Web-based Appointment Scheduling and Management Information System (ASMIS)

TESTING REPORT

Test case 1: User credential verification and two factor authentication.

Procedure

Provide correct user credentials and confirm OTP using the first demo account (see readme file).

Expected Outcome

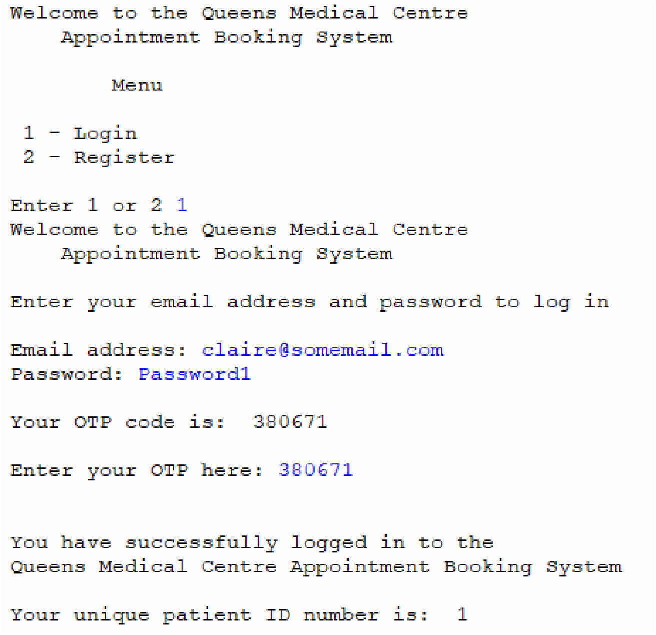
The system should provide an OTP following entry of validated user credentials. If the OTP is correctly validated, the system allows access to the Patient Menu. In the prototype, this consists of a welcome message and display of the user's unique patient id.

If incorrect user credentials are entered, an error message is displayed, and they are requested again; there is no indication of which credential was incorrect.

If an incorrect, or expired OTP is entered, the user must commence the login process again, thus mitigating brute force attacks.

Results

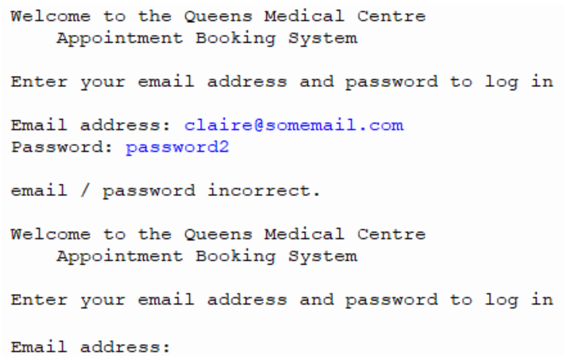
Figure 1 shows the result of a successful login following correct entry of user credentials and confirmation of OTP. In practice, the OTP would be sent to a mobile phone number previously registered on the system. The correct patient ID, i.e. '1' is displayed for the logged in user.



```
Welcome to the Queens Medical Centre
    Appointment Booking System

        Menu

 1 - Login
 2 - Register

Enter 1 or 2 1
Welcome to the Queens Medical Centre
    Appointment Booking System

Enter your email address and password to log in

Email address: claire@somemail.com
Password: Password1

Your OTP code is:  380671

Enter your OTP here: 380671


You have successfully logged in to the
Queens Medical Centre Appointment Booking System

Your unique patient ID number is:  1
```

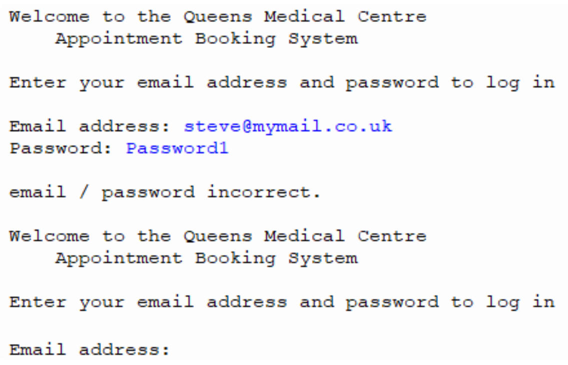
Figure 1: Successful user login

Figures 2 - 4 show that incorrect user credentials result in an error message and a new login procedure is started. No indication of which credential is incorrect is provided.



