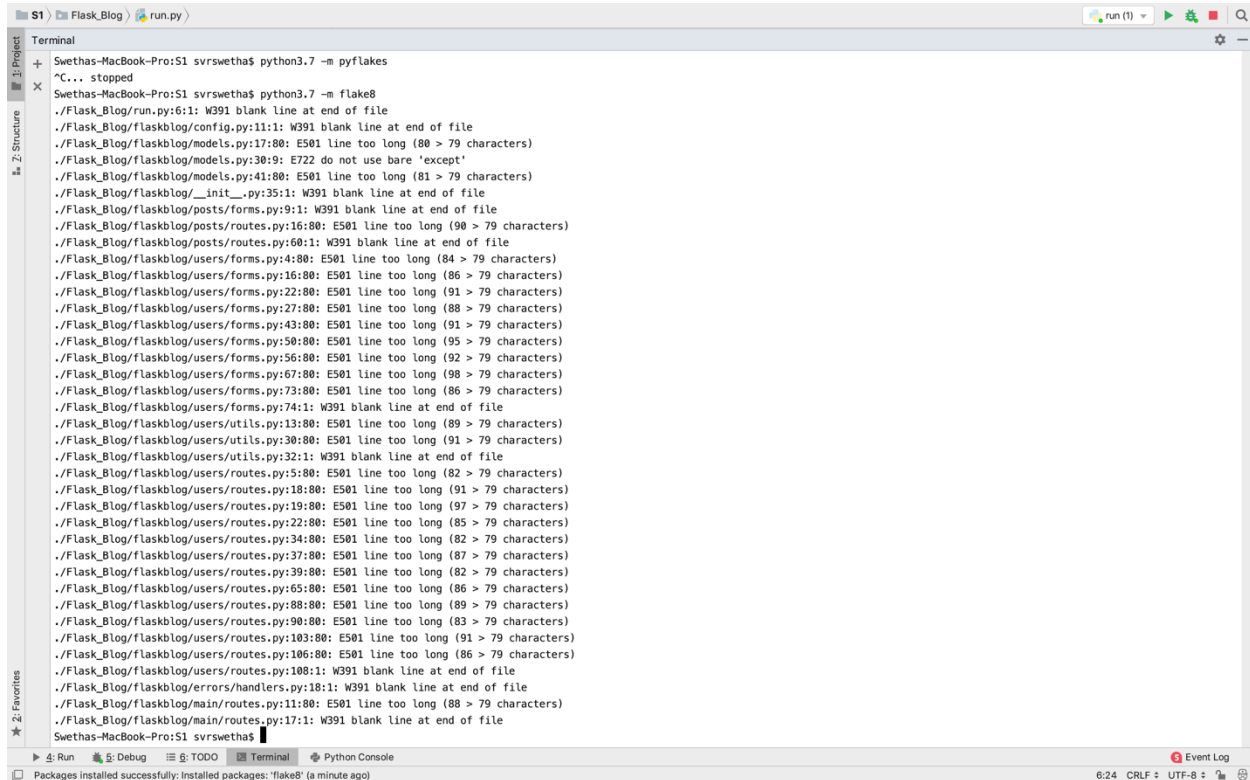# Secure Programming Assignment 4

Reviewer- Swetha Vijaya Raghavan

Reviewed – Karan Pandya

I have used two python code linter tools like flake8(Which is "the wrapper which verifies pep8, pyflakes and circular complexity ". It has low rate of false positives) and pylint. I have even provided the solution for few errors. The below screenshot provides errors/vulnerabilities concerned with the program using flake8.

Using pylint, the following screenshots gives all the vulnerabilities/errors within the program.

The following errors such as Missing-final-newline, SQLAlchemy, missing docstring (missing class docstring, missing module docstring), bare-except, Instance of 'SQLAlchemy' has no 'Table' member (no-member).

