Bank.powerzio.net vulnerabilities

MD5 encryption :

The app is using md5 encryption. MD5 has been cryptographically broken and considered insecure.

```
def md5(v):
    return hashlib.md5(v.encode()).hexdigest()
```

It should not be used for any type of encryption.

Developement mode :

The serveur is running in development mode.

```
 * Serving Flask app 'server'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://172.20.0.2:5000
Press CTRL+C to quit
```

It should be running in production mode for security purpose.

JWT Secret Token :

The JWT secret token is stored in the server.py.

```
JWT_SECRET='eexoo0Vahzuz0eech3aigoh3iez1iePh'
```

This Token should be stored in a safer place like an environment variable or Key Management Service.

Session Cookie :

The session cookie is set here :

```
resp.set_cookie('mb_session_id', token)
```

It is not set with the « Secure » and « httpOnly ». It should because it would prevent XSS attack from stealing the cookie and not send it through http so it cannot be intercepted on a rogue wifi.