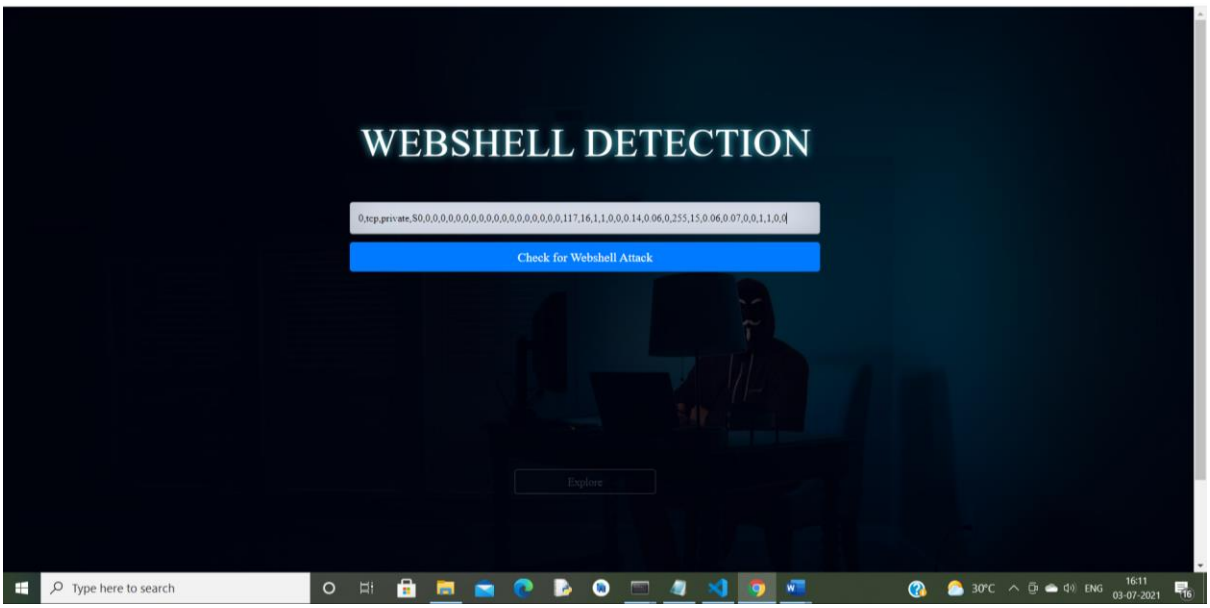
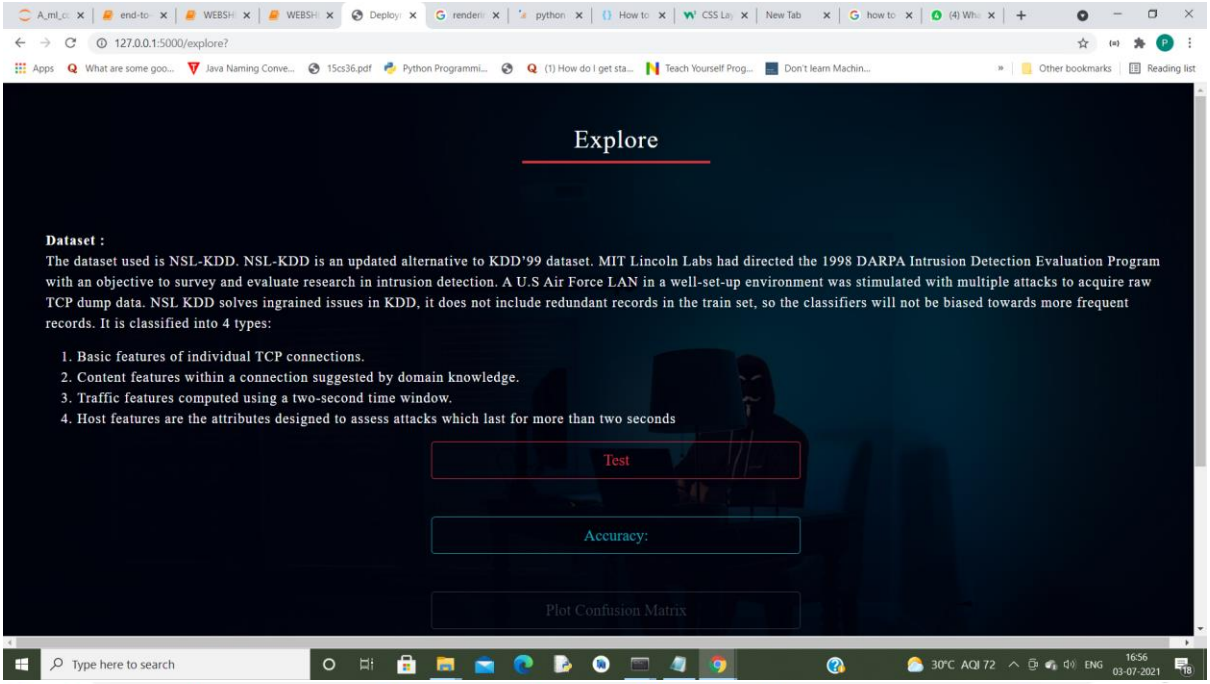