SQLAlchemy(Stackoverflow)

The underlying db-api library for sql database escapes parameters. SQLAlchemy simply passes the statement and parameters to execute, the driver does whatever is needed. If the programmer is not writing raw SQL that includes parameters, the code is not vulnerable to injection. For missing docstring, it can be fixed, at each line one of the code, before any imports we can have a doc string saying what the program does, example:
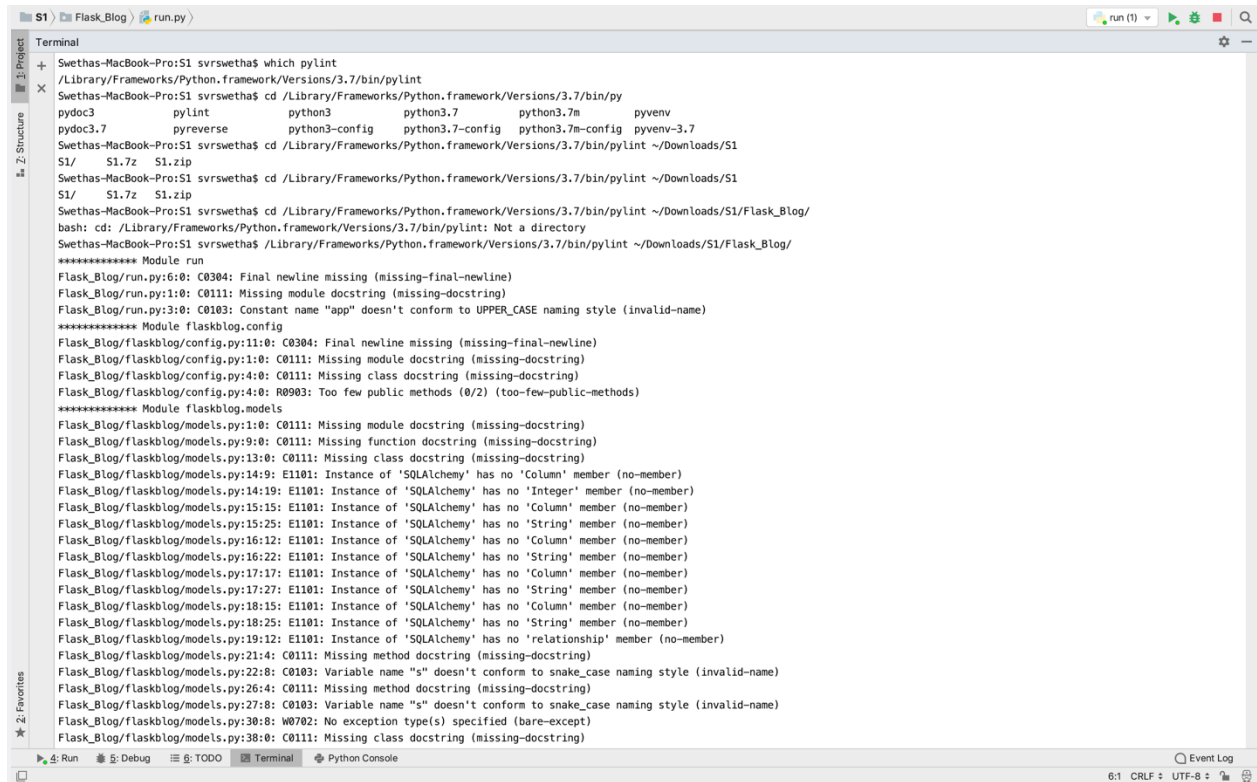
```
'''RIG, Reddit Image Grabber '''
import os
import urllib.request as web
import praw
```


Too few public methods: (Source: Wikipedia)

Too few public methods mean the class is a dictionary and aren't meant to just store data. It should have at least a few methods to operate on the data that they hold. The reason for pyflakes failing is that an imported variable is tested by exec, not directly. The reasons for pylint and PyChecker failing are for acceptable reasons.

