# NALAIYA THIRAN - IBM PROJECT REPORT

**(19EC406T - Professional Readiness for Innovation, Employability and Entrepreneurship)**

# ON

**WEB PHISHING DETECTION**

***Submitted by***

**TEAM ID: PNT2022TMID23445**

**DURGA DEVI M (113219041026)**

**SINDHU J (113219041109)**

**SUBHIKSHA P (113219041117)**

**SURTHIKA G (113219041119)**

***in partial fulfillment for the award of the degree of***

**BACHELOR OF ENGINEERING**

**IN**

**ELECTRONICS AND COMMUNICATION ENGINEERING**



**VELAMMAL ENGINEERING COLLEGE, CHENNAI-66.**

(An Autonomous Institution, Affiliated to Anna University, Chennai)

**2022-2023**

VELAMMAL ENGINEERING COLLEGE CHENNAI -66

(An Autonomous Institution, Affiliated to Anna University, Chennai)



**BONAFIDE CERTIFICATE**

Certified that this NALAIYA THIRAN – IBM PROJECT REPORT **“WEB PHISHING DETECTION”** is the Bonafide work of “DURGA DEVI M (113219041026), SINDHU J (113219041109), SUBHIKSHA P (113219041117), and SURTHIKA G (113219041119)” carried out in “PROFESSIONAL READINESS FOR INNOVATION, EMPLOYABILITY AND ENTREPRENEURSHIP (NALAIYA THIRAN-IBM PROJECT)**”** during the Academic Year 2022-2023.

**FACULTY EVALUATOR HEAD OF THE DEPARTMENT**

**Mr.K. RADHAKRISHANAN Dr.S.MARY JOANS**

**ASSISTANT PROFESSOR I PROFESSOR AND HEAD**

Dept. of Electronics and Communication Dept. of Electronics and Communication Engineering Engineering

Velammal Engineering College Velammal Engineering College

Chennai-600 066 Chennai-600 066

|  |  |  |  |
| --- | --- | --- | --- |
| **S.NO**  **1** |  | **TABLE OF CONTENT TITLE**  **ABSTRACT**  **INTRODUCTION** | **PAGE NO.**  **V**  **1** |
|  | 1.1 | Project overview | **1** |
|  | 1.2 | Purpose | **2** |
| **2** |  | **LITERATURE SURVEY** | **3** |
|  | 2.1 | Existing problems | **3** |
|  | 2.3 | Problem statement and definition | **3** |
| **3** |  | **IDEATION & PROPOSED SOLUTION** | **5** |
|  | 3.1 | Empathy Map Canvas | **5** |
|  | 3.2 | Ideation & Brainstorming | **6** |
|  | 3.3 | Proposed Solution | **6** |
|  | 3.4 | Problem Solution fit | **7** |
| **4** |  | **REQUIREMENT ANALYSIS** | **8** |
|  | 4.1 | Functional requirement | **8** |
|  | 4.2 | Non-Functional requirements | **9** |
| **5** |  | **PROJECT DESIGN** | **11** |
|  | 5.1 | Data Flow Diagrams | **11** |
|  | 5.2 | Solution & Technical Architecture | **12** |
|  | 5.3 | User Stories | **13** |
| **6** |  | **PROJECT PLANNING &SCHEDULING** | **15** |
|  | 6.1 | Sprint Planning & Estimation | **15** |
|  | 6.2 | Sprint Delivery Schedule | **16** |
|  | 6.3 | Reports from JIRA | **17** |
| **7** |  | **CODING & SOLUTIONING** | **20** |
|  |  | (Explain the features added in theproject along with code) |  |
|  | 7.1 | Feature 1 | **20** |
|  | 7.2 | Feature 2 | **21** |

|  |  |  |  |
| --- | --- | --- | --- |
| **8** |  | **TESTING** | **23** |
|  | 8.1 | Test Cases | **23** |
|  | 8.2 | User Acceptance Testing | **24** |
| **9** |  | **RESULTS** | **25** |
|  | 9.1 | Performance Metrics | **25** |
| **10** |  | **ADVANTAGES & DISADVANTAGES** | **26** |
| **11** |  | **CONCLUSION** | **27** |
| **12** |  | **FUTURE SCOPE** | **28** |
| **13** |  | **REFERENCE** | **30** |
| **14** |  | **APPENDIX** | **31** |

SOURCE CODE **31**

GITHUB & PROJECT DEMO LINK **46**

# ABSTRACT

A web service is one of the most important Internet communications software services. Using fraudulent methods to get personal information is becoming increasingly widespread these days. However, it makes our lives easier, it leads to numerous security vulnerabilities to the Internet's private structure. Web phishing is just one of the many security risks that web services face. Phishing assaults are usually detected by experienced users however, security is a primary concern for system users who are unaware of such situations. Phishing is the act of portraying malicious web runners as genuine web runners to obtain sensitive information from the end-user. Phishing is currently regarded as one of the most dangerous threats to web security. Vicious Web sites significantly encourage Internet criminal activity and inhibit the growth of Web services. As a result, there has been a tremendous push to build a comprehensive solution to prevent users from accessing such websites. We suggest a literacy-based strategy to categorize Web sites into three categories: benign, spam, and malicious. Our technology merely examines the Uniform Resource Locator (URL) itself, not the content of Web pages. As a result, it removes run-time stillness and the risk of drug users being exposed to cyber surfer-based vulnerabilities. When compared to a blacklisting service, our approach performs better on generality and content since it uses learning techniques.

# CHAPTER I

# INTRODUCTION

* 1. **PROJECT OVERVIEW:**

There are a number of users who purchase products online and make payments through e-banking. There are e-banking websites that ask users to provide sensitive data such as username, password & credit card details, etc., often for malicious reasons. This type of e-banking website is known as a phishing website. Web service is one of the key communications software services for the Internet. Web phishing is one of many security threats to web services on the Internet.

# Common threats of web phishing:

* + - Web phishing aims to steal private information, such as usernames, passwords, and credit card details, by way of impersonating a legitimate

entity.

* + - It will lead to information disclosure and property damage.
    - Large organizations may get trapped in different kinds of scams.
    - This Guided Project mainly focuses on applying a machine-learning algorithm to detect Phishing websites.

In order to detect and predict e-banking phishing websites, we proposed an intelligent, flexible and effective system that is based on using classification algorithms. We implemented classification algorithms and techniques to extract the phishing datasets criteria to classify their legitimacy. The e-banking phishing website can be detected based on some important characteristics like URL and domain identity, and security and encryption criteria in the final phishing detection rate. Once a user makes a transaction online when he makes payment through an e- banking website our system will use a data mining algorithm to detect whether the e-banking website is a phishing website or not.

