PREVENTION OF PHISHING WEBSITES

A. DURGA DEVI MADAM [1], Jannu Naveen[2],

[1]**Assistant professor, MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:- adurgadevi760@gmail.com
[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:- naveenjannu2002@gmail.com

ABSTRACT

Phishing attacks are a significant threat to online security, with attackers creating deceptive websites to steal sensitive information such as usernames, passwords, and credit card details. These fraudulent websites mimic legitimate sites, tricking users into providing their personal information. The increasing sophistication of phishing techniques demands robust and effective prevention strategies.This paper presents an overview of current methodologies and technologies used in the prevention of phishing websites. It explores various detection mechanisms including machine learning models, heuristic-based approaches, and blacklist/whitelist methods. Machine learning models are emphasized for their ability to adapt and detect new phishing patterns by analyzing website features such as URLs, domain names, and webpage content. The integration of heuristic approaches that examine specific characteristics of phishing websites provides an additional layer of detection. Blacklist and whitelist methods, though less adaptive, offer a straightforward approach to blocking known phishing sites.The paper also discusses the challenges faced in the prevention of phishing websites, such as the evasion tactics used by attackers to bypass detection mechanisms. It highlights the importance of real-time detection and the need for continuous updates to detection systems. Additionally, the role of user education in mitigating phishing attacks is examined, emphasizing the need for raising awareness about phishing tactics and safe browsing practices.In conclusion, the prevention of phishing websites requires a multi-faceted approach that combines advanced machine learning techniques, heuristic analysis, and user education. By leveraging these strategies, it is possible to enhance the detection and prevention of phishing websites, thereby safeguarding user data and maintaining the integrity of online services.

1 INTRODUCTION

Phishing attacks have emerged as one of the most pervasive threats in the digital world, posing significant risks to individuals, businesses, and institutions. These attacks typically involve the creation of deceptive websites that closely mimic legitimate sites with the intent of stealing sensitive information such as login credentials, financial details, and personal identification data. The ease with which phishing websites can be created and distributed, coupled with their increasing sophistication, makes them a formidable challenge for cybersecurity professionals.Phishing websites exploit human vulnerabilities, such as trust and lack of awareness, to achieve their malicious goals. Attackers employ a variety of tactics, including email spoofing, social engineering, and URL manipulation, to lure victims into divulging their personal information. The success of these attacks can lead to severe consequences, including financial losses, identity theft, and unauthorized access to sensitive systems.The detection and prevention of phishing websites have become critical components of cybersecurity strategies. Traditional methods, such as blacklisting known phishing domains and using heuristic rules to identify suspicious websites, have been effective to some extent but are insufficient in dealing with the dynamic nature of phishing threats. As phishing techniques evolve, so must the methods used to combat them.Recent advancements in machine learning and artificial intelligence offer promising avenues for improving the detection and prevention of phishing websites. Machine learning models can analyze vast amounts of data to identify patterns and anomalies associated with phishing attempts. These models can be trained to recognize the subtle indicators of phishing websites, such as peculiarities in URL structure, domain registration information, and content discrepancies.

2 RELEATED WORK

Prevention of Phishing Websites

The prevention of phishing websites has been the subject of extensive research, given the growing sophistication and frequency of phishing attacks. This literature survey explores the various methodologies, technologies, and strategies that have been proposed and implemented to detect and prevent phishing websites.

1. Blacklist and Whitelist Approaches

One of the earliest and most straightforward methods for preventing phishing is the use of blacklists and whitelists. Blacklists contain URLs of known phishing websites, and any attempt to access these sites is blocked. Whitelists, on the other hand, contain URLs of trusted sites, allowing access only to these pre-approved addresses. While these methods are easy to implement and provide quick protection against known threats, they suffer from limitations such as the inability to detect new or unknown phishing sites and the need for constant updates .

3 IMPLEMENTATION STUDY

Existing System:

The current landscape of phishing website prevention systems employs a combination of traditional and modern techniques to detect and block malicious sites. One of the most widely used methods is the implementation of blacklists, which contain URLs of known phishing websites. These lists are regularly updated and integrated into web browsers and security software to prevent users from accessing dangerous sites. Alongside blacklists, heuristic-based approaches are also prevalent. These methods utilize predefined rules and patterns to identify suspicious websites, examining characteristics such as URL structures, domain age, and page content for signs of phishing.Machine learning (ML) has significantly enhanced phishing detection capabilities.

