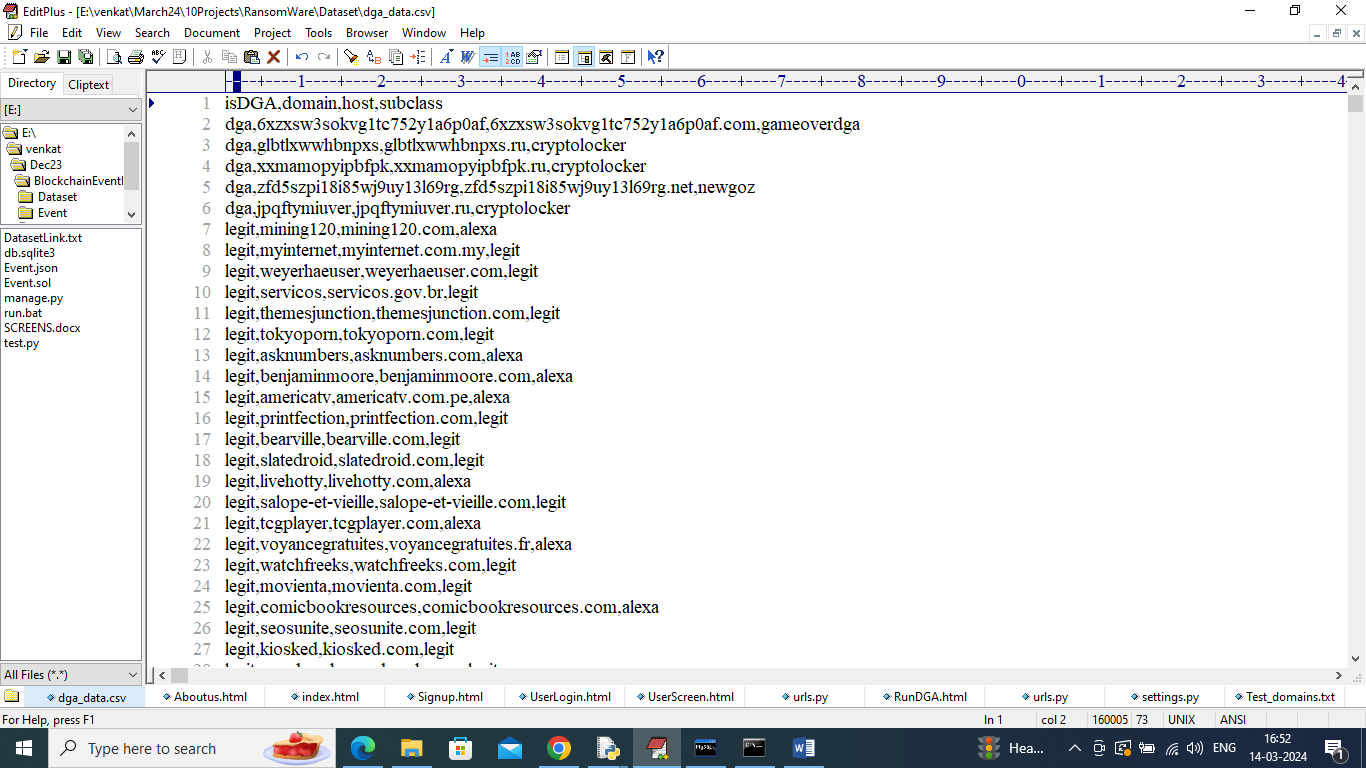
Ransomware Readiness Assessment Tool

Computers or smart devices can interact with each other’s using Internet connection but some malicious attackers will use this connection to spread malwares to victim computers. Once victim click on such malware links or files then that malware will get executed in victim laptop and start encrypting files and make victim computer unusable.

To detect such malwares many antivirus applications are exists but it required regular updates and renewal which will difficult for users. So in propose work we are developing DGA detector which will analyse all domains coming to victim system and then execute ML model on received domain to detect weather arriving domain is normal or contains any Ransomware tool. If Ransomware tool detected then ML algorithm will alert user.