# PURPOSE:

The purpose of this project is to design an intelligent system for detecting phishing websites. Phishing is one of the social attack which aims in stealing sensitive information of the users such as login credentials, credit card numbers etc. Here we have collected phishing dataset from phish Tanks as well as from phishing sites and are compared with the algorithms which classifies the phishing dataset into phishing or legitimate. We propose a web application for detection. The algorithm used is random forest in order to get better performance and accuracy. This system uses a database in order to store phishing websites which are already tested and can be used as blacklist, which makes the classification even faster, as it reduces repetition.

# CHAPTER 2 LITERATURE SURVEY

* 1. **EXISTING PROBLEM:**

There are many users who purchase products through online platform and the payment is done through e-banking. There are some fake banking websites in which they collect the more sensitive information like username, password, credit card details etc , for illegal purpose. This type of websites are called phishing website. Here web phishing is one of the security threat to webservices on the internet. we people are highly dependent on the internet. For performing online shopping and online activities like banking, mobile recharge and more activities are done only through internet. Here phishing is nothing but a type of website threat which illegally collects the original website information such as login id, password and credit card information.

# PROBLEM STATEMENT DEFINITION:

An online user needed to purchase something through an online. So he entered into the online website through internet. It takes some time to display the product. He started to see all the products. He search the necessary things in online website. At last he found the needed products. After that he entered all the credit card details, username and password for purchasing the things through online. Then he received the message "Your order is placed and transaction is successfully completed. You will receive the ordered product within 2 days”. After that within 24 hours he got a message in mobile and the bank account was empty then the customer shocked . Then only he realized that was a fake website and his bank account details was stolen by hacker.

Web phishing aims to steal private information, such as usernames, passwords, credit card details, by way of impersonating a legitimate entity. It will lead to information disclosure and property damage. This paper mainly focuses on applying a deep learning framework to detect phishing websites.

# PROBLEMS

* Malicious links will lead to a website that often steals login credentials or financial information like credit card numbers. Attachments from phishing emails can contain malware that once opened can leave the door open to the attacker to perform malicious behavior from the user's computer.
* Phishing attack examples

1. A spoofed email ostensibly from myuniversity.edu is mass distributed to as
2. The email claims that the user’s password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.
3. Email phishing scams:

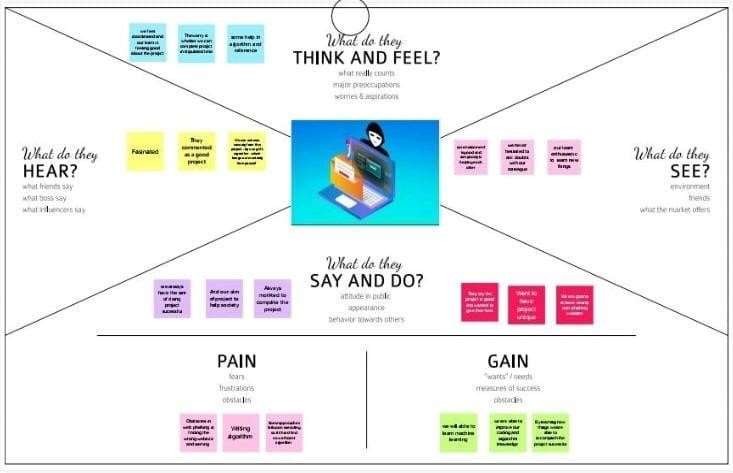
Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam. As seen above, there are some techniques attackers use to increase their success rates.For one, they will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization. Using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate.In addition, attackers will usually try to push users into action by creating a sense of urgency. For example, as previously shown, an email could threaten account expiration and place the recipient on a timer. Applying such pressure causes the user to be less diligent and more prone to error.Lastly, links inside messages resemble their legitimate counterparts, but typically have a misspelled domain name or extra subdomains.In the above example,the myuniversity.edu/renewal URL was changed to myuniversity.edurenewal.com. To overcome this we came with the solution of web phishing detection.

# CHAPTER 3

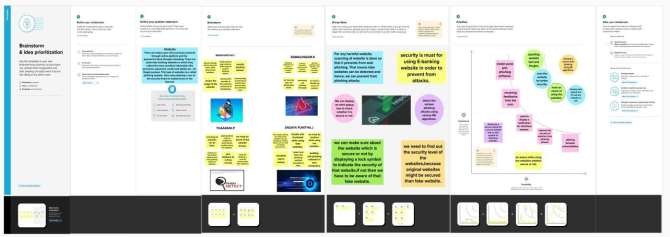
**IDEATION & PROPOSED SOLUTION**

# EMPATHY MAP CANVAS:

An empathy map is a simple, easy-to-digest visual that captures knowledge about a user’s behaviours and attitudes. It is a useful tool to helps teams better understand their users. Creating an effective solution requires understanding the true problem and the person who is experiencing it. The exercise of creating the map helps participants consider things from the user’s perspective along with his or her goals and challenges.



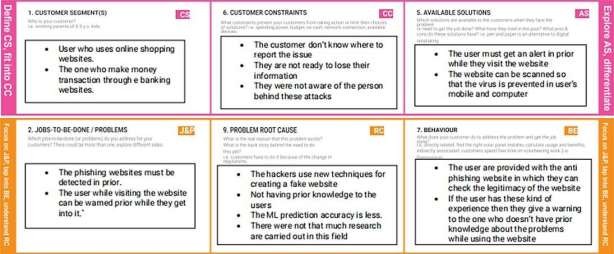
# IDEATION & BRAINSTROMING:



* 1. **PROPOSED SOLUTION:**

To overcome the problem of phishing website whenever we are clicking on one website it must show an alert box like it is a secure website or it is not a secure website Then another way is that we can scan the website in order to prevent our system or mobile from the phishing attack. Even though technologies are there we as the user have to be aware of the websites whether it is secure or not. We should not click any unwanted websites. The proposed approach has divided the hyperlink specific features into 12 different categories and used these features to train the machine learning algorithms. We have evaluated the performance of our proposed phishing detection approach on various classification algorithms using the phishing and non-phishing websites dataset.As we are using some websites but while clicking that website it display an alert box which leads to an aware of the customer which results in satisfaction of the user while using the websites, And another way is that we can scan the website in order to prevent the hacking of the information which makes even more satisfaction to the customer.