- R: 44, 0: Too few public methods (1/2) (too-few-public-methods)
- W:212,19: Used * or ** magic (star-args)
- W:212,31: Used * or ** magic (star-args)
- W:217,19: Unused argument 'self' (unused-argument)
- W:254,11: Use of eval (eval-used)
- W:267, 8: Used * or ** magic (star-args)
- W:270, 8: Used * or ** magic (star-args)
- W:249, 4: Unused import version_info (unused-import)

```
Terminal

Swethas-MacBook-Pro:S1 svrswetha$ which pylint
/Library/Frameworks/Python.framework/Versions/3.7/bin/pylint
Swethas-MacBook-Pro:S1 svrswetha$ cd /Library/Frameworks/Python.framework/Versions/3.7/bin/py
pydoc3          pylint          python3         python3.7       python3.7m      pyvenv
pydoc3.7        pyreverse       python3-config  python3.7-config python3.7m-config pyvenv-3.7
Swethas-MacBook-Pro:S1 svrswetha$ cd /Library/Frameworks/Python.framework/Versions/3.7/bin/pylint ~/Downloads/S1
S1/     S1.7z   S1.zip
Swethas-MacBook-Pro:S1 svrswetha$ cd /Library/Frameworks/Python.framework/Versions/3.7/bin/pylint ~/Downloads/S1
S1/     S1.7z   S1.zip
Swethas-MacBook-Pro:S1 svrswetha$ cd /Library/Frameworks/Python.framework/Versions/3.7/bin/pylint ~/Downloads/S1/Flask_Blog/
bash: cd: /Library/Frameworks/Python.framework/Versions/3.7/bin/pylint: Not a directory
Swethas-MacBook-Pro:S1 svrswetha$ /Library/Frameworks/Python.framework/Versions/3.7/bin/pylint ~/Downloads/S1/Flask_Blog/
************** Module run
Flask_Blog/run.py:6:0: C0304: Final newline missing (missing-final-newline)
Flask_Blog/run.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/run.py:3:0: C0103: Constant name "app" doesn't conform to UPPER_CASE naming style (invalid-name)
************** Module flaskblog.config
Flask_Blog/flaskblog/config.py:11:0: C0304: Final newline missing (missing-final-newline)
Flask_Blog/flaskblog/config.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/config.py:4:0: C0111: Missing class docstring (missing-docstring)
Flask_Blog/flaskblog/config.py:4:0: R0903: Too few public methods (0/2) (too-few-public-methods)
************** Module flaskblog.models
Flask_Blog/flaskblog/models.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/models.py:9:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/models.py:13:0: C0111: Missing class docstring (missing-docstring)
Flask_Blog/flaskblog/models.py:14:9: E1101: Instance of 'SQLAlchemy' has no 'Column' member (no-member)
Flask_Blog/flaskblog/models.py:14:19: E1101: Instance of 'SQLAlchemy' has no 'Integer' member (no-member)
Flask_Blog/flaskblog/models.py:15:15: E1101: Instance of 'SQLAlchemy' has no 'Column' member (no-member)
Flask_Blog/flaskblog/models.py:15:25: E1101: Instance of 'SQLAlchemy' has no 'String' member (no-member)
Flask_Blog/flaskblog/models.py:16:12: E1101: Instance of 'SQLAlchemy' has no 'Column' member (no-member)
Flask_Blog/flaskblog/models.py:16:22: E1101: Instance of 'SQLAlchemy' has no 'String' member (no-member)
Flask_Blog/flaskblog/models.py:17:17: E1101: Instance of 'SQLAlchemy' has no 'Column' member (no-member)
Flask_Blog/flaskblog/models.py:17:27: E1101: Instance of 'SQLAlchemy' has no 'String' member (no-member)
Flask_Blog/flaskblog/models.py:18:15: E1101: Instance of 'SQLAlchemy' has no 'Column' member (no-member)
Flask_Blog/flaskblog/models.py:18:25: E1101: Instance of 'SQLAlchemy' has no 'String' member (no-member)
Flask_Blog/flaskblog/models.py:19:12: E1101: Instance of 'SQLAlchemy' has no 'relationship' member (no-member)
Flask_Blog/flaskblog/models.py:21:4: C0111: Missing method docstring (missing-docstring)
Flask_Blog/flaskblog/models.py:22:8: C0103: Variable name "s" doesn't conform to snake_case naming style (invalid-name)
Flask_Blog/flaskblog/models.py:26:4: C0111: Missing method docstring (missing-docstring)
Flask_Blog/flaskblog/models.py:27:8: C0103: Variable name "s" doesn't conform to snake_case naming style (invalid-name)
Flask_Blog/flaskblog/models.py:30:8: W0702: No exception type(s) specified (bare-except)
Flask_Blog/flaskblog/models.py:38:0: C0111: Missing class docstring (missing-docstring)
```

```
4: Run    5: Debug    6: TODO    Terminal    Python Console                                      Event Log
                                                                              6:1  CRLF  UTF-8
```