To train ML logistic regression algorithm we are using ALEXA 1 MILLION DOMAIN dataset and this trained model can detect any domain as Legitimate or Ransomware attack.

In below screen showing dataset details



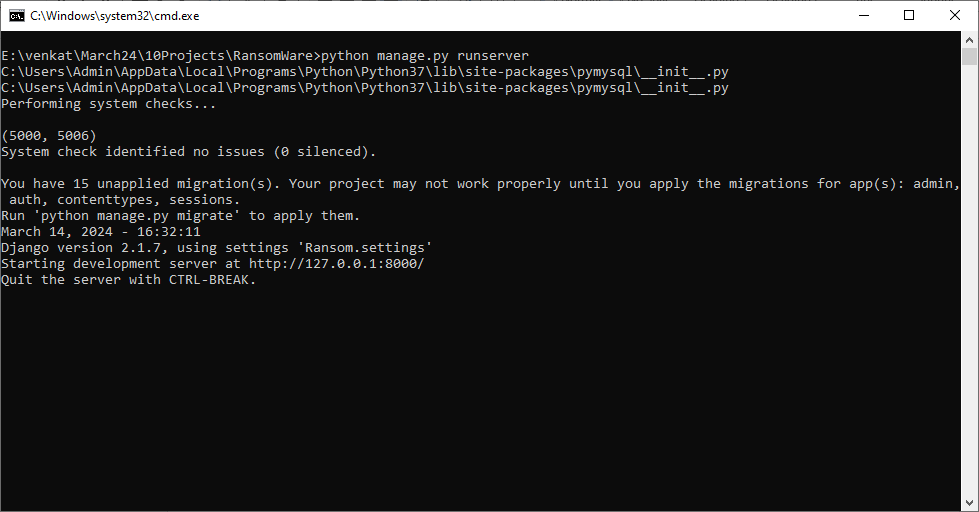
In above dataset screen first row contains dataset column names and remaining rows contains dataset values and by using this dataset we will train ML algorithm to detect Ransomware.

To implement this project we have designed following modules

1. User Signup: new user can sign up with the application
2. User Login: after sign up user can login to system
3. Generate & Load DGA Detector: using this module user can generate and load DGA model
4. Run DGA Detector: using this module use can enter any domain name and then DGA detector will predict weather domain is Legitimate or Ransomware.

