Cyber Security

Summer Internship

Mini Project

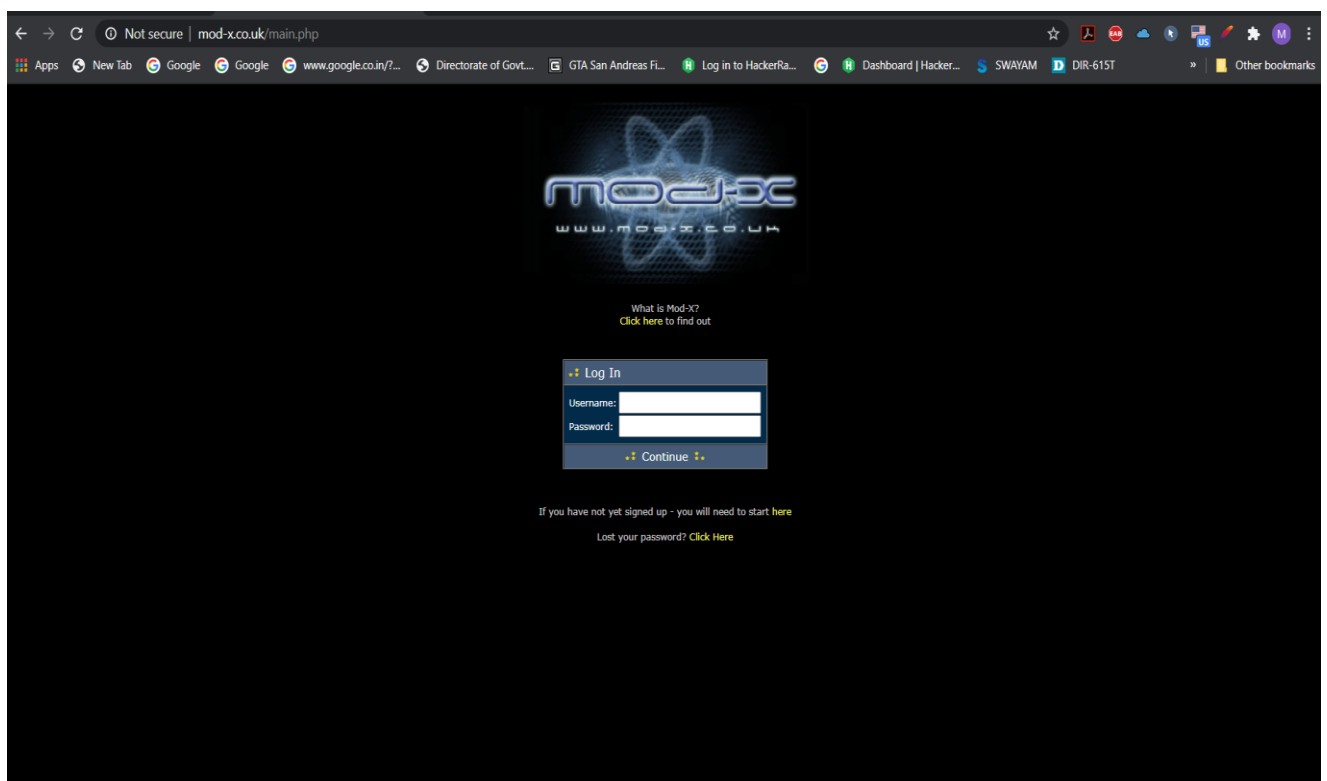## MOD-X CTF(Capture The Flag)

Md Qamruddin Jelani
B14, 121710314035
GITAM University

Steps Taken:

- Our aim is to be an agent in the Mod-x community

- To prevent the intruders this site has a different procedure to register its agents.

- We get a ZIP file with a text document in it and the only hint we get is " The information present in the text document is Encoded".

- And now we need to find the information present in the document by decoding it.

- There are various decoding techniques.

- As I am a Beginner the only way I thought is Trial and error method.

- After lot of research I found that the information in the text document is UUencoded.

Md Qamruddin Jelani
B14, 121710314035
GITAM University

- And then I started Looking for tools which decode the given Information.

- And after lots of trials I found that this text document has another Zip file in it and I need to extract that Zip file to get the required information.

- I took the help of WinZip tools to Unzip the hidden text file in a Zip Format.(This is Special Encoding Technique UUencoding).

- And After I Unzipped the file, I found out that the encoded Information is a mail from Mod-x Community.

- And this mail contains Credentials(for me) and a URL in which I have to Continue the further process.