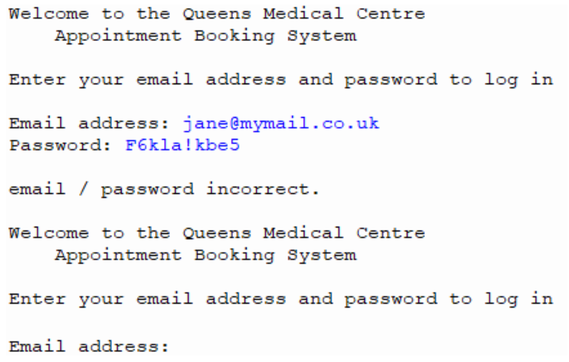
```
Welcome to the Queens Medical Centre
    Appointment Booking System

Enter your email address and password to log in

Email address: claire@somemail.com
Password: password2

email / password incorrect.

Welcome to the Queens Medical Centre
    Appointment Booking System

Enter your email address and password to log in

Email address:
```

Figure 2: Email correct, password incorrect



```
Welcome to the Queens Medical Centre
    Appointment Booking System

Enter your email address and password to log in

Email address: steve@mymail.co.uk
Password: Password1

email / password incorrect.

Welcome to the Queens Medical Centre
    Appointment Booking System

Enter your email address and password to log in

Email address:
```

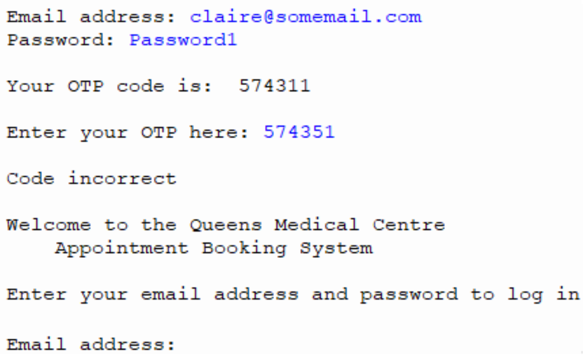
Figure 3: Email incorrect, password correct



```
Welcome to the Queens Medical Centre
    Appointment Booking System

Enter your email address and password to log in

Email address: jane@mymail.co.uk
Password: F6kla!kbe5

email / password incorrect.

Welcome to the Queens Medical Centre
    Appointment Booking System

Enter your email address and password to log in

Email address:
```

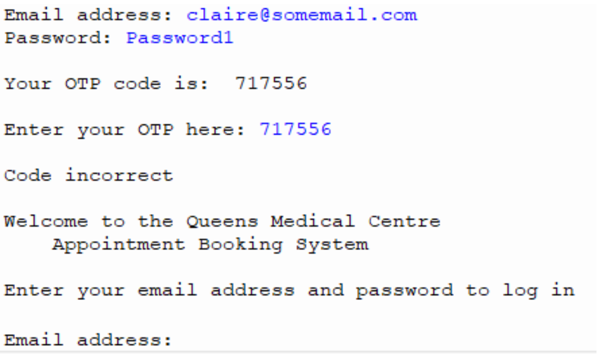
Figure 4: Email and password incorrect.

Figures 5 and 6 show the results of an incorrect and timed out OTP being entered by the user.



```
Email address: claire@somemail.com
Password: Password1

Your OTP code is:  574311

Enter your OTP here: 574351

Code incorrect

Welcome to the Queens Medical Centre
    Appointment Booking System

Enter your email address and password to log in

Email address:
```

Figure 5: Incorrect OTP



```
Email address: claire@somemail.com
Password: Password1

Your OTP code is:  717556

Enter your OTP here: 717556

Code incorrect

Welcome to the Queens Medical Centre
    Appointment Booking System

Enter your email address and password to log in

Email address:
```

Figure 6: Timed out OTP

Analysis

The system performed as expected in all scenarios. Several improvements / development opportunities for the system were identified for further discussion:

- Implementation of password masking.
- Different messages indicating incorrect OTP or timed out OTP to improve user friendliness of the system.
- The ability to request the OTP again in case of a timeout error.
- An option to return to the main menu during the login process.
- Logging of unsuccessful login attempts plus further mitigations e.g. locking of accounts, informing the registered user that login attempts have been made, requesting password reset

Test case 2: New user registration process.

Procedure.