SCREEN SHOTS

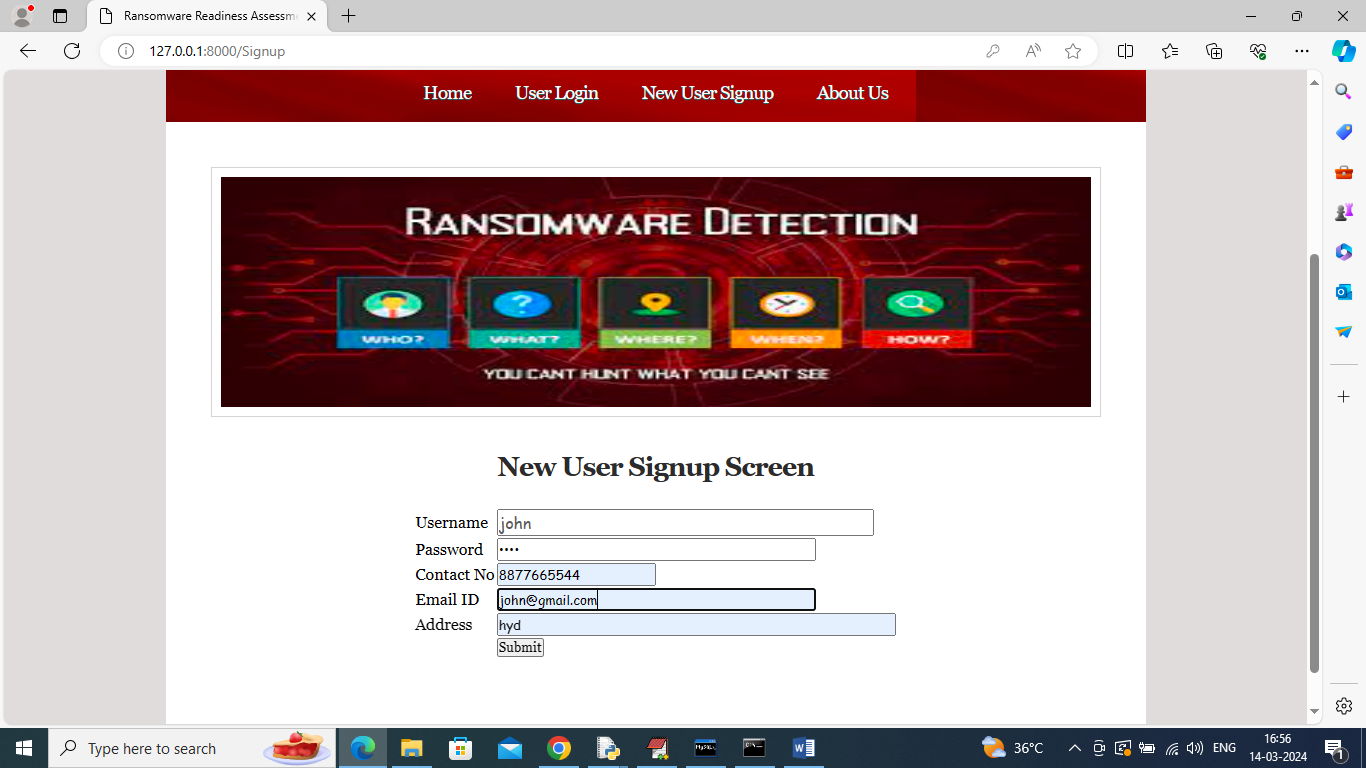
To run project double click on run.bat file to get below server screen



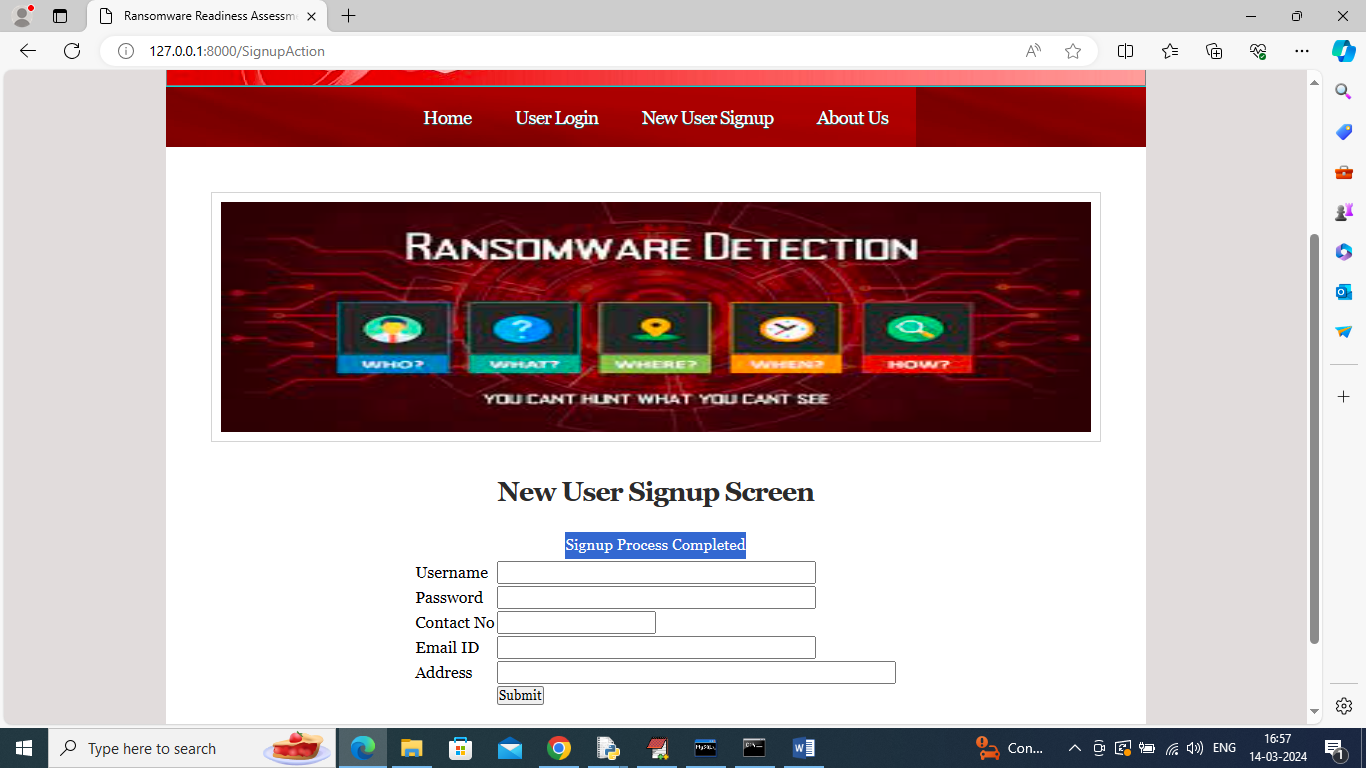
In above screen python server started and now open browser and enter URL as <http://127.0.0.1:8000/index.html> and then press enter key to get below page