- And I used the credentials and registered myself as a Mod-X agent.

Md Qamruddin Jelani
B14, 121710314035
GITAM University

Our goal is to Sign up for this website:

Md Qamruddin Jelani

B14, 121710314035

GITAM University

What is Mod-X?
Click here to find out

.: Log In

Username:
Password:

.: Continue :.

If you have not yet signed up - you will need to start here

Lost your password? Click Here

Md Qamruddin Jelani
B14, 121710314035
GITAM University

Welcome to Mod-X.

We can not tell you any more at this point - some of you will find out everything there is to know...others will never go beyond this page. The usual login procedure applies, security restrictions are in place.

Please proceed to enter Mod-X

Agent, our login procedure has had to change for security reasons - please follow the new login procedure. The login procedure details have been secured to prevent any unknown intruders.

Not just anyone can be a Mod-X agent. We need to ensure you have what it takes! Get through this initiation, and then you can become a Mod-X agent (your hint is: this is a popular encoding, not an encryption).

Click here for login procedure

Md Qamruddin Jelani
B14, 121710314035
GITAM University

When we click on the above link we get a zip file downloaded as below:
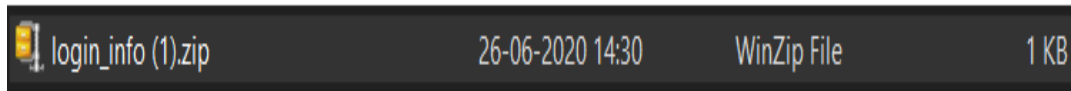
When you open the zip file you find this txt file as below:

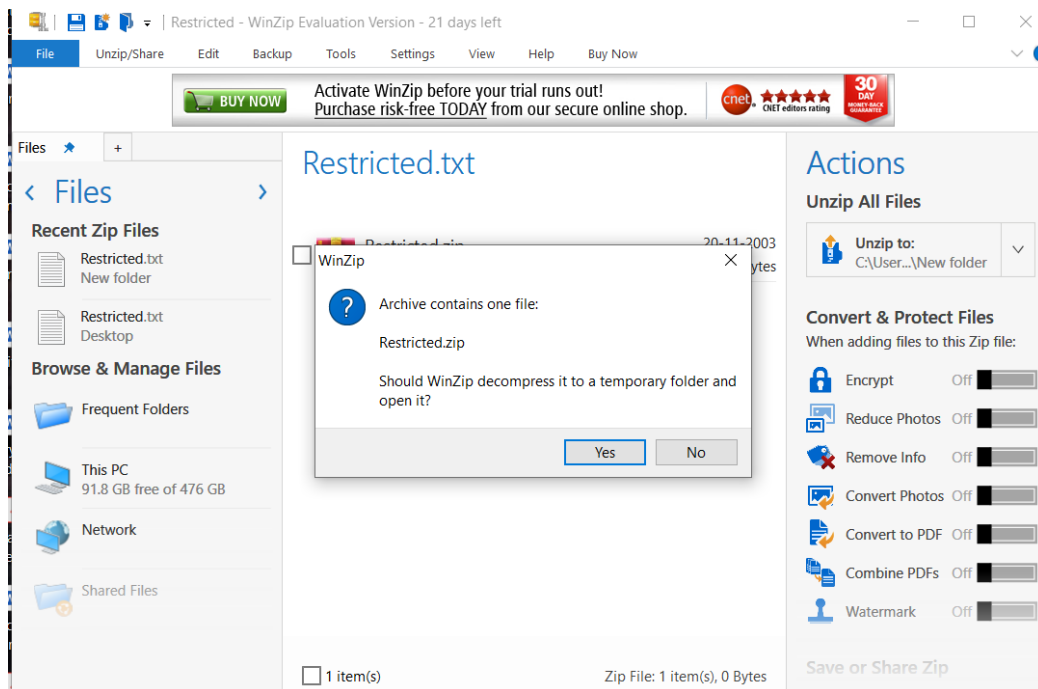Md Qamruddin Jelani

B14, 121710314035

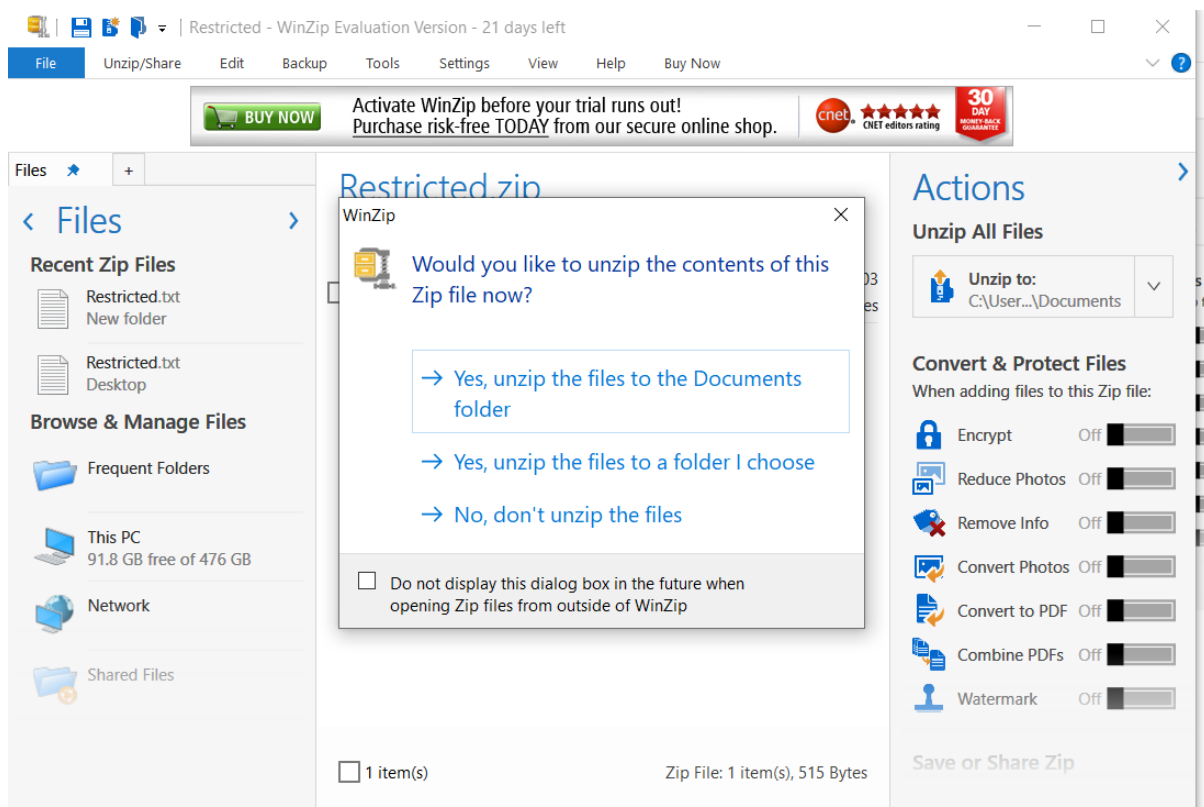GITAM University
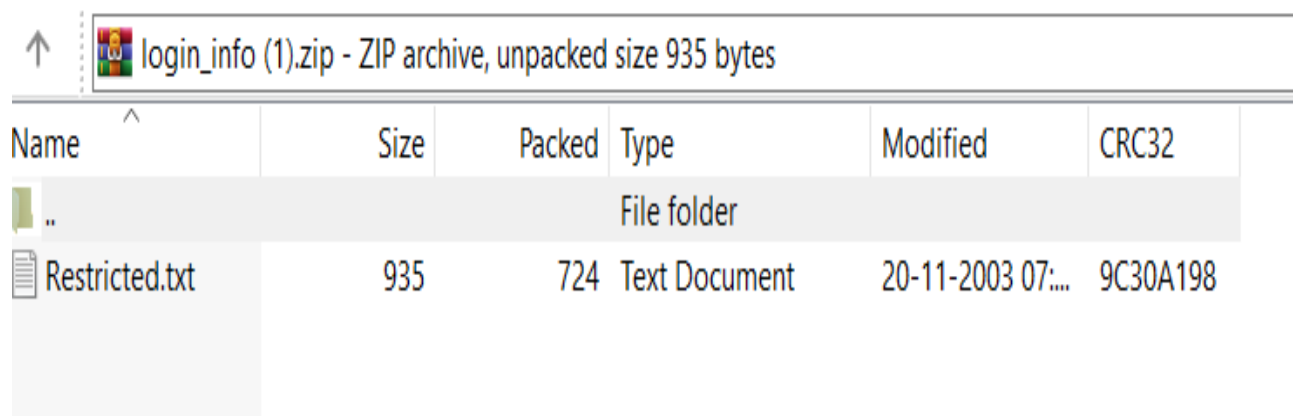
That text file contains below information:

And the information in it is encoded(UUencoding)


```
Restricted.txt - Notepad
File Edit Format View Help
begin 666 Restricted.zip
M4$L#!!0````(`%T[="]<LYX`P(`P`P('0#`..`^^^4F$5S=')I8W1E9"YT>'1M
M4\MNVT`0NQP/PSSNM@PT0!/X4N16`RE0%.GC.I9&TE;2cKH/J_K[<E;IX]"+
M'UJ2W6)^^]U3]SX=]K0][D*X][[D*Q[RXSAD2CX/S'26EU`L%%%6_6ge@E1?46NQ4,7
MR?E6P\3)J:=%@ABZY7'$P2MO"0J1Gg73Z;B1yJ#?I4ZT:!X;N@KI34)%3Y%6
MS8#>A#I-&[;E`H'%'(EY@g[/(-I',=GI;XN"H49?''YXT#LE]BNU.<!&,*(W
M0&4Y7V#,F_&11NV<-TNN-!D!>HZP5"'9Fc91^YE0-D&H2Cc5CAL\T&P:#/'A*<+
M#F6(!!IEXW?Q?13Q=@P[XLBHJ>L[UX,,;.;X3I)0S^RJX=Q+3-28)@@+IK:
MEAD@AAQR7DY)ICG%BK[:(,\=L$C>20*ECR/8BP'&'H+OOT5:+`V>,*K$$%9
MZ<;>Q1X"!WJJO;#$_8(Q+?3?K%(U<1U-:7.HI6A]A+/V[\.U,,J]DW!SMV@<37
M89W+=5QCL6/'MD07QV&&#&5-<R!#%D)%?=?%%D)MG^A^@^Y3^>]::JP9H2MZ4>3UR?F,
M[>I8,L'"..I2K'.,BP8BF<<K)YT_/IG1S#<@@VZ^,,XX$QQO'(\\WC;V?P;@P?-P
MW>^`%%%.?/.G@ggEGg9MCC^K6JL\G%H7QCJC[CGU=S/V_M2ken<N@@?.A5U`
M[AAC.U2*bOU0E0<K@#@Q#M\MM_]`E:+`0(4`!0```(`%T[="]<LYX`P(`P'P@#
M``^.``^^^^^^^^^$``(`""``"V@0````!297--T<FEC=&5=!5U1X=$9=$$%+`
M+`#P```0`@``````
`
end
```

Md Qamruddin Jelani
B14, 121710314035
GITAM University
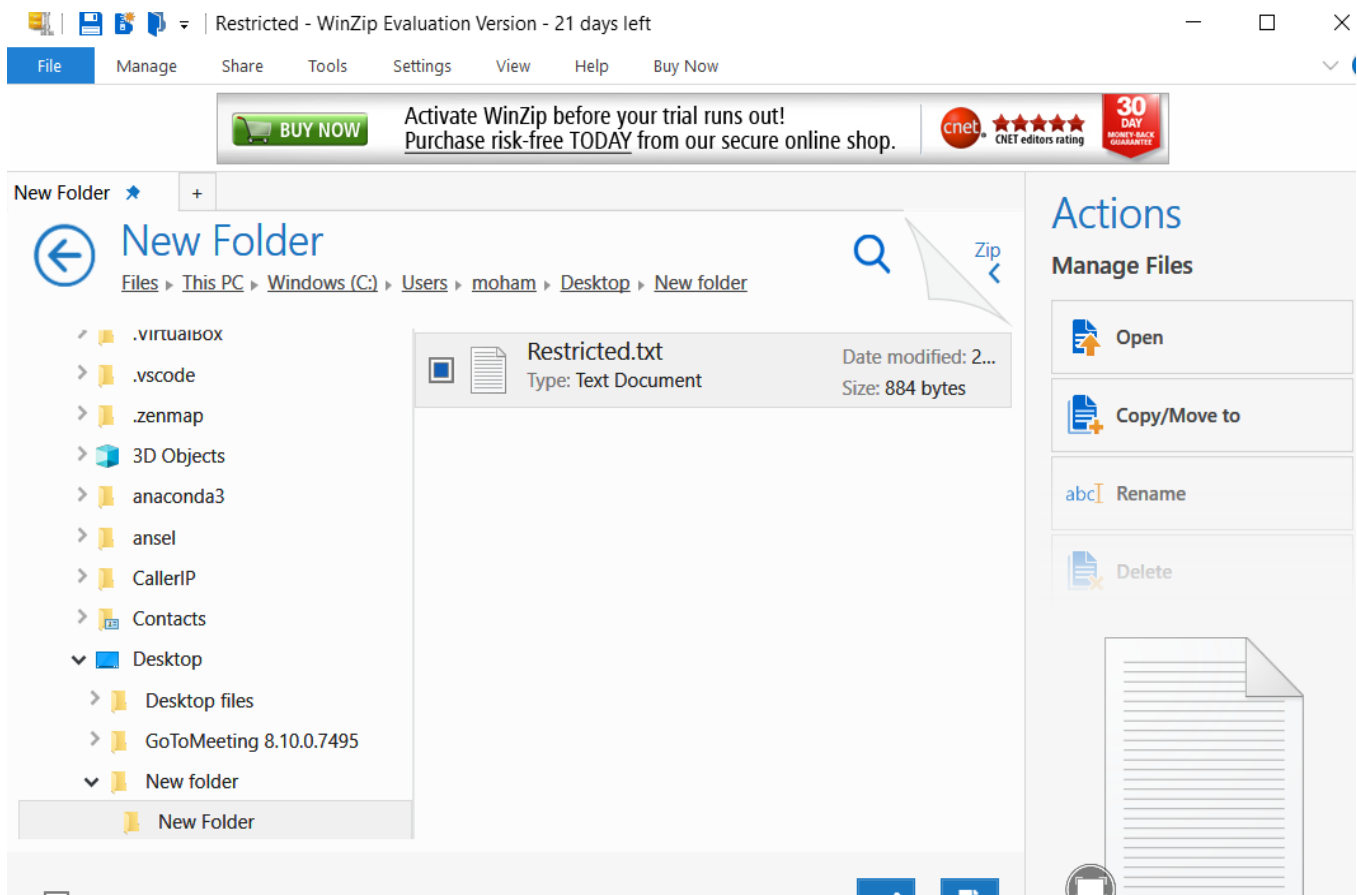
I used the below tool to open the text document I downloaded and found that it contains another Zip file in it and I decompressed it