To address the limitations of existing phishing prevention systems, a multi-layered and adaptive approach is proposed. This system integrates advanced machine learning techniques, real-time heuristic analysis, and proactive user education to provide comprehensive protection against phishing threats. The core of the proposed system is a robust machine learning framework that leverages deep learning and ensemble models to detect phishing websites. These models are trained on extensive datasets encompassing various phishing patterns and behaviors, enabling them to identify both known and novel phishing attempts with high accuracy.In addition to machine learning, the system incorporates dynamic heuristic analysis. Unlike traditional static rules, this approach continuously updates heuristics based on the latest phishing tactics observed in the wild. By analyzing real-time data such as URL structures, domain registration information, and website behavior, the system can swiftly adapt to new evasion techniques employed by attackers.Furthermore, the proposed system includes a real-time threat intelligence network that shares data across multiple platforms and stakeholders, including cybersecurity firms, internet service providers, and regulatory bodies. This collaborative effort ensures that the system is always informed of the latest phishing threats and can respond quickly to emerging attacks.

ADAVANTAGES:

The proposed system for preventing phishing websites offers several key advantages over traditional approaches, making it more effective and adaptive in combating phishing threats

IMPLEMENTATION

1 Modules Used in Project :-

Tensor flow

Tensor Flow is a free and open-source software library for dataflow and differentiable programming across a range of tasks. It is a symbolic math library, and is also used for machine learning applications such as neural networks. It is used for both research and production at Google.

Tens or Flow was developed by the Google Brain team for internal Google use. It was released under the Apache 2.0 open-source license on November 9, 2015.

Numpy

Numpy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays.

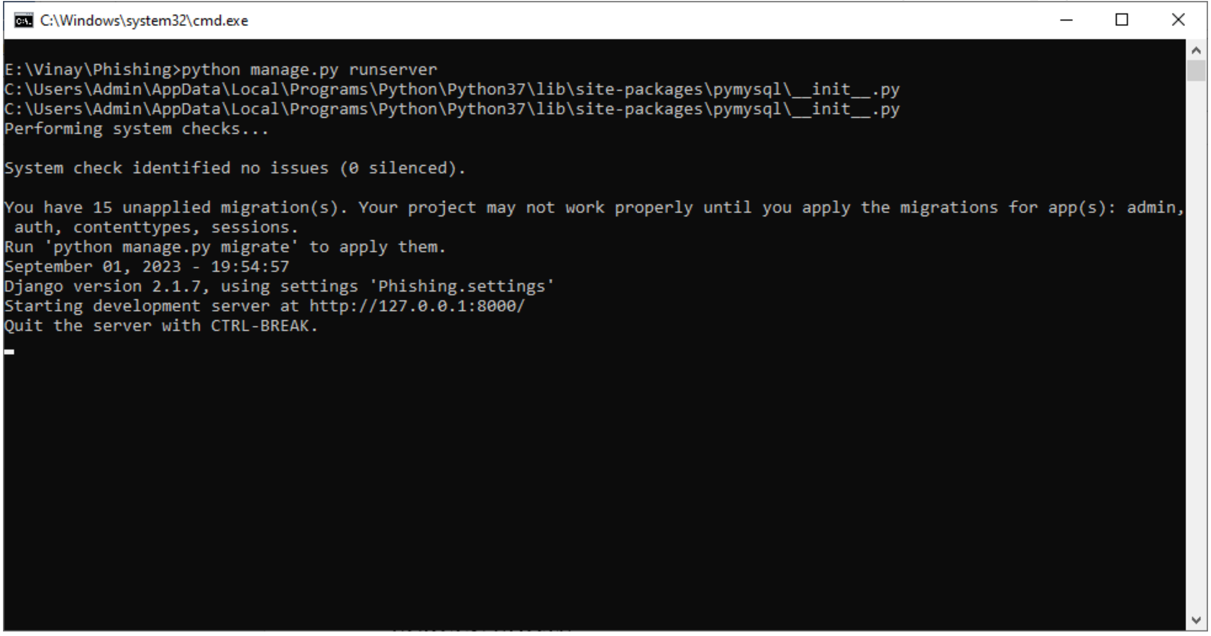
It is the fundamental package for scientific computing with Python. It contains various features including these important ones:

- A powerful N-dimensional array object
- Sophisticated (broadcasting) functions
- Tools for integrating C/C++ and Fortran code

5 RESULTS AND DISCUSSION

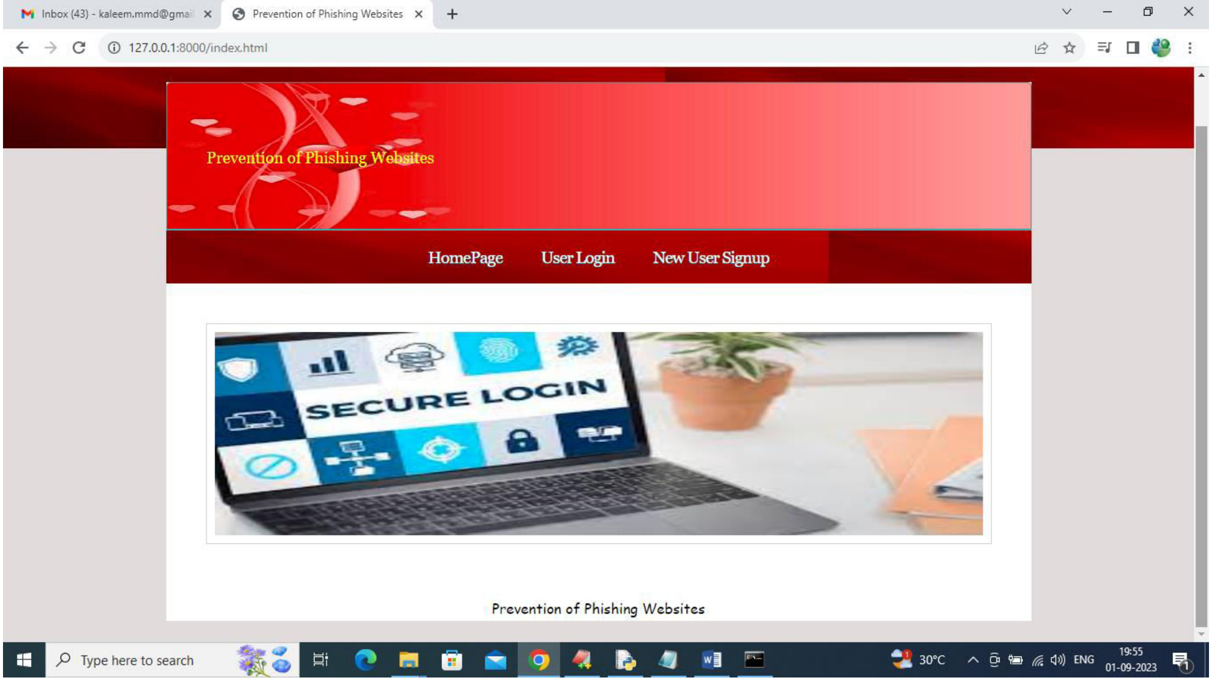
SCREENSHOTS

To run project copy content from database.txt file and paste in MYSQL console to create database and then double click on ‘ run.bat’ file to start DJANGO server and get below page



