FAST National University of

Computer and Emerging Sciences

# Information Security

# Assignment 2 – Test Report

- Name: Muneel Haider
- Roll No: 21I-0640

# Contents

**Introduction:** ........ 3

**Functional Testing:** ........ 3

**1. Registration:** ........ 3

**2. Login:** ........ 3

**3. Chat:** ........ 4

**4. Repeated Username Registration:** ........ 4

**5. Incorrect Login Credentials:** ........ 4

**6. Registered Users in creds.txt:** ........ 5

........ 5

**7. Server:** ........ 5

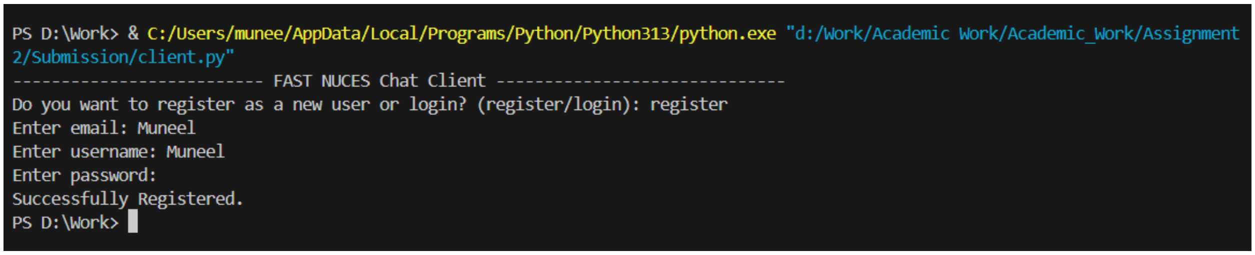
**Security Testing:** ........ 6

# Introduction:

This report highlights the functionality and security of the Server-Client question. The application utilizes Python sockets in order to accurately implement some fundamental concepts of Information Security. Some of these include Diffie-Hellman key exchange and AES encryption. The objective of this report is to validate system's functionality, ensure secure data exchange and encrypted communication between two users.

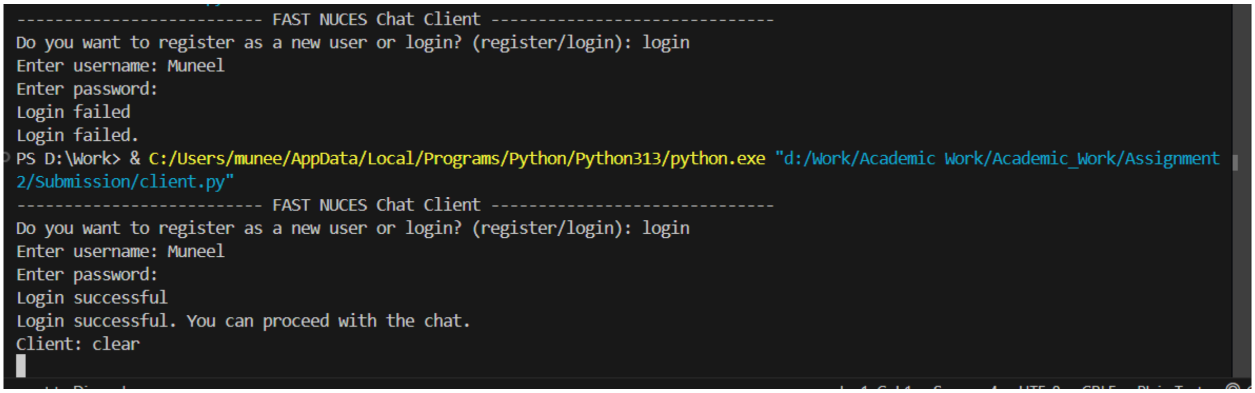
# Functional Testing:

## 1. Registration:



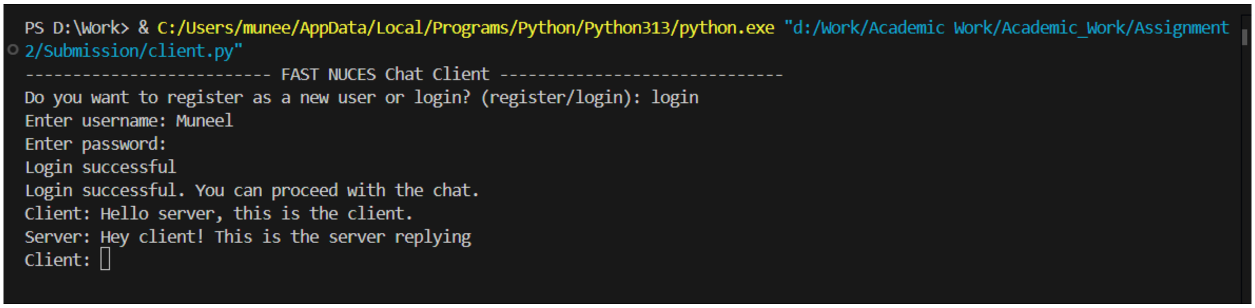
```
PS D:\Work> & C:/Users/munee/AppData/Local/Programs/Python/Python313/python.exe "d:/Work/Academic Work/Academic_Work/Assignment 2/Submission/client.py"
------------------------- FAST NUCES Chat Client -----------------------------
Do you want to register as a new user or login? (register/login): register
Enter email: Muneel
Enter username: Muneel
Enter password:
Successfully Registered.
PS D:\Work> 
```

## 2. Login:

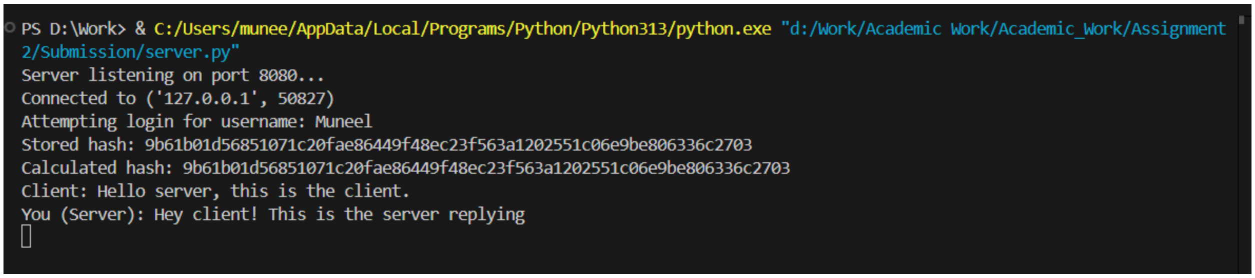


```
------------------------- FAST NUCES Chat Client -----------------------------
Do you want to register as a new user or login? (register/login): login
Enter username: Muneel
Enter password:
Login failed
Login failed.
PS D:\Work> & C:/Users/munee/AppData/Local/Programs/Python/Python313/python.exe "d:/Work/Academic Work/Academic_Work/Assignment 2/Submission/client.py"
------------------------- FAST NUCES Chat Client -----------------------------
Do you want to register as a new user or login? (register/login): login
Enter username: Muneel
Enter password:
Login successful
Login successful. You can proceed with the chat.
Client: clear
```

## 3. Chat:

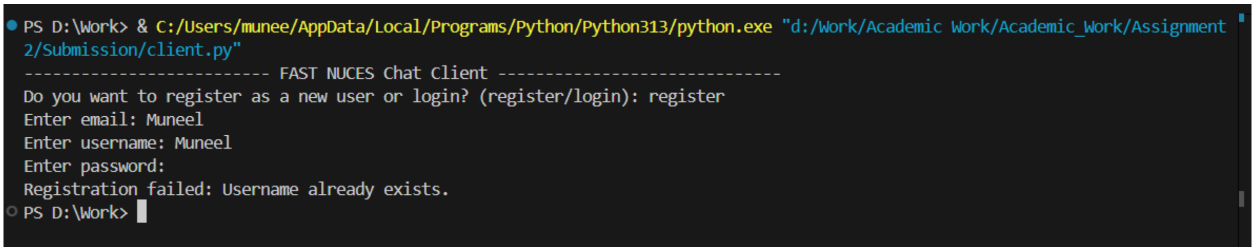


```
PS D:\Work> & C:/Users/munee/AppData/Local/Programs/Python/Python313/python.exe "d:/Work/Academic Work/Academic_Work/Assignment
2/Submission/client.py"
-------------------------- FAST NUCES Chat Client ------------------------------
Do you want to register as a new user or login? (register/login): login
Enter username: Muneel
Enter password:
Login successful
Login successful. You can proceed with the chat.
Client: Hello server, this is the client.
Server: Hey client! This is the server replying
Client:
```