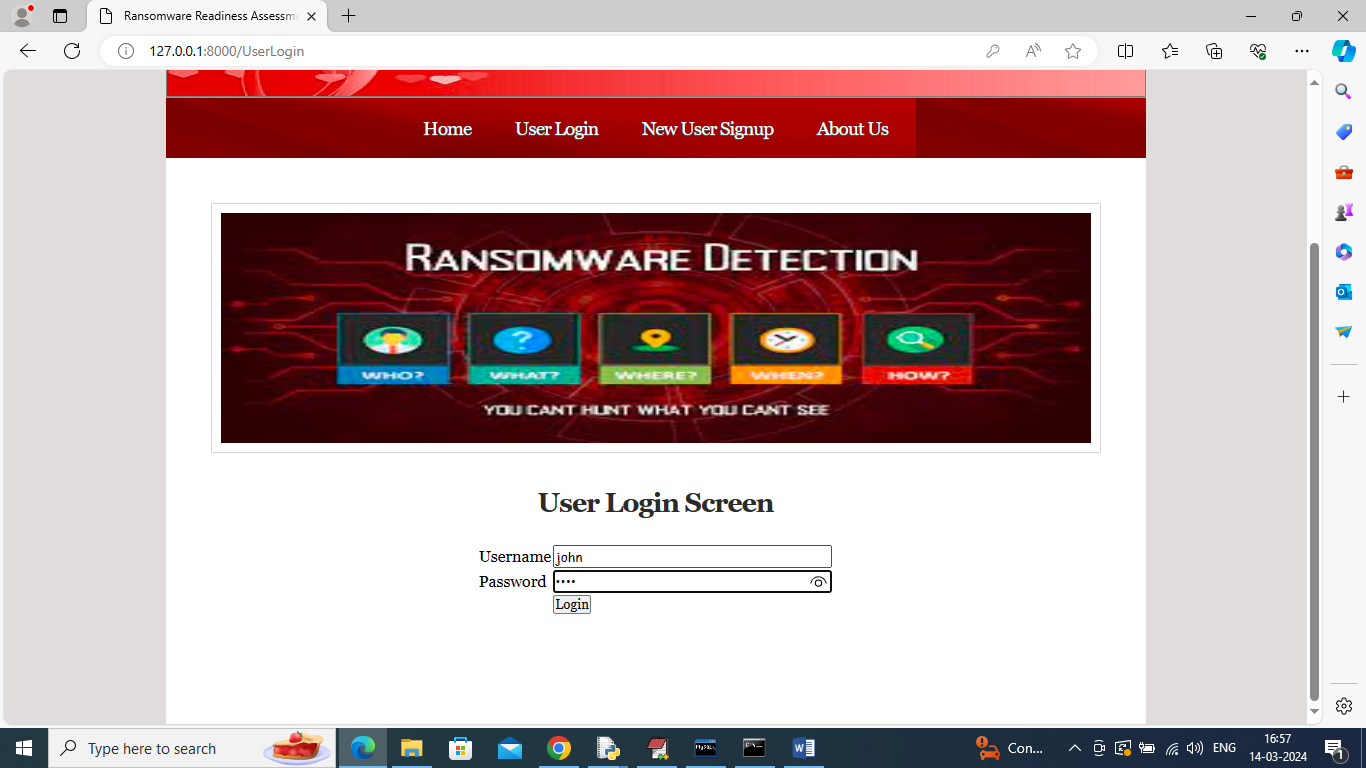
In above screen click on “New User Sign up’ link to get below page



