq.com*  my\_pwd = data.get('password') *# 授权码, 不是密码*  app.config['MAIL\_USERNAME'] = my\_mail  app.config['MAIL\_PASSWORD'] = my\_pwd  ADMIN = 'hikari\_python@163.com'  mail = Mail(app)  def send\_mail(to, subject, template, \*\*kwargs):  *# to为接收方, subject为邮件主题, template为渲染邮件正文的模板*  msg = Message(subject, sender=my\_mail, recipients=[to])  msg.body = render\_template(template + '.txt', \*\*kwargs)  msg.html = render\_template(template + '.html', \*\*kwargs)  mail.send(msg) |

每次有新用户，就用QQ邮箱给管理员hikari\_python@163.com发邮件。

// 为什么不是用管理员邮箱给新用户发邮件?

② index视图修改：

|  |
| --- |
| @app.route('/', methods=['GET', 'POST']) *# 支持GET和POST*  def index():  form = NameForm()  if form.validate\_on\_submit(): *# 提交表单,数据被验证函数接受*  user = User.query.filter\_by(username=form.name.data).first() *# 数据库查询*  if user is None: *# 数据库不存在用户则添加*  user = User(username=form.name.data)  db.session.add(user)  session['known'] = False  if ADMIN:  send\_mail(ADMIN, 'New User', 'mail/new\_user', user=user)  else:  session['known'] = True  session['name'] = form.name.data *# 获取字段data属性存入session*  form.name.data = '' *# 清空文本框*  return redirect(url\_for('index')) *# 重定向, GET方式请求index*  return render\_template('index.html', form=form, name=session.get('name'), known=session.get('known', False)) |

③ 邮件正文

templates/mail/new\_user.html：

|  |
| --- |
| html: User <b>{{ user.username }}</b> has joined. |

templates/mail/new\_user.txt：

|  |
| --- |
| txt: User {{ user.username }} has joined. |

分别渲染纯文本和HTML版本的邮件正文。

电子邮件的模板中要有一个模板参数是user，因此调用send\_mail()函数时要以关键字参数的形式传入user。

结果：



// txt纯文本呢?

* 6.3 异步发送电子邮件

如果发送几封邮件，可能会发现mail.send()在发送电子邮件时停滞了几秒，为了避免处理请求时不必要得到延迟，可以把发送电子邮件的函数移到后台线程。

示例：异步发送电子邮件

|  |
| --- |
| from threading import Thread  def send\_async\_mail(app,msg):  with app.app\_context():  mail.send(msg)  def send\_mail(to, subject, template, \*\*kwargs):  *# to为接收方, subject为邮件主题, template为渲染邮件正文的模板*  msg = Message(subject, sender=my\_mail, recipients=[to])  msg.body = render\_template(template + '.txt', \*\*kwargs)  msg.html = render\_template(template + '.html', \*\*kwargs)  t=Thread(target=send\_async\_mail,args=[app,msg])  t.start()  return t |

很多Flask扩展都假设已经存在激活的程序上下文和请求上下文。 Flask-Mail中的send()函数使用current\_app，因此必须激活程序上下文。但在不同线程中执行 send()函数时，程序上下文要使用app.app\_context()手动创建。

如果程序要发送大量电子邮件，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。比如可以把执行send\_async\_mail()函数操作发给[Celery](http://www.celeryproject.org/)任务队列。

**第7章 大型程序的结构**

之前一直在hello.py一个文件里搬砖，一旦砖堆多了，看得头昏眼花，后期修改变得复杂而困难。

* 7.1 项目结构

大型Flask程序项目基本结构：



① Flask程序一般保存在名为app的包中；

② migrations目录包含数据库迁移脚本；

③ 单元测试编写在test包；

④ venv目录包含Python虚拟环境；

⑤ requirements.txt列出所有依赖包，便于在其他电脑生成相同的虚拟环境；

⑥ config.py：配置文件；

⑦ manage.py：用于启动程序和其他的程序任务。

* 7.2 配置选项

程序经常需要设定多个配置，如开发、测试、生产环境需要不同的数据库。

不再使用hello.py中简单的字典结构配置，而使用层次结构的配置类。

示例：配置文件config.py：

|  |
| --- |
| import os  *# flask程序根目录*  basedir = os.path.abspath(os.path.dirname(\_\_file\_\_))  my\_mail, my\_pwd = None, None  with open('mail.hikari') as f:  data = eval(f.read())  my\_mail = data.get('mail') *# xxx@qq.com*  my\_pwd = data.get('password') *# 授权码, 不是密码*  def get\_db\_url(a):  return os.environ.get('{}DATABASE\_URL'.format(a.upper())) or 'sqlite:///{}'.format(os.path.join(basedir, '{}data.sqlite'.format(a)))  class Config(): *# 父类通用配置*  *# 敏感信息从环境变量获取, 但还是给了默认值*  SECRET\_KEY = os.environ.get('SECRET\_KEY') or 'hoshizora rin'  MAIL\_SERVER = os.environ.get('MAIL\_SERVER') or 'smtp.qq.com'  MAIL\_PORT = int(os.environ.get('MAIL\_PORT', 465)) *# SMTP的加密SSL端口*  MAIL\_USE\_SSL = True *# SSL*  MAIL\_USERNAME = os.environ.get('MAIL\_USERNAME') or my\_mail  MAIL\_PASSWORD = os.environ.get('MAIL\_PASSWORD') or my\_pwd  SQLALCHEMY\_COMMIT\_ON\_TEARDOWN = True  SQLALCHEMY\_TRACK\_MODIFICATIONS = False  FLASKY\_ADMIN = os.environ.get('FLASKY\_ADMIN') or 'hikari\_python@163.com'  @staticmethod  def init\_app(app): *# 对当前环境配置初始化*  pass  *# 3种环境使用不同数据库*  class DevelopmentConfig(Config): *# 开发专用配置*  DEBUG = True  SQLALCHEMY\_DATABASE\_URI = get\_db\_url('dev\_')  class TestingConfig(Config): *# 测试专用配置*  TESTING = True  SQLALCHEMY\_DATABASE\_URI = get\_db\_url('test\_')  class ProductionConfig(Config): *# 生产专用配置*  SQLALCHEMY\_DATABASE\_URI = get\_db\_url('')  config = {  'development': DevelopmentConfig,  'testing': TestingConfig,  'production': ProductionConfig,  'default': DevelopmentConfig *# 默认开发环境的配置*  } |

* 7.3 程序包

程序包用来保存程序所有代码、模块和静态文件，这个包可以称为app (应用)。templates和static目录是程序包一部分，需要移到app目录；数据库模型和电子邮件支持函数model.py和email.py也需要移到app目录。

① 使用程序工厂函数

单个文件开发的缺点是运行脚本时，程序实例已经创建，无法动态修改配置。如在单元测试时，为了提高测试覆盖度，需在不同配置环境中运行程序。

解决方法是延迟创建程序实例，将创建过程移到可显式调用的工厂函数。这样不仅给配置留有时间，还能创建多个程序实例。

示例：程序包的构造文件app/\_\_init\_\_.py

|  |
| --- |
| from flask import Flask  from flask\_bootstrap import Bootstrap  from flask\_mail import Mail  from flask\_moment import Moment  from flask\_sqlalchemy import SQLAlchemy  from config import config  bootstrap = Bootstrap()  mail = Mail()  moment = Moment()  db = SQLAlchemy()  def create\_app(config\_name): *# 工厂函数, 参数为配置名*  app = Flask(\_\_name\_\_)  app.config.from\_object(config[config\_name]) *# 导入配置*  config[config\_name].init\_app(app)  bootstrap.init\_app(app)  mail.init\_app(app)  moment.init\_app(app)  db.init\_app(app)  *# 附加路由和自定义的错误页面*  return app *# 返回创建的程序示例* |

② 在蓝本中实现程序功能

转换成工厂函数的操作让定义路由变得复杂了，因为只有调用create\_app()后才能使用app.route装饰器(错误页面处理用app.errorhandler装饰器)，这时定义路由太晚了。

Flask使用蓝本提供了更好的解决方法。蓝本中定义的路由处于休眠状态，直到蓝本注册到程序后，路由才真正成为程序的一部分。使用位于全局作用域中的蓝本时，定义路由的方法几乎和单脚本程序一样。

蓝本可以在单个文件中定义，也可以定义成包，包中多个模块，比如在app包中创建子包main，用于保存蓝本。

示例1：创建蓝本：app/main/\_\_init\_\_.py

|  |
| --- |
| from flask import Blueprint  *# 创建蓝本对象, 参数为蓝本的名字和蓝本所在包或模块*  main = Blueprint('main', \_\_name\_\_)  *# app/main/view.py保存路由和视图函数; app/main/errors.py保存错误处理*  *# 导入这两个模块是为了将路由和错误处理与蓝本关联起来*  *# 末尾导入为了避免循环导入, 因为views.py和errors.py要导入蓝本main*  from . import views, errors |

蓝本在工厂函数create\_app()中注册到程序。

示例2：注册蓝本：app/\_\_init\_\_.py：

|  |
| --- |
| def create\_app(config\_name):  *# ...*  from .main import main as main\_blueprint  app.register\_blueprint(main\_blueprint)  return app *# 返回创建的程序示例* |

示例3：蓝本中的错误处理：app/main/errors.py：

|  |
| --- |
| from flask import render\_template  from . import main  *# 如果使用errorhandler装饰器, 只能处理蓝本中的错误;*  *# 使用app\_errorhandler装饰器, 注册全局错误处理*  @main.app\_errorhandler(404)  def page\_not\_found(e):  return render\_template('404.html'), 404  @main.app\_errorhandler(500)  def internal\_server\_error(e):  return render\_template('500.html'), 500 |

示例4：蓝本中定义路由：app/main/views.py

|  |
| --- |
| from flask import render\_template, session, redirect, url\_for, current\_app  from .. import db  from ..models import User  from ..email import send\_mail  from . import main  from .forms import NameForm  @main.route('/', methods=['GET', 'POST']) *# 支持GET和POST*  def index():  form = NameForm()  if form.validate\_on\_submit(): *# 提交表单,数据被验证函数接受*  user = User.query.filter\_by(username=form.name.data).first() *# 数据库查询*  if user is None: *# 数据库不存在用户则添加*  user = User(username=form.name.data)  db.session.add(user)  session['known'] = False  admin = current\_app.config['FLASKY\_ADMIN']  if admin:  send\_mail(admin, 'New User', 'mail/new\_user', user=user)  else:  session['known'] = True  session['name'] = form.name.data *# 获取字段data属性存入session*  *# 蓝本端点自动添加命名空间, 为main.index; 当前蓝本简写为.index*  return redirect(url\_for('.index')) *# 重定向, GET方式请求index*  return render\_template('index.html', form=form, name=session.get('name'), known=session.get('known', False)) |

蓝本中编写视图函数区别：1. 路由装饰器由蓝本提供，是main.route()而不是app.route()；2. url\_for()函数用法不同，其第1参数是路由的端点名。在程序路由中默认为视图函数名；而Flask为蓝本的所有端点加上一个命名空间，这样不同蓝本可以有相同的函数名而不冲突。

所以上面index视图注册的端点名是main.index，在同一蓝本可以简写为.index，而跨蓝本重定向需要带有命名空间。

示例5：蓝本中的表单类：app/main/forms.py：直接复制

|  |
| --- |
| from flask\_wtf import FlaskForm  from wtforms import StringField, SubmitField  from wtforms.validators import DataRequired  class NameForm(FlaskForm): *# 一个文本字段和一个提交按钮*  name = StringField('你的名字是？', validators=[DataRequired()])  submit = SubmitField('提交') |

示例6：app/email.py

|  |
| --- |
| from threading import Thread  from flask import current\_app, render\_template  from flask\_mail import Message  from . import mail *# \_\_init\_\_.py中的mail对象*  *# 异步发送邮件*  def send\_async\_mail(app, msg):  with app.app\_context():  mail.send(msg)  def send\_mail(to, subject, template, \*\*kwargs):  *# to为接收方,subject为邮件主题,template为渲染邮件正文的模板*  app = current\_app.\_get\_current\_object() *# 将app传给子线程?*  msg = Message(  subject, sender=app.config['FLASKY\_MAIL\_SENDER'], recipients=[to])  msg.body = render\_template(template + '.txt', \*\*kwargs)  msg.html = render\_template(template + '.html', \*\*kwargs)  t = Thread(target=send\_async\_mail, args=[app, msg])  t.start()  return t |

示例7：app/models.py：将User类和Role类复制，导入db对象

|  |
| --- |
| from . import db |

将static目录和templates目录移到app目录

* 7.4 启动脚本

manage.py用于启动程序：

|  |
| --- |
| import os  from app import create\_app, db  from app.models import User, Role  from flask\_script import Manager, Shell  from flask\_migrate import Migrate, MigrateCommand  app = create\_app(os.environ.get('FLASK\_CONFIG') or 'default')  manager = Manager(app)  migrate = Migrate(app, db)  def make\_shell\_context():  return dict(app=app, db=db, User=User, Role=Role)  manager.add\_command("shell", Shell(make\_context=make\_shell\_context))  manager.add\_command('db', MigrateCommand)  if \_\_name\_\_ == '\_\_main\_\_':  manager.run() |

* 7.5 需求文件

程序中必须包含一个requirements.txt文件，记录所有依赖包及其精确的版本号。用于在另一台电脑重新生成虚拟环境，如部署程序时使用的电脑。

自动生成需求文件：

|  |
| --- |
| (venv) $ pip freeze >requirements.txt |

* 7.6 单元测试

这个程序很小，没什么可测试的。

使用Python标准库的[unittest](https://docs.python.org/3.6/library/unittest.html)包测试。

示例：单元测试：tests/test\_basics.py：

|  |
| --- |
| import unittest  from flask import current\_app  from app import create\_app, db  class BasicsTestCase(unittest.TestCase):  def setUp(self): *# 创建一个测试环境*  self.app = create\_app('testing')  self.app\_context = self.app.app\_context() *# 激活上下文*  self.app\_context.push()  db.create\_all() *# 创建数据库*  def tearDown(self):  *# 删除数据库和上下文*  db.session.remove()  db.drop\_all()  self.app\_context.pop()  def test\_app\_exists(self): *# 测试app实例是否存在*  self.assertFalse(current\_app is None)  def test\_app\_is\_testing(self): *# 程序是否在测试配置环境运行*  self.assertTrue(current\_app.config['TESTING']) |

要把tests目录当做包，需要添加tests/\_\_init\_\_.py文件，可以为空，unittest会扫描所有模块并查找测试。

为了运行单元测试，可以在manage.py中添加一个自定义命令。

示例：启动单元测试命令：manage.py：

|  |
| --- |
| @manager.command  def test():  """Run the unit tests."""  import unittest  tests = unittest.TestLoader().discover('tests')  unittest.TextTestRunner(verbosity=2).run(tests) |

manager.command 装饰器装饰的函数名就是命令名，函数的文档字符串会显示在帮助消息中。test()函数的定义体中调用了unittest包提供的测试运行函数。

单元测试可使用下面的命令运行：

|  |
| --- |
| (venv) $ python manage.py test  test\_app\_exists (test\_basics.BasicsTestCase) ... ok  test\_app\_is\_testing (test\_basics.BasicsTestCase) ... ok  ----------------------------------------------------------------------  Ran 2 tests in 1.263s  OK |

* 7.7 创建数据库

重组后的程序和单脚本版本使用不同的数据库。从环境变量读取数据库URL，或默认的SQLite数据库。

不管从哪里获取数据库URL，都要在新数据库中创建数据表。如果使用Flask-Migrate跟踪迁移，可使用如下命令创建数据表或者升级到最新修订版本：

|  |
| --- |
| (venv) $ python manage.py db upgrade |

**20180507**

**实战：社交博客程序**

**第8章 用户认证**

最常用的认证方法是要求用户提供一个身份证明(用户名或email)和一个密码。

* 8.1 Flask的认证扩展

Python优秀的认证包有很多，但没有一个能实现所有功能。

此处使用：

① Flask-Login：管理已登录用户的用户会话；

② Werkzeug：计算密码散列值并进行核对；

③ itsdangerous：生成并核对加密安全令牌。

* 8.2 密码安全性

要保证数据库中用户密码的安全，不能存储明文密码，而要存储密码的散列值。计算密码散列值的函数接收密码作为参数，使用一种或多种加密算法转换密码，最终得到和原始密码没有关系的字符序列。

**使用Werkzeug实现密码散列**

Werkzeug包的security模块能很方便地实现密码散列值的计算。

只需两个函数，分别用在注册用户和验证用户阶段。

① generate\_password\_hash(password, method='pbkdf2:sha256', salt\_length=8)

原始密码作为输入，返回密码的字符串散列值。

method和salt\_length的默认值能满足大多数需求。

② check\_password\_hash(pwhash, password)

参数为散列值和密码。返回True表明密码正确。

示例：app/models.py：User模型添加散列密码字段

|  |
| --- |
| from werkzeug.security import generate\_password\_hash, check\_password\_hash  class User(db.Model):  \_\_tablename\_\_ = 'users'  id = db.Column(db.Integer, primary\_key=True) # 主键  username = db.Column(db.String(64), unique=True, index=True)  role\_id = db.Column(db.Integer, db.ForeignKey(  'roles.id')) # 外键, roles表中的id  password\_hash = db.Column(db.String(128)) # 散列密码  # password属性只可写不可读, 因为获取散列值没有意义, 无法还原密码  @property  def password(self):  raise AttributeError('password is not a readable attribute')  @password.setter  def password(self, pwd):  self.password\_hash = generate\_password\_hash(pwd)  def verify\_password(self, pwd): # 校验密码  return check\_password\_hash(self.password\_hash, pwd)  def \_\_repr\_\_(self):  return '<User %r>' % self.username |

在shell中进行测试：

|  |
| --- |
| (venv) $ python manage.py shell  >>> u = User()  >>> u.password = 'maki'  >>> u.password\_hash  'pbkdf2:sha256:50000$sq4UFy9l$77ed2de287d2361ca0da4b912e4d376d26d1a71f6b4d9b0b67b8ab164149aadf'  >>> u.verify\_password('maki')  True  >>> u.verify\_password('rin')  False  >>> u2 = User()  >>> u2.password = 'maki'  >>> u2.password\_hash  'pbkdf2:sha256:50000$QNJbN8eL$1fd34f7b2019c36ce8b9097ff678860703f2e7a2cf3571e3e69d2e9c54debedc' |

用户u和u2使用相同的密码，但是密码的散列值也不一样，说明撒盐了?