# PROBLEMSOLUTION FIT:



**CHAPTER 4 REQUIREMENTANALYSIS**

# FUNCTIONALREQUIREMENTS:

|  |  |  |
| --- | --- | --- |
| **FR No.** | **Functional Requirement(Epic)** | **Sub Requirement**  **(Story/sub-Task)** |
| FR-1 | User Input | User inputs an URL in  required field to check its validation. |
| FR-2 | Website Comparison | Model compares the websites using  Blacklist and Whitelist approach |
| FR-3 | Feature Extraction | After comparing, if none found on comparison then it extracts feature using  heuristic and visual similarity approach. |
| FR-4 | Prediction | Model predicts the URL using Machine Learning algorithms  such as Logistic Regression. |
| FR-5 | Classifier | Model sends all output to  classifier and produces final result. |
|  |  | Model then displays |

|  |  |  |
| --- | --- | --- |
| FR-6 | Announcement | whether website is a  legal site or a phishing site. |
| FR-7 | Events | This model needs the capability of retrieving and displaying accurate result for a website |

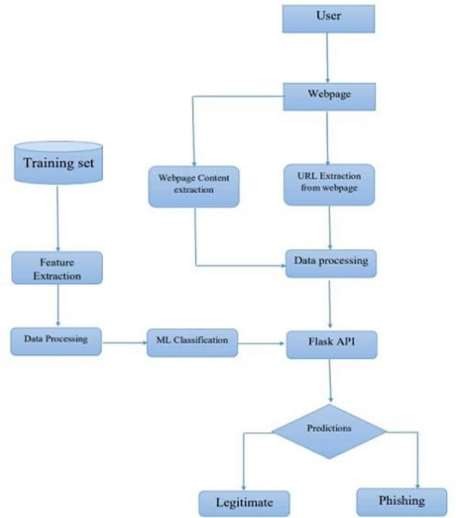
* 1. **NON-FUNCTIONALREQUIREMENTS:**

|  |  |  |
| --- | --- | --- |
| **FR No.** | **Non-Functional Requirement** | **Description** |
| NFR-1 | **Usability** | User can have full access to the particular websites they using must proceed some certain user friendly websites so  that it does not affect the datas. |
| NFR-2 | **Security** | To check whether the particular website is secure or not we can notify it by displaying an alert box while using the websites. |
|  |  | It must be a reliable |

|  |  |  |
| --- | --- | --- |
| NFR-3 | **Reliability** | source to the users  while they using the websites. |
| NFR-4 | **Performance** | The performance must be good while using the websites which the users proceeds the website. |
| NFR-5 | **Availability** | The website availability must be valid for the users to  access the resources. |
| NFR-6 | **Scalability** | It must be able to handle an increase in users and loads without disrupting the end users. |

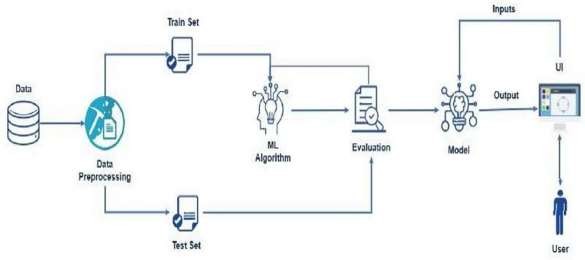
# CHAPTER 5 PROJECTDESIGN

* 1. **DATAFLOWDIAGRAMS:**



# SOLUTION &TECHNICAL ARCHITECTURE: SOLUTIONARCHITECTURE:

**TECHNICALARCHITECTURE:**



# USERSTORIES:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **User Type** | **Functional**  **Requirement**  **(Epic)** | **User Story Number** | **User Story / Task** | **Acceptance criteria** | **Priority** | **Release** |
| Customer (Mobile user) | Registration | USN-1 | As a user, I can register for the application by entering my email, password, and confirming my password. | I can access my account / dashboard | High | Sprint-1 |
|  |  | USN-2 | As a user, I will receive confirmation email once I have registered  for the application | I can receive confirmation email & click confirm | High | Sprint-1 |
|  |  | USN-3 | As a user, I can register for the application  through Facebook | I can register & access the dashboard with Facebook Login | Low | Sprint-2 |
|  |  | USN-4 | As a user, I can register for the application through Gmail |  | Medium | Sprint-1 |
|  | Login | USN-5 | As a user, I can log into the application by  entering email & password |  | High | Sprint-1 |
|  | Dashboard |  |  |  |  |  |
| Customer (Web user) | User input | USN-1 | As a user I can input the particular URL in the required | I can go access the website without any | High | Sprint-1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | field and waiting for validation. | problem |  |  |
| Customer Care Executive | Feature extraction | USN-1 | After I compare in case if none found on comparison then we can extract feature using heuristic and visual similarity approach. | As a User I can have comparison between websites for security. | High | Sprint-1 |
| Administrator | Prediction | USN-1 | Here the Model will predict the URL websites using Machine Learning algorithms such as Logistic Regression. | In this I can have correct prediction on the particular algorithms | High | Sprint-1 |
|  | Classifier | USN-2 | Here I will send all the model output to classifier in order to produce final result. | In this I will find the correct classifier for producing the result | Medium | Sprint-2 |

**CHAPTER 6**

# PROJECTPLANNING&SCHEDULING

* 1. **SPRINTPLANNING& ESTIMATION:**

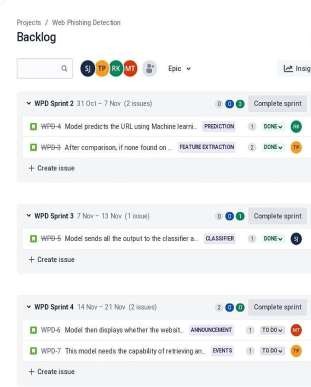
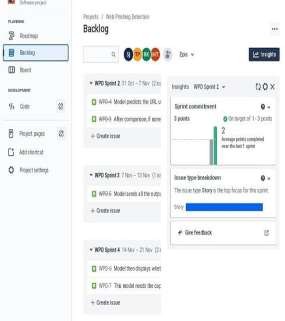
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sprint** | **Functional Requirement**  **(Epic)** | **User Story Number** | **User Story / Task** | **Story Points** | **Priority** | **Team Members** |
| Sprint-1 | User input | USN-1 | User inputs an URL in the required field to check its validation. | 1 | Medium | Durgadevi M |
| Sprint-1 | Website Comparison | USN-2 | Model compares the websites using Blacklist and Whitelist approach. | 1 | High | Sindhu J |
| Sprint-2 | Feature Extraction | USN-3 | After comparison, if none found on comparison then it extract feature using heuristic and visual similarity. | 2 | High | Subhiksha P |
| Sprint-2 | Prediction | USN-4 | Model predicts the URL using Machine learning algorithms such as logistic Regression. | 1 | Medium | Surthika G |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sprint-3 | Classifier | USN-5 | Model sends all the output to the classifier and produces the final result. | 1 | Medium | Durgadevi M |
| Sprint-4 | Announceme nt | USN-6 | Model then displays whether the website is legal site or a phishing site. | 1 | High | Sindhu J |
| Sprint-4 | Events | USN-7 | This model needsthe capability of retrieving and displaying accurate result for a website. | 1 | High | Subhiksha P |