Use the system to register a new user by entering the requested data. The data should test:

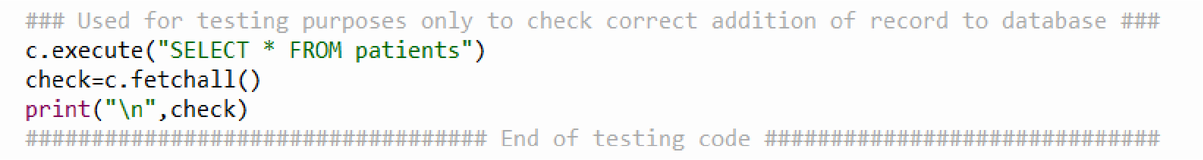
- Input validation for email addresses.
- Input validation for the password policy.
- Check to see if email is already registered.

Expected outcome.

The system should add a new record to the database providing the user is not already registered and all input validation is passed. The new password should be stored as a salted hash, not plain text. If input validation fails, then the user is requested for input again until it is valid. If the user is already registered, a message is displayed, and the user is returned to the main menu.

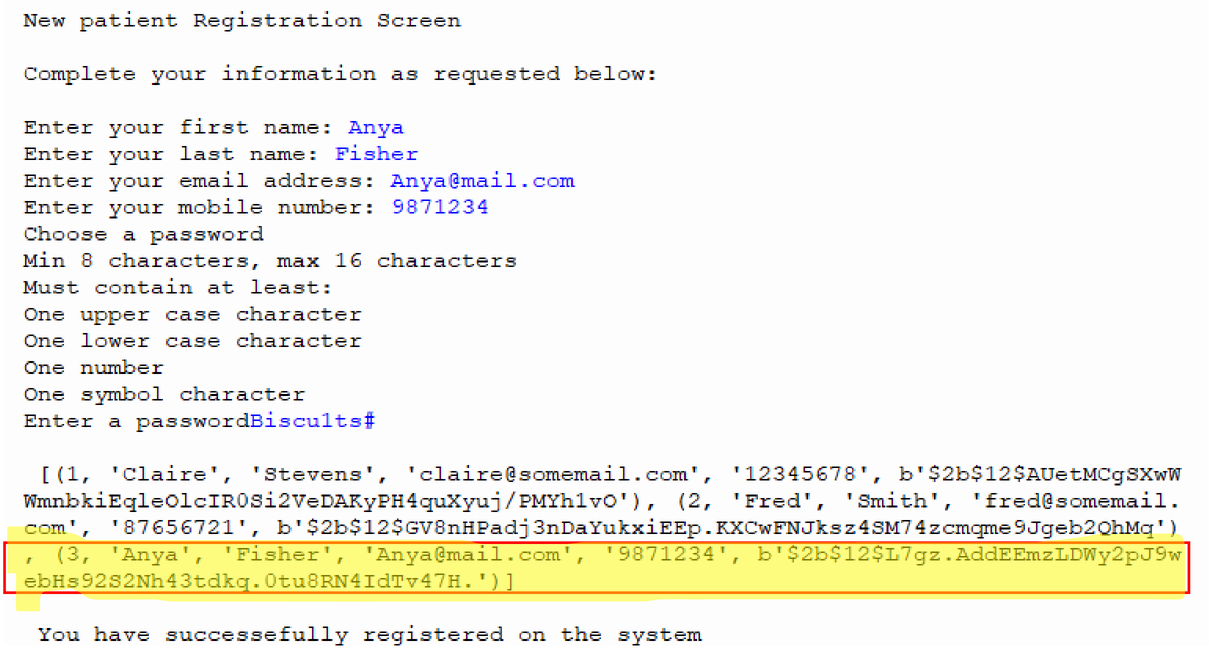
Results

Figure 8 shows the results of successful registration of a new user. For testing purposes, the code in Figure 7 was added to the relevant function to display the contents of the database after the new record has been added. This code is still present in main.py but is commented out. The new record has been added as a new row in the table (highlighted) and given the unique patient ID of ‘3’. The salted hash for the new password has been successfully created and stored in the record as indicated.



```
### Used for testing purposes only to check correct addition of record to database ###
c.execute("SELECT * FROM patients")
check=c.fetchall()
print("\n",check)
################################### End of testing code ###############################
```

Figure 7: Code added for confirming correct addition of new record to database.