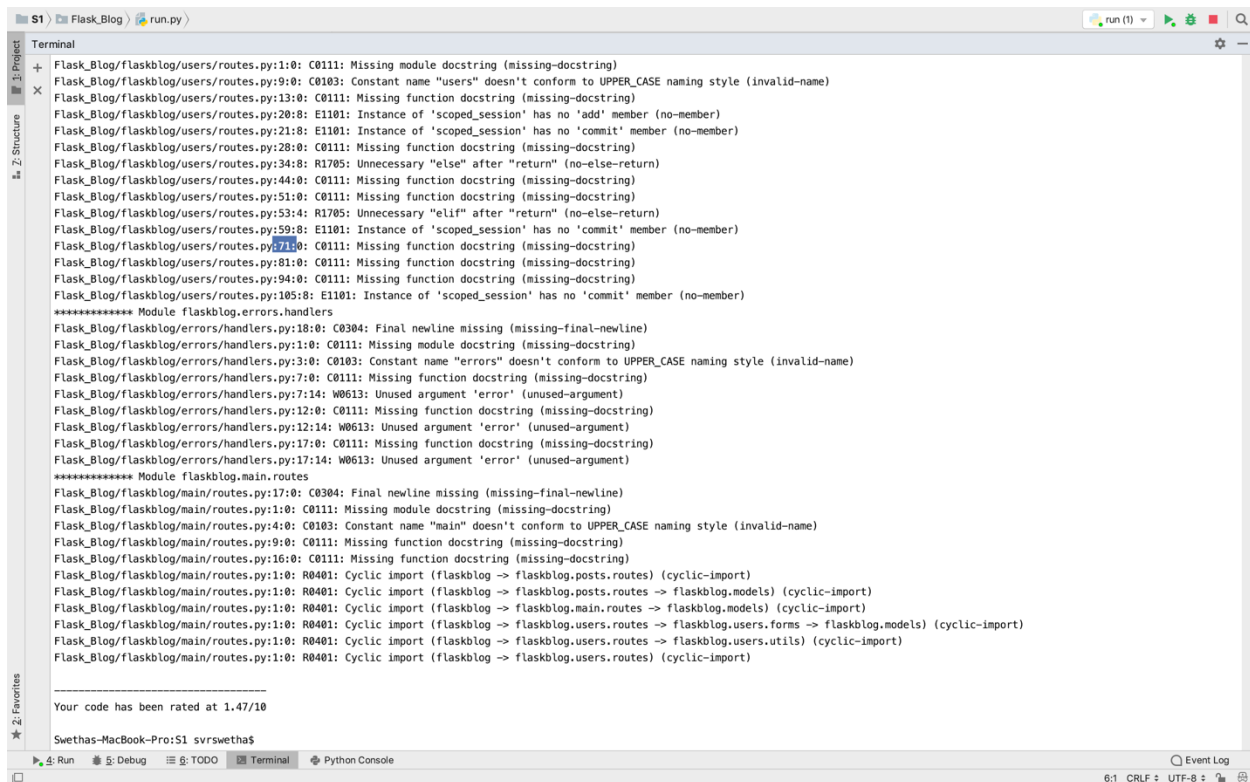Instance of 'SQLAlchemy' has no 'Table' member(no-member). The solution is:

pylint --generate-rcfile>~/.config/pylintrc

and then findout the **ignored-modules** line, rewrite it to: **ignored - modules=flask_sqlalchemy.** All the E1101 errors will be gone.

