

第 1 章 Flask 安装

[Flask](#) 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](#) 提供; 模板系统由 [Jinja2](#) 提供。[Werkzeug](#) 和 [Jinja2](#) 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。

```
< > ↻ ☆ 127.0.0.1:8888 < > ↻ ☆ 127.0.0.1:8888/user/hikari < > ↻ ☆ 127.0.0.1:8888/user/6
```

hello world! hello, hikari! hello, maki!

✧ 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
<code>current_app</code>	程序上下文	当前激活程序的程序实例
<code>g</code>	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
<code>request</code>	请求上下文	请求对象，封装了客户端发出的 HTTP 请求内容
<code>session</code>	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:

```


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


```

user.html:

```


# {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 '`<h1>maki</h1>`', 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)

```

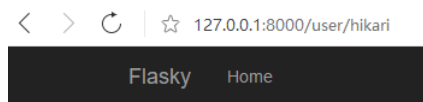
user.html:

```

{% 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:



hello, hikari!

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`hikari`

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`

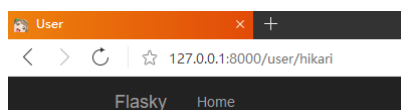
Flask 默认在程序根目录的 `static` 子目录寻找静态文件。

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` 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：

时间：2018年05月02日 周三 17:06:48

时间：2018年5月2日星期三下午5点06分

那是1 分钟前。

`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](#)学习全部格式化选项。

第 4 章 Web 表单

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** 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：

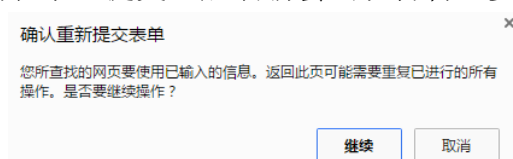
Hello, Stranger!	Hello, hikari!
<input type="text"/>	<input type="text"/>
<input type="submit" value="提交"/>	<input type="submit" value="提交"/>

不输入直接提交，提示：

请填写此字段。

✧ 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 %}
```

你似乎改名字了!

Hello, maki!

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

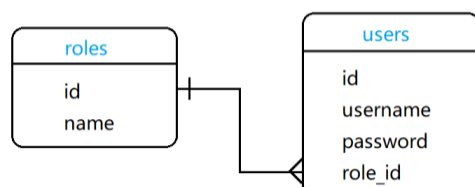
数据库按照一定规则保存数据，程序发起查询取回所需的数据。Web 程序最常用基于 [关系模型](#) 的数据库，也称为 SQL 数据库，因为它们使用结构化查询语言。不过最近几年 [文档数据库](#) 和 [键值对数据库](#) 成了流行的替代选择，这两种合称

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：



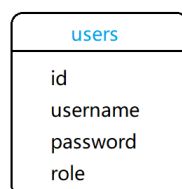
roles 表可用的用户角色，每种角色都有唯一 **id**；**users** 表是用户列表，每个用户也都有唯一 **id**，还有一个外键 **role_id** 引用 **roles** 表的 **id**，指定每个用户角色。

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些的损耗。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](#), 其集成了 [SQLAlchemy](#) 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	<i>mysql://username:password@hostname/database</i>
Postgres	<i>postgresql://username:password@hostname/database</i>
SQLite(Unix)	<i>sqlite:///absolute/path/to/database</i>
SQLite(Windows)	<i>sqlite:///c:/absolute/path/to/database</i>

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
<code>filter()</code>	把过滤器添加到原查询上，返回一个新查询
<code>filter_by()</code>	把等值过滤器添加到原查询上，返回一个新查询
<code>limit()</code>	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
<code>offset()</code>	偏移原查询返回的结果，返回一个新查询
<code>order_by()</code>	根据指定条件对原查询结果进行排序，返回一个新查询
<code>group_by()</code>	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
<code>all()</code>	以列表形式返回查询的所有结果
<code>first()</code>	返回查询的第一个结果; 没有返回 <code>None</code>
<code>first_or_404()</code>	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
<code>get()</code>	返回指定主键对应的行, 没有则返回 <code>None</code>
<code>get_or_404()</code>	返回指定主键对应的行, 没有则终止请求, 返回 404 错误响应
<code>count()</code>	返回查询结果的数量
<code>paginate()</code>	返回一个 <code>Paginate</code> 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](#)；[Flask-Migrate](#) 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.
```

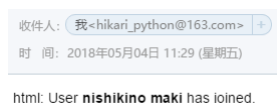
templates/mail/new_user.txt:

```
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](#) 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 # 返回创建的程序实例
```

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 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$77ed2de287d2361ca0da4b912e4d376d26d1a71f6b4d9b0b67b8ab16414
9aadf'
>>> u.verify_password('maki')
True
>>> u.verify_password('rin')
False
>>> u2 = User()
>>> u2.password = 'maki'
>>> u2.password_hash
'pbkdf2:sha256:50000$QNjbn8eL$1fd34f7b2019c36ce8b9097ff678860703f2e7a2cf3571e3e69d2e9c54d
ebedc'

```

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

邮箱

密码

☐ 记住我

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'eyJhbGciOiJIUzI1NiIsImIhdCI6MTUyNTY4Mjg0OSwiZXhwIjoxNTI1Njg2NDE5fQ.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什么操作。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：

你好, python!

你的账号还没激活!

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。

没收到邮件? [点击重新发送](#)

// 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:

你好, python!

欢迎注册 **hikari app**!

[点击此处](#)激活你的账号。

你也可以将下面链接复制到浏览器的地址栏:

<http://127.0.0.1:5000/auth/confirm/eyJhbGciOiJIUzI1NiIsImhhdCI6MTUyNTc5MDgzOSwiZXhwIjoxNTI1Nzk0NDM5fQ.eyJjb25maXJtIjoyNH0.1zTg8f7dndHLUXEsIjbreidw2erpOZBJCtdPn1rx1N5w>

感谢注册!

from hikari

注: hikari是不会看对这封邮件的回复的!

点击 [click here](#) 链接:

你已经账号已通过认证!

Hello, python !

✧ 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:

☐ 记住我

[忘记密码?](#)

新用户? [点击注册](#)

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` 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