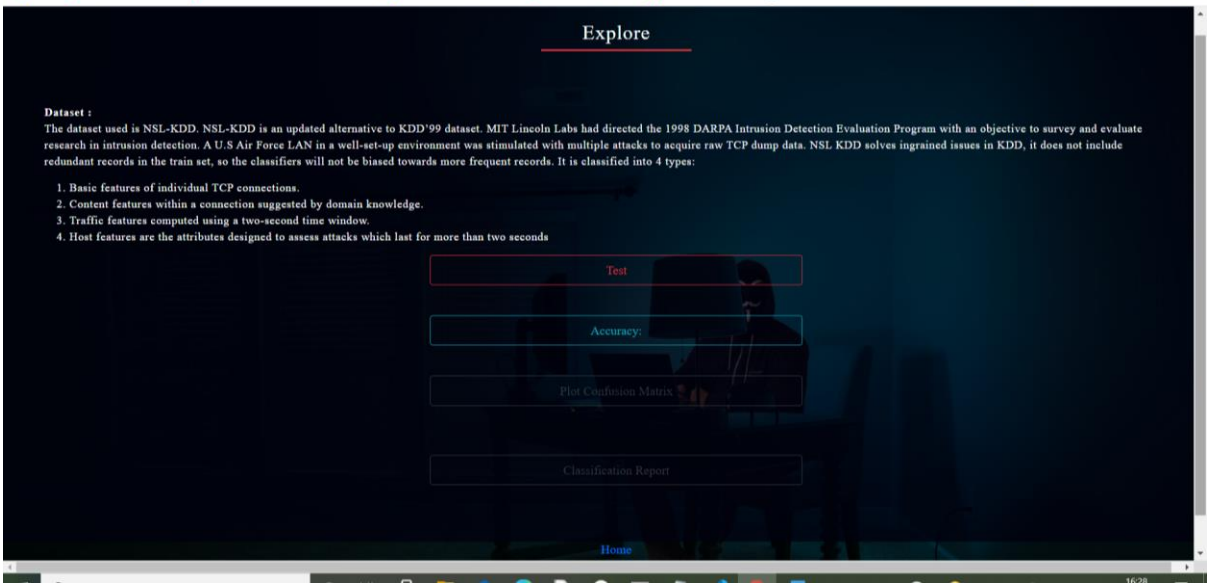
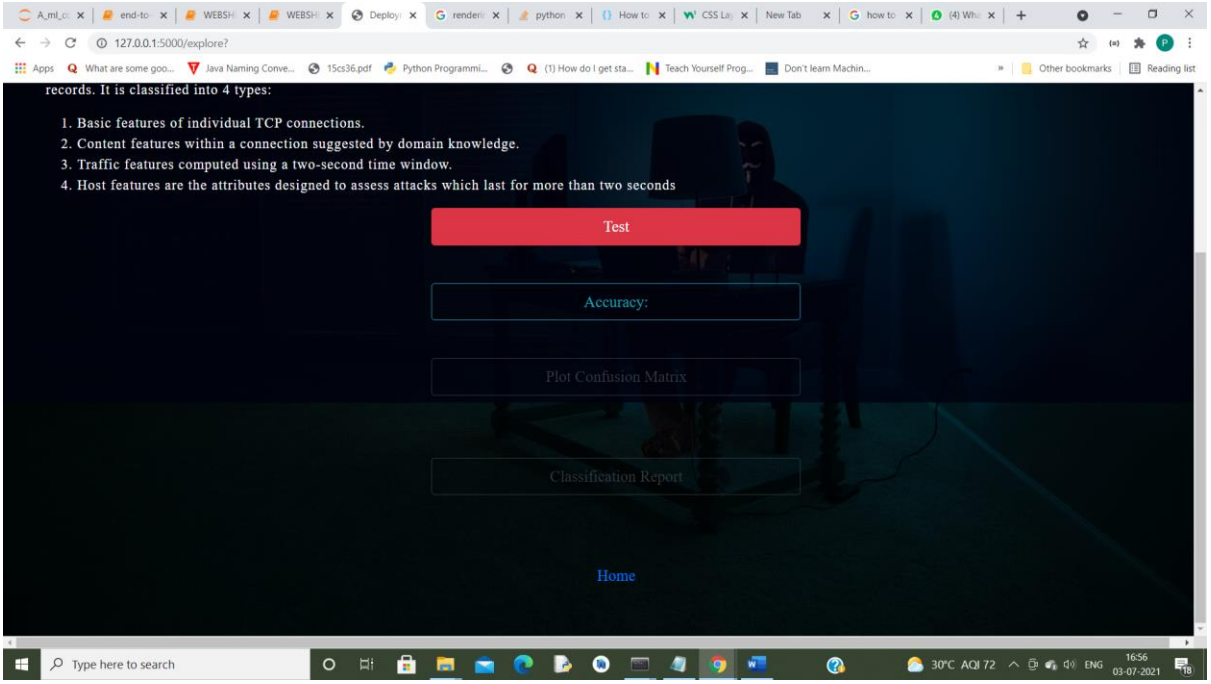
GUI sceenshots POOJA K P