Terminal

```
Flask_Blog/flaskblog/models.py:38:0: C0111: Missing class docstring (missing-docstring)
Flask_Blog/flaskblog/models.py:39:9: E1101: Instance of 'SQLAlchemy' has no 'Column' member (no-member)
Flask_Blog/flaskblog/models.py:39:19: E1101: Instance of 'SQLAlchemy' has no 'Integer' member (no-member)
Flask_Blog/flaskblog/models.py:40:12: E1101: Instance of 'SQLAlchemy' has no 'Column' member (no-member)
Flask_Blog/flaskblog/models.py:40:22: E1101: Instance of 'SQLAlchemy' has no 'String' member (no-member)
Flask_Blog/flaskblog/models.py:41:18: E1101: Instance of 'SQLAlchemy' has no 'Column' member (no-member)
Flask_Blog/flaskblog/models.py:41:28: E1101: Instance of 'SQLAlchemy' has no 'DateTime' member (no-member)
Flask_Blog/flaskblog/models.py:42:14: E1101: Instance of 'SQLAlchemy' has no 'Column' member (no-member)
Flask_Blog/flaskblog/models.py:42:24: E1101: Instance of 'SQLAlchemy' has no 'Text' member (no-member)
Flask_Blog/flaskblog/models.py:43:14: E1101: Instance of 'SQLAlchemy' has no 'Column' member (no-member)
Flask_Blog/flaskblog/models.py:43:24: E1101: Instance of 'SQLAlchemy' has no 'Integer' member (no-member)
Flask_Blog/flaskblog/models.py:43:36: E1101: Instance of 'SQLAlchemy' has no 'ForeignKey' member (no-member)
Flask_Blog/flaskblog/models.py:38:0: R0903: Too few public methods (1/2) (too-few-public-methods)
Flask_Blog/flaskblog/models.py:5:0: C0411: third party import "from flask_login import UserMixin" should be placed before "from flaskblog import db, login_manager" (wrong-import-order)
************** Module flaskblog.__init__
Flask_Blog/flaskblog/__init__.py:35:0: C0304: Final newline missing (missing-final-newline)
************** Module flaskblog
Flask_Blog/flaskblog/__init__.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/__init__.py:9:0: C0103: Constant name "db" doesn't conform to UPPER_CASE naming style (invalid-name)
Flask_Blog/flaskblog/__init__.py:10:0: C0103: Constant name "bcrypt" doesn't conform to UPPER_CASE naming style (invalid-name)
Flask_Blog/flaskblog/__init__.py:11:0: C0103: Constant name "login_manager" doesn't conform to UPPER_CASE naming style (invalid-name)
Flask_Blog/flaskblog/__init__.py:14:0: C0103: Constant name "mail" doesn't conform to UPPER_CASE naming style (invalid-name)
Flask_Blog/flaskblog/__init__.py:17:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/__init__.py:17:15: W0613: Unused argument 'config_class' (unused-argument)
************** Module flaskblog.posts.forms
Flask_Blog/flaskblog/posts/forms.py:9:0: C0304: Final newline missing (missing-final-newline)
Flask_Blog/flaskblog/posts/forms.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/posts/forms.py:6:0: C0111: Missing class docstring (missing-docstring)
************** Module flaskblog.posts.routes
Flask_Blog/flaskblog/posts/routes.py:60:0: C0304: Final newline missing (missing-final-newline)
Flask_Blog/flaskblog/posts/routes.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/posts/routes.py:8:0: C0103: Constant name "posts" doesn't conform to UPPER_CASE naming style (invalid-name)
Flask_Blog/flaskblog/posts/routes.py:16:8: W0621: Redefining name 'post' from outer scope (line 26) (redefined-outer-name)
Flask_Blog/flaskblog/posts/routes.py:13:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/posts/routes.py:17:8: E1101: Instance of 'scoped_session' has no 'add' member (no-member)
Flask_Blog/flaskblog/posts/routes.py:18:8: E1101: Instance of 'scoped_session' has no 'commit' member (no-member)
Flask_Blog/flaskblog/posts/routes.py:27:4: W0621: Redefining name 'post' from outer scope (line 26) (redefined-outer-name)
Flask_Blog/flaskblog/posts/routes.py:26:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/posts/routes.py:34:4: W0621: Redefining name 'post' from outer scope (line 26) (redefined-outer-name)
Flask_Blog/flaskblog/posts/routes.py:33:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/posts/routes.py:38:4: R1705: Unnecessary "elif" after "return" (no-else-return)
Flask_Blog/flaskblog/posts/routes.py:41:8: E1101: Instance of 'scoped_session' has no 'commit' member (no-member)
```

4: Run   5: Debug   6: TODO   Terminal   Python Console   Event Log
6:1   CRLF   UTF-8

In _init_.py, there are many possible vulnerabilities. There is Unnecessary "elif" after "return" (no-else-return) in routes.py. There are many as such listed above in the screenshot.