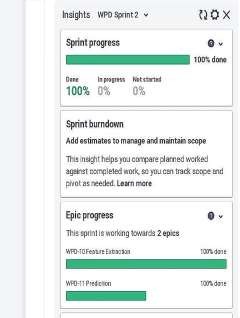
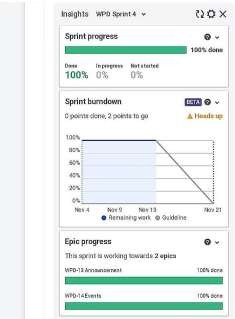
# SPRINTDELIVERYSCHEDULE:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sprint** | **Total Story Points** | **Duration** | **Sprint Start Date** | **Sprint End Date (Planned)** | **Story Points Completed (as on Planned End Date)** | **Sprint Release Date (Actual)** |
| Sprint-1 | 20 | 6 Days | 24 Oct 2022 | 29 Oct 2022 | 20 | 29 Oct 2022 |
| Sprint-2 | 20 | 6 Days | 31 Oct 2022 | 05 Nov 2022 | 20 | 05 Nov 2022 |
| Sprint-3 | 20 | 6 Days | 07 Nov 2022 | 12 Nov 2022 | 20 | 12 Nov 2022 |
| Sprint-4 | 20 | 6 Days | 14 Nov 2022 | 19 Nov 2022 | 20 | 19 Nov 2022 |

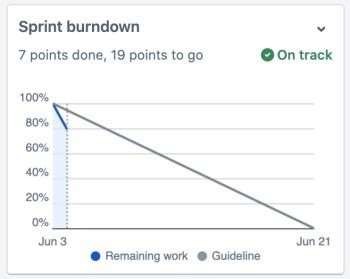
* 1. **REPORTS FROM JIRA: 1.BACKLOG:(BACKLOG-1 & BACKLOG-2)**

# SPRINTPROGRESS(FINALPROGRESS& INSIGHTS):



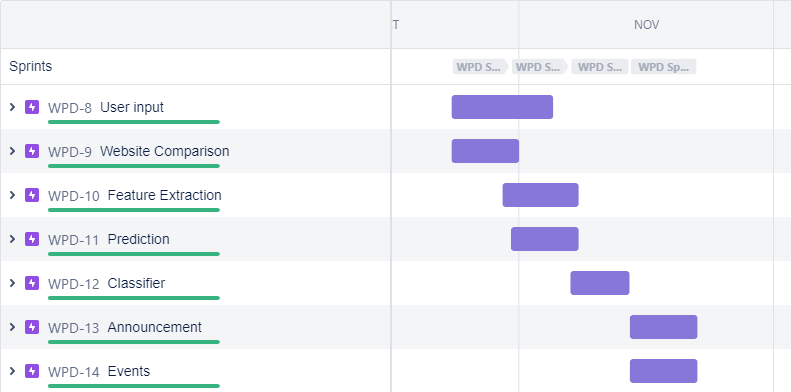
1. **SPRINTBURNDOWN:**



# SPRINT 1 &2:





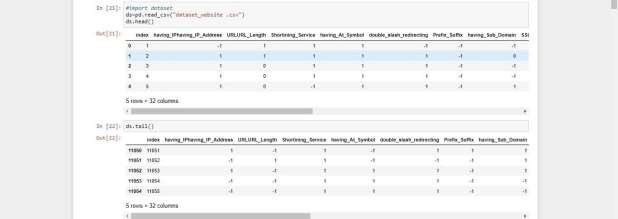
1. **SPRINT 4&5:**

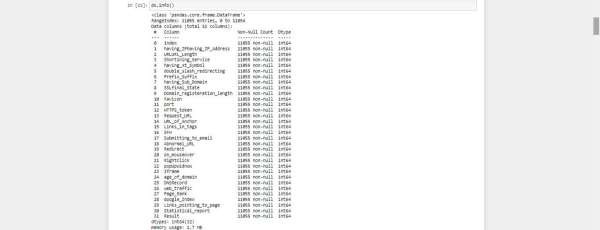
# CHAPTER 7 CODING& SOLUTIONING

* 1. **FEATURE 1:**

As a userbeforeusinganywebsitetheybringing thatwebsiteintoour

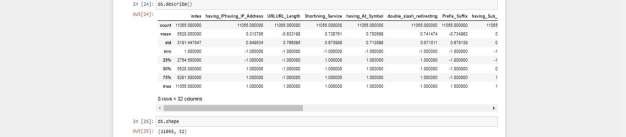
project URL and typing it . As the user types,it results whether it is a safe website or unsafe website in that porject URL so that before they entering into that website and giving thier personal information they may get aware of usage of that particular website to prevent the fake websites to be used by the user .By entering the website it predicts the safe or unsafe website.

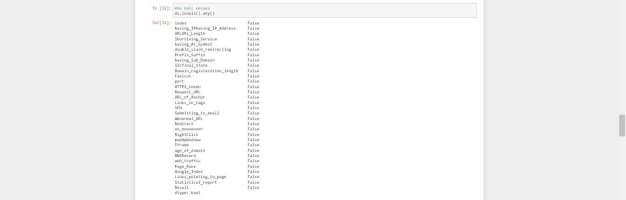


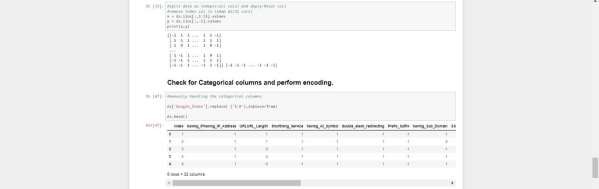


# FEATURE 2:

Here the user enters the URL in our project workspace, it predicts the safe or unsafe website in which the user will get alert of entering into that website as it alerts with a wordings namely **"it is safe website,and it is secure! or it is an unsafe website be cautious!".**By displaying the messageuser will surely be alert of using the website.









