Отчет по (Security Misconfiguration - 15.7.2 - 15)

Tester's name: Stanley Ford

Lab No. "15.7.2" :

- General information:
  - Testing period: 02.02.2023
  - Test object: http://51.250.73.193:8083/
- Description of actions:

  In general, you can do everything in a simple and manual way. It was mentioned that there are some doubts about the app.py file. Next, I addressed it directly, via the URL, assigning app.py after the slash.

```
from flask import Flask
from flask_login import LoginManager
from models import db


def create_app():
    app = Flask(__name__, static_folder='.', static_url_path='')

    db.create_all()

    app.config['SECRET_KEY'] = 'flag{B3_C@r3fu11y_with_st@tic_p@th}' # This is flag

    login_manager = LoginManager()
    login_manager.login_view = 'auth.login'
    login_manager.init_app(app)

    from models import User

    @login_manager.user_loader
    def load_user(user_id):
        # since the user_id is just the primary key of our user table, use it in the query for the user
        return db.query(User).get(int(user_id))

    # blueprint for auth routes in our app
    from auth import auth as auth_blueprint
    app.register_blueprint(auth_blueprint)

    # blueprint for non-auth parts of app
    from main import main as main_blueprint
    app.register_blueprint(main_blueprint)

    app.run(host='0.0.0.0', debug=False, port=80)


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

  So, the very possibility of viewing the code is already alarming. Not a good practice. However, let's take a look: the static folder is specified as ".", i.e. the root folder, and this is already an incorrect configuration of the web server. That must have been the default.

  You could use scanners like dirbuster, burp to find some more files in the project. And, most likely, there would also be such carelessness with the settings, but the brutting process would take some time. And so, the result is visible in just one action.

  In the same file, there is also a secret flag that needs to be found:
  flag{B3_C@r3fu11y_with_st@tic_p@th}

  At this stage, the laboratory can be considered completed.

Self-Assessment Questions:

- List the tools (programs and utilities) that you used to solve this lab:Web browser (Google Chrome)

- List the vulnerabilities you were able to find:Security Misconfiguration

- Give advice on how to improve security:

  Do not leave credentials in configs. Pay attention to the default settings and, where possible, change them to restrict access.