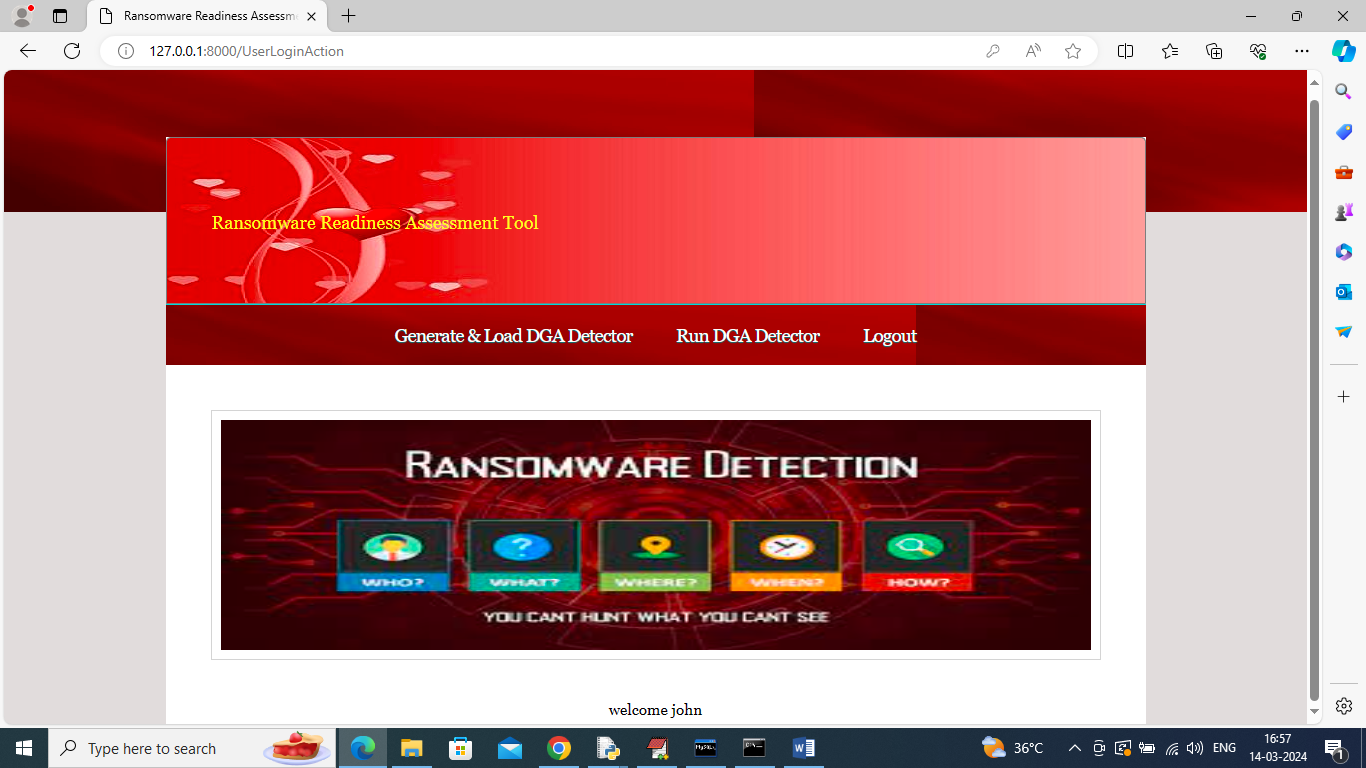
In above screen user is entering sign up details and then press button to get below page