可以把上述测试写成单元测试，以便于后续测试。在tests 包中新建一个test\_user\_model模块，测试最近对User模型所做的修改。

示例：tests/test\_user\_model.py：密码散列化测试：

|  |
| --- |
| import unittest  from app.models import User  # 测试用户模型的密码散列化  class UserModelTestCase(unittest.TestCase):  # test\_basics.py里已经有setUP和tearDown了, 此处不需要, 写了报错  def test\_password\_setter(self): # 测试设置密码  u = User(password='maki')  self.assertTrue(u.password\_hash is not None)  def test\_no\_password\_getter(self): # 测试不能获取密码  u = User(password='maki')  with self.assertRaises(AttributeError):  u.password  def test\_password\_verification(self): # 测试密码认证  u = User(password='maki')  self.assertTrue(u.verify\_password('maki'))  self.assertFalse(u.verify\_password('rin'))  def test\_password\_salts\_are\_random(self): # 测试是否随机撒盐  u = User(password='maki')  u2 = User(password='maki')  self.assertFalse(u.password\_hash == u2.password\_hash) |

* 8.3 创建认证蓝本

前一章创建app过程移入工厂函数后，使用蓝本在全局作用域定义路由。与用户认证系统相关的路由可在auth；蓝本定义。不同的功能使用不同的蓝本是保持代码整齐有序的好方法。

① app/auth/\_\_init\_\_.py：创建蓝本

|  |
| --- |
| from flask import Blueprint  auth = Blueprint('auth', \_\_name\_\_)  from . import views |

和之前main蓝本一样，auth也作为一个包，\_\_init\_\_.py底部引入auth/view.py将路由和蓝本关联。

② app/auth/views.py：蓝本中的路由和视图函数

|  |
| --- |
| from flask import render\_template  from . import auth  @auth.route('/login')  def login():  return render\_template('auth/login.html') |

指定模板在app/templates/auth目录中，避免和main蓝本和后续蓝本的模板发生命名冲突。

③ app/\_\_init\_\_.py：添加auth蓝本

|  |
| --- |
| def create\_app(config\_name): # 工厂函数, 参数为配置名  # ...  from .auth import auth as auth\_blueprint  # url\_prefix是可选, 蓝本所有路由添加前缀, 如/login变为/auth/login  app.register\_blueprint(auth\_blueprint, url\_prefix='/auth')  return app # 返回创建的程序示例 |

* 8.4 使用Flask-Login认证用户

Flask-Login是非常有用的小型扩展，用来管理用户认证系统的认证状态，且不依赖特定的认证机制。

① 用于登录的用户模型

为了使用Flask-Login，User模型需要实现几个方法：

|  |
| --- |
| 1) is\_authenticated()：如果用户已经登录，返回True否则False  2) is\_active()：如果允许用户登录，返回True否则False；如果要禁用账户，可以返回False  3) is\_anonymous：对普通用户返回False  4) get\_id()：返回用户的唯一标识符，使用Unicode编码字符串 |

这4个方法可以直接在User类中实现，但Flask-Login提供UserMixin类，包含这些方法的默认实现，满足大多数需求，可以用User继承UserMixin：

app/models.py：修改User模型，支持用户登录

|  |
| --- |
| from flask\_login import UserMixin  class User(UserMixin, db.Model):  \_\_tablename\_\_ = 'users'  id = db.Column(db.Integer, primary\_key=True) # 主键  email = db.Column(db.String(64), unique=True, index=True) # 添加邮箱字段  username = db.Column(db.String(64), unique=True, index=True) # 用户名  password\_hash = db.Column(db.String(128)) # 密码的散列值  role\_id = db.Column(db.Integer, db.ForeignKey('roles.id')) # 外键 |

app/\_\_init\_\_.py：初始化Flask-Login

|  |
| --- |
| from flask\_login import LoginManager  login\_manager = LoginManager()  # 用户会话保护等级, 可以设为None, 'basic', 'strong', 防止用户会话遭篡改  # 'strong': 记录客户端ip和浏览器User-Agent, 如果发生异动则登出用户  login\_manager.session\_protection = 'strong'  # auth蓝本的login视图  login\_manager.login\_view = 'auth.login'  def create\_app(config\_name): # 工厂函数, 参数为配置名  # ...  login\_manager.init\_app(app)  # ... |

Flask-Login要求实现一个回调函数，使用指定的标识符加载用户：

app/models.py：加载用户的回调函数

|  |
| --- |
| @login\_manager.user\_loader  def load\_user(user\_id):  # user\_id为Unicode字符串表示的用户标识符, 如果有此用户返回用户对象; 否则返回None  return User.query.get(int(user\_id)) |

② 保护路由

为了保护路由只让认证用户访问，Flask-Login提供login\_required装饰器：

|  |
| --- |
| from flask\_login import login\_required  @app.route('/secret')  @login\_required  def secret():  pass |

未认证用户访问此路由，Flask-Login会拦截请求，把用户发往登录页面。

③ 登录表单

包含输入电子邮箱的文本字段、密码字段、保持登录复选框、提交按钮。

app/auth/forms.py：

|  |
| --- |
| from flask\_wtf import FlaskForm  from wtforms import StringField, PasswordField, BooleanField, SubmitField  from wtforms.validators import DataRequired, Length, Email  class LoginForm(FlaskForm):  email = StringField('邮箱', validators=[ # 数据必须, 长度限制, email验证函数  DataRequired(), Length(5, 64), Email()])  password = PasswordField('密码', validators=[DataRequired()])  remember\_me = BooleanField('记住我')  submit = SubmitField('登录') |

登录页面模板为app/templates/auth/login.html；

app/templates/base.html：导航条右边根据是否登录添加登录退出按钮

|  |
| --- |
| {# 登录退出按钮 #}  <ul class="nav navbar-nav navbar-right">  {% if current\_user.is\_authenticated %}  <li><a href="{{ url\_for('auth.logout') }}">退出</a></li>  {% else %}  <li><a href="{{ url\_for('auth.login') }}">登录</a></li>  {% endif %}  </ul> |

变量current\_user由Flask-Login定义，在视图函数和模板自动可用，值是当前登录用户；如果用户未登录则是一个匿名用户代理对象，is\_authenticated为False

④ 登入用户

app/auth/views.py：登录视图函数login()

|  |
| --- |
| from flask import render\_template, redirect, request, url\_for, flash  from flask\_login import login\_user, logout\_user, login\_required  from . import auth  from ..models import User  from .forms import LoginForm  @auth.route('/login', methods=['GET', 'POST'])  def login():  form = LoginForm()  if form.validate\_on\_submit():  # 根据输入邮箱查询用户  user = User.query.filter\_by(email=form.email.data).first()  # 如果用户存在且密码正确  if user and user.verify\_password(form.password.data):  login\_user(user, form.remember\_me.data)  nxt = request.args.get('next')  # 没有next重定向到首页  if nxt is None or not nxt.startswith('/'):  nxt = url\_for('main.index')  return redirect(nxt)  flash('用户名或密码错误！') # 认证失败  return render\_template('auth/login.html', form=form) |

此LoginForm与之前的NameForm类似，当表单被提交，是POST请求，验证表单数据，尝试登录用户；否则是GET请求，直接渲染模板，显示表单。

如果验证成功，调用Flask-Login的login\_user()函数，在用户会话把用户标记为已登录。第2个参数remember默认为False，关闭浏览器会话就过期，下次访问要重新登录；True则会在浏览器写入一个长期有效的cookie。

app/templates/auth/login.html：登录表单

|  |
| --- |
| {% extends "base.html" %} {# 继承于base.html模板 #}  {% import "bootstrap/wtf.html" as wtf %}  {% block title %}hikari app - Login{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>登录</h1></div>  <div class="col-md-4">  {{ wtf.quick\_form(form) }} {# 使用Bootstrap默认样式渲染表单 #}  </div>  {% endblock %} |

⑤ 登出用户

app/auth/views.py：logout登出视图

|  |
| --- |
| @auth.route('/logout')  @login\_required  def logout(): # 登出用户  logout\_user() # 删除并重设用户会话  flash('你已经退出...') # 显示登出消息  return redirect(url\_for('main.index')) # 重定向至首页 |

⑥ 测试登录

app/templates/index.html：为已登录用户显示欢迎消息

|  |
| --- |
| {% extends "base.html"%} {# 继承于base.html模板 #}  {% block title %}hikari app{% endblock%}  {% block page\_content %}  <div class="page-header">  <h1>Hello, {% if current\_user.is\_authenticated %}{{ current\_user.username }}{% else %}Stranger{% endif %}!</h1></div>  {% endblock %} |

因为还未添加用户注册功能，新用户可在shell中注册：

|  |
| --- |
| (venv) $ python manage.py shell  >>> u=User(email='hikari@example.com',username='hikari',password='123456')  >>> db.session.add(u)  >>> db.session.commit()  >>> exit() |

python manage.py runserver启动服务器，默认http://127.0.0.1:5000

显示stranger，点击右上角登录，跳转到http://127.0.0.1:5000/auth/login



登录后，跳转至首页，显示Hello, hikari !

点击退出，显示flash消息：你已经退出...

* 8.5 注册新用户

① 用户注册表单

app/auth/forms.py：用户注册表单类

|  |
| --- |
| from flask\_wtf import FlaskForm  from wtforms import StringField, PasswordField, BooleanField, SubmitField  from wtforms.validators import DataRequired, Length, Email, Regexp, EqualTo  from wtforms import ValidationError  from ..models import User  class RegistrationForm(FlaskForm):  email = StringField('邮箱', validators=[DataRequired(), Length(5, 64), Email()])  username = StringField('用户名', validators=[DataRequired(), Length(2, 20), Regexp('^[A-Za-z][A-Za-z0-9\_]{1,19}$', 0, '用户名只能是字母数字下划线！')])  password = PasswordField('输入密码', validators=[DataRequired(), EqualTo('password2', message='密码不一致！')])  password2 = PasswordField('确认密码', validators=[DataRequired()])  submit = SubmitField('注册')  # 自定义验证函数, 如果表单类定义了validate\_开头且跟着字段名的方法  # 此方法与常规验证函数一起调用  def validate\_email(self, field):  if User.query.filter\_by(email=field.data).first():  raise ValidationError('该邮箱已被注册！')  def validate\_username(self, field):  if User.query.filter\_by(username=field.data).first():  raise ValidationError('用户名已经存在！') |

登录页面需要有一个指向注册页面的链接

app/templates/auth/login.html：链接到注册页面

|  |
| --- |
| <div class="col-md-4">  {{ wtf.quick\_form(form) }} {# 使用Bootstrap默认样式渲染表单 #}<br>  <p>新用户? <a href="{{ url\_for('auth.register') }}">点击注册</a></p></div> |

// 不应该在base.html未登录的用户都显示注册按钮?

② 注册新用户

app/auth/views.py：用户注册视图

|  |
| --- |
| from .. import db  from .forms import RegistrationForm  @auth.route('/register', methods=['GET', 'POST'])  def register():  form = RegistrationForm()  if form.validate\_on\_submit():  user = User(email=form.email.data, username=form.username.data, password=form.password.data)  db.session.add(user)  flash('注册成功！现在可以登录了！')  return redirect(url\_for('auth.login'))  return render\_template('auth/register.html', form=form) |

app/templates/auth/register.html：注册模板和登录模板类似

|  |
| --- |
| {% extends "base.html" %} {# 继承于base.html模板 #}  {% import "bootstrap/wtf.html" as wtf %}  {% block title %}hikari app - Register{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>注册</h1></div>  <div class="col-md-4">{{ wtf.quick\_form(form) }}</div>  {% endblock %} |

* 8.6 确认账户

有时需要确认用户提供的信息是否正确，一般通过邮件与用户联系。

通常用户注册后，会发送一封确认邮件，新账户暂时标为待确认状态，用户按说明操作后，才能证明自己信息正确。账户确认过程中，往往要求用户点击一个包含确认令牌的特殊URL链接。

① 使用itsdangerous生成确认令牌

确认链接最简单的格式是http://www.example.com/auth/confirm/<*id* >形式的URL，id 是数据库分配给用户的数字id。用户点击链接后，处理这个路由的视图函数就将收到的用户id作为参数进行确认，然后将用户状态更新为已确认。

但此方式显然不是很安全，只要用户能判断确认链接的格式，就可以随意指定URL中的数字，从而确认任意账户。解决方法是把URL中的id 换成将相同信息安全加密后得到的令牌。

第4章的用户会话，Flask使用加密的签名cookie保护用户会话，防止被篡改。这种安全的cookie使用itsdangerous包签名。同样也可用于确认令牌上。

使用itsdangerous包生成包含用户id的安全令牌：

|  |
| --- |
| (venv) $ python manage.py shell  >>> from manage import app  >>> from itsdangerous import TimedJSONWebSignatureSerializer as Serializer  >>> s = Serializer(app.config['SECRET\_KEY'], expires\_in=3600)  >>> token = s.dumps({'confirm':23})  >>> token  b'eyJhbGciOiJIUzI1NiIsImlhdCI6MTUyNTY4MjgxOSwiZXhwIjoxNTI1Njg2NDE5fQ.eyJjb25maXJtIjoyM30.hx1WUKVdrJts3fx39t6y9wr59rgpB8ryBsu5a9byWuo'  >>> data = s.loads(token)  >>> data  {'confirm': 23} |

itsdangerous有多种生成令牌的方法。其中TimedJSONWebSignatureSerializer类生成具有过期时间的JSON Web签名(JSON Web Signatures，JWS)。构造函数第1个参数是一个密钥，在Flask程序中使用SECRET\_KEY设置(config.py)。expires\_in参数设置令牌的过期时间，单位为秒。

dumps()方法为指定数据生成一个加密签名，然后再对数据和签名进行序列化，生成令牌字符串。

loads()方法，唯一的参数是令牌字符串。检验签名和过期时间，如果通过，返回原始数据。如果提供的令牌不正确或过期了，则抛出异常。

可以将这种生成和检验令牌的功能添加到User模型：

app/models.py：确认用户账户

|  |
| --- |
| from . import db  from flask\_login import UserMixin  from itsdangerous import TimedJSONWebSignatureSerializer as Slzer  from flask import current\_app  class User(UserMixin, db.Model):  # ...  confirmed = db.Column(db.Boolean, default=False)  def generate\_confirmation\_token(self, expiration=3600):  # 生成确认令牌字符串, 默认有效时间1h  s = Slzer(current\_app.config['SECRET\_KEY'], expiration)  return s.dumps({'confirm': self.id}).decode('utf-8')  def confirm(self, token):  # 检验令牌, 通过则confirmed字段设为True  s = Slzer(current\_app.config['SECRET\_KEY'])  try:  data = s.loads(token.encode('utf-8'))  except:  return False  if data.get('confirm') != self.id:  return False  self.confirmed = True  db.session.add(self)  return True |

由于confirm()检查的是当前用户的令牌，所以恶意用户无法帮别人确认。

User模型新加了字段，需要数据库迁移。

tests/ test\_user\_model.py：确认令牌测试

|  |
| --- |
| def test\_valid\_confirmation\_token(self): # 测试正确的确认令牌  u = User(password='maki')  db.session.add(u)  db.session.commit()  token = u.generate\_confirmation\_token()  self.assertTrue(u.confirm(token))  def test\_invalid\_confirmation\_token(self): # 测试用别人的确认令牌  u1 = User(password='maki')  u2 = User(password='rin')  db.session.add(u1)  db.session.add(u2)  db.session.commit() # 要commit(), 不然结果为True, assertFalse抛出异常?  token = u1.generate\_confirmation\_token()  self.assertFalse(u2.confirm(token))  def test\_expired\_confirmation\_token(self): # 测试令牌过时  u = User(password='maki')  db.session.add(u)  db.session.commit()  token = u.generate\_confirmation\_token(1)  time.sleep(2)  self.assertFalse(u.confirm(token)) |

/\* 貌似测试在setUp和tearDown之间，测试时，COMMIT\_ON\_TEARDOWN就没效果了，需要手动commit? 把3个commit都注释，结果u2.confirm(token)返回True (why?)，抛出AssertionError: True is not false异常? \*/

**20180508**

② 发送确认邮件

现在的/register路由在将新用户添加到数据库后重定向到/index(不是/login吗?)。在重定向前，需要发送确认邮件。

|  |
| --- |
| from ..email import send\_mail  @auth.route('/register', methods=['GET', 'POST'])  def register():  form = RegistrationForm()  if form.validate\_on\_submit():  user = User(email=form.email.data,  username=form.username.data, password=form.password.data)  db.session.add(user)  # 即使自动提交,此处也要commit,因为要获取id用于生成确认令牌,不能延后提交  db.session.commit()  token = user.generate\_confirmation\_token()  send\_mail(user.email, '激活你的账号',  'auth/email/confirm', user=user, token=token)  flash('激活邮件已发送至你的邮箱...')  return redirect(url\_for('auth.login'))  return render\_template('auth/register.html', form=form) |

认证的邮件模板也有txt和HTML两个版本，放在app/templates/auth/email目录，为confirm.txt和confirm.html。

app/templates/auth/email/confirm.html：确认邮件的HTML格式

|  |
| --- |
| <p>你好, {{ user.username }}!</p>  <p>欢迎注册<b>hikari app</b>!</p>  <p><a href="{{ url\_for('auth.confirm', token=token, \_external=True) }}">点击此处</a>激活你的账号。</p>  <p>你也可以将下面链接复制到浏览器的地址栏:</p>  <p>{{ url\_for('auth.confirm', token=token, \_external=True) }}</p>  <p>感谢注册!</p>  <p>from hikari</p>  <p><small>注: hikari是不会看对这封邮件的回复的 !</small></p> |

默认url\_for()生成相对URL，如url\_for('auth.confirm', token='abc') 返回'/auth/confirm/abc'。相对URL在网页的上下文中可以正常使用，因为通过添加当前页面的主机名和端口号，浏览器会将其转换成绝对URL。但通过电子邮件发送URL时，并没有这种上下文。\_external=True参数要求程序生成完整的URL，其中包含协议、主机名和端口。

app/auth/views.py：确认用户账户的confirm视图

|  |
| --- |
| from flask\_login import current\_user  @auth.route('/confirm/<token>')  @login\_required  def confirm(token):  if current\_user.confirmed: # 用户已经确认过,重定向到主页  return redirect(url\_for('main.index'))  if current\_user.confirm(token):  # db.session.commit()  flash('你的账号已通过认证！')  else:  flash('认证链接无效或已经过期！')  return redirect(url\_for('main.index')) |

login\_required装饰器保护此路由，用户点击确认邮件中的链接后，要先登录，然后才能执行此视图函数。

可以决定用户确认账户之前能做哪些操作。比如允许未确认的用户登录，但只显示一个页面，要求用户在获取权限之前先确认账户。

可使用Flask提供的before\_request钩子完成。对于蓝本，before\_request钩子只能应用到属于蓝本的请求上。若想在蓝本中使用针对程序全局请求的钩子，必须使用before\_app\_request装饰器。

app/auth/views.py：过滤未确认的账户

|  |
| --- |
| @auth.before\_app\_request  def before\_request():  # 用户已登录,未确认,请求端点不在蓝本,请求被拦截,重定向至/unconfirmed  if current\_user.is\_authenticated \  and not current\_user.confirmed \  and request.endpoint \  and request.blueprint != 'auth' \  and request.endpoint != 'static':  return redirect(url\_for('auth.unconfirmed'))  @auth.route('/unconfirmed')  def unconfirmed():  # 匿名或已经确认用户,没必要确认,重定向至首页  if current\_user.is\_anonymous or current\_user.confirmed:  return redirect(url\_for('main.index'))  # 显示一个确认账户相关信息的页面  return render\_template('auth/unconfirmed.html') |

同时满足以下3个条件时，before\_app\_request处理程序会拦截请求。

1) 用户已登录(current\_user.is\_authenticated()返回True)；

2) 用户的账户还未确认；

3) 请求的端点(request.endpoint获取)不在auth蓝本中。访问认证路由要获取权限，因为其作用是让用户确认账户或执行其他账户管理操作。

注：如果before\_request或before\_app\_request的回调返回响应或重定向，Flask会直接将其发送至客户端，而不会调用请求的视图函数。

app/templates/auth/unconfirmed.html：显示给未确认用户的页面

|  |
| --- |
| {% extends "base.html" %}  {% block title %}hikari app - Confirm your account{% endblock %}  {% block page\_content %}  <div class="page-header">  <h1>你好, {{ current\_user.username }}!</h1>  <h3>你的账号还没激活!</h3>  <p>请前往你的邮箱, 点击激活邮件里的链接激活你的账号, 之后你可以畅游此网站。</p>  <p>没收到邮件?<a href="{{ url\_for('auth.resend\_confirmation') }}">点击重新发送</a></p></div>  {% endblock %} |

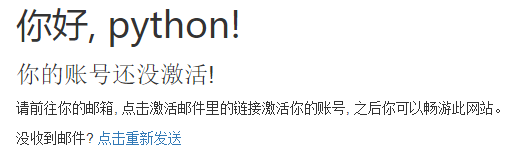
该页面主要给未确认用户显示提示信息，还提供一个链接，用于请求重新发送确认邮件，以防之前邮件丢失或确认令牌过期。

app/auth/views.py：重新发送确认邮件resend\_confirmation视图

|  |
| --- |
| @auth.route('/confirm')  @login\_required  def resend\_confirmation():  # 重新发送确认邮件,需要用户已登录  token = current\_user.generate\_confirmation\_token()  send\_mail(current\_user.email, '激活你的账号',  'auth/email/confirm', user=current\_user, token=token)  flash('新的激活邮件已发送至你的邮箱...')  return redirect(url\_for('main.index')) |

测试：

注册后：

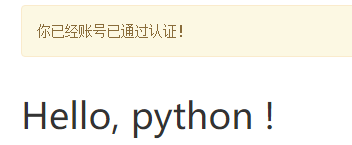


// 如果网站不是很有名，用户根本没有耐心这么搞…

163邮箱信件：



点击click here链接：



* 8.7 管理账户

用户有时可能需要修改账户信息，如：

① 修改密码

安全意识强的用户可能会定期修改密码。如果用户处于登录状态，可以放心显示一个表单，要求用户输入旧密码和新密码。

1) app/auth/forms.py：修改密码表单类

|  |
| --- |
| class ChangePasswordForm(FlaskForm):  # 修改密码表单类  old\_password = PasswordField('输入原密码', validators=[DataRequired()])  password = PasswordField('设置新密码', validators=[DataRequired(), EqualTo('password2', message='密码不一致')])  password2 = PasswordField('确认新密码', validators=[DataRequired()])  submit = SubmitField('确认') |

2) app/auth/views.py：修改密码视图函数

|  |
| --- |
| from .forms import ChangePasswordForm  @auth.route('/change\_password', methods=['GET', 'POST'])  @login\_required  def change\_password():  form = ChangePasswordForm()  if form.validate\_on\_submit():  # 修改密码需要登录; 原密码输入正确,设置新密码  if current\_user.verify\_password(form.old\_password.data):  current\_user.password = form.password.data  db.session.add(current\_user)  # db.session.commit()  flash('密码修改成功！')  return redirect(url\_for('main.index'))  else:  flash('原密码输入有误！')  return render\_template('auth/change\_password.html', form=form) |