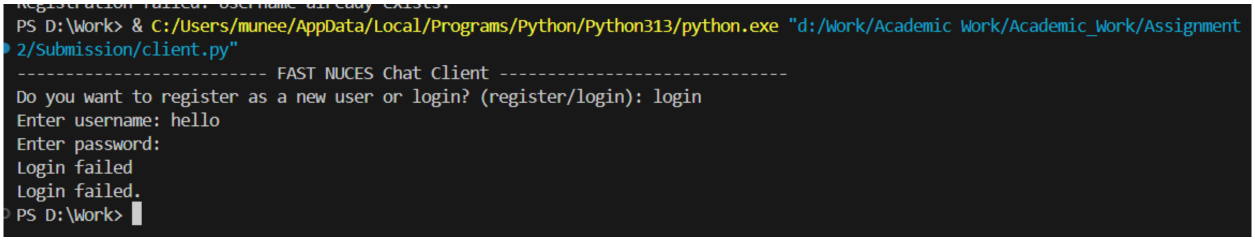
```
PS D:\Work> & C:/Users/munee/AppData/Local/Programs/Python/Python313/python.exe "d:/Work/Academic Work/Academic_Work/Assignment
2/Submission/server.py"
Server listening on port 8080...
Connected to ('127.0.0.1', 50827)
Attempting login for username: Muneel
Stored hash: 9b61b01d56851071c20fae86449f48ec23f563a1202551c06e9be806336c2703
Calculated hash: 9b61b01d56851071c20fae86449f48ec23f563a1202551c06e9be806336c2703
Client: Hello server, this is the client.
You (Server): Hey client! This is the server replying
```

## 4. Repeated Username Registration:



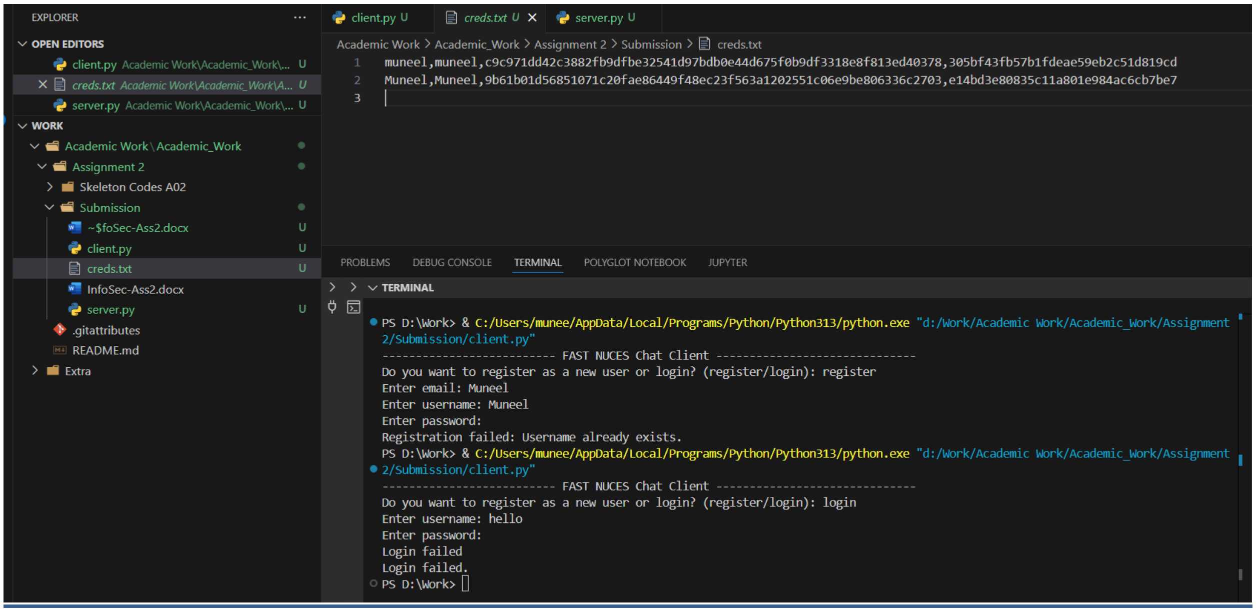
```
PS D:\Work> & C:/Users/munee/AppData/Local/Programs/Python/Python313/python.exe "d:/Work/Academic Work/Academic_Work/Assignment
2/Submission/client.py"
-------------------------- FAST NUCES Chat Client ------------------------------
Do you want to register as a new user or login? (register/login): register
Enter email: Muneel
Enter username: Muneel
Enter password:
Registration failed: Username already exists.
PS D:\Work>
```