In above screen user sign up completed and now click on ‘User Login’ link to get below page



In above screen user is login and after login will get below page



In above screen user can click on ‘Generate & Load DGA Detector’ link to get below page

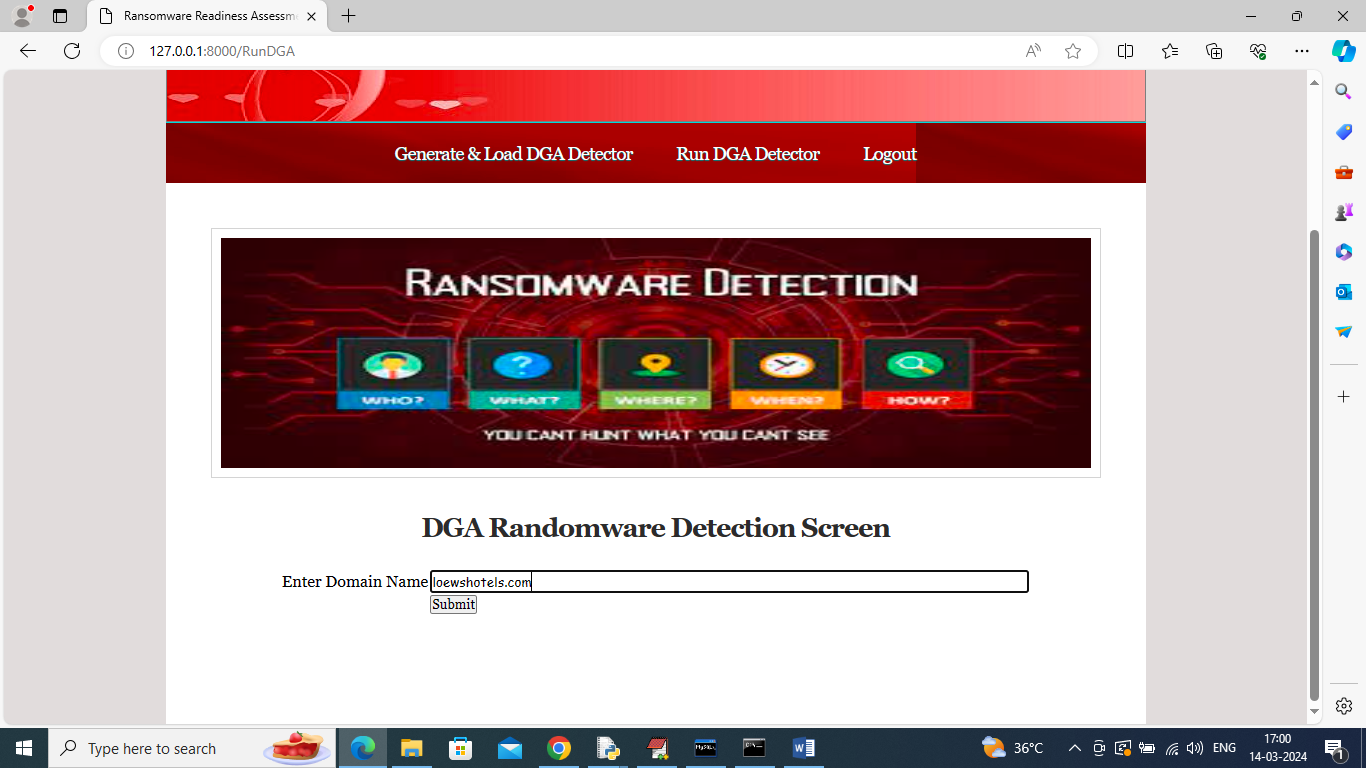


In above screen DGA detector detection accuracy is 95% and in first line can DGA can detect 9 different Ransomware attacks and those attack names are