Terminal

```
Flask_Blog/flaskblog/posts/routes.py:41:8: E1101: Instance of 'scoped_session' has no 'commit' member (no-member)
Flask_Blog/flaskblog/posts/routes.py:54:4: W0621: Redefining name 'post' from outer scope (line 26) (redefined-outer-name)
Flask_Blog/flaskblog/posts/routes.py:53:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/posts/routes.py:57:4: E1101: Instance of 'scoped_session' has no 'delete' member (no-member)
Flask_Blog/flaskblog/posts/routes.py:58:4: E1101: Instance of 'scoped_session' has no 'commit' member (no-member)
************** Module flaskblog.users.forms
Flask_Blog/flaskblog/users/forms.py:74:0: C0304: Final newline missing (missing-final-newline)
Flask_Blog/flaskblog/users/forms.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/users/forms.py:9:0: C0111: Missing class docstring (missing-docstring)
Flask_Blog/flaskblog/users/forms.py:19:4: C0111: Missing method docstring (missing-docstring)
Flask_Blog/flaskblog/users/forms.py:19:4: R0201: Method could be a function (no-self-use)
Flask_Blog/flaskblog/users/forms.py:24:4: C0111: Missing method docstring (missing-docstring)
Flask_Blog/flaskblog/users/forms.py:24:4: R0201: Method could be a function (no-self-use)
Flask_Blog/flaskblog/users/forms.py:30:0: C0111: Missing class docstring (missing-docstring)
Flask_Blog/flaskblog/users/forms.py:38:0: C0111: Missing class docstring (missing-docstring)
Flask_Blog/flaskblog/users/forms.py:46:4: C0111: Missing method docstring (missing-docstring)
Flask_Blog/flaskblog/users/forms.py:46:4: R0201: Method could be a function (no-self-use)
Flask_Blog/flaskblog/users/forms.py:52:4: C0111: Missing method docstring (missing-docstring)
Flask_Blog/flaskblog/users/forms.py:52:4: R0201: Method could be a function (no-self-use)
Flask_Blog/flaskblog/users/forms.py:59:0: C0111: Missing class docstring (missing-docstring)
Flask_Blog/flaskblog/users/forms.py:64:4: C0111: Missing method docstring (missing-docstring)
Flask_Blog/flaskblog/users/forms.py:64:4: R0201: Method could be a function (no-self-use)
Flask_Blog/flaskblog/users/forms.py:70:0: C0111: Missing class docstring (missing-docstring)
************** Module flaskblog.users.utils
Flask_Blog/flaskblog/users/utils.py:32:0: C0304: Final newline missing (missing-final-newline)
Flask_Blog/flaskblog/users/utils.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/users/utils.py:9:0: C0111: Missing class docstring (missing-docstring)
Flask_Blog/flaskblog/users/utils.py:23:0: C0111: Missing function docstring (missing-docstring)
************** Module flaskblog.users.routes
Flask_Blog/flaskblog/users/routes.py:108:0: C0304: Final newline missing (missing-final-newline)
Flask_Blog/flaskblog/users/routes.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:9:0: C0103: Constant name "users" doesn't conform to UPPER_CASE naming style (invalid-name)
Flask_Blog/flaskblog/users/routes.py:13:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:20:8: E1101: Instance of 'scoped_session' has no 'add' member (no-member)
Flask_Blog/flaskblog/users/routes.py:21:8: E1101: Instance of 'scoped_session' has no 'commit' member (no-member)
Flask_Blog/flaskblog/users/routes.py:28:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:34:8: R1705: Unnecessary "else" after "return" (no-else-return)
Flask_Blog/flaskblog/users/routes.py:44:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:51:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:53:4: R1705: Unnecessary "elif" after "return" (no-else-return)
Flask_Blog/flaskblog/users/routes.py:59:8: E1101: Instance of 'scoped_session' has no 'commit' member (no-member)
Flask_Blog/flaskblog/users/routes.py:71:0: C0111: Missing function docstring (missing-docstring)
```