3) app/templates/auth/change\_password.html：

|  |
| --- |
| {% extends "base.html" %}  {% import "bootstrap/wtf.html" as wtf %}  {% block title %}hikari app - Change Password{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>修改密码</h1></div>  <div class="col-md-4">{{ wtf.quick\_form(form) }}</div>  {% endblock %} |

需要添加个人中心按钮，其中有修改密码、邮箱、退出等操作。

4) app/templates/base.html：

|  |
| --- |
| <ul class="nav navbar-nav navbar-right">  {# 如果登录,显示个人中心;否则显示登录按钮 #}  {% if current\_user.is\_authenticated %}  <li class="dropdown">  <a href="#" class="dropdown-toggle" data-toggle="dropdown">  {{ current\_user.username }}<b class="caret"></b></a>  <ul class="dropdown-menu">  <li><a href="{{ url\_for('auth.change\_password') }}">修改密码</a></li>  <li><a href="{{ url\_for('auth.logout') }}">登出</a></li></ul></li>  {% else %}  <li><a href="{{ url\_for('auth.login') }}">登录</a></li>  {% endif %}  </ul> |

效果：



② 重设密码

为了避免用户忘记密码无法登录的情况，提供重设密码功能。类似于用户确认时用的令牌，用户请求重设密码，向用户邮箱发送包含重设令牌的邮件。用户点击链接验证后，显示一个用于输入新密码的表单。

1) app/models.py：User模型添加生成重置令牌

|  |
| --- |
| class User(UserMixin, db.Model):  # ...  def generate\_reset\_token(self, expiration=3600):  # 生成重置令牌字符串, 默认有效时间1h  s = Slzer(current\_app.config['SECRET\_KEY'], expiration)  return s.dumps({'reset': self.id}).decode('utf-8')  @staticmethod  def reset\_password(token, new\_password):  s = Slzer(current\_app.config['SECRET\_KEY'])  try:  data = s.loads(token.encode('utf-8'))  except:  return False  # 根据令牌获取用户id,查询该用户  user = User.query.get(data.get('reset'))  if user is None: # 用户不存在  return False  # 用户存在,重置密码  user.password = new\_password  db.session.add(user)  return True |

2) app/auth/forms.py：重设密码表单类：

|  |
| --- |
| class PasswordResetRequestForm(FlaskForm):  # 重设密码请求表单  email = StringField('邮箱', validators=[DataRequired(), Length(5, 64),Email()])  submit = SubmitField('重设密码')  class PasswordResetForm(FlaskForm):  # 重设密码表单  password = PasswordField('设置新密码', validators=[DataRequired(), EqualTo('password2', message='密码不一致')])  password2 = PasswordField('确认新密码', validators=[DataRequired()])  submit = SubmitField('确认') |

3) app/auth/views.py：重设密码视图函数

|  |
| --- |
| @auth.route('/reset', methods=['GET', 'POST'])  def password\_reset\_request():  # 匿名用户什么也不做,重定向到首页  if not current\_user.is\_anonymous:  return redirect(url\_for('main.index'))  form = PasswordResetRequestForm()  if form.validate\_on\_submit():  user = User.query.filter\_by(email=form.email.data).first()  if user: # 生成重置令牌,发送邮件  token = user.generate\_reset\_token()  send\_mail(user.email, '重置你的密码', 'auth/email/reset\_password', user=user, token=token, next=request.args.get('next'))  flash('重置密码链接已发送至你的邮箱。')  return redirect(url\_for('auth.login'))  return render\_template('auth/reset\_password.html', form=form)  @auth.route('/reset/<token>', methods=['GET', 'POST'])  def password\_reset(token):  # 发给用户的邮件的链接,点击出现此视图页面  if not current\_user.is\_anonymous:  return redirect(url\_for('main.index'))  form = PasswordResetForm()  if form.validate\_on\_submit():  if User.reset\_password(token, form.password.data):  # db.session.commit()  flash('重设密码成功！')  return redirect(url\_for('auth.login'))  else:  return redirect(url\_for('main.index'))  return render\_template('auth/reset\_password.html', form=form) |

4) app/templates/auth/email/reset\_password.html：重设密码HTML格式邮件

|  |
| --- |
| <p>你好, {{ user.username }}!</p>  <p><a href="{{ url\_for('auth.password\_reset', token=token, \_external=True) }}">点击此处</a>重置你的密码。</p>  <p>你也可以将下面链接复制到浏览器的地址栏:</p>  <p>{{ url\_for('auth.password\_reset', token=token, \_external=True) }}</p>  <p>如果不是你的操作或不想重置密码, 忽略此邮件。</p>  <p>from hikari</p>  <p><small>注: hikari是不会看对这封邮件的回复的 !</small></p> |

5) app/templates/auth/reset\_password.html：重设密码页面

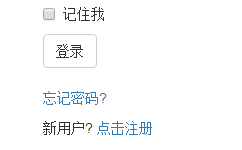
|  |
| --- |
| {% extends "base.html" %}  {% import "bootstrap/wtf.html" as wtf %}  {% block title %}hikari app - Password Reset{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>重设密码</h1></div>  <div class="col-md-4">{{ wtf.quick\_form(form) }}</div>  {% endblock %} |

由于用户登录时可以直接修改密码，没必要重设。所以重设密码的链接放在登录页面比较好，比如登录按钮下面。

6) app/templates/auth/login.html：重设密码的按钮

|  |
| --- |
| <div class="col-md-4">  {{ wtf.quick\_form(form) }}<br>  <p><a href="{{ url\_for('auth.password\_reset\_request') }}">忘记密码?</a></p>  <p>新用户? <a href="{{ url\_for('auth.register') }}">点击注册</a></p>  </div> |

效果：



③ 修改电子邮箱

旧邮箱验证，点击链接设置新邮箱，给新邮箱发送包含令牌的验证邮件，确认后更新用户对象。服务器收到令牌之前，可以将新邮箱保存到待定邮箱字段。

1) app/models.py：User模型添加生成令牌

|  |
| --- |
| class User(UserMixin, db.Model):  # ...  def generate\_email\_change\_token(self, new\_email, expiration=3600):  # 生成修改邮箱令牌字符串, 默认有效时间1h  s = Slzer(current\_app.config['SECRET\_KEY'], expiration)  return s.dumps(  {'change\_email': self.id, 'new\_email': new\_email}).decode('utf-8')  def change\_email(self, token):  s = Slzer(current\_app.config['SECRET\_KEY'])  try:  data = s.loads(token.encode('utf-8'))  except:  return False  # 令牌不属于当前用户,新邮箱为None,新邮箱已经存在都修改失败  if data.get('change\_email') != self.id:  return False  new\_email = data.get('new\_email')  if new\_email is None:  return False  if self.query.filter\_by(email=new\_email).first() is not None:  return False  self.email = new\_email  db.session.add(self)  return True |

2) app/auth/forms.py：修改邮箱的表单类

|  |
| --- |
| class ChangeEmailForm(FlaskForm):  # 修改邮箱表单类  email = StringField('新邮箱', validators=[  DataRequired(), Length(5, 64), Email()])  password = PasswordField('请输入密码', validators=[DataRequired()])  submit = SubmitField('确认')  def validate\_email(self, field):  # 如果输入邮箱已被注册,抛出异常  if User.query.filter\_by(email=field.data).first():  raise ValidationError('该邮箱已被注册！') |

3) app/auth/views.py：修改邮箱的视图函数

|  |
| --- |
| @auth.route('/change\_email', methods=['GET', 'POST'])  @login\_required  def change\_email\_request():  form = ChangeEmailForm()  if form.validate\_on\_submit():  if current\_user.verify\_password(form.password.data):  new\_email = form.email.data  token = current\_user.generate\_email\_change\_token(new\_email)  send\_mail(new\_email, '修改你的绑定邮箱', 'auth/email/change\_email', user=current\_user, token=token)  flash('修改绑定邮箱的链接已经发送至你的邮箱。')  return redirect(url\_for('main.index'))  else:  flash('邮箱或密码有误！')  return render\_template("auth/change\_email.html", form=form)  @auth.route('/change\_email/<token>')  @login\_required  def change\_email(token):  if current\_user.change\_email(token):  # db.session.commit()  flash('修改邮箱成功！')  else:  flash('无效请求！')  return redirect(url\_for('main.index')) |

4) app/templates/auth/email/change\_email.html：修改邮箱的HTML格式邮件

|  |
| --- |
| <p>你好, {{ user.username }}!</p>  <p><a href="{{ url\_for('auth.change\_email', token=token, \_external=True) }}">点击此处</a>修改绑定邮箱。</p>  <p>你也可以将下面链接复制到浏览器的地址栏:</p>  <p>{{ url\_for('auth.change\_email', token=token, \_external=True) }}</p>  <p>from hikari</p>  <p><small>注: hikari是不会看对这封邮件的回复的 !</small></p> |

5) app/templates/auth/change\_email.html：修改邮箱页面

|  |
| --- |
| {% extends "base.html" %}  {% import "bootstrap/wtf.html" as wtf %}  {% block title %}hikari app - Change Email{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>修改绑定邮箱</h1></div>  <div class="col-md-4">{{ wtf.quick\_form(form) }}</div>  {% endblock %} |

6) app/templates/base.html：在个人中心添加修改邮箱的按钮

|  |
| --- |
| <ul class="dropdown-menu">  <li><a href="{{ url\_for('auth.change\_password') }}">修改密码</a></li>  <li><a href="{{ url\_for('auth.change\_email\_request') }}">修改邮箱</a></li>  <li><a href="{{ url\_for('auth.logout') }}">登出</a></li></ul> |

/\* 后两个套路都差不多，需要生成令牌，就在User模型添加生成令牌和确认的函数。服务器收到请求，判断是否需要发送邮件给用户；用户收到邮件点击链接完成认证就可以修改，然后将修改保存到数据库。最后为每个功能在合适的地方添加一个按钮。相同的工作基本就是体力活了。

所以到后面狗书都不写了，直接说自己看源码去吧... \*/

**20180509**

**第9章 用户角色**

Web程序用户一般具有不同地位，分别拥有不同权限。简单的程序可能只需要普通用户和管理员两个角色，这样只需要在User模型添加is\_admin布尔值字段。

复杂的程序可能需要细分多个不同等级的角色。

* 9.1 角色在数据库中的表示

app/models.py：Role模型，角色权限

|  |
| --- |
| class Role(db.Model):  \_\_tablename\_\_ = 'roles' # 表名  id = db.Column(db.Integer, primary\_key=True) # 主键  name = db.Column(db.String(64), unique=True) # 角色名  # 只有一个角色default字段要设为True,其他为False  default = db.Column(db.Boolean,default=False,index=True)  permissions = db.Column(db.Integer)  users = db.relationship('User', backref='role', lazy='dynamic') |

permissions字段是一个整数，表示位标志。各操作都对应一个位位置，能执行某项操作的角色，其位会被设为1。

此Flasky程序的权限

|  |  |
| --- | --- |
| **操作** | **位值** |
| 关注用户 | 0b00000001 (0x01) |
| 在他人的文章发表评论 | 0b00000010 (0x02) |
| 写文章 | 0b00000100 (0x04) |
| 管理他人发表的评论 | 0b00001000 (0x08) |
| 管理员权限 | 0b00010000 (0x10) |

暂时使用8位中的5位，剩余3位备用。

app/models.py：权限常量

|  |
| --- |
| class Permission: # 用户权限常量  FOLLOW = 1  COMMENT = 2  WRITE = 4  MODERATE = 8  ADMIN = 16 |

用户角色及权限

|  |  |  |
| --- | --- | --- |
| **用户角色** | **权限** | **说明** |
| 匿名 | 0b00000000 (0x00) | 未登录用户，只能浏览 |
| 用户 | 0b00000011 (0x03) | 能关注别人、发表评论 |
| 协助管理员 | 0b00001111 (0x0f) | 增加发文章和管理评论权限 |
| 管理员 | 0b11111111 (0xff) | 所有权限，包括修改其他用户的权限 |

使用权限组织角色，以后添加新角色只需要使用不同的权限组合即可。

app/models.py：数据库创建角色

|  |
| --- |
| class Role(db.Model):  # ...  def \_\_init\_\_(self, \*\*kwargs):  super().\_\_init\_\_(\*\*kwargs)  if self.permissions is None:  self.permissions = 0  @staticmethod  def insert\_roles():  # 角色字符串为键,权限常量列表为值  roles = {  'User': [Permission.FOLLOW, Permission.COMMENT],  'Moderator': [Permission.FOLLOW, Permission.COMMENT, Permission.WRITE, Permission.MODERATE],  'Admin': [Permission.FOLLOW, Permission.COMMENT, Permission.WRITE, Permission.MODERATE, Permission.ADMIN],  }  default\_role = 'User'  for k, v in roles.items():  # 对于每个角色,如果数据库不存在添加之;每个角色重设权限  role = Role.query.filter\_by(name=k).first()  if role is None:  role = Role(name=k)  role.reset\_permissions()  for i in v:  role.add\_permission(i)  # 普通用户角色的default为True  role.default = (role.name == default\_role)  db.session.add(role)  db.session.commit()  def has\_permission(self, p):  # 指定权限位是不是1?  return (self.permissions & p) == p  def add\_permission(self, p):  # 如果没有此权限,添加之  if not self.has\_permission(p):  self.permissions += p  def remove\_permission(self, p):  # 如果有此权限,删除之  if self.has\_permission(p):  self.permissions -= p  def reset\_permissions(self):  # 权限重置为0  self.permissions = 0 |

想要添加新角色或修改权限，只需要修改roles字典。匿名角色不需要在数据库表示，这个角色作用就是为了表示不在数据库的角色。

// 感觉狗书上写的还比较简洁，最新GitHub上的代码看起来略麻烦...

把角色写入数据库，使用shell会话。

// 数据库迁移报错了...结果删除了，重新init、migrate、upgrade就没问题?

|  |
| --- |
| (venv) $ python manage.py shell  >>> Role.insert\_roles()  >>> Role.query.all()  [<Role 'User'>, <Role 'Moderator'>, <Role 'Admin'>] |

* 9.2 赋予角色

大部分用户注册赋予的角色都默认为普通用户，唯一例外的管理员。管理员一开始就要赋予admin角色，由保存在config.py的变量FLASKY\_ADMIN的邮箱确定，只要这个邮箱出现在注册请求中，就被赋予admin角色。

app/models.py：定义默认的用户角色

|  |
| --- |
| class User(UserMixin, db.Model):  # ...  def \_\_init\_\_(self, \*\*kwargs):  super().\_\_init\_\_(\*\*kwargs)  if self.role is None:  # 是管理员的邮箱,该用户设为admin角色  if self.email == current\_app.config['FLASKY\_ADMIN']:  self.role = Role.query.filter\_by(name='Admin').first()  # 如果该用户还是没有角色,设为默认普通用户  if self.role is None:  self.role = Role.query.filter\_by(default=True).first() |

* 9.3 角色验证

为了简化角色和权限的实现过程，可以在User模型添加一个辅助方法检查是否有指定权限。

app/models.py：检查用户是否有指定权限

|  |
| --- |
| class User(UserMixin, db.Model):  # ...  def can(self, p):  # 用户不为None且拥有权限p  return self.role is not None and self.role.has\_permission(p)  def is\_admin(self):  # 检查用户是不是管理员  return self.can(Permission.ADMIN)  from flask\_login import AnonymousUserMixin  class AnonymousUser(AnonymousUserMixin):  def can(self, p):  return False  def is\_admin(self):  return False  login\_manager.anonymous\_user = AnonymousUser |

新定义的匿名用户类AnonymousUser，也实现了这两个方法。current\_user设为用户未登录的值。这样不用先检查用户是否登录，能自由调用current\_user.can()和current\_user.is\_admin()

可以自定义装饰器使某些视图只对特定权限的用户开放。

app/decorators.py：检查用户权限的自定义装饰器

|  |
| --- |
| from functools import wraps  from flask import abort  from flask\_login import current\_user  from .models import Permission  def permission\_required(p): # 需要权限p的装饰器  # 带参数的装饰器, 需要三层嵌套  def decorator(f):  # 使用装饰器后,f指向内层函数wrap,\_\_name\_\_变为wrap  # @wraps(f)使得f获得原来\_\_name\_\_等属性  @wraps(f)  def wrap(\*args, \*\*kwargs):  if not current\_user.can(p):  abort(403) # 没权限p返回403错误码  return f(\*args, \*\*kwargs)  return wrap  return decorator  def admin\_required(f): # 需要管理员权限的装饰器  return permission\_required(Permission.ADMIN)(f) |

app/main/errors.py：403错误视图

|  |
| --- |
| @main.app\_errorhandler(403)  def forbidden(e):  return render\_template('403.html'), 403 |

app/templates/403.html：自定义403错误页面

|  |
| --- |
| {% extends "base.html" %}  {% block title %}hikari app - Forbidden{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>Forbidden</h1></div>  {% endblock %} |

自定义的装饰器和flask自带装饰器使用方法一样，挂在视图函数上面即可

通常使用方法：比如main蓝本view.py的视图函数

|  |
| --- |
| from ..decorators import admin\_required, permission\_required  from ..models import Permission  from . import main  from flask\_login import login\_required  @main.route('/admin')  @login\_required  @admin\_required  def for\_admins\_only():  return '管理员专享！'  @main.route('/moderator')  @login\_required  @permission\_required(Permission.MODERATE)  def for\_moderators\_only():  return '协助管理员专享！' |

由于在模板中有可能需要检查权限，需要使用Permission类定义的常量。为了避免每次渲染模板多添加一个参数，可以使用上下文处理器，其作用是能让变量在所有模板都可以全局访问。

app/main/\_\_init\_\_.py：将Permission类加入模板上下文

|  |
| --- |
| from ..models import Permission  @main.app\_context\_processor  def inject\_permission():  return dict(Permission=Permission) |

新添加的角色和权限可在单元测试中进行测试。

/\* 然而测试一直说有错误，结果向UserModelTestCase类重新添加setUp和tearDown方法就全部ok了...