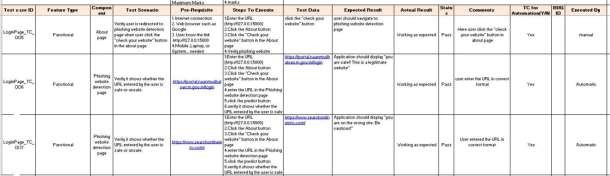


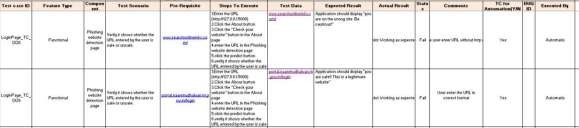


# TESTCASES:

**CHAPTER-8 TESTING**







# USERACCEPTANCETESTING:

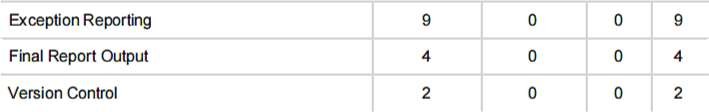
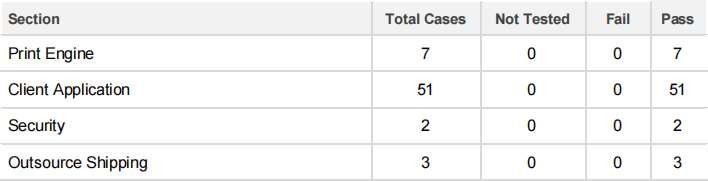
Here we briefly explained the test coverage and open issues of the Web Phishing Detection project at the time of the release to User Acceptance Testing (UAT).

# DEFECT ANALYSIS:

This report shows the number of resolved or closed bugs at each severity level, and how they were resolved



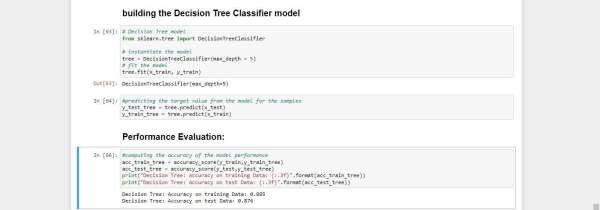
# TEST CASE ANALYSIS:

This report shows the number of test cases that have passed, failed, and untested

# CHAPTER 9 RESULTS

* 1. **PERFORMANCE METRICS:**

In this performance metrics,we have built a decision tree model classifier we predicted the accuracy of the training data and also the testing data.



# ADVANTAGES:

**CHAPTER 10 ADVANTAGES&DISADVANTAGES**

* + - Here we can easily predict the websitesecurity of the userwhlieusingthe particular website from the web browser.
    - By using our project URL the user can easily can get aware of the secure level of the particular website.
    - Sometimes the user need not get scare about giving their personal information if they predicted the particular website to be safe or unsafe if it is a safe website they can proceedfurther or if it's unsafemeanstheycan be even morecautious.

# DISADVANTAGES:

* + - As it depends on internet connectivity,wehave to make sure of a properinternet connection to proceedourproject URLplatform.
    - Here we have to enter the originalwebsite foridentifcation.
    - According to this predictionmight take a longer due to the availability of the internet services.

# CHAPTER 11 CONCLUSION

Our project aims to enhance detection method to detect phishing website using machine learning technology. Also , classifiers generated by machine learning algorithms identify legitimate phishing websites.The proposed technique can detect new temporary phishing sites and reduce the damage caused by phishing attacks. The performance of the proposed technique based on machine learning is more effective that previous phishing detection technologies. In the future, it will be useful to investigate the impact of feature selection using various algorithms.

# CHAPTER 12 FUTURESCOPE

In future in our project we try to inbuilt our URL with google for a safer access for the user to maintain a proper functioning of our project and also we will be using a pop up box for the alert of the user in order to make sure about the security level of the particular website in the usersystem or mobile so that theycan get aware of the usage of thewebsite.

In future we can develop an application for mobile phones and browser extension so it will automatically detect the legitimacy of the websites and warn the user if website is suspicious.

# REFERENCE

1. Higashino, M., Et Al. An Anti-phishing Training System For Security Awareness And Education Considering Prevention Of Information Leakage. In 2019 5th International Conference On Information Management (icim). 2019.
2. H. Bleau, Global Fraud And Cybercrime Forecast,. 2017.
3. Michel Lange, V., Et Al., Planning And Production Of Grammatical And Lexical Verbs In Multiword Messages. Plos One, 2017. 12(11): P. E0186685- e018668.
4. S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, “Who falls for phish?: a demographic

analysis of phishing susceptibility and effectiveness of interventions,” in Proceedings of the 28th international conference

on Human factors in computing systems, ser. CHI ’10. New York, NY, USA: ACM, 2010, pp. 373–382.

1. B. Krebs, “HBGary Federal hacked by Anonymous,” http:

//krebsonsecurity.com/2011/02/hbgary-federal-hacked-by- anonymous/, 2011, accessed December 2011.

1. B. Schneier, “Lockheed Martin hack linked to RSA’s SecurID breach,” <http://www.schneier.com/blog/archives/2011/05/lockheed>martin.html, 2011, accessed December 2011.
2. C. Whittaker, B. Ryner, and M. Nazif, “Large-scale automatic classification of phishing pages,” in NDSS ’10, 2010.
3. X. Dong, J. Clark, and J. Jacob, “Modelling user-phishing interaction,” in Human System Interactions, 2008 Conference on, may 2008, pp. 627 –632.

# APPENDIX

**SOURCECODES :**

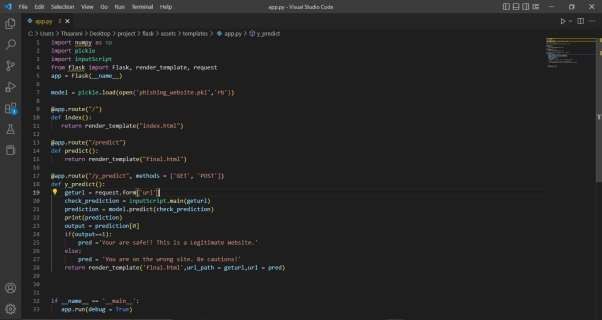
In the application, the user provides any website URL to check and the corresponding parameter values are generated by analysing the URL using which legitimate websites are detected.