Md Qamruddin Jelani
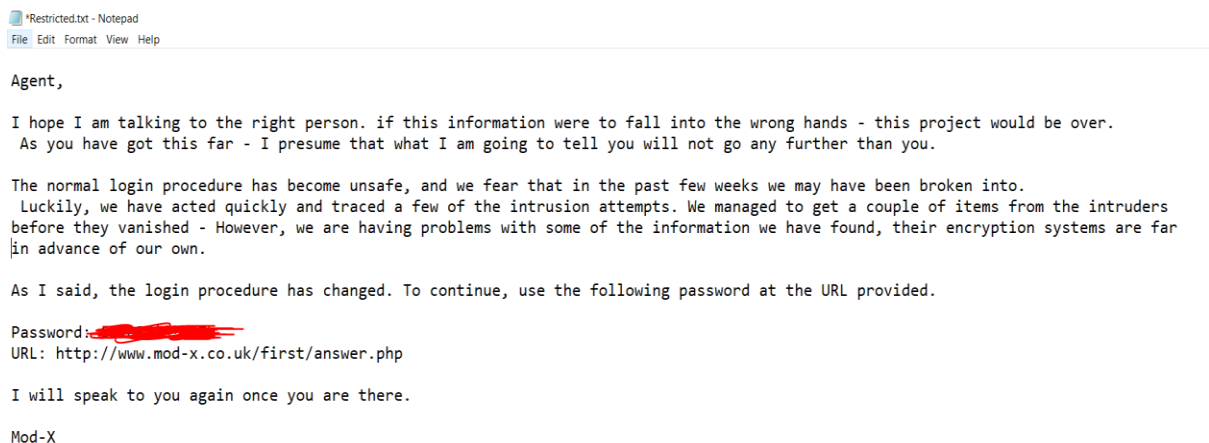
B14, 121710314035

GITAM University

I unzipped the files and It has another file named similarly as previous file Restricted.txt