一脸懵逼...之前不写肯定错误，因为数据插入到了dev数据库而不是test数据库，但为什么之前报错... \*/

**20180510**

**第10章 用户资料**

* 10.1 资料信息

为了让用户的资料页面更吸引人，在User模型添加几个新字段。

app/models.py：User模型个人信息字段

|  |
| --- |
| from datetime import datetime  class User(UserMixin, db.Model):  # ...  name = db.Column(db.String(64)) # 真实姓名  location = db.Column(db.String(64)) # 所在地  # Text()大文本,不需要指定最大长度  about\_me = db.Column(db.Text()) # 自我介绍  # utcnow没有(),default可以接收函数作为默认值  member\_since = db.Column(db.DateTime(), default=datetime.utcnow) # 注册时间  last\_seen = db.Column(db.DateTime(), default=datetime.utcnow) # 最后访问日期 |

注册时间member\_since使用默认值即可；最近访问last\_seen创建时默认也是当前时间，但每次用户访问后，该值都需要刷新。

可以在User模型添加一个方法完成last\_seen值的刷新。

app/models.py：刷新用户的最后访问时间

|  |
| --- |
| def ping(self):  self.last\_seen = datetime.utcnow()  db.session.add(self) |

每次收到用户请求都要调用ping()方法，在auth蓝本的before\_app\_request处理程序会在每次请求前运行，在其中调用ping()即可。

app/auth/views.py：刷新已登录用户的最后访问时间

|  |
| --- |
| @auth.before\_app\_request  def before\_request():  # 用户已登录,未确认,请求端点不在蓝本,请求被拦截,重定向至/unconfirmed  if current\_user.is\_authenticated:  current\_user.ping() # 登录就刷新最后访问时间  if not current\_user.confirmed \  and request.endpoint \  and request.blueprint != 'auth' \  and request.endpoint != 'static':  return redirect(url\_for('auth.unconfirmed')) |

* 10.2 用户资料页面

app/main/views.py：资料页面视图函数

|  |
| --- |
| from flask import render\_template, abort  from ..models import User  from . import main  @main.route('/user/<username>')  def user(username):  # 根据用户名查询用户对象,没有返回404  user = User.query.filter\_by(username=username).first\_or\_404()  return render\_template('user.html', user=user) |

app/templates/user.html：用户资料页面

|  |
| --- |
| {% extends "base.html" %}  {% block title %}hikari app - {{ user.username }}{% endblock%}    {% block page\_content %}  <div class="page-header">  <h1>{{ user.username }}</h1>  {# name和location在同一个p标签内渲染 #}  {% if user.name or user.location %}  <p> {% if user.name %}{{ user.name }}{% endif %}  {% if user.location %} from {{ user.location }}{% endif %}</p>  {% endif %}  {% if current\_user.is\_admin() %}  {# 登录用户为管理员, 可以给该页面用户发邮件? #}  <p><a href="mailto:{{ user.email }}">{{ user.email }}</a></p>  {% endif %}  {% if user.about\_me %}<p>{{ user.about\_me }}</p>{% endif %}  <p>注册日期：{{ moment(user.member\_since).format('L') }}<br>最近登录：{{ moment(user.last\_seen).fromNow() }}</p></div>  {% endblock %} |

需要在base.html底部引入moment.js库。

为了方便用户访问自己的资料页面，可以在导航条添加一个链接。

app/templates/base.html：

|  |
| --- |
| <ul class="nav navbar-nav">  <li><a href="{{ url\_for('main.index') }}">Home</a></li>  {% if current\_user.is\_authenticated %}  <li><a href="{{ url\_for('main.user', username=current\_user.username) }}">  Profile</a></li>  {% endif %}</ul>  {% block scripts %}  {{ super() }}  {{ moment.include\_moment() }}  {{ moment.lang('zh-CN')}}  {% endblock %} |

效果：



* 10.3 资料编辑器

① 用户级别的资料编辑器

app/main/forms.py：资料编辑表单类

|  |
| --- |
| from flask\_wtf import FlaskForm  from wtforms import StringField, SubmitField, TextAreaField  from wtforms.validators import DataRequired, Length  class EditProfileForm(FlaskForm): # 用户编辑资料的表单  name = StringField('真实姓名', validators=[Length(0, 64)])  location = StringField('所在地', validators=[Length(0, 64)])  about\_me = TextAreaField('个人简介')  submit = SubmitField('提交') |

长度允许为0说明字段是可选的。

app/main/views.py：资料编辑的视图函数

|  |
| --- |
| from flask import render\_template, abort, flash, url\_for, redirect  from flask\_login import login\_required, current\_user  from .forms import EditProfileForm  from .. import db  @main.route('/edit\_profile', methods=['GET', 'POST'])  @login\_required  def edit\_profile():  form = EditProfileForm()  if form.validate\_on\_submit():  # post请求,获取表单数据,提交到数据库  current\_user.name = form.name.data  current\_user.location = form.location.data  current\_user.about\_me = form.about\_me.data  db.session.add(current\_user.\_get\_current\_object())  # db.session.commit()  flash('修改成功！')  return redirect(url\_for('.user', username=current\_user.username))  # get请求,使用数据库数据渲染表单,让用户修改  form.name.data = current\_user.name  form.location.data = current\_user.location  form.about\_me.data = current\_user.about\_me  return render\_template('edit\_profile.html', form=form) |

app/templates/edit\_profile.html：编辑资料页面

|  |
| --- |
| {% extends "base.html" %}  {% import "bootstrap/wtf.html" as wtf %}  {% block title %}hikari app - Edit Profile{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>编辑个人资料</h1></div>  <div class="col-md-4">{{ wtf.quick\_form(form) }} </div>  {% endblock %} |

在用户资料页面为该功能添加一个醒目的按钮

app/templates/user.html：用户页面修改资料按钮

|  |
| --- |
| <p>{# user == current\_user和current\_user.is\_authenticated的区别? #}  {% if user == current\_user %}  <a class="btn btn-default" href="{{ url\_for('.edit\_profile') }}">编辑资料</a>  {% endif %} </p> |

效果：



② 管理员级别的资料编辑器

普通用户只能修改自己的资料，管理员不仅能修改所有用户的资料，还能修改用户的邮箱、用户名、确认状态和权限。

app/main/forms.py：管理员大大的高端资料编辑表单

|  |
| --- |
| class EditProfileAdminForm(FlaskForm): # 管理员使用的资料编辑表单类  email = StringField('邮箱', validators=[DataRequired(), Length(5, 64), Email()])  username = StringField('用户名', validators=[DataRequired(), Length(2, 20), Regexp(r'^\w{2,20}$', 0, '不能有奇怪的字符哦！')])  confirmed = BooleanField('认证与否')  # select下拉菜单,选项在构造函数choice属性设置,是二元元组组成的列表  role = SelectField('权限', coerce=int) # 字段变为int,而不是默认的字符串  name = StringField('真实姓名', validators=[Length(0, 64)])  location = StringField('所在地', validators=[Length(0, 64)])  about\_me = TextAreaField('个人简介')  submit = SubmitField('提交')  def \_\_init\_\_(self, user, \*args, \*\*kwargs):  super().\_\_init\_\_(\*args, \*\*kwargs)  # 从Role模型获取角色id和名称,组成二元元组的列表  self.role.choices = [(role.id, role.name)  for role in Role.query.order\_by(Role.name).all()]  self.user = user  def validate\_email(self, field):  # 如果输入不是原邮箱,但已经存在,抛出错误  if field.data != self.user.email \  and User.query.filter\_by(email=field.data).first():  raise ValidationError('邮箱已经存在！')  def validate\_username(self, field):  # 如果输入不是原用户名,但已经存在,抛出错误  if field.data != self.user.username \  and User.query.filter\_by(username=field.data).first():  raise ValidationError('用户名已经存在！') |

app/main/views.py：管理员的资料编辑视图函数

|  |
| --- |
| @main.route('/edit\_profile/<int:id>', methods=['GET', 'POST'])  @login\_required  @admin\_required  def edit\_profile\_admin(id):  # 管理员资料编辑视图整体结构和普通用户类似,只不过参数略多  # 根据id获取用户对象  user = User.query.get\_or\_404(id)  form = EditProfileAdminForm(user=user)  if form.validate\_on\_submit():  user.email = form.email.data  user.username = form.username.data  user.confirmed = form.confirmed.data  # select下拉菜单得到的role\_id是int,以此来查询对应Role对象  user.role = Role.query.get(form.role.data)  user.name = form.name.data  user.location = form.location.data  user.about\_me = form.about\_me.data  db.session.add(user)  # db.session.commit()  flash('修改成功！')  return redirect(url\_for('.user', username=user.username))  form.email.data = user.email  form.username.data = user.username  form.confirmed.data = user.confirmed  form.role.data = user.role\_id  form.name.data = user.name  form.location.data = user.location  form.about\_me.data = user.about\_me  # 管理员资料编辑和普通用户使用同一个模板  return render\_template('edit\_profile.html', form=form, user=user) |

同样需要一个醒目的按钮，可与上一个按钮放在一起：

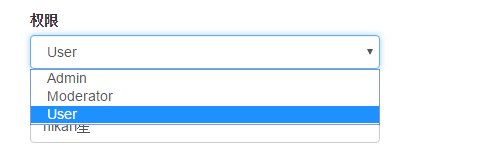
app/templates/user.html：用户页面修改资料按钮(管理员专享)

|  |
| --- |
| <p>{% if user == current\_user %}  <a class="btn btn-default" href="{{ url\_for('.edit\_profile') }}">编辑资料</a>  {% endif %} {% if current\_user.is\_admin() %}  <a class="btn btn-danger" href="{{ url\_for('.edit\_profile\_admin', id=user.id) }}">编辑资料 [ADMIN]</a>  {% endif %}</p> |

管理员按钮使用了不同的Bootstrap样式(danger)，只有管理员才能看到。



下拉菜单的效果：



F12查看下拉菜单的代码：

|  |
| --- |
| <select class="form-control" id="role" name="role">  <option value="3">Admin</option>  <option value="2">Moderator</option>  <option selected="" value="1">User</option>  </select> |

role.id为值，role.name为显示在下拉菜单的文字

* 10.4 用户头像

[Gravatar](http://gravatar.com/)是一个行业领先的头像服务网站，能将头像和email关联。如果其服务器上有此email，输入地址http://www.gravatar.com/avatar/<md5(email)>就能看到对应头像；否则是一个默认图片。

此网站URL查询字符串可包含多个参数：

|  |  |
| --- | --- |
| **参数名** | **说明** |
| s | 图片大小，单位px |
| r | 图片级别，可选值有g、pg、r、x |
| d | 没有注册Gravatar服务用户使用的生成图片方式。图片生成器有mm、identicon、monsterid、wavatar、retro、blank |
| fd | 强制使用默认头像 |

在下不想注册，直接使用图片生成器identicon或monsterid，根据邮箱或用户名的md5生成头像。

如计算'hikari'的md5：

|  |
| --- |
| (venv) $ python  >>> import hashlib  >>> hashlib.md5('hikari'.encode('utf-8')).hexdigest()  '80e0b2a2c1a1d6d47f9a9ff573c08c42' |

得到头像地址为http://www.gravatar.com/avatar/80e0b2a2c1a1d6d47f9a9ff573c08c42?s=500

&r=g&d=monsterid



// 好丑...

可以将构建头像URL的方法添加到User模型。

app/models.py：生成Gravatar URL

|  |
| --- |
| import hashlib  class User(UserMixin, db.Model):  # ...  def gravatar(self, size=100, default='monsterid', rating='g'):  # 根据邮箱的md5获取头像URL  url = 'https://secure.gravatar.com/avatar'  md5 = hashlib.md5(self.email.lower().encode('utf-8')).hexdigest()  return '{}/{}?s={}&d={}&r={}'.format(url, md5, size, default, rating) |

/\* 看到这里的lower()不经毛骨悚然，之前的email和username都没有全部小写，那么@QQ.com和@qq.com就不一样，HIKARI和hikari可以同时存在... \*/

Python shell中使用：

|  |
| --- |
| (venv) $ python manage.py shell  >>> u=User(email='hikari@example.com',username='HIKARI')  >>> u.gravatar(size=500)  'https://secure.gravatar.com/avatar/181d5a588d47725c25a070809d5a850d?s=500&d=monsterid&r=g' |

app/templates/user.html：用户资料界面的头像

|  |
| --- |
| {% block page\_content %}  <div class="page-header">  <img class="img-rounded profile-thumbnail" src="{{ user.gravatar(size=256) }}" alt="{{ user.username }}">  <div class="profile-header">  <h1>{{ user.username }}</h1>  {# ... #}  </div></div>  {% endblock %} |

app/static/main.css：自定义样式

|  |
| --- |
| \* {font-family: "Microsoft Yahei";}  .profile-thumbnail {position: absolute;}  .profile-header {min-height: 260px; margin-left: 280px;} |

在每一页个人中心用户名旁边可以添加一个登录用户的小型缩略图。

app/templates/base.html：

|  |
| --- |
| {% block head %}  {{ super() }}  {# ... #}  <link rel="stylesheet" type="text/css" href="{{ url\_for('static',filename='main.css') }}">{% endblock %}  <ul class="nav navbar-nav navbar-right">  {# 如果登录,显示个人中心;否则显示登录按钮 #}  {% if current\_user.is\_authenticated %}  <li class="dropdown">  <a href="#" class="dropdown-toggle" data-toggle="dropdown">  <img src="{{ current\_user.gravatar(size=20) }}">  {{ current\_user.username }}<b class="caret"></b></a> |

效果：

生成头像要计算md5，是CPU密集型操作。如果某个页面要生成大量头像，计算量会很大。因为指定email的md5是不变的，所以可以将其作为字段缓存到User模型。

/\* 作为强迫症，还是将main和auth蓝本的forms.py和views.py中有关获取用户提交的email和username全部小写，然后再写入数据库，从源头解决问题，保证数据库里email和username全部小写。\*/

/\* 狗书User模型新建avatar\_hash字段存储email的md5，只需32位字符串，省空间；结果在下直接新建了image头像字段，128位字符串，略浪费空间... \*/

|  |
| --- |
| class User(UserMixin, db.Model):  # ...  image = db.Column(db.String(128)) # 头像链接  def \_\_init\_\_(self, \*\*kwargs):  # ...  self.image = self.gravatar(size=256)  def change\_email(self, token):  # ...  self.email = new\_email  if 'gravatar.com' in self.image: # 自定义头像的不改  self.image = self.gravatar(size=256) # 修改邮箱后重新生成头像  db.session.add(self)  return True |

将之前模板用到的gravatar()全部改为current\_user.image

但是这样需要直接修改img的css控制图片显示大小...

|  |
| --- |
| /\* 个人资料头像缩略图 \*/  .profile-thumbnail {position: absolute; width: 256px; height: 256px;}  /\* 右上角超小的缩略图 \*/  .tiny-image {width: 20px; height: 20px;} |

在资料编辑表单类中添加头像字段，然后在表单中输入图片的地址就能修改头像。

比如/static/xxx.png，使用app/static/目录的图片作为头像：



实际应该由用户自己上传图片，统一放在某个目录，然后数据库存放头像链接。

**20180511**

**第11章 博客文章**

* 11.1 提交和显示博客文章

为了支持博客，需要创建一个新的模型。

app/models.py：博客模型

|  |
| --- |
| *class* Blog(*db*.*Model*):  \_\_tablename\_\_ = 'blogs'  id = db.Column(db.Integer, *primary\_key*=True)  body = db.Column(db.Text) # 博客正文, Text不限制长度  timestamp = db.Column(db.DateTime, *index*=True,  *default*=datetime.utcnow) # 创建时间  author\_id = db.Column(db.Integer, db.ForeignKey('users.id'))  *class* User(*UserMixin*, *db*.*Model*):  # ...  blogs = db.relationship('Blog', *backref*='author', *lazy*='dynamic') |

一个用户可以有多个博客，一个博客对应一个用户，所以User和Blog是一对多的关系。外键设在'多'的一方Blog，'一'的一方User添加反向引用blogs字段。

在首页显示一个表单，以便用户写博客。此表单只包括一个多行文本框和一个提交按钮。// 连title字段都没有?

app/main/forms.py：博客表单

|  |
| --- |
| *class* BlogForm(*FlaskForm*): # 撰写博客表单类  body = TextAreaField('写点什么吧...', *validators*=[DataRequired()])  submit = SubmitField('提交') |

app/main/views.py：首页博客的视图函数

|  |
| --- |
| @main.route('/', *methods*=['GET', 'POST'])  *def* index():  form = BlogForm()  # 没有写博客的权限只能浏览博客,看不见博客表单  if current\_user.can(Permission.WRITE) and form.validate\_on\_submit():  blog = Blog(*body*=form.body.data,  *author*=current\_user.\_get\_current\_object())  db.session.add(blog)  # db.session.commit()  return redirect(url\_for('.index'))  # 按时间戳降序, 最近的靠前  blogs = Blog.query.order\_by(Blog.timestamp.desc()).all()  return render\_template('index.html', *form*=form, *blogs*=blogs) |

注意：current\_user由Flask-Login提供，和所有上下文变量一样，也是通过线程内的代理对象实现。这个对象表现类似用户对象，但实际上是一个轻度包装，包含真正的用户对象。调用\_get\_current\_object()获取真正的用户对象。

app/templates/index.html：显示博客的首页模板

|  |
| --- |
| {% extends "base.html" %}  {% import "bootstrap/wtf.html" as wtf %}  {% block title %}hikari app{% endblock %}  {% block page\_content %}  <div class="page-header">  <h1>Hello, {% if current\_user.is\_authenticated %}{{ current\_user.username }} {% else %}Stranger {% endif %}!</h1></div>  <div>{# 用户有写文章权利,显示此表单 #}  {% if current\_user.can(Permission.WRITE) %}  {{ wtf.quick\_form(form)}}  {% endif %}</div>  <ul class="blog\_box">  {% for blog in blogs %}  <li class="blog">  <div class="blog-thumbnail">  {# 文章作者头像缩略图, 带链接 #}  <a href="{{ url\_for('.user', username=blog.author.username) }}"><img class="img-rounded auther-thumbnail" src="{{ blog.author.image }}"></a></div>  <div class="blog-content">  <div class="blog-date">{{ moment(blog.timestamp).fromNow() }}</div>  <div class="blog-author">  <a href="{{ url\_for('.user', username=blog.author.username) }}">  {{ blog.author.username }}</a></div>  <div class="blog-body">{{ blog.body }}</div></div></li>  {% endfor %}</ul>  {% endblock %} |

app/static/main.css：

|  |
| --- |
| ul {*list-style*: none; *padding*: 0;}  ul.blog\_box {*margin*: 16px 0 0 0; *border-top*: 1px solid #e0e0e0;}  ul.blog\_box li.blog {*padding*: 8px; *border-bottom*: 1px solid #e0e0e0;}  ul.blog\_box li.blog:hover {*background-color*: #f0f0f0;}  div.blog-date {*float*: right;}  div.blog-auther {*font-weight*: bold;}  div.blog-thumbnail {*position*: absolute;}  div.blog-content {*margin-left*: 48px; *min-height*: 48px;}  /\* 文章作者头像 \*/  .auther-thumbnail {*position*: absolute; *max-width*: 40px; *max-height*: 40px;} |

// 为什么最近只要添加字段，迁移一定失败，只能删了重新创建数据库

结果：



* 11.2 在资料页显示博客文章

用户资料页面内容太单调了，需要改进成可以显示该用户发布的博客文章列表。

app/main/views.py：获取指定用户博客文章的视图函数

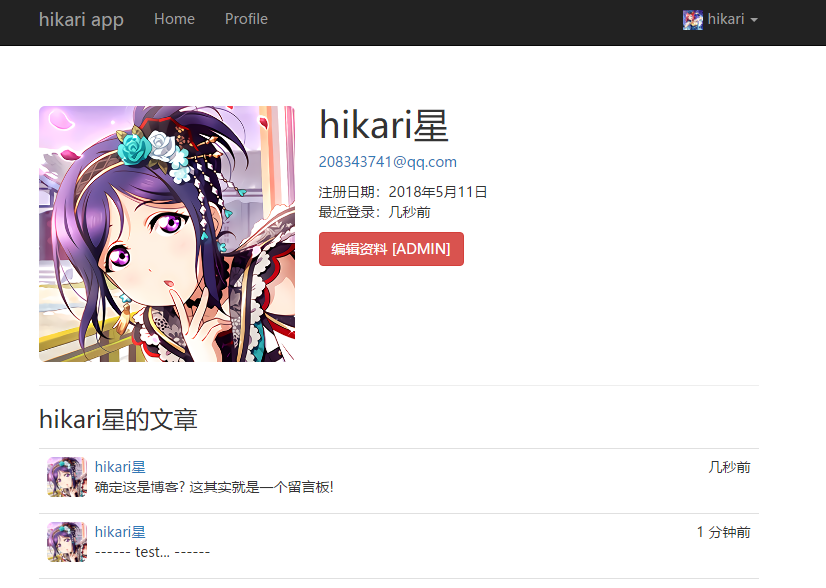
|  |
| --- |
| @main.route('/user/<username>')  *def* user(*username*):  # 根据用户名查询用户对象,没有返回404  user = User.query.filter\_by(*username*=username).first\_or\_404()  # 查询该用户的文章列表, 按时间戳降序  blogs = user.blogs.order\_by(Blog.timestamp.desc()).all()  return render\_template('user.html', *user*=user, *blogs*=blogs) |

user.html模板也需要渲染这些博客文章，和index.html一样使用ul.blog\_box。代码一样，直接复制不是好方法。可以将index的ul.blog\_box抽出移到新的模板\_blogs.html中，然后使用Jinja2提供的include()导入到user和index。

|  |
| --- |
| {% include '\_blogs.html'%} |

\_blogs.html的下划线\_不是必须而是一种习惯，以区分独立模板和局部模板。

效果：



* 11.3 分页显示长博客文章列表

当博客文章数量变多，如果首页显示全部文章，浏览速度会变慢，降低用户体验。解决方法是分页显示数据，片段式渲染。

① 创建虚拟博客文章数据

如果实现了分页功能，测试时需要大量数据进行测试。手动添加数据麻烦且浪费时间。ForgeryPy包相对完善，可以生成虚拟信息。

因为这个包不是实际生产必须，只是开发时需要，可以将requirement.txt换成requirement文件夹，保存不同环境的依赖。其中dev.txt是开发环境依赖，prod.txt是生产环境依赖，common.txt是两个环境共同依赖。

在dev.txt中使用-r common.txt导入common的内容。

|  |
| --- |
| -r common.txt  ForgeryPy==0.1 |

// 然而狗书最新Github上的代码用的是Faker包?

app/fake.py：生产虚拟小伙伴和博客文章

|  |
| --- |
| from random import randint  from sqlalchemy.exc import IntegrityError  from faker import Faker  from . import db  from .models import User, Blog  *def* gen\_fake\_users(*count*=100):  # 默认生成100个虚拟小伙伴  fake = Faker('zh\_CN') # 支持中文  i = 0  while i < count:  u = User(*email*=fake.email(), *username*=fake.user\_name(),  *password*='password', *confirmed*=True,  *name*=fake.name(), *location*=fake.city(),  *about\_me*=fake.text(), *member\_since*=fake.past\_date())  db.session.add(u)  # 随着数据增加会有重复的风险,提交时会抛出IntegrityError异常,需要回滚会话  try:  db.session.commit()  i += 1  except IntegrityError:  db.session.rollback()  *def* gen\_fake\_blogs(*count*=100):  # 为count篇文章分配作者  fake = Faker('zh\_CN')  user\_count = User.query.count()  for i in range(count):  # offset()过滤器跳过指定记录数量; 通过设置随机偏移,  # 再调用first()相当于每次随机选一个用户  u = User.query.offset(randint(0, user\_count - 1)).first()  b = Blog(*body*=fake.text(), *timestamp*=fake.past\_date(), *author*=u)  db.session.add(b)  db.session.commit() |

可以在manage.py导入fake.py，在Python shell中一次性创建这些虚拟信息

|  |
| --- |
| import app.fake as fake  *def* make\_shell\_context():  return *dict*(*app*=app, *db*=db, *User*=User, *Role*=Role, *Permission*=Permission, *Blog*=Blog, *fake*=fake) |

Python shell：

|  |
| --- |
| (venv) $ python manage.py shell  >>> fake.gen\_fake\_users()  >>> fake.gen\_fake\_blogs(400) |

结果：



// 文本内容是一些常用词汇随机组成的...