# BUILDING THE PYTHON FLASK APPLICATION:

In the flask application, the URL is taken from the HTML page and it is scraped to get the different factors or the behavior of the URL. These factors are then given to the model to know if the URL is phishing or safe and is sent back to the HTML page to notify the user.

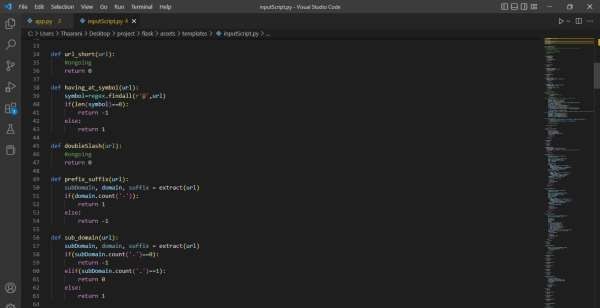
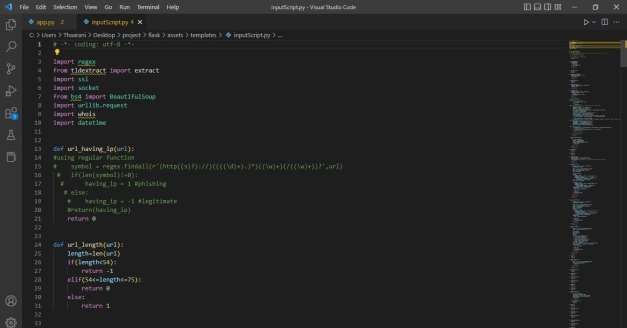
# APP.PYSOURCECODE:

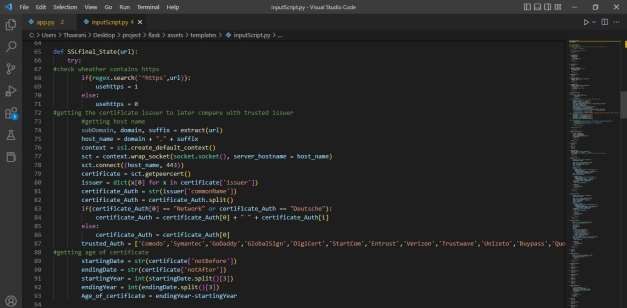
Here we havedone the app.pycode inorder to executethe Flask application.

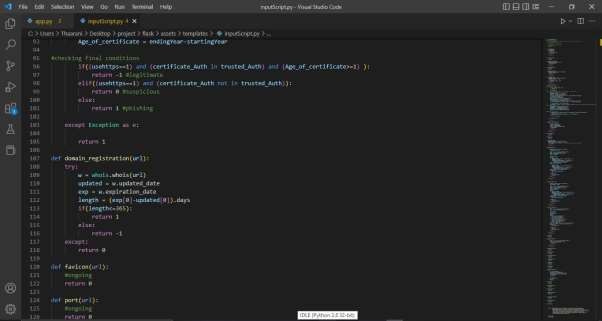


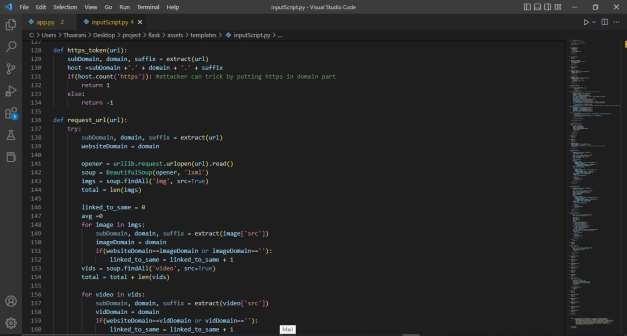
# INPUTSCRIPT.PYSOURCECODE:

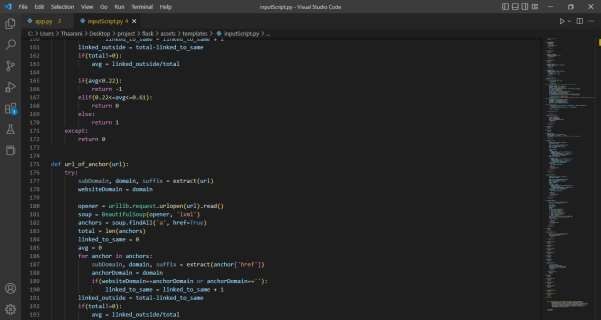
Afterexecuting the flaskapplication, we haveexecuted the inputscript.py file.