## 5. Incorrect Login Credentials:



```
Registration failed: Username already exists.
PS D:\Work> & C:/Users/munee/AppData/Local/Programs/Python/Python313/python.exe "d:/Work/Academic Work/Academic_Work/Assignment
2/Submission/client.py"
-------------------------- FAST NUCES Chat Client ------------------------------
Do you want to register as a new user or login? (register/login): login
Enter username: hello
Enter password:
Login failed
Login failed.
PS D:\Work>
```

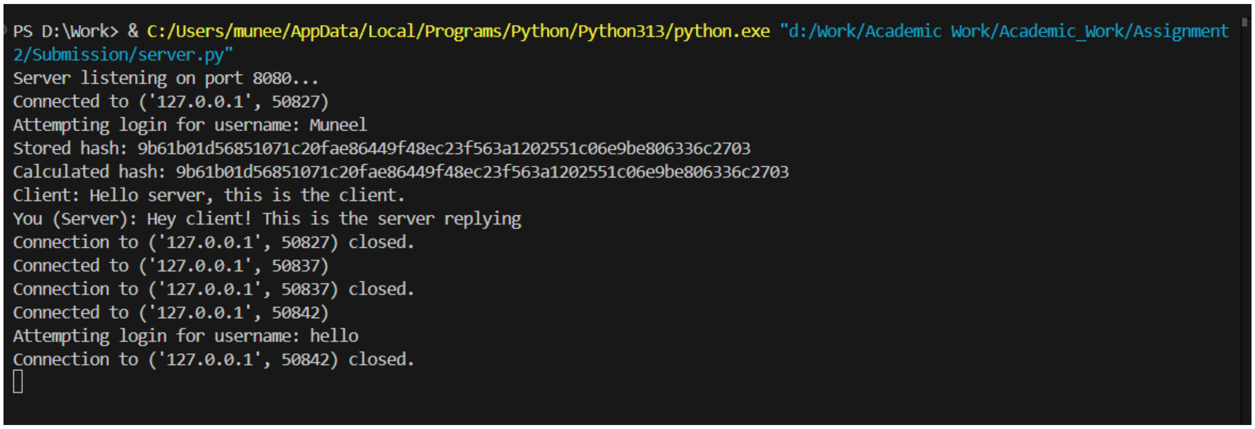
## 6. Registered Users in creds.txt:



```
muneel,muneel,c9c971dd42c3882fb9dfbe32541d97bdb0e44d675f0b9df3318e8f813ed40378,305bf43fb57b1fdeae59eb2c51d819cd
Muneel,Muneel,9b61b01d56851071c20fae86449f48ec23f563a1202551c06e9be806336c2703,e14bd3e80835c11a801e984ac6cb7be7
```