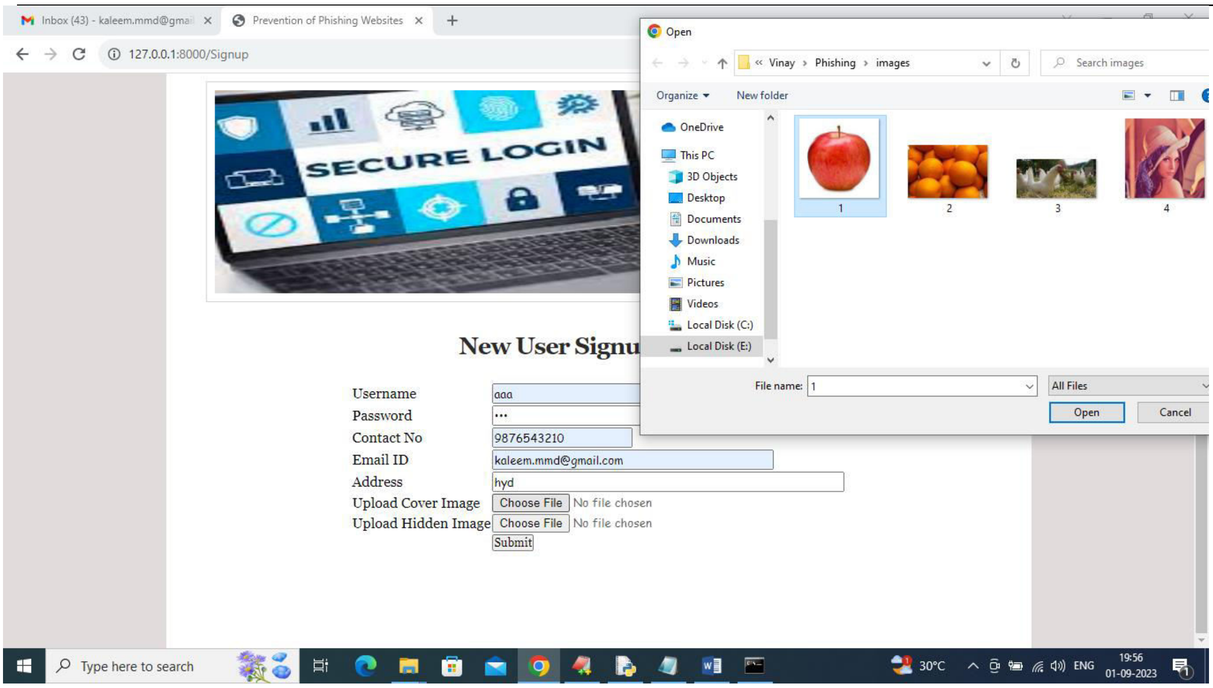
```
E:\Vinay\Phishing>python manage.py runserver
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
Performing system checks...

System check identified no issues (0 silenced).

You have 15 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin,
 auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
September 01, 2023 - 19:54:57
Django version 2.1.7, using settings 'Phishing.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

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



Inbox (43) - kaleem.mmd@gmail