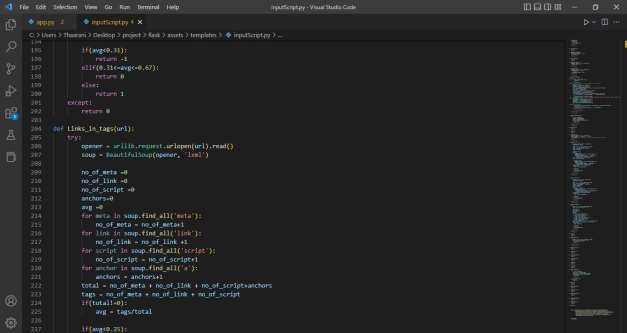


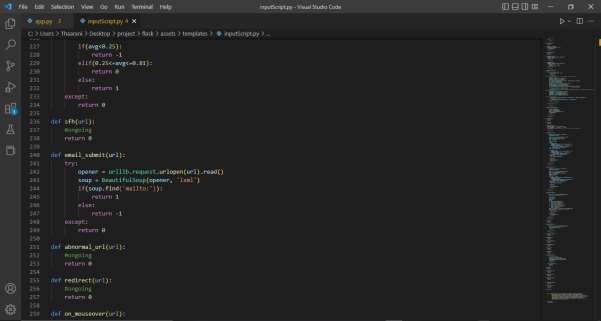


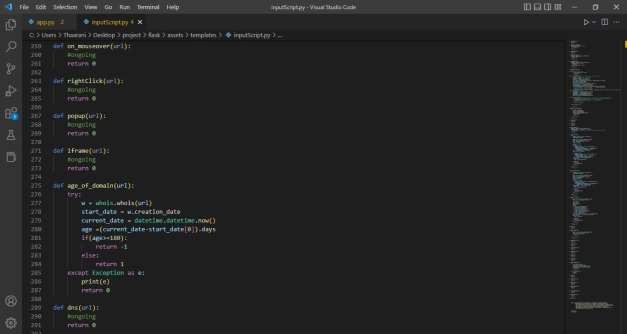


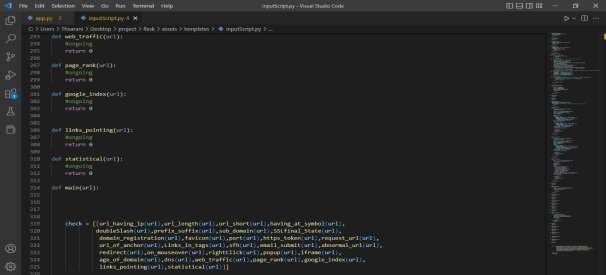


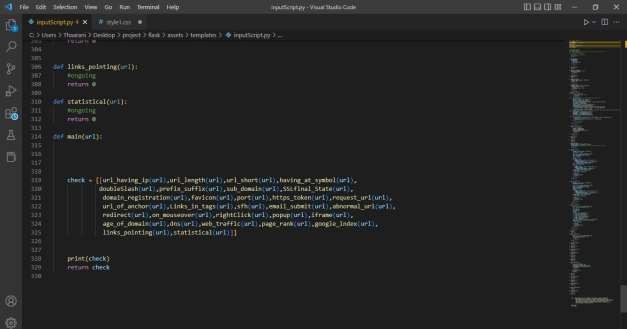








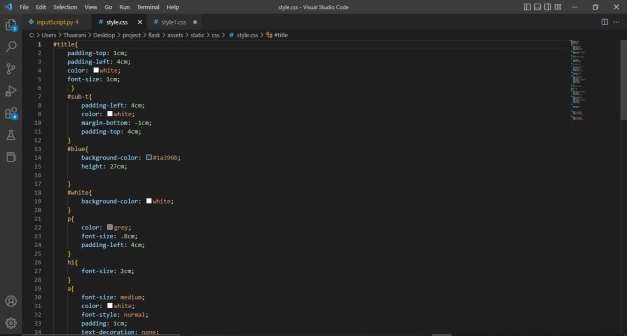


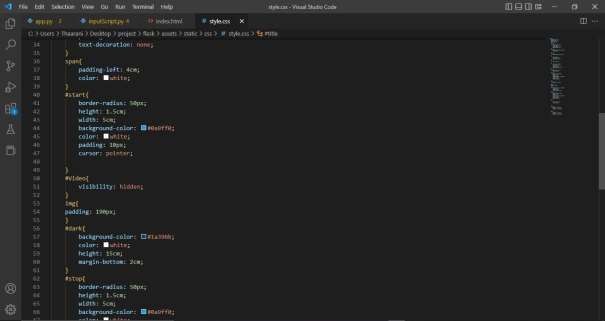


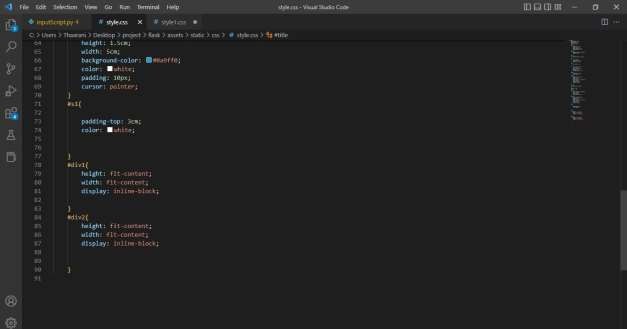
# Build An HTML Page

We Build an HTML page to take the URL as a text and upon clicking on the button for submission it has to redirect to the URL for “y\_predict” which returns if the URL given is phishing or safe. The output is to be then displayed on the page. The HTML pages are put under the templates folder and any style sheets if present is kept in the static folder.

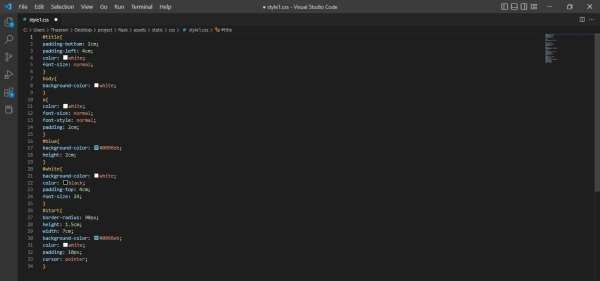
# here we first built a css file called style.css file



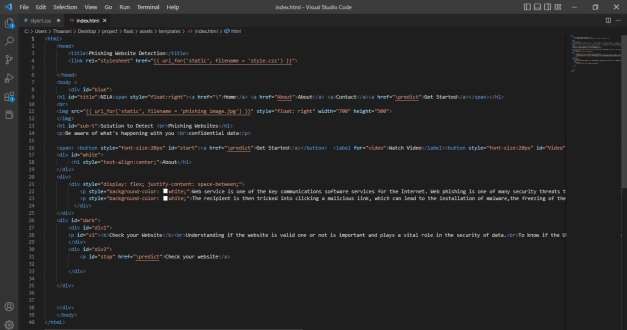




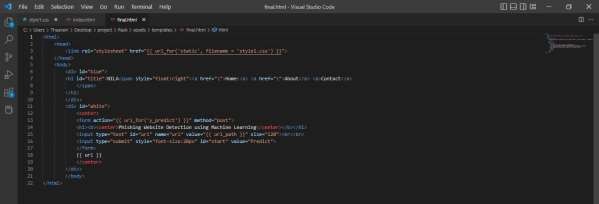
**style1.css**



# now moving on to the index.html source file



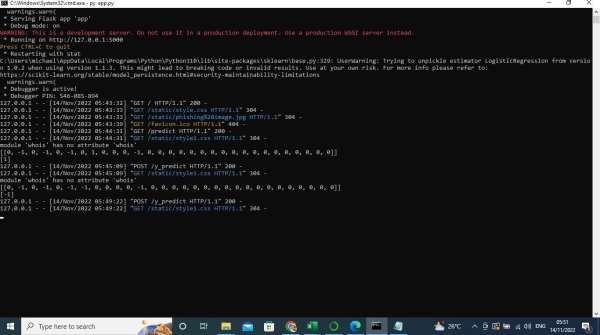
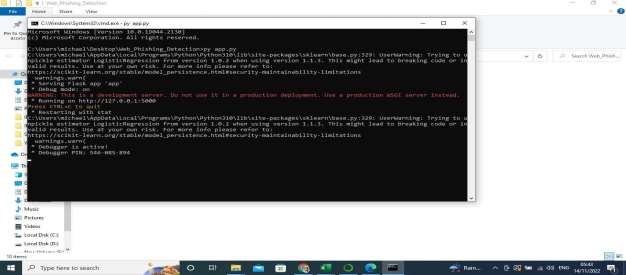
**now final.html source file**