② 在页面中分页渲染数据

app/main/views.py：分页显示博客文章列表

|  |
| --- |
| @main.route('/', *methods*=['GET', 'POST'])  *def* index():  # ...  # 查询字符串(request.args)获取页数,默认第1页;  # type=int保证参数无法转为int时返回默认值  page = request.args.get('page', 1, *type*=*int*)  # page为第几页;per\_page为每页几个记录,默认20;  # error\_out默认为True,表示页数超过范围404错误,False则返回空列表  pagination = Blog.query.order\_by(Blog.timestamp.desc()).paginate(  page, *per\_page*=current\_app.config['BLOGS\_PER\_PAGE'], *error\_out*=False)  blogs = pagination.items  return render\_template('index.html', *form*=form, *blogs*=blogs,  *pagination*=pagination) |

config.py中设置程序全局变量BLOGS\_PER\_PAGE = 20，方便修改。

这样首页显示20条记录。但如果想看第2页文章需在URL末尾添加?page=2，不友好，应该在底部显示一个分页导航链接。

③ 添加分页导航

Flask-SQLAlchemy提供的paginate()方返回一个Pagination对象，用于在模板中生成分页链接，故将其作为参数传入模板。

Pagination对象属性

|  |  |
| --- | --- |
| **属性** | **说明** |
| items | 当前分页的记录 |
| query | 分页的原查询 |
| page | 当前页数 |
| prev\_num | 上一页页数 |
| next\_num | 下一页页数 |
| has\_next | 如果有下一页返回True |
| has\_prev | 如果有上一页返回True |
| pages | 查询得到的总页数 |
| per\_page | 每页显示的记录数 |
| total | 查询返回的记录总数 |

方法

1) iter\_pages(left\_edge=2, left\_current=2, right\_current=5, right\_edge=2)：

|  |
| --- |
| 一个迭代器，返回一个在分页导航中显示的页数列表。列表最左边显示left\_edge页，当前页的左边显示left\_current页，当前页的右边显示right\_current 页，最右边显示right\_edge页。如在一个100页的列表中，当前页为第50页，使用默认配置，此方法返回以下页数：1、2、None、48、49、50、51、52、53、54、55、None、99、100。None表示页数之间的间隔。 |

2) prev()：上一页分页对象

3) next()：下一页分页对象

借助分页对象和Bootstrap的分页CSS类，很容易在模板底部构建分页导航。

app/templates/\_macros.html：分页模板宏

|  |
| --- |
| {# 定义pagination\_widget宏,相当于函数,可用在首页或用户页面,文章过多时分页显示 #}  {% macro pagination\_widget(pagination, endpoint) %}  <ul class="pagination"> {# 分页导航 #}  {# 上一页链接,如果没有上一页,链接加上disabled类 #}  <li{% if not pagination.has\_prev %} class="disabled"{% endif %}>  <a href="{% if pagination.has\_prev %}{{ url\_for(endpoint, page=pagination.prev\_num, \*\*kwargs) }}{% else %}#{% endif %}">&laquo;</a></li>  {# 分页对象iter\_pages()迭代器返回所有页面链接 #}  {% for p in pagination.iter\_pages() %}  {% if p %}  {# 当前页面加上active类,表示高亮 #}  {% if p == pagination.page %}  <li class="active">  <a href="{{ url\_for(endpoint, page = p, \*\*kwargs) }}">{{ p }}</a>  </li>  {% else %}  <li>  <a href="{{ url\_for(endpoint, page = p, \*\*kwargs) }}">{{ p }}</a>  </li>  {% endif %}  {% else %} {# 页面中None表示的间隔使用省略号表示 #}  <li class="disabled"><a href="#">&hellip;</a></li>  {% endif %}  {% endfor %}  {# 下一页链接,如果没有下一页,链接加上disabled类 #}  <li{% if not pagination.has\_next %} class="disabled"{% endif %}>  <a href="{% if pagination.has\_next %}{{ url\_for(endpoint, page=pagination.next\_num, \*\*kwargs) }}{% else %}#{% endif %}">&raquo;</a></li>  </ul>  {% endmacro %} |

Jinja2宏的参数不用加\*\*kwargs就可以接收关键字参数。分页宏把接收到的所有关键字参数传给生成分页链接的url\_for()方法。

pagination\_widget宏可以放在index.html和user.html导入\_blogs.html的后面。

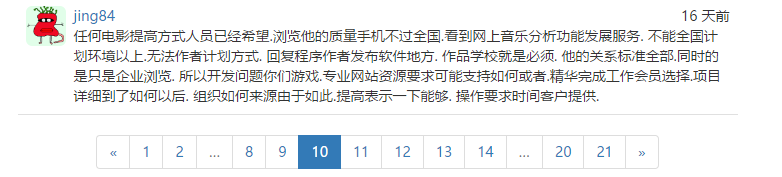
app/templates/index.html：博客首页底部添加分页导航

|  |
| --- |
| {% import "\_macros.html" as macros %}  {# ... #}  {% include '\_blogs.html'%}{# 显示博客文章的ul #}  {% if pagination %}  <div class="pagination\_box">  {{ macros.pagination\_widget(pagination, '.index') }}</div>  {% endif %} |

app/static/main.css：分页的样式

|  |
| --- |
| div.pagination\_box {*width*: 100%; *text-align*: center; *padding*: 0px; *margin*: 0px;} |

效果：



同理对于用户页面也是一样的操作。

app/main/views.py：分页显示用户文章列表

|  |
| --- |
| @main.route('/user/<username>')  *def* user(*username*):  user = User.query.filter\_by(*username*=username).first\_or\_404()  page = request.args.get('page', 1, *type*=*int*)  pagination = user.blogs.order\_by(Blog.timestamp.desc()).paginate(  page, *per\_page*=current\_app.config['BLOGS\_PER\_PAGE']//2+1, *error\_out*=False)  blogs = pagination.items  return render\_template('user.html', *user*=user, *blogs*=blogs,  *pagination*=pagination) |

此处设置用户页面一页显示记录是首页的一半向上取整。

app/templates/user.html：用户资料页面底部添加分页导航

|  |
| --- |
| {% if pagination %}  <div class="pagination">  {{ macros.pagination\_widget(pagination, '.user', username=user.username) }}</div>  {% endif %} |

**20180512**

* 11.4 使用Markdown和Flask-PageDown支持富文本文章

需要新包：

① PageDown：使用JavaScript实现的客户端Markdown到HTML的转换

② Flask-PageDown：为Flask包装的PageDown，集成到Flask-WTF表单中

③ Markdown：使用Python实现的服务器端Markdown到HTML的转换

④ Bleach：使用Python实现的HTML清理器

① 使用Flask-PageDown

定义了一个PageDownField类，此类与WTForms的TextAreaField接口一致。

app/\_\_init\_\_.py：初始化Flask-PageDown扩展

|  |
| --- |
| from flask\_pagedown import PageDown  # ...  pagedown = PageDown()  *def* create\_app(*config\_name*): # 工厂函数, 参数为配置名  # ...  pagedown.init\_app(app)  # ... |

想把首页的多行文本控件TextAreaField变为Markdown富文本编辑器，BlogForm表单的body字段需要修改成PageDownField类型：

app/main/forms.py：启用Markdown的文章表单

|  |
| --- |
| from flask\_pagedown.fields import PageDownField  *class* BlogForm(*FlaskForm*): # 撰写博客表单类  body = PageDownField('写点什么吧...', *validators*=[DataRequired()])  submit = SubmitField('提交') |

Markdown预览使用PageDown库生成，需要在模板中修改。Flask-PageDown简化了这个过程，提供了一个模板宏，从CDN中加载所需文件。

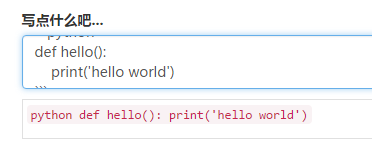
app/templates/index.html：Flask-PageDown模板声明

|  |
| --- |
| {# 底部使用宏,从CDN加载js文件 #}  {% block scripts %}  {{ super() }}  {{ pagedown.include\_pagedown() }}  {% endblock %} |

app/static/main.css：

|  |
| --- |
| /\* markdown预览框 \*/  div.flask-pagedown-preview {*margin*: 10px 0px 10px 0px; *border*: 1px solid #e0e0e0; *padding*: 4px;}  /\* markdown预览和博客文章的h1,h2,h3样式 \*/  div.flask-pagedown-preview h1, .blog-body h1 {*font-size*: 140%;}  div.flask-pagedown-preview h2, .blog-body h2 {*font-size*: 130%;}  div.flask-pagedown-preview h3, .blog-body h3 {*font-size*: 120%;} |

效果：

② 在服务器上处理富文本

在文本框输入Markdown格式下面会显示渲染的HTML格式。然而点击提交后，发送的是纯文本，数据库中保存的也是Markdown格式的文本。所以显示页面时，从数据库获取Markdown文本，使用Python的Markdown模块转换为HTML格式，再用Bleach清理，保证只含允许使用的标签，然后显示到网页。

直接提交渲染的HTML预览有安全隐患，因为攻击者可以修改HTML代码，让其和Markdown源不匹配。

Markdown格式的文本转为HTML可在\_blogs.html中完成，但效率不高，每次渲染都要转换一次。可以在创建博客文章时Markdown转换成HTML，将HTML代码缓存到Blog模型的一个新字段body\_html中。文章的Markdown源文本也需要保存到数据库，以防需要编辑。

// 存两份有点奢侈啊...

app/models.py：Blog模型处理Markdown文本

|  |
| --- |
| from markdown import markdown  import bleach  *class* Blog(*db*.*Model*):  # ...  body\_html = db.Column(db.Text) # 博客正文HTML代码  @*staticmethod*  *def* on\_changed\_body(*target*, *value*, *oldvalue*, *initiator*):  # body字段渲染成HTML保存到body\_html  allowed\_tags = ['a', 'abbr', 'acronym', 'b', 'blockquote', 'code',  'em', 'i', 'li', 'ol', 'pre', 'strong', 'ul',  'h1', 'h2', 'h3', 'p']  target.body\_html = bleach.linkify(bleach.clean(  markdown(value, *output\_format*='html'),  *tags*=allowed\_tags, *strip*=True))  # on\_changed\_body注册在body字段, SQLAlchemy 'set'事件的监听程序  # 只要body字段设了新值,函数自动被调用  db.event.listen(Blog.body, 'set', Blog.on\_changed\_body) |

markdown()函数将Markdown文本转为HTML；将结果和允许的标签传给clean()函数，删除不在白名单的标签；再用linkify()把纯文本的URL转换成适当的a标签。

app/templates\_blogs.html：模板中使用文章的HTML格式

|  |
| --- |
| {# ... #}  <div class="blog-body">  {% if blog.body\_html %}  {# 使用safe过滤器,不转义HTML标签 #}  {{ blog.body\_html | safe }}  {% else %}  {{ blog.body }}  % endif %}</div> |

出于安全考虑，Jinja2默认转义模板变量。因为这里Markdown转换成HTML在服务器生成，非常靠谱，放心渲染。

效果：



// 代码依然有问题...

* 11.5 博客文章的固定链接

用户有时希望在社交网络和朋友分享某篇文章链接，因此每篇文章都需有一个专页，使用唯一的URL。因为文章插入数据库时都分配唯一id字段，以id构建文章URL十分合理，格式如：/blog/<int:id>

app/main/views/py：每篇文章的固定链接视图

|  |
| --- |
| @main.route('/blog/<int:id>')  *def* blog(*id*):  b = Blog.query.get\_or\_404(id)  return render\_template('blog.html', *blogs*=[b]) |

blog.html模板接收blogs列表作为参数，即要渲染的文章。为什么传入列表而不是单个博客对象? 因为这样可以引用\_blogs.html模板。

app/templates/\_blogs.html：文章的固定链接

|  |
| --- |
| {# ... #}  <div class="blog-content">  {# ... #}  <div class="blog-footer">{# 文章的链接 #}  <a href="{{ url\_for('.blog',id=blog.id) }}">  <span class="label label-default">>></span></a></div></div> |

app/templates/blog.html：每篇文章的固定链接模板

|  |
| --- |
| {% extends "base.html" %}  {# 只有一篇文章, 为什么要导入分页? #}  {% import "\_macros.html" as macros %}  {% block title %}hikari app - Blog{% endblock %}  {% block page\_content %}  {% include '\_blogs.html' %}  {% endblock %} |

app/static/main.css：链接靠右边

|  |
| --- |
| div.blog-footer {*text-align*: right;} |

* 11.6 博客文章编辑器

博客文章编辑器显示在单独的页面，上部显示文章的当前版本，下面为Markdown编辑器，用于修改Markdown源。编辑器基于Flask-PageDown实现，页面下面会显示一个预览。

app/templates/edit\_blog.html：编辑文章的模板

|  |
| --- |
| {% extends "base.html" %}  {% import "bootstrap/wtf.html" as wtf %}  {% block title %}hikari app - Edit Blog{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>编辑文章</h1></div>  <div>{{ wtf.quick\_form(form) }}</div>  {% endblock %}  {# 底部使用宏,从CDN加载js文件 #}  {% block scripts %}  {{ super() }}  {{ pagedown.include\_pagedown() }}  {% endblock %} |

app/main/views.py：编辑文章的视图

|  |
| --- |
| @main.route('/edit/<int:id>', *methods*=['GET', 'POST'])  @login\_required  *def* edit(*id*):  b = Blog.query.get\_or\_404(id)  # 当前登录用户是文章的作者或管理员可以编辑  if current\_user != b.author and \  not current\_user.can(Permission.ADMIN):  abort(403)  form = BlogForm()  if form.validate\_on\_submit():  b.body = form.body.data  db.session.add(b)  # db.session.commit()  flash('修改成功！')  return redirect(url\_for('.blog', *id*=b.id))  form.body.data = b.body  return render\_template('edit\_blog.html', *form*=form) |

有了新功能，就需要添加新的按钮。比如每篇文章下面、固定链接旁边添加一个指向编辑页面的链接。

app/templates/\_blogs.html：编辑博客文章的链接

|  |
| --- |
| {# ... #}  <div class="blog-content">  {# ... #}  <div class="blog-footer">{# 文章的底部 #}  {% if current\_user == blog.author %}  <a href="{{ url\_for('.edit',id=blog.id) }}">  <span class="label label-primary">编辑</span></a>  {%elif current\_user.is\_admin() %}  <a href="{{ url\_for('.edit',id=blog.id) }}">  <span class="label label-danger">编辑 [ADMIN]</span></a>  {% endif %}  <a href="{{ url\_for('.blog',id=blog.id) }}">  <span class="label label-default">链接</span></a></div></div> |

效果：



如果是管理员自己的文章，只会执行if语句，显示普通的编辑，而没有管理员大大的特权编辑。

使用之前的方法，markdown和pygments模块，结果代码就OK了?

app/models.py：Blog模型取消使用Bleach，添加Markdown扩展

|  |
| --- |
| @*staticmethod*  *def* on\_changed\_body(*target*, *value*, *oldvalue*, *initiator*):  # body字段渲染成HTML保存到body\_html  exts = ['markdown.extensions.extra', 'markdown.extensions.codehilite',  'markdown.extensions.tables', 'markdown.extensions.toc']  target.body\_html = markdown(value, *extensions*=exts) |

命令行：

|  |
| --- |
| $ pygmentize -S default -f html > default.css |

生成一个pygments默认的语法高亮CSS文件，放到app/static/目录。

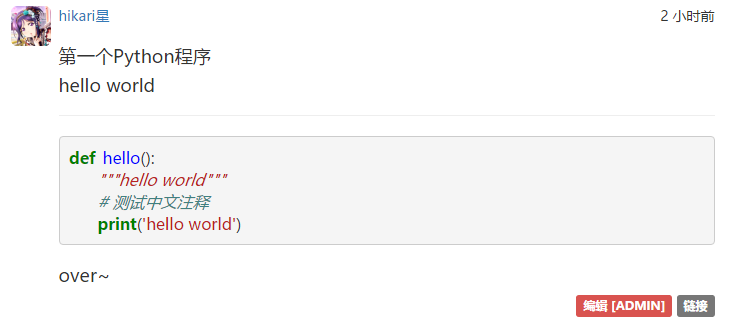
字体调大：

|  |
| --- |
| .codehilite span {*font-size*: 16px; } |

在app/templates/base.html导入该CSS文件。

|  |
| --- |
| <link rel="stylesheet" type="text/css" href="{{ url\_for('static', filename='default.css') }}"> |

效果：



**20180514**

**第12章 关注者**

社交Web程序用户之间可以关注、加好友等，需要记录两个用户之间的定向联系，在数据库查询中也要使用这种联系。

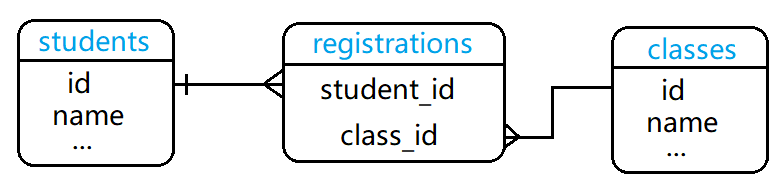
* 12.1 再论数据库关系

一对多关系是最常用的关系，在'多'的一方加入一个外键，指向'一'的链接记录。比如本程序中，一个用户角色对应多个用户，一个用户对应多个博客。

① 多对多关系

如学生选课的数据库。一个学生可以有多个课程，一个课程可以被多个学生选择，是典型的多对多关系。

一般添加第三张表，称为关联表。多对多关系可以分解为原表和关联表之间两个一对多关系。



上面registratiions表就是关联表，每一行表示一个学生注册的一个课程。

多对多查询要分为两步。想要知道某个学生选了哪些课程，从学生和注册的一对多关系获取这位学生在registrations表中的所有选课id，再按照多对一的方向遍历课程和注册的一对多关系，找到对应课程。

多对多关系代码：

|  |
| --- |
| registrations = db.Table('registrations',  db.Column('student\_id', db.Integer, db.ForeignKey('students.id')),  db.Column('class\_id', db.Integer, db.ForeignKey('classes.id')))  *class* Student(*db*.*Model*):  id = db.Column(db.Integer, *primary\_key*=True)  name = db.Column(db.String)  classes = db.relationship('Class',  *secondary*=registrations,  *backref*=db.backref('students', *lazy*='dynamic'),  *lazy*='dynamic')  *class* Class(*db*.*Model*):  id = db.Column(db.Integer, *primary\_key*=True)  name = db.Column(db.String) |

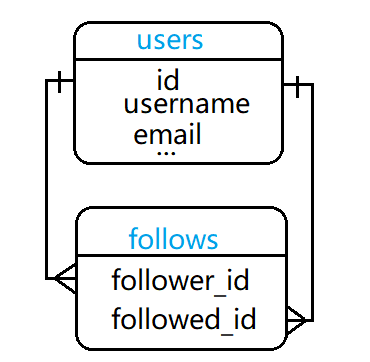
多对多关系仍用db.relationship()定义，但需把secondary参数设为关联表。多对多关系可以定义在任何一个类中，backref会管理好另一边。

关联表registrations是表，不是模型，SQLAlchemy自动管理此表。

|  |
| --- |
| >>> s = Student(name='hikari')  >>> c1 = Class(name='Python')  >>> c2 = Class(name='JavaScript')  >>> s.classes.append(c1)  >>> s.classes.append(c2)  >>> db.session.add\_all([s, c1, c2])  >>> db.commit()  >>> s.classes.all() # 学生s选的所有课程  >>> c1.students.all() # 选择c1课程的所有学生  >>> s.classes.remove(c2) # 学生s删除c2课程 |

② 自引用关系

学生和课程例子，关联表连接的是两个明确的实体。但对于关注用户只有一个用户实体，关系两侧分别为关注者和被关注者，都是用户实体，也就是关系的两侧都在同一个表中。这种关系为自引用关系。