Prevention of Phishing Websites
127.0.0.1:8000/index.html
Prevention of Phishing Websites
HomePage
User Login
New User Signup
SECURE LOGIN
Prevention of Phishing Websites
Type here to search
30°C
ENG
19:55
01-09-2023

In above screen click on ‘ New User Signup’ link to get below page

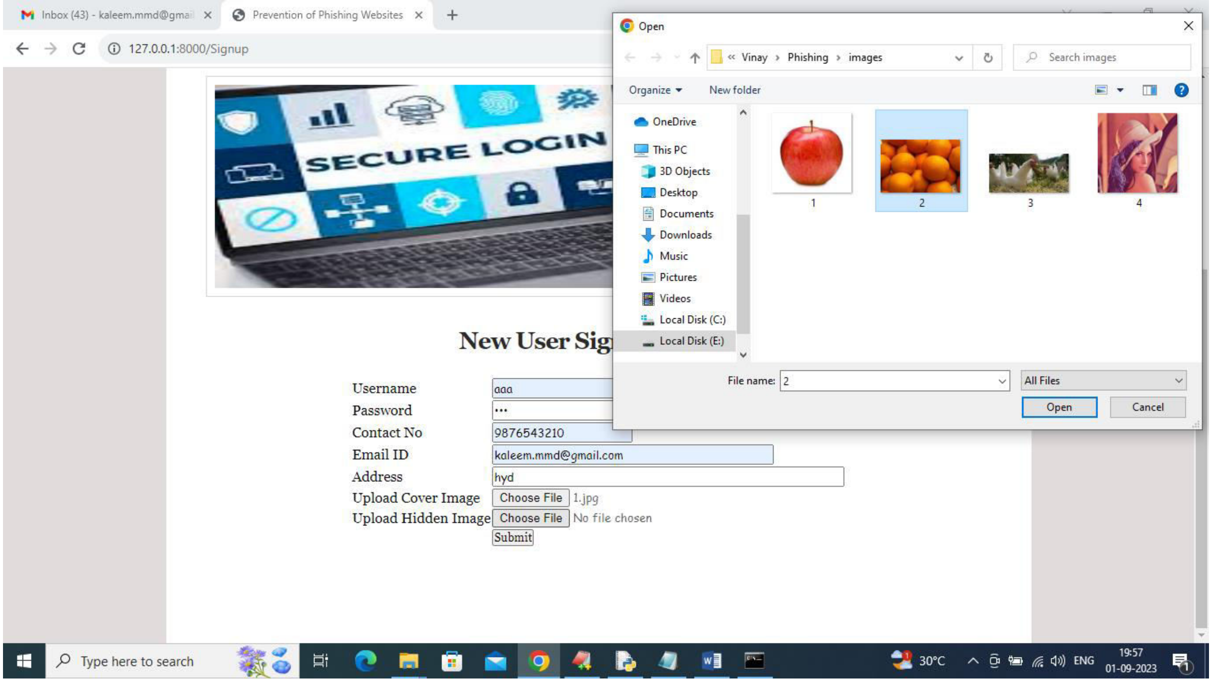


New User Signu

Username	aaa
Password	•••
Contact No	9876543210
Email ID	kaleem.mmd@gmail.com
Address	hyd
Upload Cover Image	Choose File No file chosen
Upload Hidden Image	Choose File No file chosen
	Submit

File name: 1