'alexa' 'bamital' 'cryptolocker' 'gameoverdga' 'goz' 'legit' 'necurs' 'newgoz' 'nivdort'

In above names ALEXA and LIGIT are normal domains

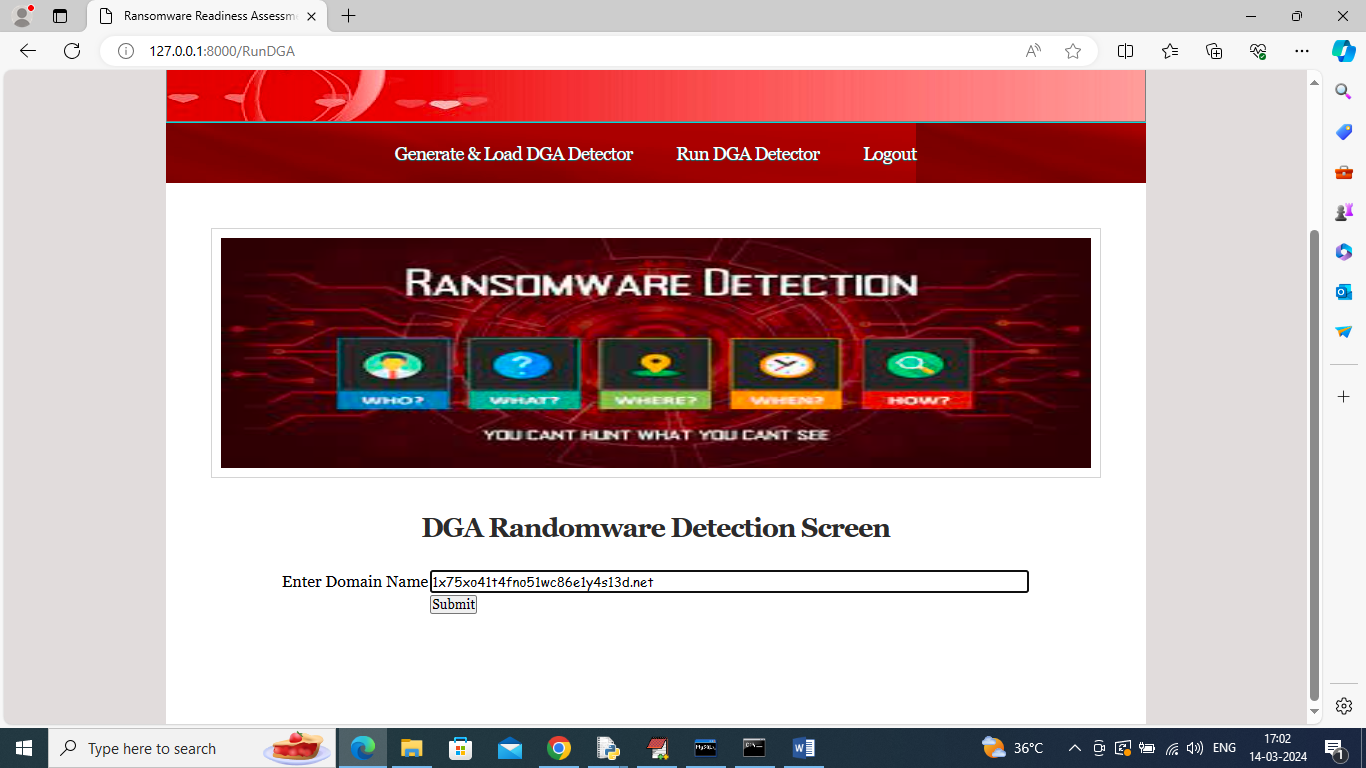
Now click on ‘Run DGA Detector’ link to get below page