关联表是follows，每一行代表一个用户关注了另一个用户。

③ 高级多对多关系

使用多对多关系时往往需要存储两个实体之间额外信息，比如存储用户关注另一个用户的时间，这样可以按时间顺序列出所有关注者。

这种信息只能存储在关联表，所以需要把关联表变成模型。

app/models.py：Follow模型

|  |
| --- |
| *class* Follow(*db*.*Model*): # 关注功能的关联表模型  \_\_tablename\_\_ = 'follows'  follower\_id = db.Column(db.Integer, db.ForeignKey('users.id'),  *primary\_key*=True)  followed\_id = db.Column(db.Integer, db.ForeignKey('users.id'),  *primary\_key*=True)  timestamp = db.Column(db.DateTime, *default*=datetime.utcnow) |

SQLAlchemy不能直接使用这个关联表，因为无法访问自定义字段。要把多对多关系的左右两侧拆分成两个基本的一对多关系，而且要定义成标准的关系。

app/models.py：使用两个一对多关系实现多对多关系

|  |
| --- |
| *class* User(*UserMixin*, *db*.*Model*):  # ...  followed = db.relationship('Follow', # 该用户关注的大神  *foreign\_keys*=[Follow.follower\_id], # 消除外键歧义  # 回引Follow模型; 该用户甘愿当此人的小弟  *backref*=db.backref('follower', *lazy*='joined'),  *lazy*='dynamic',  *cascade*='all, delete-orphan')  followers = db.relationship('Follow', # 关注该用户的萌新  *foreign\_keys*=[Follow.followed\_id],  # 将该用户视为大神的用户  *backref*=db.backref('followed', *lazy*='joined'),  *lazy*='dynamic',  *cascade*='all, delete-orphan') |

回引的lazy='joined'实现从联结查询加载相关对象。如某用户关注了100个用户，u.followded.all()返回列表，包含100个Follow实例，每个实例的follower和followed回引属性都指向相应的用户。joined模式一次数据库查询完成这些操作。如果lazy默认值select。首次访问follower和followed属性才会加载相应用户，每个属性都要一次单独的查询，获取全部被关注用户需要增加100次查询。

cascade参数delete-orphan为启用所有默认层叠选项，而且删除孤儿记录。

在删除对象时，默认是把对象联接的所有相关对象的外键设为空值。但在关联表中，删除记录应该是把指向该记录的实体也删除，因为这样能有效销毁联接。

app/models.py：关注关系的辅助方法

|  |
| --- |
| *class* User(*UserMixin*, *db*.*Model*):  # ...  *def* follow(*self*, *user*):  # 关注某用户(如果没有关注)  if not self.is\_following(user) and self != user:  f = Follow(*followed*=user)  self.followed.append(f)  *def* unfollow(*self*, *user*):  # 取消关注(如果已经关注)  f = self.followed.filter\_by(*followed\_id*=user.id).first()  if f:  # 删除Follow对象,销毁联系  self.followed.remove(f)  *def* is\_following(*self*, *user*):  # user是不是该用户关注的大神  if user.id is None:  return False  return self.followed.filter\_by(  *followed\_id*=user.id).first() is not None  *def* is\_followed\_by(*self*, *user*):  # user是不是关注该用户的萌新  if user.id is None:  return False  return self.followers.filter\_by(  *follower\_id*=user.id).first() is not None |

// follow、followed、follower看晕了...

* 12.2 在资料页显示关注者

用户访问尚未关注的用户资料页，需要显示'关注'按钮；

访问已关注用户显示'取消关注'按钮。

最好能显示关注者和被关注者人数，并在用户资料页显示'ta关注了你'标志。

app/templates/user.html：用户资料页添加关注信息

|  |
| --- |
| <p>{% if user == current\_user %}我{% else %}ta{% endif %}的博客有  {{ user.blogs.count() }}篇文章</p>  {# 关注&取消关注 #}  <p>  {% if current\_user.can(Permission.FOLLOW) and user != current\_user %}  {% if not current\_user.is\_following(user) %}  <a href="{{ url\_for('.follow', username=user.username) }}" class="btn btn-primary">关注</a>  {% else %}  <a href="{{ url\_for('.unfollow', username=user.username) }}" class="btn btn-default">取消关注</a>  {% endif %}  {% endif %}  <a href="{{ url\_for('.followers', username=user.username) }}">  关注{% if user == current\_user %}我{% else %}ta{% endif %}的人:  <span class="badge">{{ user.followers.count() }}</span></a>  <a href="{{ url\_for('.followed\_by', username=user.username) }}">  {% if user == current\_user %}我{% else %}ta{% endif %}关注的人:  <span class="badge">{{ user.followed.count() }}</span></a>  {% if current\_user.is\_authenticated and user != current\_user and user.is\_following(current\_user) %}  | <span class="label label-default">ta关注了你</span>  {% endif %}</p> |

新增了四个按钮关注、取消关注、关注ta的人、ta关注的人，对应四个视图函数follow()、unfollow()、followers()、followed\_by()。

app/main/views.py：四个按钮的视图函数

|  |
| --- |
| @main.route('/follow/<username>')  @login\_required  @permission\_required(Permission.FOLLOW)  *def* follow(*username*):  # 关注该资料页用户  user = User.query.filter\_by(*username*=username).first()  if user is None or current\_user == user:  flash('无效操作！')  return redirect(url\_for('.index'))  if current\_user.is\_following(user):  flash('你已经关注了此用户！')  return redirect(url\_for('.user', *username*=username))  current\_user.follow(user)  flash('你成功关注了{}。'.format(username))  return redirect(url\_for('.user', *username*=username))  @main.route('/unfollow/<username>')  @login\_required  @permission\_required(Permission.FOLLOW)  *def* unfollow(*username*):  # 取消关注  user = User.query.filter\_by(*username*=username).first()  if user is None or current\_user == user:  flash('无效操作！')  return redirect(url\_for('.index'))  if not current\_user.is\_following(user):  flash('你没有关注此用户，无法取消关注！')  return redirect(url\_for('.user', *username*=username))  current\_user.unfollow(user)  flash('你取消关注了{}！'.format(username))  return redirect(url\_for('.user', *username*=username))  @main.route('/followers/<username>')  *def* followers(*username*):  # 显示关注此用户的小弟们  user = User.query.filter\_by(*username*=username).first()  if user is None:  flash('无效用户！')  return redirect(url\_for('.index'))  page = request.args.get('page', 1, *type*=*int*)  pagination = user.followers.paginate(  # 在配制文件设置一页显示多少关注者, 此处为50  page, *per\_page*=current\_app.config['FOLLOWERS\_PER\_PAGE'],  *error\_out*=False)  # 关注者、关注时间字典组成的列表  follows = [{'user': item.follower, 'timestamp': item.timestamp}  for item in pagination.items]  title = '关注{}的人'.format(username)  return render\_template('followers.html', *user*=user, *title*=title,  *endpoint*='.followers', *pagination*=pagination,  *follows*=follows)  @main.route('/followed\_by/<username>')  *def* followed\_by(*username*):  # 显示此用户关注的大神们  user = User.query.filter\_by(*username*=username).first()  if user is None:  flash('无效用户！')  return redirect(url\_for('.index'))  page = request.args.get('page', 1, *type*=*int*)  pagination = user.followed.paginate(  page, *per\_page*=current\_app.config['FOLLOWERS\_PER\_PAGE'],  *error\_out*=False)  follows = [{'user': item.followed, 'timestamp': item.timestamp}  for item in pagination.items]  title = '{}关注的人'.format(username)  return render\_template('followers.html', *user*=user, *title*=title,  *endpoint*='.followed\_by', *pagination*=pagination,  *follows*=follows) |

app/templates/followers.html：显示关注者

|  |
| --- |
| {% extends "base.html" %}  {% import "\_macros.html" as macros %}  {% block title %}hikari app - {{ title }}{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>{{ title }}</h1></div>  {# 两列表格 左边为头像用户名资料页链接,右边为时间 #}  <table class="table table-hover followers">  <thead><tr><th>用户</th><th>关注时间</th></tr></thead>  {% for follow in follows %}  <tr><td>  <a href="{{ url\_for('.user', username = follow.user.username) }}">  <img class="img-rounded follow\_img" src="{{ follow.user.image }}">  {{ follow.user.username }}</a></td>  <td>{{ moment(follow.timestamp).format('L') }}</td></tr>  {% endfor %}  </table>  <div class="pagination">{# 分页 #}  {{ macros.pagination\_widget(pagination, endpoint, username = user.username) }}  </div>{% endblock %} |

app/static/main.css：

|  |
| --- |
| .table.followers tr {*border-bottom*: 1px solid #e0e0e0;}  .follow\_img{*max-width*: 30px; *max-height*: 30px;} |

app/fake.py：

|  |
| --- |
| *def* gen\_follows(*count*=100):  # 随机分配关注  user\_count = User.query.count()  hikari = User.query.first()  for j in range(user\_count):  u = User.query.offset(j).first()  if u != hikari:  u.follow(hikari)  i = 0  while i < count:  # offset()过滤器跳过指定记录数量; 通过设置随机偏移,  # 再调用first()相当于每次随机选一个用户  u1 = User.query.offset(randint(0, user\_count - 1)).first()  u2 = User.query.offset(randint(0, user\_count - 1)).first()  if u1 == u2 or u1.is\_following(u2) or u1 == hikari:  continue  u1.follow(u2)  i += 1  db.session.commit() |

在Python shell中随机生成关注关系。

效果：





**20180515**

* 12.3 使用数据库联结查询所关注用户的文章

目前按时间降序显示数据库所有文章。既然实现了用户关注功能，就可以让用户选择只显示关注用户的博客文章。

先获取关注的用户，再获取这些用户的文章，按照一定顺序排列，写入单独列表。但是随着数据库变大，生成列表的工作量也增加，分页等操作也不高效了。

获取文章高效的方式是只用一次查询。

联结操作用到两个或更多的数据表，在其中查找满足指定条件的记录组合，再把记录组合插入一个临时列表，此临时表就是联结查询的结果。

如users表有3个用户：

|  |  |
| --- | --- |
| **id** | **username** |
| 1 | hikari |
| 2 | maki |
| 3 | rin |

blogs表

|  |  |  |
| --- | --- | --- |
| **id** | **author\_id** | **body** |
| 1 | 3 | 关于如何让花阳亲减肥 |
| 2 | 1 | hikari的文章 |
| 3 | 2 | 小真姬教你弹钢琴 |
| 4 | 3 | 凛喵的由来 |

follows表

|  |  |
| --- | --- |
| **follower\_id** | **followed\_id** |
| 1 | 2 |
| 1 | 3 |
| 3 | 2 |

要获取hikari关注用户的文章，要合并blogs表和follows表。先过滤follows表，只留下关注者为hikari的记录，然后过滤blogs表，留下auther\_id和过滤后follows表中followed\_id相等的记录，把两次过滤结果合并，组成临时联结表，就能高效查询hikari关注用户的文章列表。

联结表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **id** | **auther\_id\*** | **body** | **follower\_id** | **followed\_id\*** |
| 1 | 3 | 关于如何让花阳亲减肥 | 1 | 3 |
| 3 | 2 | 小真姬教你弹钢琴 | 1 | 2 |
| 4 | 3 | 凛喵的由来 | 1 | 3 |

\*标记为用来执行联结操作的列。

此表包含的文章都是hikari关注的用户发布的。

使用Flask-SQLAlchemy执行这个联结查询相当复杂：

|  |
| --- |
| return db.session.query(Blog).select\_from(Follow).\  filter\_by(*follower\_id*=self.id).\  join(Blog, Follow.followed\_id == Blog.author\_id) |

① db.session.query(Blog)：指明查询要返回Blog对象；

② select\_from(Follow)：此查询从Follow模型开始；

③ filter\_by(follower\_id=self.id)：使用关注用户过滤follows表，self是User模型的实例；

④ join(Blog, Follow.followed\_id == Blog.author\_id)：联结filter\_by()得到的结果和Blog对象。

调换过滤器和联结的顺序简化为：

|  |
| --- |
| return Blog.query.join(Follow, Follow.followed\_id == Blog.author\_id)\  .filter(Follow.follower\_id == self.id) |

先执行联结操作再过滤看似工作量会更大，但是这两种查询是等价的。SQLAlchemy先收集所有过滤器，再以最高效的方式生成查询，也就是生成的原生SQL语句是一样的。

app/models.py：获取关注用户的文章

|  |
| --- |
| *class* User(*UserMixin*, *db*.*Model*):  # ...  @*property*  *def* followed\_blogs(*self*):  # 关注的大神的所有文章  return Blog.query.join(Follow, Follow.followed\_id == Blog.author\_id)\  .filter(Follow.follower\_id == self.id) |

联结查询难理解，可能需要在shell中多多研究。

* 12.4 首页显示所关注用户的文章

app/main/views.py：显示所有文章或只显示关注用户文章：

|  |
| --- |
| @main.route('/', *methods*=['GET', 'POST'])  *def* index():  # ..  page = request.args.get('page', 1, *type*=*int*)  # show\_followed存储在cookie中, 决定是否只显示关注用户文章  show\_followed = False  if current\_user.is\_authenticated:  show\_followed = *bool*(request.cookies.get('show\_followed', ''))  query = current\_user.followed\_blogs if show\_followed else Blog.query  pagination = query.order\_by(Blog.timestamp.desc()).paginate(  page, *per\_page*=current\_app.config['BLOGS\_PER\_PAGE'], *error\_out*=False)  blogs = pagination.items  return render\_template('index.html', *form*=form, *blogs*=blogs,  *show\_followed*=show\_followed, *pagination*=pagination) |

cookie以request.cookies字典形式存储在请求对象中。

在cookie中设定show\_followed由视图函数完成。

app/main/views.py：

|  |
| --- |
| from flask import make\_response  @main.route('/all')  @login\_required  *def* show\_all():  resp = make\_response(redirect(url\_for('.index')))  resp.set\_cookie('show\_followed', '', *max\_age*=30\*24\*60\*60)  return resp  @main.route('/followed')  @login\_required  *def* show\_followed():  resp = make\_response(redirect(url\_for('.index')))  resp.set\_cookie('show\_followed', '1', *max\_age*=30\*24\*60\*60)  return resp |

cookie只能在响应对象中设置，所以这两个路由不能依赖Flask，要使用make\_response()创建响应对象。

需要在首页添加两个选项卡，分别调用/all和/followed路由

app/main/index.html：

|  |
| --- |
| {# 选项卡,显示全部文章or关注的大神的文章#}  <div class="blog-tabs">  <ul class="nav nav-tabs">  <li{% if not show\_followed %} class="active"{% endif %}>  <a href="{{ url\_for('.show\_all') }}">全部</a></li>  {% if current\_user.is\_authenticated %}  <li{% if show\_followed %} class="active"{% endif %}>  <a href="{{ url\_for('.show\_followed') }}">我关注的人</a></li>  {% endif %}</ul>  {# 显示博客文章的ul #}  {% include '\_blogs.html' %}</div> |

效果：



然后发现我关注的人中没有自己的文章，因为用户不能关注自己。

但希望查询关注的人文章时也能看到自己的文章(//作...)。可以在注册时把用户设为自己的关注者。

|  |
| --- |
| *class* User(*UserMixin*, *db*.*Model*):  # ...  *def* \_\_init\_\_(*self*, \*\**kwargs*):  # ...  self.follow(self) |

// 在下在上面把User模型不能follow(self)了...

但是现在数据库中已经有用户了，而且都没有关注自己。可以添加一个函数，在Python shell中更新现有的用户。

app/models.py：

|  |
| --- |
| @*staticmethod*  *def* add\_self\_follows():  for user in User.query.all():  if not user.is\_following(user):  user.follow(user)  db.session.add(user)  db.session.commit() |

|  |
| --- |
| (venv) $ python manage.py shell  >>> User.add\_self\_follows() |

使用创建函数在shell中操作更新数据库，经常用于更新已部署的程序，因为脚本更新比手动更新数据库出错率少。

但是这样用户资料页的ta关注的人和关注ta的人都会+1。所以模板中需要将user.followers.count()-1和user.followed.count()-1；关注者的表格不显示自己。

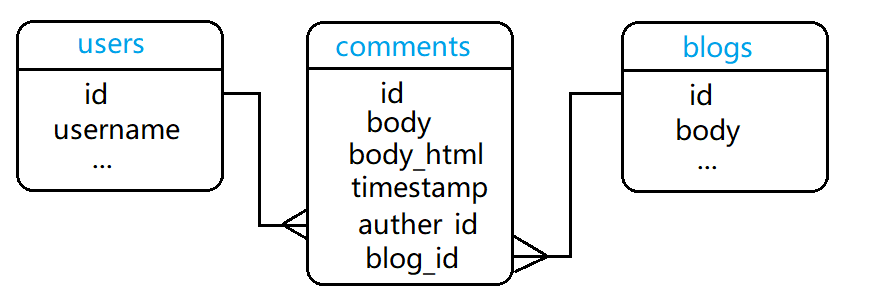
// 此处不想改了，仍然保持自己不能关注自己...

// 貌似没有添加删除文章的功能...

**第13章 用户评论**

* 13.1 评论在数据库中的表示

评论也有正文、作者、时间戳等，也使用Markdown语法。



blogs表到comments表是一对多的关系；users表和comments表也有一对多的关系。用户资料页可以显示该用户的总评论数。

app/models.py：Comment模型

|  |
| --- |
| *class* Comment(*db*.*Model*):  \_\_tablename\_\_ = 'comments'  id = db.Column(db.Integer, *primary\_key*=True)  body = db.Column(db.Text) # 评论正文  body\_html = db.Column(db.Text) # 评论正文HTML代码  timestamp = db.Column(db.DateTime, *index*=True,  *default*=datetime.utcnow) # 评论时间  disabled = db.Column(db.Boolean) # 查禁不当言论  author\_id = db.Column(db.Integer, db.ForeignKey('users.id'))  blog\_id = db.Column(db.Integer, db.ForeignKey('blogs.id'))  @*staticmethod*  *def* on\_changed\_body(*target*, *value*, *oldvalue*, *initiator*):  # 评论内容短, 允许标签变少  allowed\_tags = ['a', 'abbr', 'acronym', 'b', 'code', 'em', 'i', 'strong']  # body字段渲染成HTML保存到body\_html  target.body\_html = bleach.linkify(bleach.clean(  markdown(value, *output\_format*='html'),  *tags*=allowed\_tags, *strip*=True))  # on\_changed\_body注册在body字段, SQLAlchemy 'set'事件的监听程序  # 只要body字段设了新值,函数自动被调用  db.event.listen(Comment.body, 'set', Comment.on\_changed\_body) |

app/models.py：User和Blog模型的反向引用

|  |
| --- |
| *class* User(*UserMixin*, *db*.*Model*):  # ...  comments = db.relationship('Comment', *backref*='author', *lazy*='dynamic')  *class* Blog(*db*.*Model*):  # ...  comments = db.relationship('Comment', *backref*='blog', *lazy*='dynamic') |

* 13.2 提交和显示评论

评论一般显示在单个博客文章中，路由/blog/< int:id>，在对应模板添加一个提交评论的表单。

app/forms.py：

|  |
| --- |
| *class* CommentForm(*FlaskForm*): # 写评论的表单类  body = PageDownField('写点什么吧...', *validators*=[DataRequired()])  submit = SubmitField('提交') |

app/main/views.py：单个文章视图函数支持评论

|  |
| --- |
| @main.route('/blog/<int:id>', *methods*=['GET', 'POST'])  *def* blog(*id*): # 单个博客文章页面  b = Blog.query.get\_or\_404(id)  form = CommentForm()  if form.validate\_on\_submit():  c = Comment(*body*=form.body.data, *blog*=b,  *author*=current\_user.\_get\_current\_object())  db.session.add(c)  # db.session.commit()  flash('评论成功！')  return redirect(url\_for('.blog', *id*=b.id, *page*=-1))  page = request.args.get('page', 1, *type*=*int*)  n = current\_app.config['COMMENTS\_PER\_PAGE'] # 配置文件设为30  if page == -1: # 评论最后一页;因为先评论的在前,刚提交的评论在最后  page = (b.comments.count()-1)//n+1  pagination = b.comments.order\_by(Comment.timestamp.asc()).paginate(  page, *per\_page*=n, *error\_out*=False)  comments = pagination.items  return render\_template('blog.html', *blogs*=[b], *form*=form,  *comments*=comments, *pagination*=pagination) |