In above screen entering signup details and give valid EMAIL ID to receive OTP emails and then upload cover and hidden image and in above screen uploading apple as the cover image

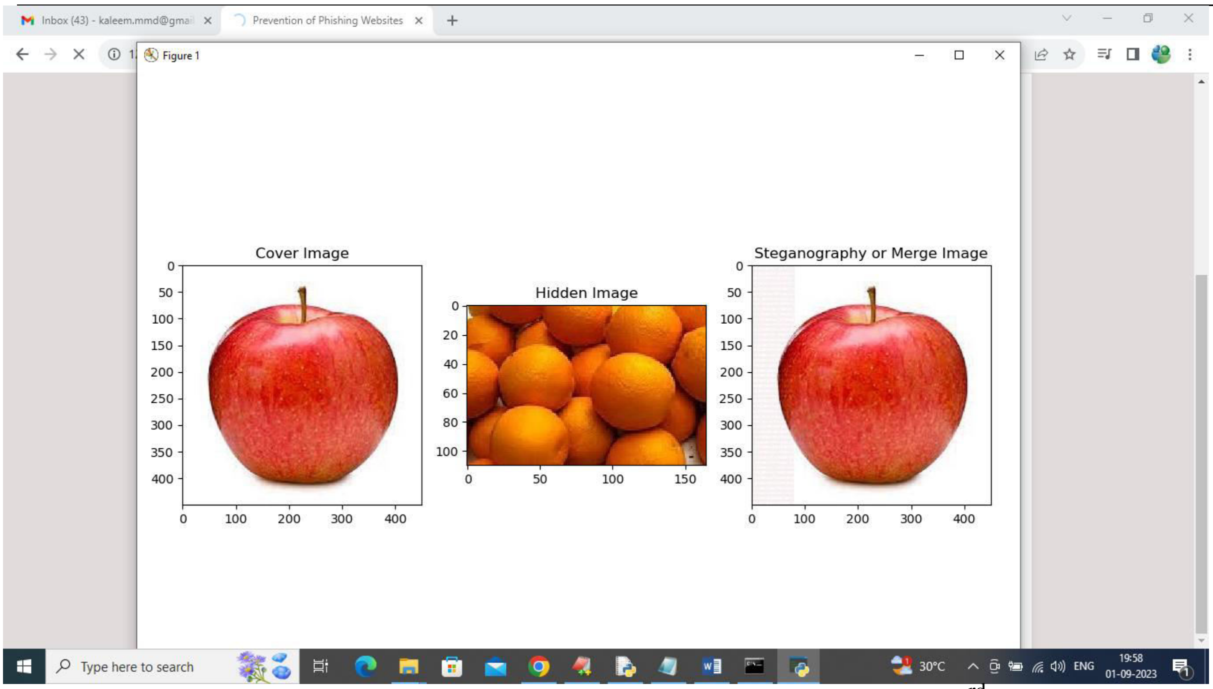


New User Sig

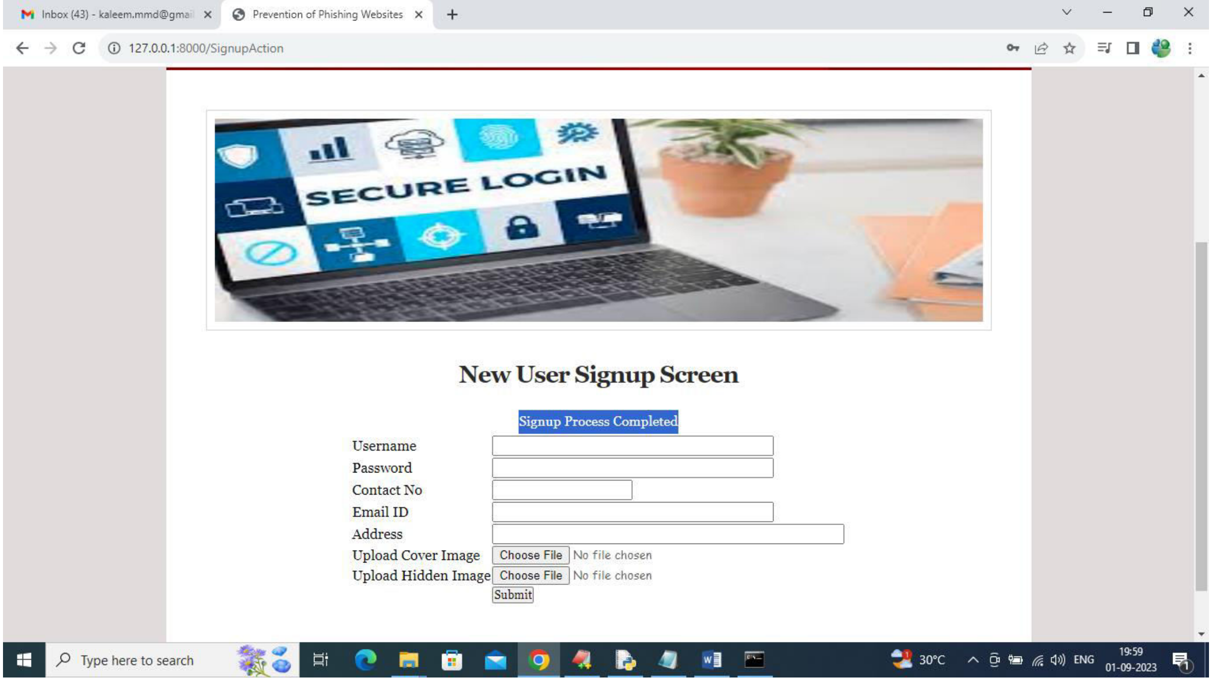
Username	aaa
Password	•••
Contact No	9876543210
Email ID	kaleem.mmd@gmail.com
Address	hyd
Upload Cover Image	Choose File 1.jpg
Upload Hidden Image	Choose File No file chosen
	Submit

File name: 2

In above screen uploading orange image as the secret or hidden image and then click on ‘ submit’ button to get below output