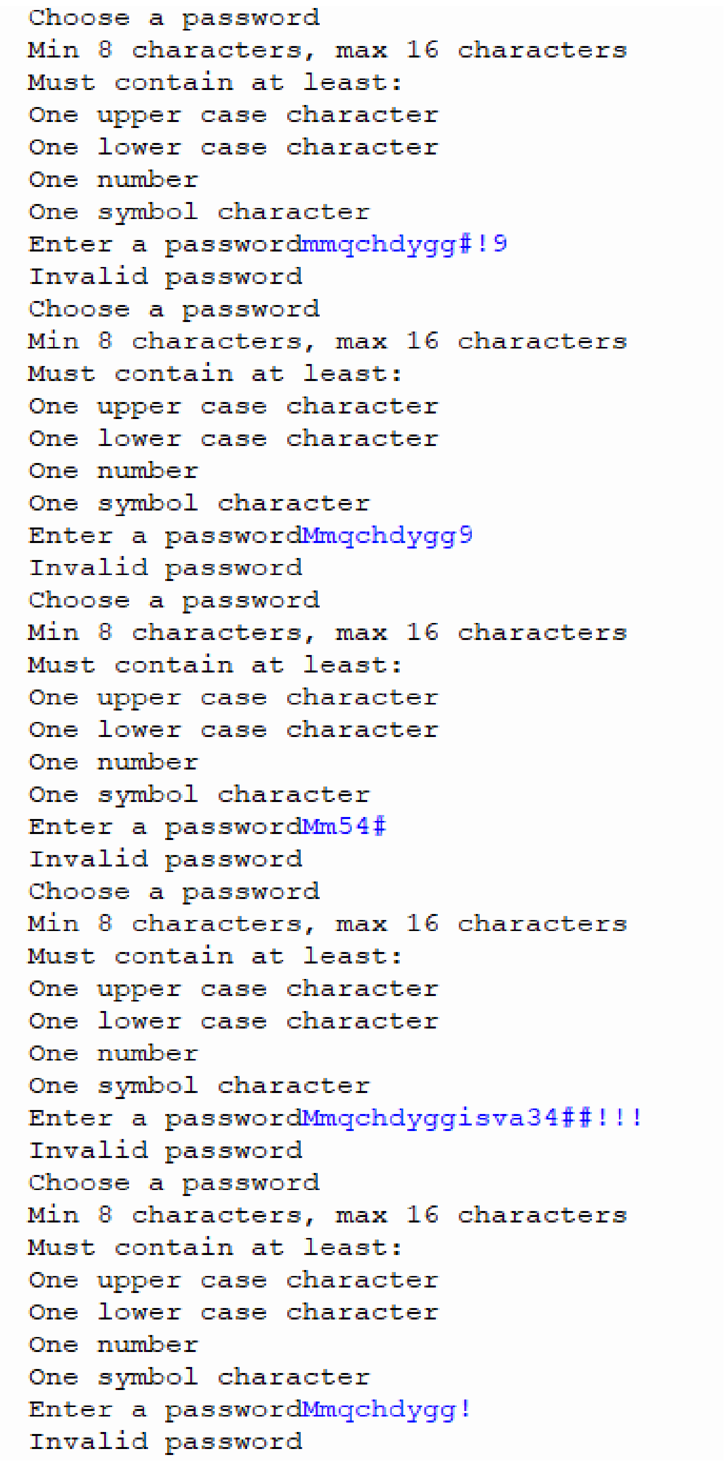


```
New patient Registration Screen

Complete your information as requested below:

Enter your first name: Anya
Enter your last name: Fisher
Enter your email address: Anya@mail.com
Enter your mobile number: 9871234
Choose a password
Min 8 characters, max 16 characters
Must contain at least:
One upper case character
One lower case character
One number
One symbol character
Enter a passwordBiscu1ts#

 [(1, 'Claire', 'Stevens', 'claire@somemail.com', '12345678', b'$2b$12$AUetMCgSXwW
WmnbkiEqleOlcIR0Si2VeDAKyPH4quXyuj/PMYh1vO'), (2, 'Fred', 'Smith', 'fred@somemail.
com', '87656721', b'$2b$12$GV8nHPadj3nDaYukxiEEp.KXCwFNJksz4SM74zcmqme9Jgeb2QhMq')
, (3, 'Anya', 'Fisher', 'Anya@mail.com', '9871234', b'$2b$12$L7gz.AddEEmzLDWy2pJ9w
ebHs92S2Nh43tdkq.0tu8RN4IdTv47H.')]

 You have successefully registered on the system
```

Figure 8: Results of successful new user registration.