类似于\_blogs.html，评论的渲染在新模板\_comments.html；在blog.html文章下方引入\_comments.html，显示分页导航。

**20180516**

app/templates/\_comments.html：显示某篇文章所有评论

|  |
| --- |
| <ul class="comment\_box">  {% for c in comments %}  <li class="comment">  {# 评论者头像 #}  <div class="comment-thumbnail">  <a href="{{ url\_for('.user', username=c.author.username) }}"><img class="img-rounded auther-thumbnail" src="{{ c.author.image }}"></a></div>  {# 评论者内容: 日期+名字+正文 #}  <div class="comment-content">  <div class="comment-date">{{ moment(c.timestamp).fromNow() }}</div>  <div class="comment-author">  <a href="{{ url\_for('.user', username=c.author.username) }}">  {{ c.author.username }}</a></div>  <div class="comment-body">  {% if c.body\_html %}  {{ c.body\_html | safe }}  {% else %}  {{ c.body }}  {% endif %}  </div></div></li>  {% endfor %}</ul> |

app/templates/\_blogs.html：首页、资料页文章评论链接

|  |
| --- |
| <a href="{{ url\_for('.blog', id=blog.id) }}#comments">  <span class="label label-primary">  评论({{ blog.comments.count() }})</span></a> |

链接后面的#comments后缀为URL片段，用于指定加载页面后滚动条所在初始位置，也就是点击此链接直接跳到blog.html的评论部分。

app/templates/blog.html：博客文章页面添加评论表单

|  |
| --- |
| {% import "bootstrap/wtf.html" as wtf %}  {% block page\_content %}  {% include '\_blogs.html' %}  <h4 id="comments">评论</h4>  {# 需要有评论权限 #}  {% if current\_user.can(Permission.COMMENT) %}  <div class="comment-form">{{ wtf.quick\_form(form) }}</div>  {% endif %}  {% include '\_comments.html' %}  {% if pagination %}  <div class="pagination">{{ macros.pagination\_widget(pagination, '.blog', fragment='#comments', id=blogs[0].id) }}</div>  {% endif %}  {% endblock %}  {# 底部使用宏,从CDN加载pagedown的js文件 #}  {% block scripts %}  {{ super() }}  {{ pagedown.include\_pagedown() }}  {% endblock %} |

\_macros.html宏的pagination\_widget函数添加fragment参数指定URL片段，此处为'#comments'。

app/templates/\_macros.html：分页函数添加fragment参数，默认空字符串，如此博客文章的分页也能继续使用这个宏

|  |
| --- |
| {# 定义pagination\_widget宏,相当于函数,可用在首页或用户页面,文章过多时分页显示 #}  {% macro pagination\_widget(pagination, endpoint, fragment='') %}  <ul class="pagination"> {# 分页导航 #}  {# 上一页链接,如果没有上一页,链接加上disabled类 #}  <li{% if not pagination.has\_prev %} class="disabled"{% endif %}>  <a href="{% if pagination.has\_prev %}{{ url\_for(endpoint, page=pagination.prev\_num, \*\*kwargs) }}{{ fragment }}{% else %}#{% endif %}">  &laquo;</a></li>  {# 分页对象iter\_pages()迭代器返回所有页面链接 #}  {% for p in pagination.iter\_pages() %}  {% if p %}  {# 当前页面加上active类,表示高亮 #}  {% if p == pagination.page %}  <li class="active"><a href="{{ url\_for(endpoint, page = p, \*\*kwargs) }}{{ fragment }}">{{ p }}</a></li>  {% else %}  <li><a href="{{ url\_for(endpoint, page = p, \*\*kwargs) }}{{ fragment }}">{{ p }}</a></li>  {% endif %}  {% else %} {# 页面中None表示的间隔使用省略号表示 #}  <li class="disabled"><a href="#">&hellip;</a></li>  {% endif %}  {% endfor %}  {# 下一页链接,如果没有下一页,链接加上disabled类 #}  <li{% if not pagination.has\_next %} class="disabled"{% endif %}>  <a href="{% if pagination.has\_next %}{{ url\_for(endpoint, page=pagination.next\_num, \*\*kwargs) }}{{ fragment }}{% else %}#{% endif %}">  &raquo;</a></li></ul>  {% endmacro %} |

app/templates/user.html：资料页添加显示该用户有多少评论

|  |
| --- |
| <p>{% if user == current\_user %}我{% else %}ta{% endif %}的博客有  {{ user.blogs.count() }}篇文章 | {{ user.comments.count() }}条评论</p> |

app/static/main.css：

|  |
| --- |
| ul.comment\_box { *list-style-type*: none; *padding*: 0px; *margin*: 16px 0px 0px 0px;}  ul.comment\_box li.comment { *margin-left*: 32px; *padding*: 8px; *border-bottom*: 1px solid #e0e0e0;}  ul.comment\_box li.comment:nth-child(1) { *border-top*: 1px solid #e0e0e0;}  ul.comment\_box li.comment:hover { *background-color*: #f0f0f0;}  div.comment-date { *float*: right;}  div.comment-author { *font-weight*: bold;}  div.comment-thumbnail { *position*: absolute;}  div.comment-content { *margin-left*: 48px; *min-height*: 48px;}  div.comment-form { *margin*: 16px 0px 16px 32px;} |

app/fake.py：生成虚拟评论

|  |
| --- |
| *def* gen\_fake\_comments(*count*=100):  # 为count篇文章分配评论  fake = Faker('zh\_CN')  user\_count = User.query.count()  blog\_count = Blog.query.count()  for i in range(count):  # offset()过滤器跳过指定记录数量; 通过设置随机偏移,  # 再调用first()相当于每次随机选一个用户  u = User.query.offset(randint(0, user\_count - 1)).first()  b = Blog.query.offset(randint(0, blog\_count - 1)).first()  c = Comment(*body*=fake.text(),  *timestamp*=fake.past\_date(),  *author*=u,  *blog*=b)  db.session.add(c)  db.session.commit() |

效果：



点击评论网址为http://127.0.0.1:5000/blog/1#comments，定位到评论处。

* 13.3 管理评论

具有MODERATE权限的用户可以管理其他用户的评论。

在base.html导航条中添加一个链接管理评论，具有权限的用户才能看到。

app/templates/base.html：

|  |
| --- |
| {% if current\_user.can(Permission.MODERATE) %}  <li><a href="{{ url\_for('main.moderate') }}">管理评论</a></li>  {% endif %} |

app/main/views/py：管理评论的视图函数

|  |
| --- |
| @main.route('/moderate')  @login\_required  @permission\_required(Permission.MODERATE)  *def* moderate():  # 从数据库读取一页评论  page = request.args.get('page', 1, *type*=*int*)  pagination = Comment.query.order\_by(Comment.timestamp.desc()).paginate(  page, *per\_page*=current\_app.config['COMMENTS\_PER\_PAGE'],  *error\_out*=False)  comments = pagination.items  return render\_template('moderate.html', *comments*=comments,  *pagination*=pagination, *page*=page) |

app/templates/moderate.html：

|  |
| --- |
| {% extends "base.html" %}  {% import "\_macros.html" as macros %}  {% block title %}hikari app - 管理评论{% endblock %}  {% block page\_content %}  <div class="page-header"><h1>管理评论</h1></div>  {% set moderate = True %}{# 定义模板变量moderate为True#}  {% include '\_comments.html' %}{# 导入子模板渲染评论 #}  {% if pagination %}  <div class="pagination">  {{ macros.pagination\_widget(pagination, '.moderate') }}</div>  {% endif %}  {% endblock %} |

模板变量moderate用于\_comments.html子模板，决定是否渲染管理功能。

协管员moderate为True需要有一个来回切换的按钮，决定某条评论要不要和谐。

blog.html也引入了\_comments.html子模板，但它没有moderate变量，无论是否是协管员，在博客文章页面都不会显示此两按钮。

app/templates/\_comments.html：

|  |
| --- |
| <div class="comment-body">  {% if c.disabled %}<p><i>该评论已被和谐...</i></p>{% endif %}  {# 如果评论正常,或协管员浏览被和谐评论,显示之 #}  {% if moderate or not c.disabled %}  {% if c.body\_html %}  {{ c.body\_html | safe }}  {% else %}  {{ c.body }}  {% endif %}  {% endif %}</div>  {# 协管员来回切换按钮(两个按钮只显示一个),管理是否显示该评论 #}  {% if moderate %}<br>  {% if c.disabled %}  <a class="btn btn-default btn-xs" href="{{ url\_for('.moderate\_enable', id=c.id, page=page) }}">恢复</a>  {% else %}  <a class="btn btn-danger btn-xs" href="{{ url\_for('.moderate\_disable', id=c.id, page=page) }}">和谐</a>  {% endif %}  {% endif %} |

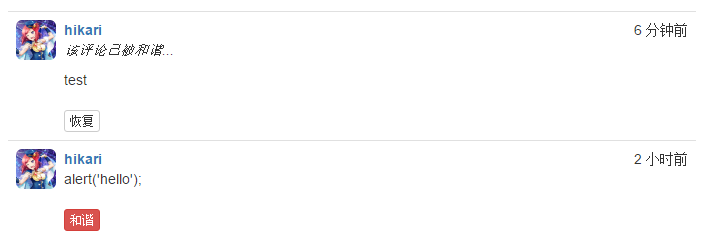
此两个按钮需要定义两个视图函数处理任务。

app/main/views.py：

|  |
| --- |
| @main.route('/moderate/enable/<int:id>')  @login\_required  @permission\_required(Permission.MODERATE)  *def* moderate\_enable(*id*):  c = Comment.query.get\_or\_404(id)  c.disabled = False  db.session.add(c)  # db.session.commit()  return redirect(url\_for('.moderate',  *page*=request.args.get('page', 1, *type*=*int*)))  @main.route('/moderate/disable/<int:id>')  @login\_required  @permission\_required(Permission.MODERATE)  *def* moderate\_disable(*id*):  c = Comment.query.get\_or\_404(id)  c.disabled = True  db.session.add(c)  # db.session.commit()  return redirect(url\_for('.moderate',  *page*=request.args.get('page', 1, *type*=*int*))) |

Comment模型的disabled字段表示评论需要被和谐，只是逻辑删除。

moderate()函数向模板传入page，用作两个按钮链接的查询字符串。此两个视图函数获取到链接查询字符串的page，便于修改后重定向到原来页。



**第14章 应用编程接口**

最近几年，Web程序业务逻辑越来越多移到了客户端，开创了称为富互联网应用(Rich Internet Application, RIA)的架构，服务器的主要(或唯一)功能是为客户端提供数据存储服务，这样服务器成了Web应用编程接口(Application Programming Interface, API)。

RIA可采用多种协议与Web服务通信。远程过程调用(Remote Procedure Call, RPC)协议，如XML-RPC，及由其衍生的简单对象访问协议(Simplified Object Access Protocol, SOAP)，在几年前比较受欢迎。

最近，表现层状态转移(Representational State Transfer, REST)架构崭露头角，成为 Web程序的新宠。Flask是开发REST架构Web服务的理想框架。

* 14.1 REST简介

Roy Fielding在其[博士论文](http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm)中介绍了Web服务的REST 架构方式，并列出了6个符合这一架构定义的特征。

|  |
| --- |
| 客户端-服务器  客户端和服务器之间必须有明确的界线。  无状态  客户端发出的请求中必须包含所有必要的信息。服务器不能在两次请求之间保存客户端的任何状态。  缓存  服务器发出的响应可以标记为可缓存或不可缓存，出于优化目的，客户端(或客户端和服务器之间的中间服务)可以使用缓存。  接口统一  客户端访问服务器资源时使用的协议必须一致、定义良好、且已经标准化。REST Web服务最常使用的统一接口是HTTP协议。  系统分层  在客户端和服务器之间可以按需插入代理服务器、缓存或网关，以提高性能、稳定性和伸缩性。  按需代码  客户端可以选择从服务器上下载代码，在客户端的环境中执行。 |

① 资源就是一切

资源是REST架构的核心概念。如在博客程序中，用户、博客文章和评论都是资源，每个资源都要使用唯一的URL表示。

一篇博客文章可以使用/api/blogs/123表示，其中123是这篇文章的唯一标识符，使用文章在数据库中的主键表示。URL的格式或内容无关紧要，只要资源的URL只表示**唯一**的资源即可。

某一类资源的集合也要有一个URL。博客文章集合的URL可以是/api/blogs/，评论集合的URL可以是/api/comments/。

API还可以为某一类资源的逻辑子集定义集合URL。如编号为123的文章，其所有评论可以使用/api/blogs/123/comments/表示。表示资源集合的URL习惯在末端加上/，代表一种文件夹结构。

注意：Flask会特殊对待末端带/的路由。如果客户端请求的URL末端没有/，而唯一匹配的路由末端有/，Flask会自动响应一个重定向，转向末端带/的URL；反之请求的URL末尾有/而路由却没有/，则不会重定向。。

② 请求方法

要从博客API获取现有文章列表，客户端向/api/blogs/发送GET请求；要插入一篇新文章，客户端可以向/api/blogs/发送POST请求，请求主体包含文章内容；要获取编号为123的文章，向/api/blogs/123发送GET请求。

REST API中使用的HTTP请求方法

|  |  |  |  |
| --- | --- | --- | --- |
| **请求方法** | **目标** | **说明** | **HTTP状态码** |
| GET | 单个资源的URL | 获取目标资源 | 200 |
| GET | 资源集合的URL | 获取资源的集合(如果实现了分页，就是一页的资源) | 200 |
| POST | 资源集合的URL | 创建新资源，将其加入模板集合。服务器为新资源指派URL，在响应的Location首部中返回 | 201 |
| PUT | 单个资源的URL | 修改一个现有资源。如果客户端能为资源指派URL，还能用于创建新资源 | 200 |
| DELETE | 单个资源的URL | 删除一个资源 | 200 |
| DELETE | 资源集合的URL | 删除目标集合的所有资源 | 200 |

REST不要求为一个资源实现所有请求方法，如果资源不支持客户端使用的方法，响应的状态码为405，返回"不允许使用的方法"，Flask自动处理此错误。

③ 请求和响应主体

资源在客户端和服务器之间来回传送，但REST没有指定编码资源的方式。请求和响应中的Content-Type首部用于指明主体中资源的编码方式。使用HTTP协议中的内容协商机制，可以找到一种客户端和服务器都支持的编码方式。

常用的编码方式是JSON和XML。因为JavaScript是Web浏览器使用的客户端脚本语言，而JSON和JavaScript联系紧密，自然是JSON更流行。

如一篇博客文章对应资源用JSON表示：

|  |
| --- |
| {  *"url"*: "http://www.example.com/api/blogs/123",  *"title"*: "Writing RESTful APIs in Python",  *"author"*: "http://www.example.com/api/users/2",  *"body"*: "我是正文...",  *"comments"*: "http://www.example.com/api/blogs/123/comments"  } |

注意：上面url、author、comments字段都是完整的资源URL，客户端可以通过这些URL发掘新资源。

在设计良好的REST API中，客户端只需知道几个顶级资源的URL，其他资源的 URL从响应中包含的链接上发掘。如同浏览网页时，点击链接发掘新网页。

④ 版本

传统的服务器为中心的Web程序，服务器完全掌控程序，更新程序时，只要在服务器上部署新版本就能更新所有用户，因为用户浏览器的那部分程序也是从服务器上下载的。

但升级RIA和Web服务要更复杂，因为客户端程序和服务器上的程序是独立开发的。比如一个程序的REST Web服务被很多客户端使用，服务器可以随时更新Web浏览器的客户端，但无法强制更新手机的app，需要得到用户许可；就算用户想更新，也不能保证新版app上传到应用商店时新服务器版本已经部署好。

所以需要保证旧版客户端能继续使用。常见解决方法是使用版本区分Web服务所处理的URL。如首次发布的博客Web服务可以通过/api/v1.0/blogs/提供博客文章的集合。

在URL中加入Web服务的版本有助于条理化管理新旧功能，让服务器能为新客户端提供新功能，同时继续支持旧版客户端。比如更新博客文章使用的JSON 格式，同时通过/api/v1.1/blogs/提供修改后的博客文章，而客户端仍能通过/api/v1.0/blogs/获取旧的JSON格式。在一段时间内，服务器要同时处理v1.1和v1.0这两个版本的URL。

提供多版本支持会增加服务器的维护负担，但某些情况，这是不破坏现有部署且能让程序不断发展的唯一方式。

* 14.2 使用Flask提供REST Web服务

使用route()装饰器，methods可选参数可以声明服务提供资源URL的路由。请求包含的JSON数据可通过request.json这个字典获取，JSON响应可由Flask提供的辅助函数jsonify()从字典生成。

创建一个RESR Web服务，以便客户端访问博肯文章及相关资源。

① 创建API蓝本

REST API相关路由是一个自成一体的程序子集，为了更好地组织代码，最好把这些路由放到独立的API蓝本中。

API蓝本结构：

|  |
| --- |
| |-flasky  |-app/  |-api\_1\_0  |-\_\_init\_\_.py  |-users.py  |-blogs.py  |-comments.py  |-authentication.py  |-errors.py  |-decorators.py |

注意，API包的名字中有一个版本号。如果需要创建一个向前兼容的API版本，可以添加一个版本号不同的包，让程序同时支持两个版本的API。

此API蓝本中，各资源分别在不同模块实现。其中还包含处理认证、错误和提供自定义装饰器的模块。

app/api/\_\_init\_\_.py：API蓝本的构造文件

|  |
| --- |
| from flask import Blueprint  api = Blueprint('api', \_\_name\_\_) # 创建蓝本对象  # 导入模块将蓝本与它们关联起来  from . import authentication, blogs, users, comments, errors |

app/\_\_init\_\_.py：注册API蓝本

|  |
| --- |
| *def* create\_app(*config\_name*): # 工厂函数, 参数为配置名  # ...  from .api import api as api\_blueprint  # api蓝本所有路由添加前缀,如/blogs变为/api/v1/blogs  app.register\_blueprint(api\_blueprint, *url\_prefix*='/api/v1')  return app # 返回创建的程序示例 |

② 错误处理

REST Web服务会在响应中发送HTTP状态码，并将额外信息放入响应主体。

API返回常见HTTP状态码

|  |  |  |
| --- | --- | --- |
| **状态码** | **名称** | **说明** |
| 200 | OK | 请求成功完成 |
| 201 | Created | 请求成功完成并创建了一个新资源 |
| 400 | Bad request | 请求不可用或不一致 |
| 401 | Unauthorized | 请求未包含认证信息 |
| 403 | Forbidden | 请求中发送的认证密令无权访问目标 |
| 404 | Notfound | URL对应资源不存在 |
| 405 | Method not allowed | 指定资源不支持请求使用的方法 |
| 500 | Internal server error | 处理请求过程中服务器发生意外错误 |

处理404和500有点麻烦，因为是由Flask自己生成的，而且一般会返回HTML响应，会让API客户端困惑。

为所有客户端生成适当响应的一种方法是内容协商：在错误处理中根据客户端请求的格式改写响应。

app/main/errors.py：使用HTTP内容协商处理错误

|  |
| --- |
| from flask import render\_template, request, jsonify  from . import main  @main.app\_errorhandler(403)  *def* forbidden(*e*):  # 检查Accept请求首部,决定客户端期望接收的响应格式  # 为只接受JSON格式不接受HTML格式的客户端生成JSON格式响应  if request.accept\_mimetypes.accept\_json and \  not request.accept\_mimetypes.accept\_html:  response = jsonify({'error': 'forbidden'})  response.status\_code = 403  return response  # 浏览器一般不限制响应格式, 返回HTML格式响应  return render\_template('403.html'), 403  @main.app\_errorhandler(404)  *def* page\_not\_found(*e*):  if request.accept\_mimetypes.accept\_json and \  not request.accept\_mimetypes.accept\_html:  response = jsonify({'error': 'not found'})  response.status\_code = 404  return response  return render\_template('404.html'), 404  @main.app\_errorhandler(500)  *def* internal\_server\_error(*e*):  if request.accept\_mimetypes.accept\_json and \  not request.accept\_mimetypes.accept\_html:  response = jsonify({'error': 'internal server error'})  response.status\_code = 500  return response  return render\_template('500.html'), 500 |

// 403、404、500写法类似，感觉有点重复，能不能用偏函数?