In above screen first we can see cover image then secret image and 3rd image is the merge or steganography image and after merging you can see slight difference in 3rd image compare to first image and now close above image to get below page

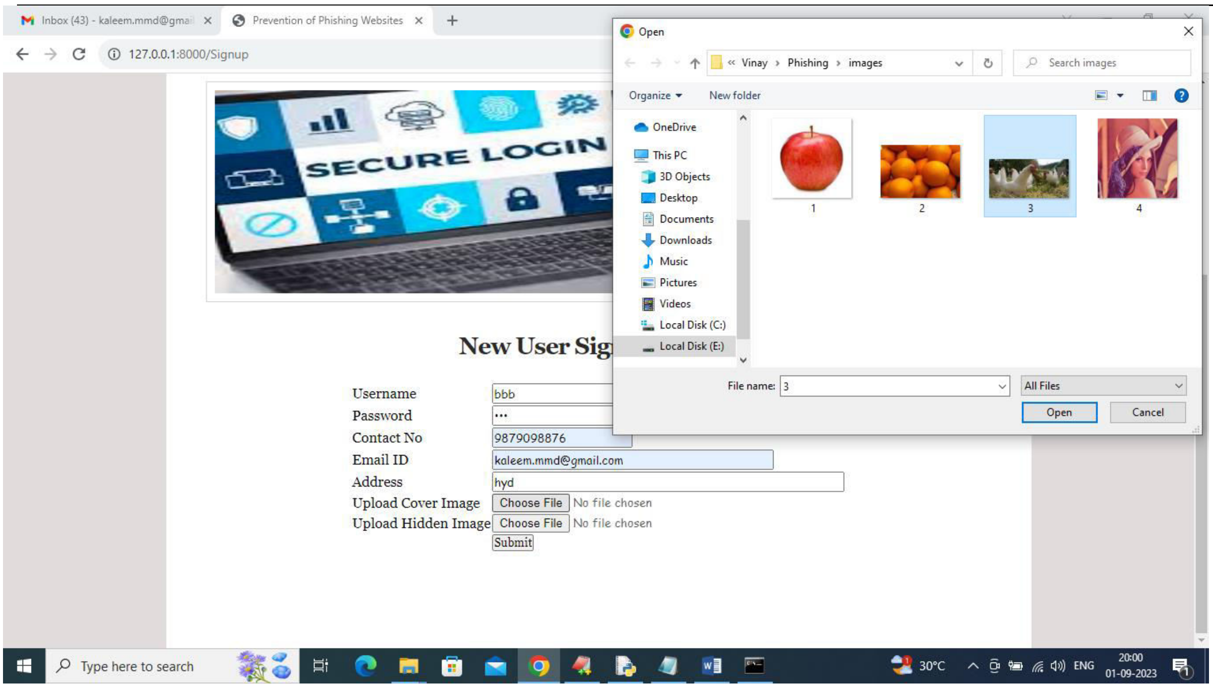

Inbox (43) - kaleem.mmd@gmail
Prevention of Phishing Websites
127.0.0.1:8000/SignupAction
SECURE LOGIN
Type here to search
30°C
ENG
19:59
01-09-2023

New User Signup Screen

Signup Process Completed

Username
Password
Contact No
Email ID
Address
Upload Cover Image Choose File No file chosen
Upload Hidden Image Choose File No file chosen