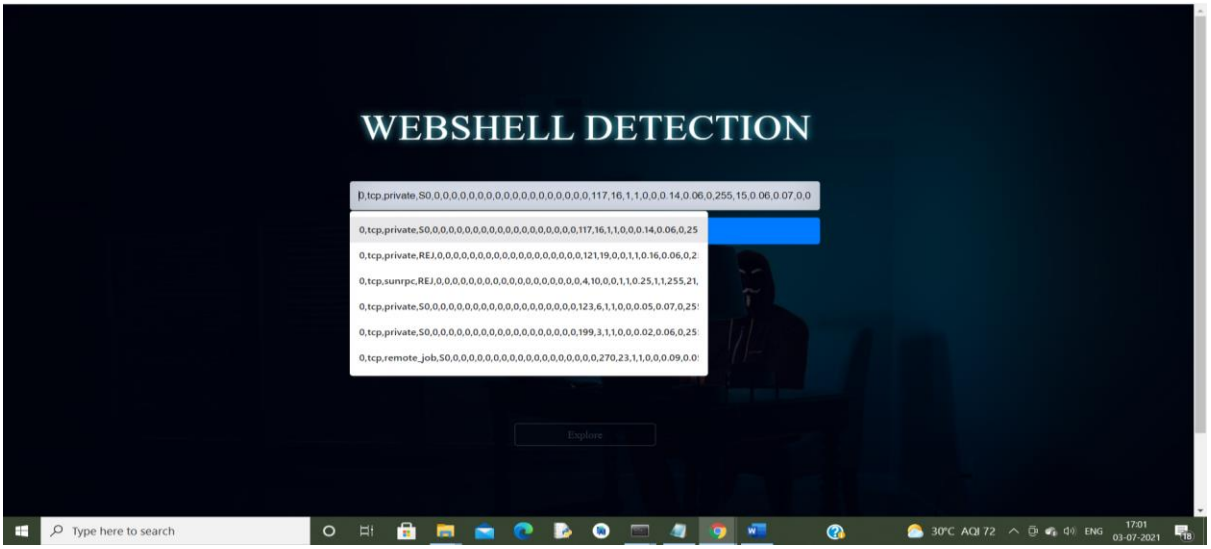


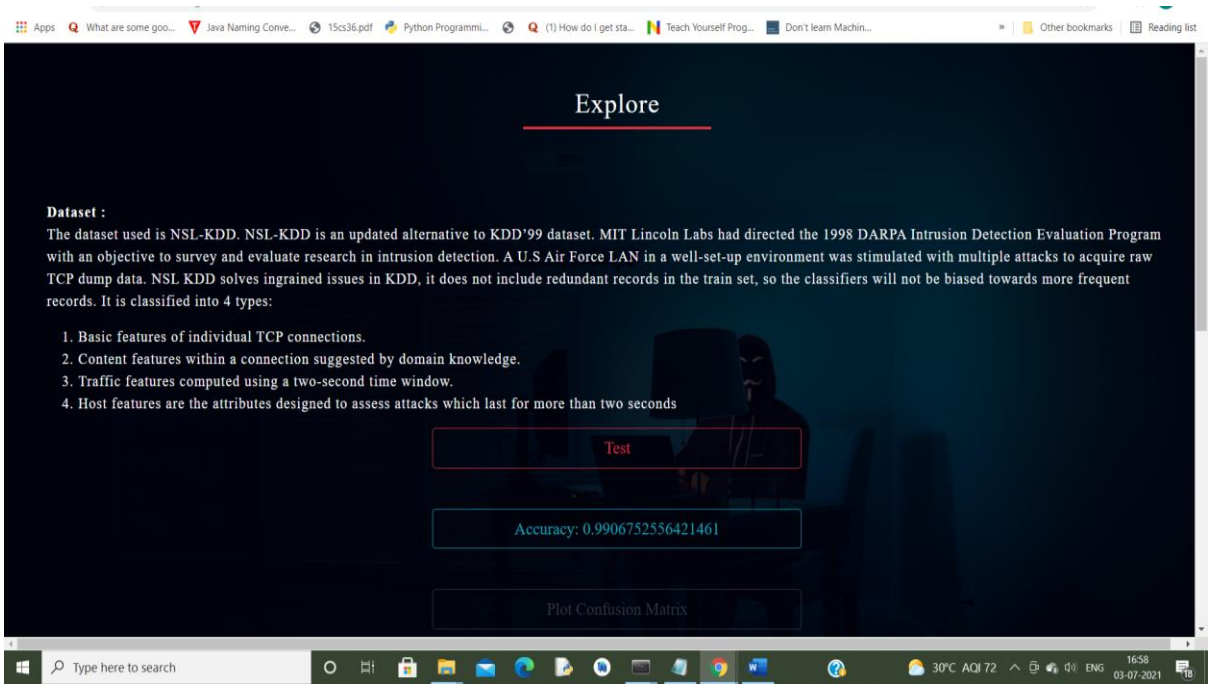


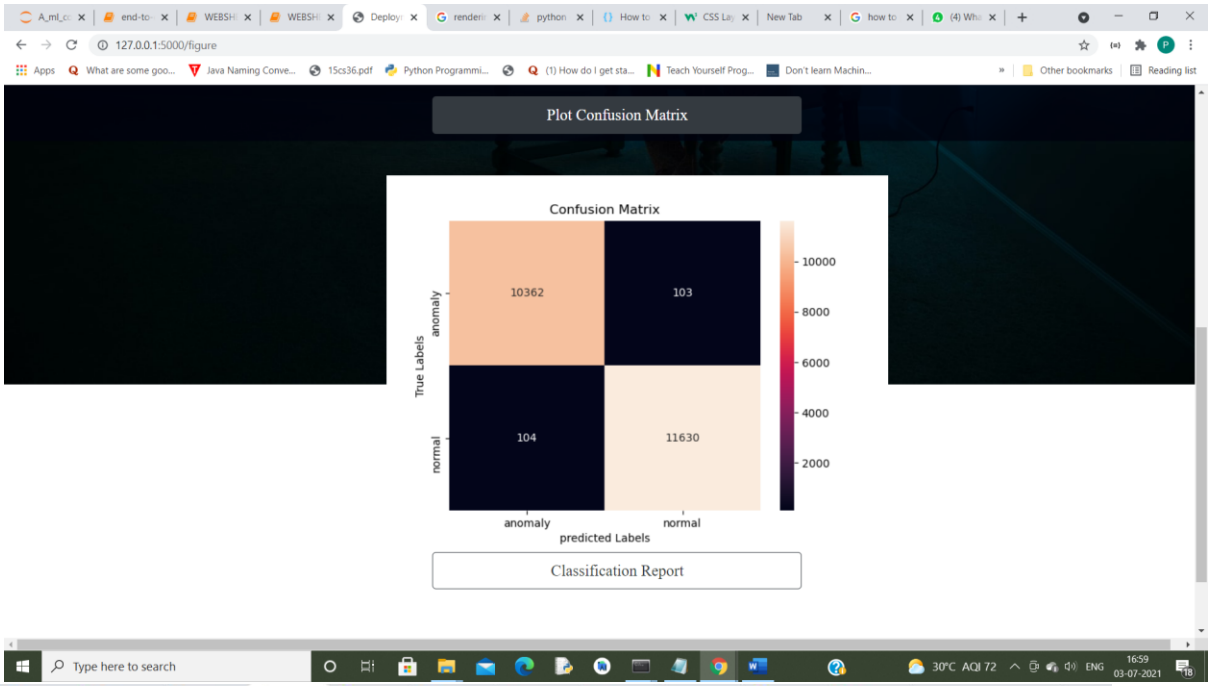


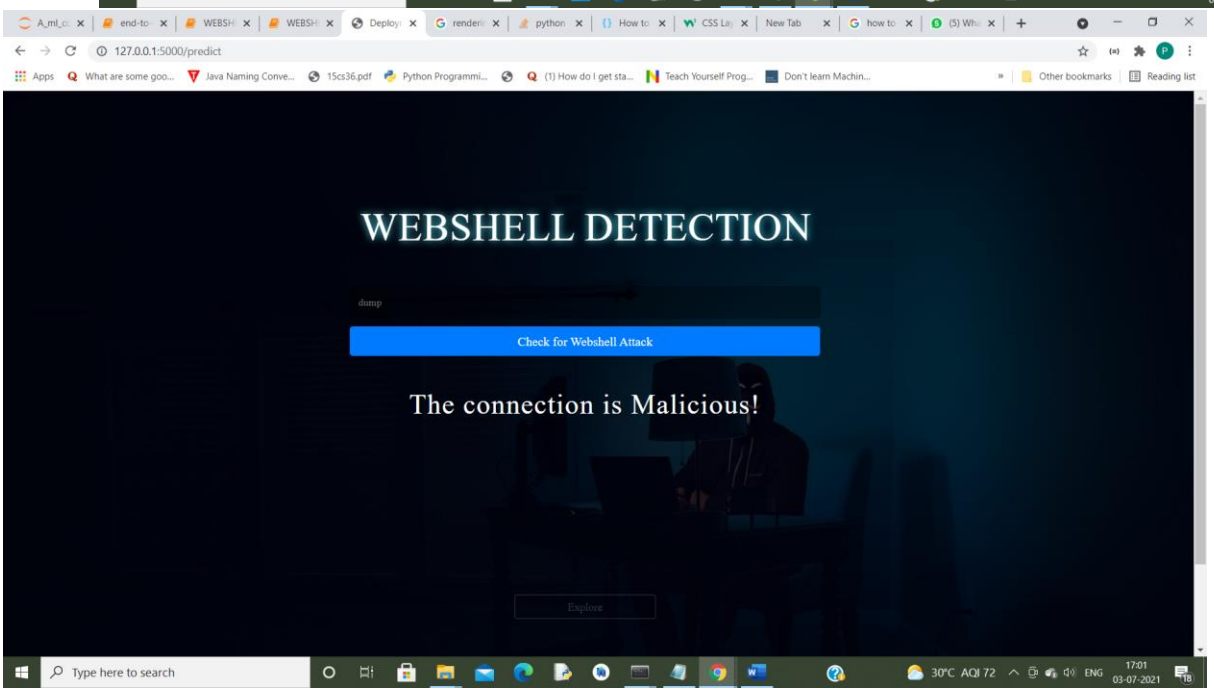

127.0.0.1:5000/explore?
records. It is classified into 4 types:
1. Basic features of individual TCP connections.
2. Content features within a connection suggested by domain knowledge.
3. Traffic features computed using a two-second time window.
4. Host features are the attributes designed to assess attacks which last for more than two seconds
Test
Accuracy:
Plot Confusion Matrix
Classification Report
Home