Md Qamruddin Jelani
B14, 121710314035
GITAM University

Now open the unzipped file:
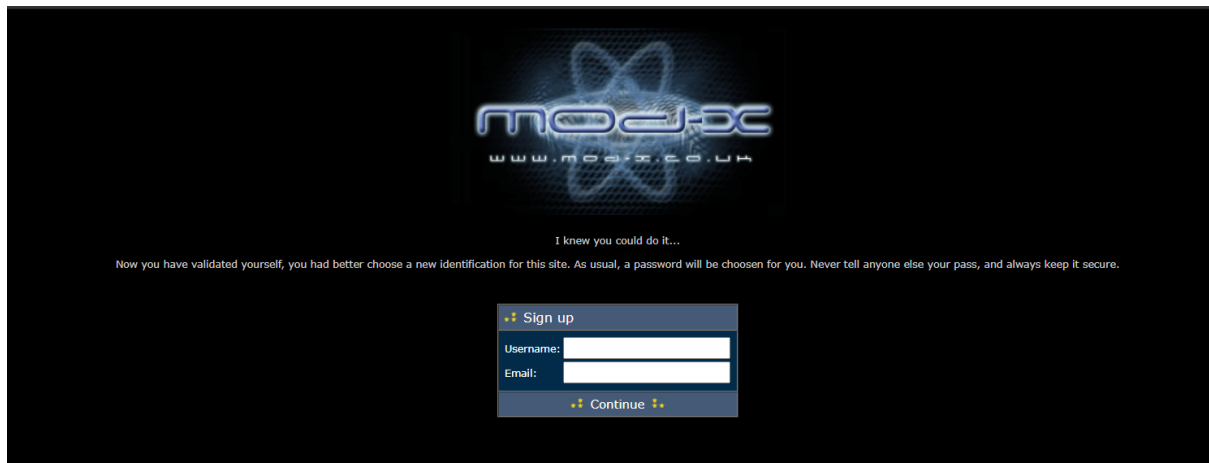
And it has a decoded message from Mod-x

Agent,

I hope I am talking to the right person. if this information were to fall into the wrong hands - this project would be over. As you have got this far - I presume that what I am going to tell you will not go any further than you.

The normal login procedure has become unsafe, and we fear that in the past few weeks we may have been broken into. Luckily, we have acted quickly and traced a few of the intrusion attempts. We managed to get a couple of items from the intruders before they vanished - However, we are having problems with some of the information we have found, their encryption systems are far in advance of our own.

As I said, the login procedure has changed. To continue, use the following password at the URL provided.

Password:
URL: http://www.mod-x.co.uk/first/answer.php
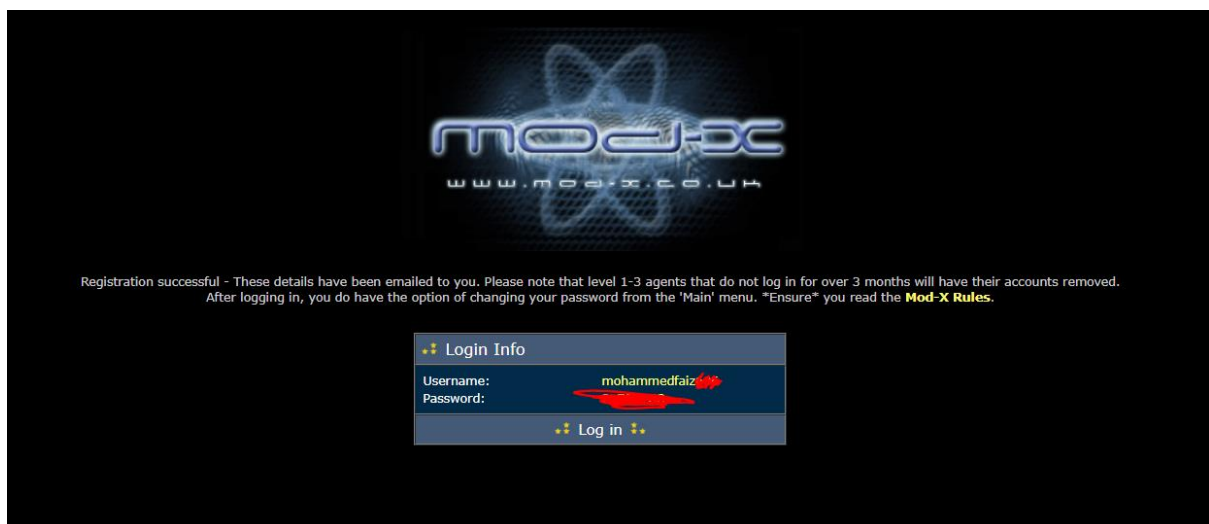
I will speak to you again once you are there.

Mod-X

Md Qamruddin Jelani
B14, 121710314035
GITAM University

Using the provided Credentials I created my account:

I was provided with a unique Password

Md Qamruddin Jelani
B14, 121710314035
GITAM University

And this is the Final page of Mod-X(Central Command):

Md Qamruddin Jelani
B14, 121710314035
GITAM University