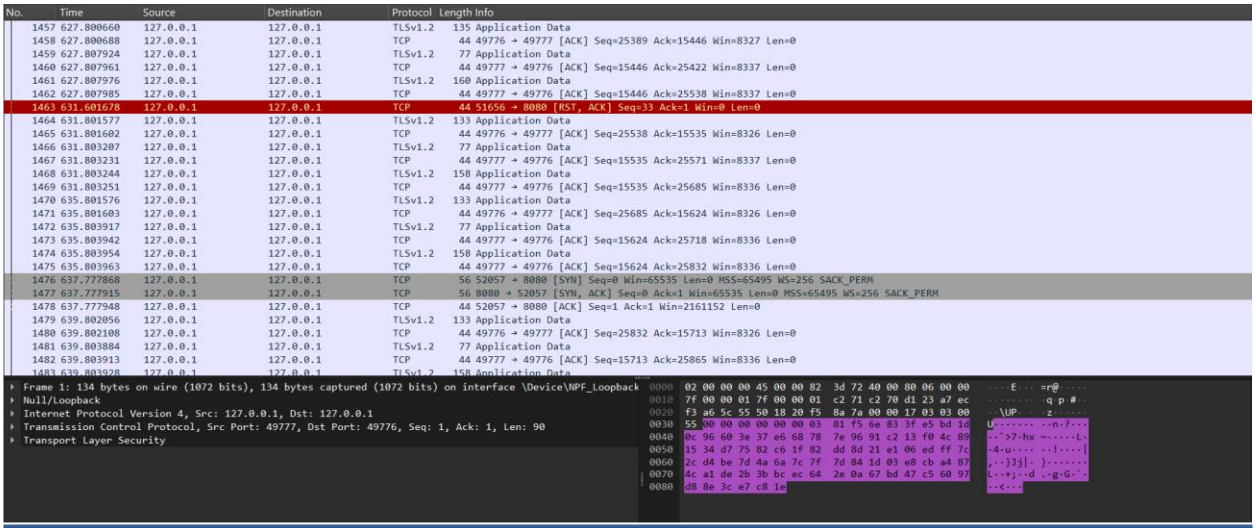
```
PS D:\Work> & C:/Users/munee/AppData/Local/Programs/Python/Python313/python.exe "d:/Work/Academic Work/Academic_Work/Assignment
2/Submission/client.py"
------------------------- FAST NUCES Chat Client -----------------------------
Do you want to register as a new user or login? (register/login): register
Enter email: Muneel
Enter username: Muneel
Enter password:
Registration failed: Username already exists.
PS D:\Work> & C:/Users/munee/AppData/Local/Programs/Python/Python313/python.exe "d:/Work/Academic Work/Academic_Work/Assignment
2/Submission/client.py"
------------------------- FAST NUCES Chat Client -----------------------------
Do you want to register as a new user or login? (register/login): login
Enter username: hello
Enter password:
Login failed
Login failed.
PS D:\Work>
```

## 7. Server:



```
PS D:\Work> & C:/Users/munee/AppData/Local/Programs/Python/Python313/python.exe "d:/Work/Academic Work/Academic_Work/Assignment
2/Submission/server.py"
Server listening on port 8080...
Connected to ('127.0.0.1', 50827)
Attempting login for username: Muneel
Stored hash: 9b61b01d56851071c20fae86449f48ec23f563a1202551c06e9be806336c2703
Calculated hash: 9b61b01d56851071c20fae86449f48ec23f563a1202551c06e9be806336c2703
Client: Hello server, this is the client.
You (Server): Hey client! This is the server replying
Connection to ('127.0.0.1', 50827) closed.
Connected to ('127.0.0.1', 50837)
Connection to ('127.0.0.1', 50837) closed.
Connected to ('127.0.0.1', 50842)
Attempting login for username: hello
Connection to ('127.0.0.1', 50842) closed.
```