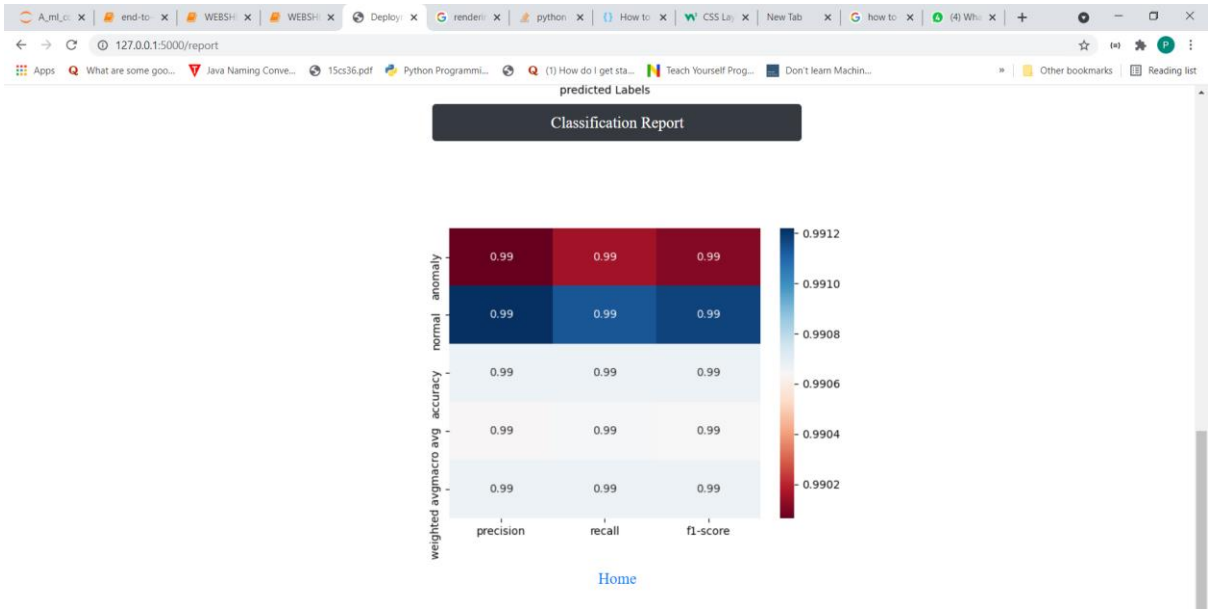
Outputs


WEBSHELL DETECTION
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,117,16,1,1,0,0,0.14,0.06,0,255,15,0.06,0.07,0,0
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,117,16,1,1,0,0,0.14,0.06,0,25
0,tcp,private,REJ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,121,19,0,0,1,1,0.16,0.06,0,2
0,tcp,sunrpc,REJ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,4,10,0,0,1,1,0.25,1,1,255,21,
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,123,6,1,1,0,0,0.05,0.07,0,25
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,199,3,1,1,0,0,0.02,0.06,0,25
0,tcp,remote_job,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,270,23,1,1,0,0,0.09,0.0
Explore


Explore
Dataset :
The dataset used is NSL-KDD. NSL-KDD is an updated alternative to KDD'99 dataset. MIT Lincoln Labs had directed the 1998 DARPA Intrusion Detection Evaluation Program with an objective to survey and evaluate research in intrusion detection. A U.S Air Force LAN in a well-set-up environment was stimulated with multiple attacks to acquire raw TCP dump data. NSL KDD solves ingrained issues in KDD, it does not include redundant records in the train set, so the classifiers will not be biased towards more frequent records. It is classified into 4 types:
1. Basic features of individual TCP connections.
2. Content features within a connection suggested by domain knowledge.
3. Traffic features computed using a two-second time window.
4. Host features are the attributes designed to assess attacks which last for more than two seconds
Test
Accuracy: 0.9906752556421461
Plot Confusion Matrix


127.0.0.1:5000/figure
Plot Confusion Matrix
Confusion Matrix
10362
103
104
11630
True Labels
anomaly
normal
predicted Labels
10000
8000
6000
4000
2000
Classification Report


127.0.0.1:5000/predict
WEBSHELL DETECTION
dump
Check for Webshell Attack
The connection is Malicious!
Explore


127.0.0.1:5000/report
predicted Labels
Classification Report
0.99
anomaly
normal
accuracy
macro avg
weighted avg
precision
recall
f1-score
0.9912
0.9910
0.9908
0.9906
0.9904
0.9902
Home