# FINAL OUTPUT:

After executing the source codes we get the following outputs as follows

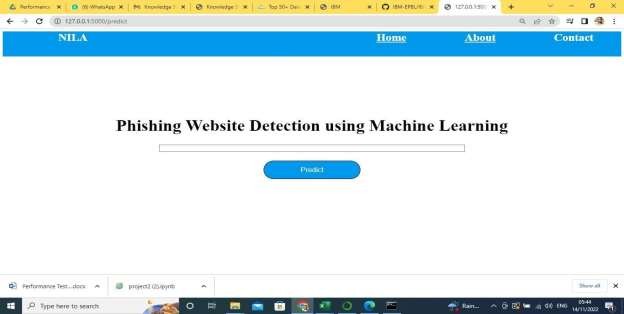
first we get a command prompt output with the URL over there we have to copy that particular URL and paste it in your web browser. In our project we have used google chrome web browser for the execution.



after the URL has been pasted we get the home page of our project web phishing detection

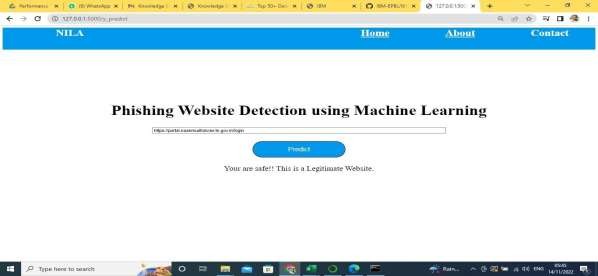


Here we have two options to predict the website one is we can click on check your website or you can click on get started to proceed your website prediction the diplay screen is as follows



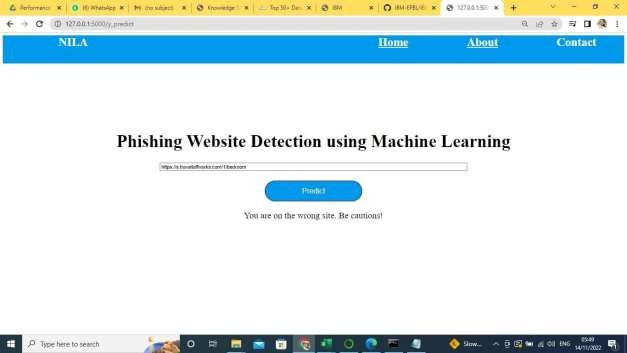
# PREDICTION OF SAFE WEBSITE:

Here we have used the original website as a prediction so now we have pasted that URL in our project web page and we clicked on Predict and here the result will be produced as **"YOU ARE SAFE! THIS IS A LEGITIMATE WEBSITE."**

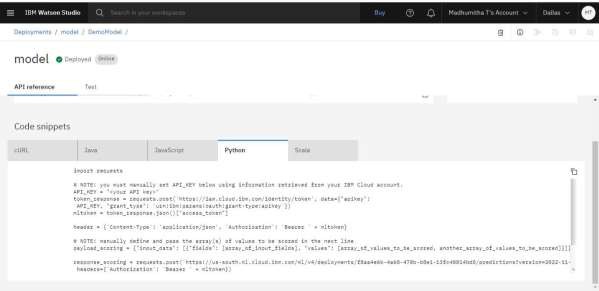


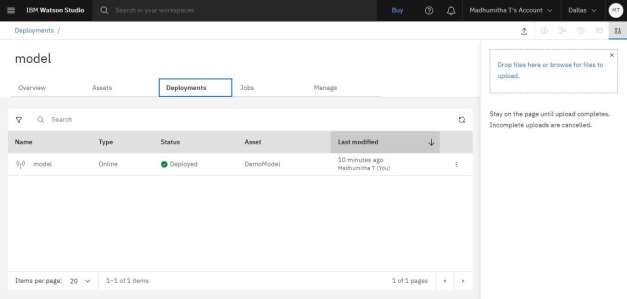
# PREDICTION OF UNSAFE WEBSITE:

Here we have used a fake website as a prediction so now we again pasted the fake URL in our project web page and we clicked on Predict and here the result will be produced as **"YOU ARE ON THE WRONG SITE BE CAUTIONS!"**

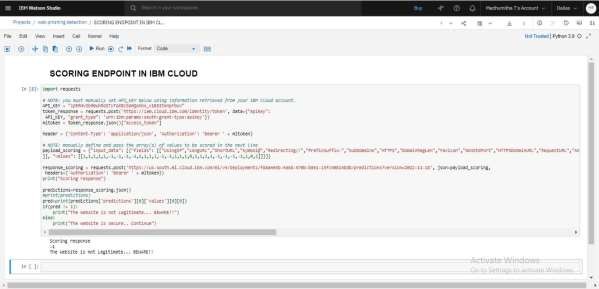


# IBM CLOUD DEPLOYMENT:

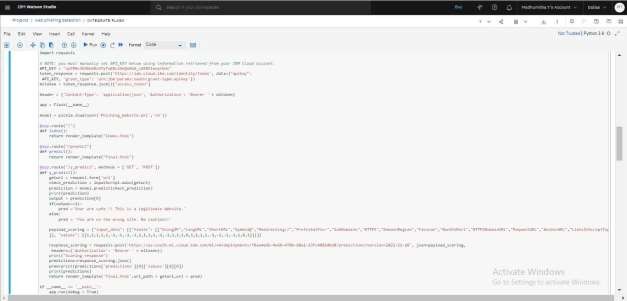




**SCORING ENDPOINTS IN IBM CLOUD:**



# INTEGRATING FLASK WITH IBM CLOUD:



**LINKS:**

**GITHUB LINK:** [IBM-EPBL/IBM-Project-22344-1659849670: Web Phishing](https://github.com/IBM-EPBL/IBM-Project-22344-1659849670)

[Detection (github.com)](https://github.com/IBM-EPBL/IBM-Project-22344-1659849670)

# VIDEO LINK: [click here](https://drive.google.com/file/d/1A2TBay-F2oRMmKUHV7Xne5yhtvLx6AD8/view?usp=share_link)