Figure 9 shows the results of different violations of the required password policy when registering. In order, the violations of the policy are:

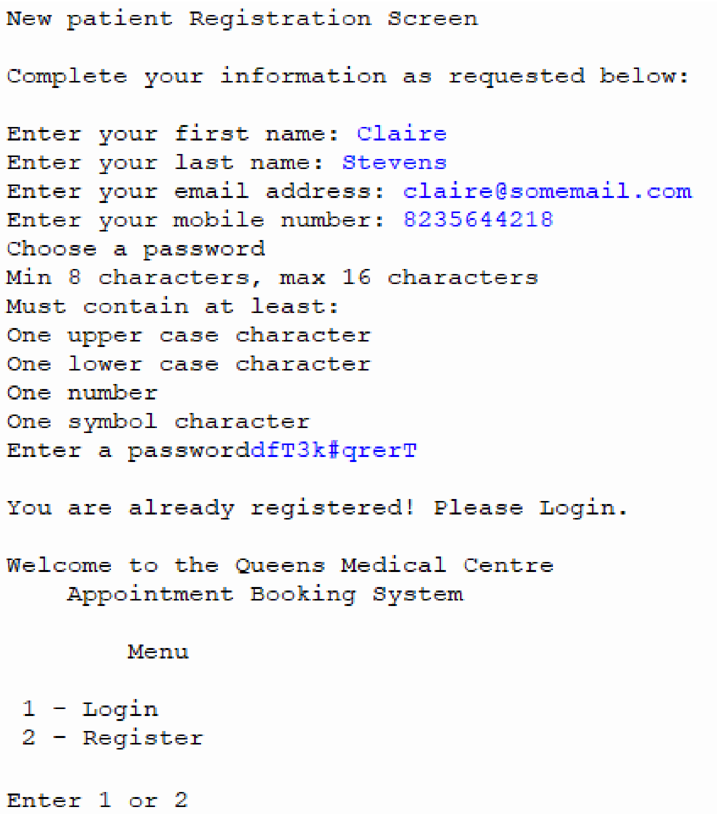
- No capital
- No special character
- Minimum length
- Maximum length
- No number



```
Choose a password
Min 8 characters, max 16 characters
Must contain at least:
One upper case character
One lower case character
One number
One symbol character
Enter a passwordmmqchdygg#!9
Invalid password
Choose a password
Min 8 characters, max 16 characters
Must contain at least:
One upper case character
One lower case character
One number
One symbol character
Enter a passwordMmqchdygg9
Invalid password
Choose a password
Min 8 characters, max 16 characters
Must contain at least:
One upper case character
One lower case character
One number
One symbol character
Enter a passwordMm54#
Invalid password
Choose a password
Min 8 characters, max 16 characters
Must contain at least:
One upper case character
One lower case character
One number
One symbol character
Enter a passwordMmqchdyggisva34##!!!
Invalid password
Choose a password
Min 8 characters, max 16 characters
Must contain at least:
One upper case character
One lower case character
One number
One symbol character
Enter a passwordMmqchdygg!
Invalid password
```

Figure 9: Violations of password policy during login.

Figure 10 shows the result of trying to register with the same email address as a record already present in the database. The registration is rejected, and the user is returned to the main menu.



```
New patient Registration Screen

Complete your information as requested below:

Enter your first name: Claire
Enter your last name: Stevens
Enter your email address: claire@somemail.com
Enter your mobile number: 8235644218
Choose a password
Min 8 characters, max 16 characters
Must contain at least:
One upper case character
One lower case character
One number
One symbol character
Enter a passworddfT3k#qrerT

You are already registered! Please Login.

Welcome to the Queens Medical Centre
    Appointment Booking System

        Menu

 1 - Login
 2 - Register

Enter 1 or 2
```

Figure 10: Attempt to register with an email already present on the system.

Analysis

The system performed as expected in all scenarios. Several improvements / development opportunities for the system were identified for further discussion:

- Password masking when selecting a password to prevent eavesdropping.
- Password confirmation when selecting a password to eliminate typos.
- Logging of unsuccessful registration attempts to prevent spamming accounts.
- Contacting registered users if someone tries to register using their email address.
- More detailed checking of email addresses e.g. domain blacklists / can the email address receive mail / requiring account activation via email.
- Requiring account activation using 2FA.

Conclusion

The testing has demonstrated that the system has fulfilled the objectives of implementing the following security features:

1. Salting and hashing of passwords.
2. Application of a strict password policy when registering on the system to ensure good quality passwords are chosen by users. In this case, the requirement was set at: length between 8 & 16 characters, at least one upper case, one lower case, one number, one special character and no spaces.
3. Two factor authentication.