# Security Testing:



```
No.     Time        Source       Destination  Protocol  Length Info
   1457 627.800660  127.0.0.1    127.0.0.1    TLSv1.2   135 Application Data
   1458 627.800688  127.0.0.1    127.0.0.1    TCP        44 49776 → 49777 [ACK] Seq=25389 Ack=15446 Win=8327 Len=0
   1459 627.807924  127.0.0.1    127.0.0.1    TLSv1.2    77 Application Data
   1460 627.807961  127.0.0.1    127.0.0.1    TCP        44 49777 → 49776 [ACK] Seq=15446 Ack=25422 Win=8337 Len=0
   1461 627.807976  127.0.0.1    127.0.0.1    TLSv1.2   160 Application Data
   1462 627.807985  127.0.0.1    127.0.0.1    TCP        44 49777 → 49776 [ACK] Seq=15446 Ack=25538 Win=8337 Len=0
   1463 631.601678  127.0.0.1    127.0.0.1    TCP        44 51656 → 8080 [RST, ACK] Seq=33 Ack=1 Win=0 Len=0
   1464 631.801577  127.0.0.1    127.0.0.1    TLSv1.2   133 Application Data
   1465 631.801602  127.0.0.1    127.0.0.1    TCP        44 49776 → 49777 [ACK] Seq=25538 Ack=15535 Win=8326 Len=0
   1466 631.803207  127.0.0.1    127.0.0.1    TLSv1.2    77 Application Data
   1467 631.803231  127.0.0.1    127.0.0.1    TCP        44 49777 → 49776 [ACK] Seq=15535 Ack=25571 Win=8337 Len=0
   1468 631.803244  127.0.0.1    127.0.0.1    TLSv1.2   158 Application Data
   1469 631.803251  127.0.0.1    127.0.0.1    TCP        44 49777 → 49776 [ACK] Seq=15535 Ack=25685 Win=8336 Len=0
   1470 635.801576  127.0.0.1    127.0.0.1    TLSv1.2   133 Application Data
   1471 635.801603  127.0.0.1    127.0.0.1    TCP        44 49776 → 49777 [ACK] Seq=25685 Ack=15624 Win=8326 Len=0
   1472 635.803917  127.0.0.1    127.0.0.1    TLSv1.2    77 Application Data
   1473 635.803942  127.0.0.1    127.0.0.1    TCP        44 49777 → 49776 [ACK] Seq=15624 Ack=25718 Win=8336 Len=0
   1474 635.803954  127.0.0.1    127.0.0.1    TLSv1.2   158 Application Data
   1475 635.803963  127.0.0.1    127.0.0.1    TCP        44 49777 → 49776 [ACK] Seq=15624 Ack=25832 Win=8336 Len=0
   1476 637.777868  127.0.0.1    127.0.0.1    TCP        56 52057 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   1477 637.777915  127.0.0.1    127.0.0.1    TCP        56 8080 → 52057 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   1478 637.777948  127.0.0.1    127.0.0.1    TCP        44 52057 → 8080 [ACK] Seq=1 Ack=1 Win=2161152 Len=0
   1479 639.802056  127.0.0.1    127.0.0.1    TLSv1.2   133 Application Data
   1480 639.802108  127.0.0.1    127.0.0.1    TCP        44 49776 → 49777 [ACK] Seq=25832 Ack=15713 Win=8326 Len=0
   1481 639.803884  127.0.0.1    127.0.0.1    TLSv1.2    77 Application Data
   1482 639.803913  127.0.0.1    127.0.0.1    TCP        44 49777 → 49776 [ACK] Seq=15713 Ack=25865 Win=8336 Len=0
   1483 639.803928  127.0.0.1    127.0.0.1    TLSv1.2   158 Application Data
```

```
▸ Frame 1: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_Loopback
▸ Null/Loopback
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Transmission Control Protocol, Src Port: 49777, Dst Port: 49776, Seq: 1, Ack: 1, Len: 90
▸ Transport Layer Security
```

```
0000  02 00 00 00 45 00 00 82  3d 72 40 00 80 06 00 00   ····E··· =r@·····
0010  7f 00 00 01 7f 00 00 01  c2 71 c2 70 d1 23 a7 ec   ········ ·q·p·#··
0020  f3 a6 5c 55 50 18 20 f5  8a 7a 00 00 17 03 03 00   ··\UP· · ·z······
0030  55 00 00 00 00 00 00 03  81 f5 6e 83 3f e5 bd 1d   U······· ··n·?···
0040  0c 96 60 3e 37 e6 68 78  7e 96 91 c2 13 f0 4c 89   ··`>7·hx ~·····L·
0050  15 34 d7 75 82 c6 1f 82  dd 8d 21 e1 06 ed ff 7c   ·4·u···· ··!····|
0060  2c d4 be 7d 4a 6a 7c 7f  7d 84 1d 03 e8 cb a4 87   ,··}Jj|· }·······
0070  4c a1 de 2b 3b bc ec 64  2e 0a 67 bd 47 c5 60 97   L··+;··d .·g·G·`·
0080  d8 8e 3c e7 c8 1e                                  ··<···
```