4: Run   5: Debug   6: TODO   Terminal   Python Console   Event Log
6:1   CRLF   UTF-8

```
Flask_Blog/flaskblog/users/routes.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:9:0: C0103: Constant name "users" doesn't conform to UPPER_CASE naming style (invalid-name)
Flask_Blog/flaskblog/users/routes.py:13:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:20:8: E1101: Instance of 'scoped_session' has no 'add' member (no-member)
Flask_Blog/flaskblog/users/routes.py:21:8: E1101: Instance of 'scoped_session' has no 'commit' member (no-member)
Flask_Blog/flaskblog/users/routes.py:28:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:34:8: R1705: Unnecessary "else" after "return" (no-else-return)
Flask_Blog/flaskblog/users/routes.py:44:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:51:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:53:4: R1705: Unnecessary "elif" after "return" (no-else-return)
Flask_Blog/flaskblog/users/routes.py:59:8: E1101: Instance of 'scoped_session' has no 'commit' member (no-member)
Flask_Blog/flaskblog/users/routes.py:71:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:81:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:94:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/users/routes.py:105:8: E1101: Instance of 'scoped_session' has no 'commit' member (no-member)
************** Module flaskblog.errors.handlers
Flask_Blog/flaskblog/errors/handlers.py:18:0: C0304: Final newline missing (missing-final-newline)
Flask_Blog/flaskblog/errors/handlers.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/errors/handlers.py:3:0: C0103: Constant name "errors" doesn't conform to UPPER_CASE naming style (invalid-name)
Flask_Blog/flaskblog/errors/handlers.py:7:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/errors/handlers.py:7:14: W0613: Unused argument 'error' (unused-argument)
Flask_Blog/flaskblog/errors/handlers.py:12:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/errors/handlers.py:12:14: W0613: Unused argument 'error' (unused-argument)
Flask_Blog/flaskblog/errors/handlers.py:17:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/errors/handlers.py:17:14: W0613: Unused argument 'error' (unused-argument)
************** Module flaskblog.main.routes
Flask_Blog/flaskblog/main/routes.py:17:0: C0304: Final newline missing (missing-final-newline)
Flask_Blog/flaskblog/main/routes.py:1:0: C0111: Missing module docstring (missing-docstring)
Flask_Blog/flaskblog/main/routes.py:4:0: C0103: Constant name "main" doesn't conform to UPPER_CASE naming style (invalid-name)
Flask_Blog/flaskblog/main/routes.py:9:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/main/routes.py:16:0: C0111: Missing function docstring (missing-docstring)
Flask_Blog/flaskblog/main/routes.py:1:0: R0401: Cyclic import (flaskblog -> flaskblog.posts.routes) (cyclic-import)
Flask_Blog/flaskblog/main/routes.py:1:0: R0401: Cyclic import (flaskblog -> flaskblog.posts.routes -> flaskblog.models) (cyclic-import)
Flask_Blog/flaskblog/main/routes.py:1:0: R0401: Cyclic import (flaskblog -> flaskblog.main.routes -> flaskblog.models) (cyclic-import)
Flask_Blog/flaskblog/main/routes.py:1:0: R0401: Cyclic import (flaskblog -> flaskblog.users.routes -> flaskblog.users.forms -> flaskblog.models) (cyclic-import)
Flask_Blog/flaskblog/main/routes.py:1:0: R0401: Cyclic import (flaskblog -> flaskblog.users.routes -> flaskblog.users.utils) (cyclic-import)
Flask_Blog/flaskblog/main/routes.py:1:0: R0401: Cyclic import (flaskblog -> flaskblog.users.routes) (cyclic-import)

---------------------------------
Your code has been rated at 1.47/10

Swethas-MacBook-Pro:S1 svrswetha$
```

The code has been rated at 1.47/10. All the above screenshots are obtained using pylint and flake8.

```
    id INTEGER NOT NULL,
    title VARCHAR(100) NOT NULL,
    date_posted DATETIME NOT NULL,
    content TEXT NOT NULL,
    user_id INTEGER NOT NULL,
    PRIMARY KEY (id),
    FOREIGN KEY(user_id) REFERENCES user (id)
)▯~  ▯_tableuseruser CREATE TABLE user (
    id INTEGER NOT NULL,
    username VARCHAR(20) NOT NULL,
    email VARCHAR(120) NOT NULL,
    image_file VARCHAR(20) NOT NULL,
    password VARCHAR(60) NOT NULL,
    PRIMARY KEY (id),
    UNIQUE (username),
    UNIQUE (email)
)'  ; ▯indexsqlite_autoindex_user_2user '  ; ▯indexsqlite_autoindex_user_1user ▯▯▯▯▯▯
```

Sql injection: (Source: quora, stackoverflow) The above sql tables in sites.db may result in sql injection. %s simply is a string formatting syntax. It can be understood as a placeholder which will be evaluated as string when executed. As it is formatted as string, any passed executable (and possibly dangerous) statement, e.g. like where username = 'admin' will be actually a whole string in your execution and no interpreted code statement. **References** are Below:
https://stackoverflow.com/questions/31949733/is-a-sqlalchemy-query-vulnerable-to-injection-attacks, https://www.quora.com/How-does-s-prevent-SQL-injection-in-Python
https://stackoverflow.com/questions/7877522/how-do-i-disable-missing-docstring-warnings-at-a-file-level-in-pylint