In above screen in entered some domain name and this domain names you can take from ‘Test\_domain.txt’ file and now click on ‘Submit’ button to get below page

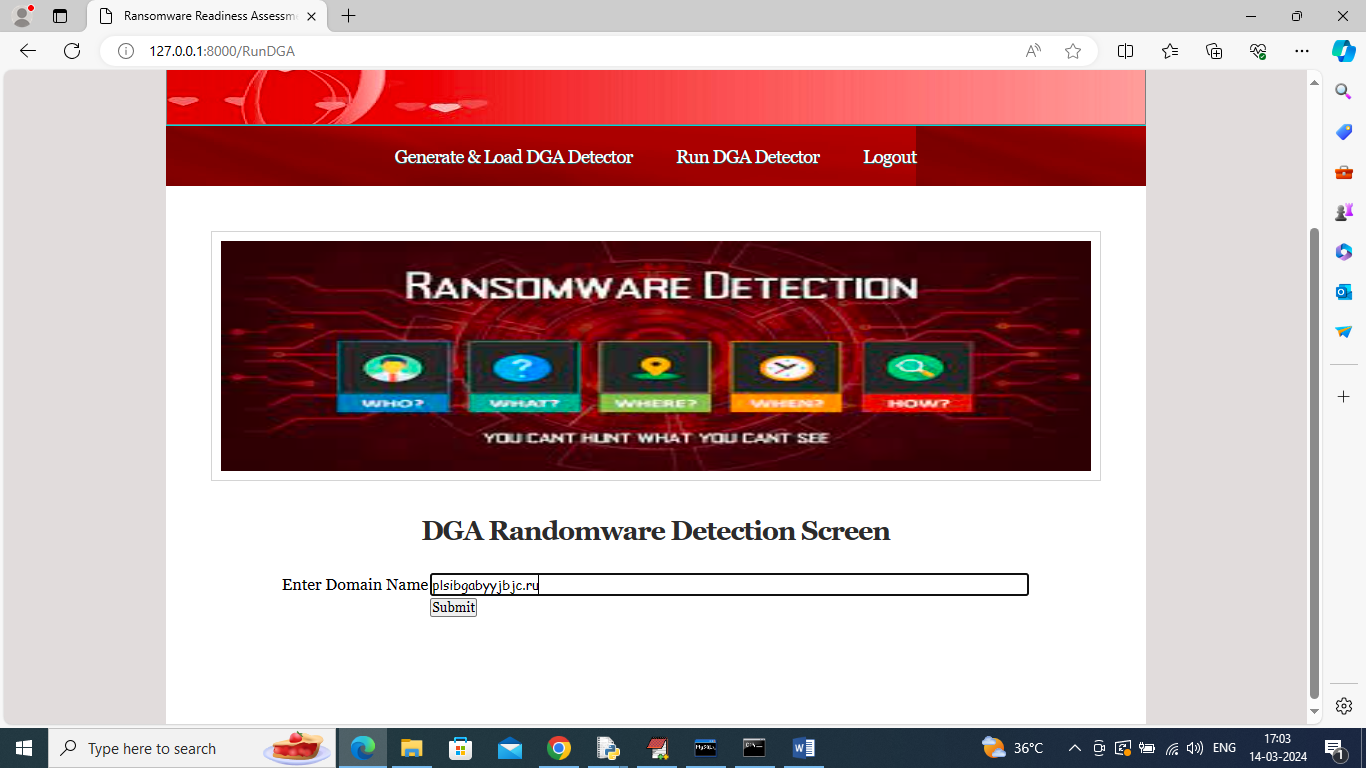


In above screen in blue colour text after ==🡺 symbol can see domain detected as ‘ALEXA’ and similarly you can enter some domain and get detection result.



For above domain will get below result





For above domain will get below detection result



In above screen domain detected as ‘crypto locker’.

Similarly enter any domain and get result