Documentation of security improvements

Application code

Hash password before store to database

```
import bcrypt
```

```
    password = data.get('password')  # SECURITY ISSUE: Password stored in
plaintext
    hash_password = bcrypt.hashpw(password.encode("utf-8"),
bcrypt.gensalt(rounds=12))
```

Validate input

```
from validator_collection import is_email, is_string
```

```
    # SECURITY ISSUE: No input validation
    username = data.get('username')
    password = data.get('password')  # SECURITY ISSUE: Password stored in
plaintext
    hash_password = bcrypt.hashpw(password.encode("utf-8"),
bcrypt.gensalt(rounds=12))
    email = data.get('email')
    if is_string(username, minimum_length=3, maximum_length=20) == False:
        raise Exception("Invalid username string pattern.")
    if is_email(email) == False:
        raise Exception("Invalid email pattern.")
```

Prevent SQL injection

```
        # SECURITY ISSUE: SQL Injection vulnerability
        query = "INSERT INTO users (username, password, email) VALUES ('?', '?',
'?')"
        cursor.execute(query, (username, hash_password, email))
        conn.commit()
```

```
    # SECURITY ISSUE: SQL Injection vulnerability
    cursor.execute("SELECT id, username, email FROM users WHERE username LIKE ?",
(f"%{query}%",))
```

Get DEBUG value from environment for manage debug mode

Run application on single interface instead of all interfaces

```
    # SECURITY ISSUE: Debug mode enabled
    debug_mode = os.environ.get("DEBUG", "False") == True
    app.run(host='127.0.0.1', port=int(os.environ.get('PORT', 5000)),
debug=debug_mode)
```

Application dependencies

Use newest version for each dependencies and specify library version

```
flask==3.1.0
# SECURITY ISSUE: Outdated package with known vulnerabilities
werkzeug==3.1.3
# SECURITY ISSUE: Pinned to vulnerable version
Jinja2==3.1.6
# SECURITY ISSUE: No version pinning
requests==2.32.3
# SECURITY ISSUE: Using development libraries in production
pytest==8.3.5
# Dependencies for the application
gunicorn==23.0.0

# password security
bcrypt==4.3.0
# input validation
validator_collection==1.5.0
```