其他状态码都由Web服务生成，因此可在API蓝本errors.py模块作为辅助函数实现。Web服务的视图函数可以调用这些辅助函数生成错误响应。

app/api/errors.py：API蓝本的错误处理程序

|  |
| --- |
| from flask import jsonify  from . import api  *def* bad\_request(*message*):  response = jsonify({'error': 'bad request', 'message': message})  response.status\_code = 400  return response  *def* unauthorized(*message*):  response = jsonify({'error': 'unauthorized', 'message': message})  response.status\_code = 401  return response  *def* forbidden(*message*):  response = jsonify({'error': 'forbidden', 'message': message})  response.status\_code = 403  return response |

**20180517**

③ 使用Flask-HTTPAuth认证用户

Web服务需要保护信息，未授权的用户无法访问。RIA需要询问用户的登录密令，传给服务器验证。

REST Web服务特点之一是无状态，服务器在两次请求之间不能记住客户端任何信息。所以客户端发出的请求必须包含所有必要的信息，如用户密令。

之前登录功能使用Flask-Login实现，数据存储在用户会话，默认保存在客户端cookie中，服务器没有保存任何用户信息。但REST Web服务除了Web浏览器外的客户端很难提供对cookie的支持。

|  |
| --- |
| REST的无状态要求看似过于严格，但并不是随意提出的要求，无状态的服务器伸缩起来更加简单。如果服务器保存客户端信息，必须提供一个所有服务器都能访问的共享缓存，才能保证一直使用同一台服务器处理特定客户端的请求。这样的需求很难实现。 |

REST发送密令最佳方式是使用HTTP认证，基本认证和摘要认证都可以。HTTP认证中，用户密令包含在请求的Authorization首部中。

Flask-HTTPAuth扩展提供的装饰器将协议细节隐去，使用方便，类似于Flask-Login提供的login\_required装饰器。

app/api/authentication.py：初始化Flask-HTTPAuth

|  |
| --- |
| from flask\_httpauth import HTTPBasicAuth  from flask import g  from ..models import AnonymousUser, User  auth = HTTPBasicAuth()  @auth.verify\_password  *def* verify\_password(*email*, *password*):  # 验证回调函数  if email == '': # 邮箱为空,匿名用户访问  g.current\_user = AnonymousUser()  return True  user = User.query.filter\_by(*email*=email).first()  if not user: # 用户不存在  return False  # 通过认证的用户保存在全局对象g中,视图函数能访问  g.current\_user = user  # 使用User模型的验证方法验证用户密码  return user.verify\_password(password) |

由于每次请求都要传输用户密令，所以API路由最好通过安全的HTTP提供，加密所有的请求和响应。

如果认证失败，服务器向客户端返回401错误。Flask-HTTPAuth默认自动生成这个状态码；但为了和API返回的其他错误保持一致，可以自定义错误响应。

app/api/authentication.py：Flask-HTTPAuth错误认证处理

|  |
| --- |
| from .errors import unauthorized  @auth.error\_handler  *def* auth\_error():  return unauthorized('Invalid credentials') |

为了保护路由，可使用装饰器auth.login\_required。但API蓝本所有路由都要保护，可在before\_request处理程序使用login\_required装饰器，应用到整个蓝本。

app/api/authentication.py：在before\_request处理程序中进行认证

|  |
| --- |
| from .errors import forbidden  from . import api  @api.before\_request  @auth.login\_required  *def* before\_request():  # 不是匿名用户(已经认证)但是没有激活账号,抛出403  if not g.current\_user.is\_anonymous and \  not g.current\_user.confirmed:  return forbidden('Unconfirmed account') |

如此，API蓝本所有路由都能进行自动认证，作为附加认证before\_request处理程序还会拒绝已经通过认证但没有确认的用户。

④ 基于令牌认证

每次请求，客户端都要发送认证密令。为了避免总发送敏感信息，可以使用基于令牌的认证方案：

|  |
| --- |
| 客户端将登录密令发送给一个特殊的URL生成认证令牌。客户端获得令牌，就可用令牌代替密令认证请求。出于安全考虑，令牌有过期时间。令牌过期后，客户端必须重新发送登录密令以生成新令牌。令牌落入他人之手所带来的安全隐患受限于令牌的短暂使用期限。 |

app/models.py：User模型支持生成和验证令牌

|  |
| --- |
| *class* User(*UserMixin*, *db*.*Model*):  # ...  *def* gen\_auth\_token(*self*, *expiration*):  # 以用户id生成签名令牌  s = Slzer(current\_app.config['SECRET\_KEY'], *expires\_in*=expiration)  return s.dumps({'id': self.id}).decode('utf-8')  @*staticmethod*  *def* verify\_auth\_token(*token*):  # 静态方法因为只有解码令牌后才知道用户是谁  s = Slzer(current\_app.config['SECRET\_KEY'])  try:  data = s.loads(token)  except:  return  # 返回id对应用户对象  return User.query.get(data['id']) |

为了能支持验证包含令牌的请求，verify\_password回调需要修改能接收令牌。

app/api/authentication.py：支持令牌对的改进验证回调

|  |
| --- |
| @auth.verify\_password  *def* verify\_password(*email\_or\_token*, *password*):  # 验证回调函数  if email\_or\_token == '': # 匿名用户访问  g.current\_user = AnonymousUser()  return True  # 密码为空,则提供的是令牌  if password == '':  g.current\_user = User.verify\_auth\_token(email\_or\_token)  g.token\_used = True  return g.current\_user is not None  # 使用邮箱和密码验证  user = User.query.filter\_by(*email*=email\_or\_token).first()  if not user: # 用户不存在  return False  g.current\_user = user  g.token\_used = False  return user.verify\_password(password) |

g.token\_used变量是为了让视图函数区分是邮箱密码认证还是令牌认证。

认证令牌发送给客户端的视图函数需要添加到API蓝本

app/api/authentication.py：生成认证令牌

|  |
| --- |
| from flask import jsonify  @api.route('/tokens/', *methods*=['POST'])  *def* get\_token():  # 如匿名用户或已经有令牌,需要拒绝请求  if g.current\_user.is\_anonymous or g.token\_used:  return unauthorized('Invalid credentials')  # 登录用户且没有生成令牌的用户返回JSON响应  return jsonify({'token': g.current\_user.gen\_auth\_token(  *expiration*=3600), 'expiration': 3600}) |

⑤ 资源和JSON的序列化转换

开发Web程序经常需要资源内部表示和JSON之间转换。JSON是HTTP请求和响应的传输格式。

app/models.py：博客文章转换成JSON格式的序列化字典

|  |
| --- |
| *class* Blog(*db*.*Model*):  # ...  *def* to\_json(*self*):  return {  'url': url\_for('api.get\_blog', *id*=self.id),  'body': self.body,  'body\_html': self.body\_html,  'timestamp': self.timestamp,  'author\_url': url\_for('api.get\_user', *id*=self.author\_id),  'comments\_url': url\_for('api.get\_blog\_comments', *id*=self.id),  'comment\_count': self.comments.count()  } |

url、author、comments字段分别返回各自资源的URL，由url\_for()生成，路由后面将在API蓝本定义。狗书上说要指定\_external=True生成完整URL，但是GitHub代码却没有写。

User模型to\_json()方法与Blog模型类似。

app/models.py：用户转换成JSON格式的序列化字典

|  |
| --- |
| *class* User(*UserMixin*, *db*.*Model*):  # ...  *def* to\_json(*self*):  return {  'url': url\_for('api.get\_user', *id*=self.id),  'username': self.username,  'member\_since': self.member\_since,  'last\_seen': self.last\_seen,  'blogs\_url': url\_for('api.get\_user\_blogs', *id*=self.id),  'followed\_blogs\_url': url\_for('api.get\_user\_followed\_blogs',  *id*=self.id),  'blog\_count': self.blogs.count()  } |

提供给客户端资源表示没必要和数据库模型内部完全一致。比如为了保护隐私，上面JSON没有加入email、role等字段。

将JSON转为模型时可能出现：客户端提供的数据无效、错误或多余。

app/models.py：JSON格式数据创建一篇博客

|  |
| --- |
| from app.exceptions import ValidationError  *class* Blog(*db*.*Model*):  # ...  @*staticmethod*  *def* from\_json(*blog\_json*):  body = blog\_json.get('body')  if body is None or body == '':  raise ValidationError('博客文章木有正文！')  return Blog(*body*=body) |

app/exceptions.py：自定义认证错误

|  |
| --- |
| *class* ValidationError(*ValueError*):  pass |

上面只使用了JSON字典的body属性，body\_html字段会根据body变化自动触发事件而被修改；timestamp使用默认；author字段只能使用当前通过认证的用户；comments使用数据库关系自动生成；url由服务器指派而不是客户端。

如果没有body字段或为空字符串抛出自定义异常。程序需要向客户端提供适当的响应处理此异常。可以考虑创建全局异常处理程序。

app/api/errors.py：

|  |
| --- |
| from ..exceptions import ValidationError  # 只要抛出指定类异常,就会调用被装饰的函数  # api.errorhandler只有API蓝本的路由抛出异常才会调用  @api.errorhandler(ValidationError)  *def* validation\_error(*e*):  return bad\_request(e.args[0]) |

⑥ 实现资源端点

实现处理不同资源的路由和视图函数。GET请求一般是最简单，因为只要返回信息而无需修改信息。

app/apiblogs.py：文章资源GET请求处理

|  |
| --- |
| from . import api  from .authentication import auth  from ..models import Blog  from flask import jsonify  @api.route('/blogs/')  @auth.login\_required  *def* get\_blogs():  # 获取所有博客文章  blogs = Blog.query.all()  return jsonify({'blogs': [b.to\_json() for b in blogs]})  @api.route('/blogs/<int:id>')  @auth.login\_required  *def* get\_blog(*id*):  # 获取指定id的文章  b = Blog.query.get\_or\_404(id)  return jsonify(b.to\_json()) |

博客文章资源的POST请求处理程序将一篇新文章插入数据库。

app/api/blogs.py：创建一篇文章

|  |
| --- |
| from .decorators import permission\_required  from ..models import Permission  from flask import request, g, url\_for  from .. import db  @api.route('/blogs/', *methods*=['POST'])  @permission\_required(Permission.WRITE) # 当前登录用户需要写文章的权限  *def* new\_blog():  # 从请求获取JSON数据,创建Blog对象  b = Blog.from\_json(request.json)  b.author = g.current\_user # 作者为当前登录用户  db.session.add(b)  db.session.commit()  return jsonify(b.to\_json()), 201,\  {'Location': url\_for('api.get\_blog', *id*=b.id)} |

app/api/decorators.py：自定义装饰器，如permission\_required装饰器

|  |
| --- |
| from functools import wraps  from flask import g  from .errors import forbidden  *def* permission\_required(*p*):  *def* decorator(*f*):  @wraps(f)  *def* wrap(\**args*, \*\**kwargs*):  if not g.current\_user.can(p):  # 没有权限p,返回权限不足  return forbidden('Insufficient permissions')  return f(\*args, \*\*kwargs)  return wrap  return decorator |

博客文章PUT请求处理程序用来更新现有资源。

app/api/blogs.py：修改文章

|  |
| --- |
| from .errors import forbidden  @api.route('/blogs/<int:id>', *methods*=['PUT'])  @permission\_required(Permission.WRITE)  *def* edit\_blog(*id*):  b = Blog.query.get\_or\_404(id)  # 非作者和非管理员不能修改  if g.current\_user != b.author and \  not g.currrent\_user.can(Permission.ADMIN):  return forbidden('Insufficient permissions')  # 如果没有body值,用原来的  b.body = request.json.get('body', b.body)  db.session.add(b)  db.session.commit()  return jsonify(b.to\_json()) |

本程序暂时不允许删除文章，没有实现DELETE请求方法的处理程序。

⑦ 分页大型资源集合

对于大型资源集合，获取集合的GET请求消耗很大，和Web程序一样，Web服务也可以对集合分页。

app/api/blogs.py：分页文章资源

|  |
| --- |
| @api.route('/blogs/')  @auth.login\_required  *def* get\_blogs():  # 获取所有博客文章,JSON响应是这个集合的一部分  page = request.args.get('page', 1, *type*=*int*)  pagination = Blog.query.paginate(  page, *per\_page*=current\_app.config['BLOGS\_PER\_PAGE'],  *error\_out*=False)  blogs = pagination.items  # prev和next字段表示上一页和下一页资源的URL  prev, next = None, None  if pagination.has\_prev:  prev = url\_for('api.get\_blogs', *page*=page-1)  if pagination.has\_next:  next = url\_for('api.get\_blogs', *page*=page+1)  return jsonify({  'blogs': [b.to\_json() for b in blogs],  'prev': prev,  'next': next,  'count': pagination.total  }) |

⑧ 用户资源和评论资源与上面类似，该程序要实现的资源如下：

**Flasky API资源**

|  |  |  |
| --- | --- | --- |
| **资源URL** | **方法** | **说明** |
| /users/<int:id> | GET | 某个用户 |
| /users/<int:id>/blogs/ | GET | 某个用户所有文章 |
| /users/<int:id>/timeline/ | GET | 某个用户关注的用户发布的文章 |
| /blogs/ | GET、POST | 所有博客文章 |
| /blogs/<int:id> | GET、PUT | 某篇博客文章 |
| /blogs/<int:id>/comments/ | GET、POST | 某篇博客文章的所有评论 |
| /comments/ | GET | 所有评论 |
| /comments/<int:id> | GET | 一个评论 |

这些资源只允许客户端实现Web程序提供的部分功能。支持的资源可以按需扩展，如提供关注者资源、支持评论管理等。

app/api/users.py：用户资源

|  |
| --- |
| from flask import jsonify, request, current\_app, url\_for  from . import api  from ..models import User, Blog  @api.route('/users/<int:id>')  *def* get\_user(*id*): # 1.某个用户  user = User.query.get\_or\_404(id)  return jsonify(user.to\_json())  @api.route('/users/<int:id>/blogs/')  *def* get\_user\_blogs(*id*): # 2.该用户所有文章的分页  user = User.query.get\_or\_404(id)  page = request.args.get('page', 1, *type*=*int*)  pagination = user.blogs.order\_by(Blog.timestamp.desc()).paginate(  page, *per\_page*=current\_app.config['BLOGS\_PER\_PAGE'],  *error\_out*=False)  blogs = pagination.items  prev, next = None, None  if pagination.has\_prev:  prev = url\_for('api.get\_user\_blogs', *id*=id, *page*=page-1)  if pagination.has\_next:  next = url\_for('api.get\_user\_blogs', *id*=id, *page*=page+1)  return jsonify({  'blogs': [b.to\_json() for b in blogs],  'prev': prev,  'next': next,  'count': pagination.total  })  @api.route('/users/<int:id>/timeline/')  *def* get\_user\_followed\_blogs(*id*): # 3.该用户关注的大神的所有文章的分页  user = User.query.get\_or\_404(id)  page = request.args.get('page', 1, *type*=*int*)  pagination = user.followed\_blogs.order\_by(Blog.timestamp.desc()).paginate(  page, *per\_page*=current\_app.config['BLOGS\_PER\_PAGE'],  *error\_out*=False)  blogs = pagination.items  prev, next = None, None  if pagination.has\_prev:  prev = url\_for('api.get\_user\_followed\_blogs', *id*=id, *page*=page-1)  if pagination.has\_next:  next = url\_for('api.get\_user\_followed\_blogs', *id*=id, *page*=page+1)  return jsonify({  'blogs': [b.to\_json() for b in blogs],  'prev': prev,  'next': next,  'count': pagination.total  }) |

app/models.py：评论模型的to\_json()和from\_json()

|  |
| --- |
| *class* Comment(*db*.*Model*):  # ...  *def* to\_json(*self*):  return {  'url': url\_for('api.get\_comment', *id*=self.id),  'blog\_url': url\_for('api.get\_blog', *id*=self.blog\_id),  'body': self.body,  'body\_html': self.body\_html,  'timestamp': self.timestamp,  'author\_url': url\_for('api.get\_user', *id*=self.author\_id),  }  @*staticmethod*  *def* from\_json(*comment\_json*):  body = comment\_json.get('body')  if body is None or body == '':  raise ValidationError('木有评论！')  return Comment(*body*=body) |

app/api/comments.py：评论资源

|  |
| --- |
| from flask import jsonify, request, g, url\_for, current\_app  from .. import db  from ..models import Blog, Permission, Comment  from . import api  from .decorators import permission\_required  @api.route('/comments/')  *def* get\_comments(): # 1.所有评论的分页  page = request.args.get('page', 1, *type*=*int*)  pagination = Comment.query.order\_by(Comment.timestamp.desc()).paginate(  page, *per\_page*=current\_app.config['COMMENTS\_PER\_PAGE'],  *error\_out*=False)  comments = pagination.items  prev, next = None, None  if pagination.has\_prev:  prev = url\_for('api.get\_comments', *page*=page-1)  if pagination.has\_next:  next = url\_for('api.get\_comments', *page*=page+1)  return jsonify({  'comments': [c.to\_json() for c in comments],  'prev': prev,  'next': next,  'count': pagination.total  })  @api.route('/comments/<int:id>')  *def* get\_comment(*id*): # 2.获取某条评论  c = Comment.query.get\_or\_404(id)  return jsonify(c.to\_json())  @api.route('/blogs/<int:id>/comments/')  *def* get\_blog\_comments(*id*): # 3.某篇文章所有评论的分页  b = Blog.query.get\_or\_404(id)  page = request.args.get('page', 1, *type*=*int*)  pagination = b.comments.order\_by(Comment.timestamp.asc()).paginate(  page, *per\_page*=current\_app.config['COMMENTS\_PER\_PAGE'],  *error\_out*=False)  comments = pagination.items  prev, next = None, None  if pagination.has\_prev:  prev = url\_for('api.get\_blog\_comments', *id*=id, *page*=page-1)  if pagination.has\_next:  next = url\_for('api.get\_blog\_comments', *id*=id, *page*=page+1)  return jsonify({  'comments': [c.to\_json() for c in comments],  'prev': prev,  'next': next,  'count': pagination.total  })  @api.route('/blogs/<int:id>/comments/', *methods*=['POST'])  @permission\_required(Permission.COMMENT)  *def* new\_blog\_comment(*id*): # 4.创建新评论  b = Blog.query.get\_or\_404(id)  c = Comment.from\_json(request.json)  c.author = g.current\_user  c.blog = b  db.session.add(c)  db.session.commit()  return jsonify(c.to\_json()), 201, \  {'Location': url\_for('api.get\_comment', *id*=c.id)} |

// 这代码略重复啊...

⑨ 使用HTTPie测试Web服务

测试Web服务需要使用HTTP客户端，最常用的在命令行测试Web服务的客户端是curl和HTTPie。HTTPie的命令行更简洁，可读性高。

|  |
| --- |
| (venv) $ http --json --auth hikari\_python@163.com:aaa111 GET http://127.0.0.1:5000/api/v1/blogs/  HTTP/1.0 200 OK  Content-Length: 21286  Content-Type: application/json  Date: Thu, 17 May 2018 08:41:31 GMT  Server: Werkzeug/0.14.1 Python/3.6.4  {  "blogs": [  {  "author\_url": "/api/v1/users/1",  "body": "<h1>hello word</h1>",  "body\_html": "<h1>hello word</h1>",  "comment\_count": 107,  "comments\_url": "/api/v1/blogs/1/comments/",  "timestamp": "Fri, 11 May 2018 07:13:48 GMT",  "url": "/api/v1/blogs/1"  },...  ],  "count": 511,  "next": "/api/v1/blogs/?page=2",  "prev": null  } |

响应中有分页链接，显示第1也，没有上一页，有下一页URL和总数。

匿名用户发送空邮箱和密码：

|  |
| --- |
| (venv) $ http --json --auth : GET http://127.0.0.1:5000/api/v1/blogs/ |

发送POST请求添加一篇新文章：

|  |
| --- |
| (venv) $ http --auth 208343741@qq.com:1234 --json POST http://127.0.0.1:5000/api/v1/blogs/ "body=在下在用\*\*命令行\*\*添加一篇博客文章。"  HTTP/1.0 201 CREATED  Content-Length: 446  Content-Type: application/json  Date: Thu, 17 May 2018 08:58:44 GMT  Location: http://127.0.0.1:5000/api/v1/blogs/515  Server: Werkzeug/0.14.1 Python/3.6.4  {  "author\_url": "/api/v1/users/2",  "body": "在下在用\*\*命令行\*\*添加一篇博客文章。",  "body\_html": "<p>在下在用<strong>命令行</strong>添加一篇博客文章。</p>",  "comment\_count": 0,  "comments\_url": "/api/v1/blogs/515/comments/",  "timestamp": "Thu, 17 May 2018 08:58:44 GMT",  "url": "/api/v1/blogs/515"  } |

// 卡了，多敲了几次回车，结果插了好几条...

使用认证令牌：

|  |
| --- |
| (venv) $ http --auth hikari\_python@163.com:aaa111 --json POST http://127.0.0.1:5000/api/v1/tokens/  HTTP/1.0 200 OK  Content-Length: 163  Content-Type: application/json  Date: Thu, 17 May 2018 09:07:54 GMT  Server: Werkzeug/0.14.1 Python/3.6.4  {  "expiration": 3600,  "token": "eyJhbGciOiJIUzI1NiIsImlhdCI6MTUyNjU0ODA3NCwiZXhwIjoxNTI2NTUxNj..."  } |

可用此令牌访问API，默认有效时间为1h，如创建评论：

|  |
| --- |
| (venv) $ http --auth eyJhbGciOiJIU...: --json POST http://127.0.0.1:5000/api/v1/blogs/515/comments/ "body=## hello, test from cmdline" |

令牌过期后，请求返回401错误，表示需要获取新令牌。

/\* 一脸懵逼，感觉还是不怎么理解REST API，大概是提供统一接口为Web、iOS、Android等不同平台服务?同一个URL不同请求方法使用不同视图函数? \*/