Submit

Inabove screen signup task completed and similarly add another user for fund transfer



New User Sig

Username bbb

Password •••

Contact No 9879098876

Email ID kaleem.mmd@gmail.com

Address hyd

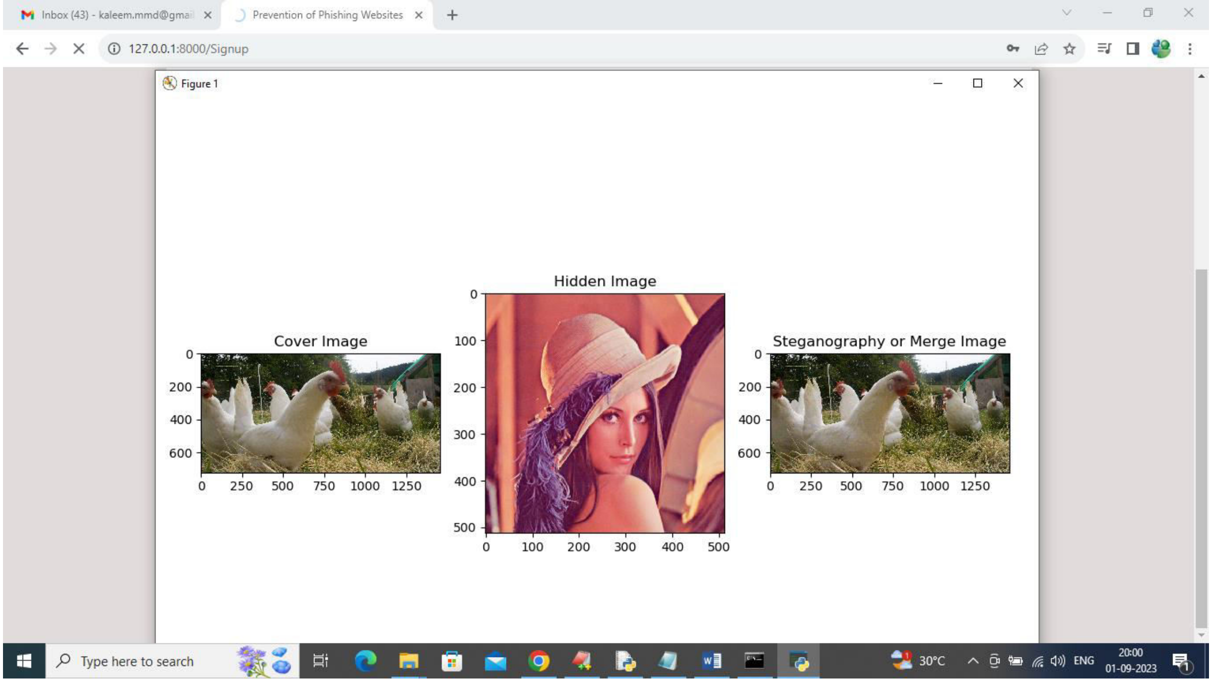
Upload Cover Image Choose File No file chosen

Upload Hidden Image Choose File No file chosen

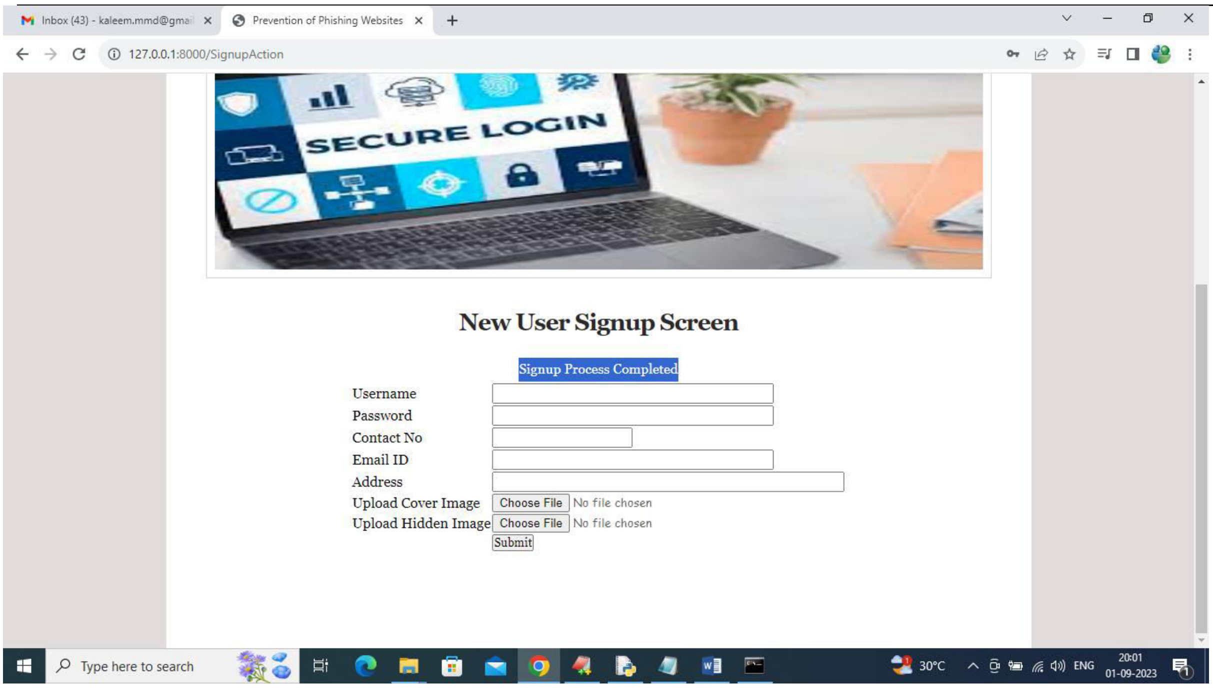
Submit

File name: 3

Inabove screen adding another user and will get below output



Inabove screen can see all image details and now close above image to get below output



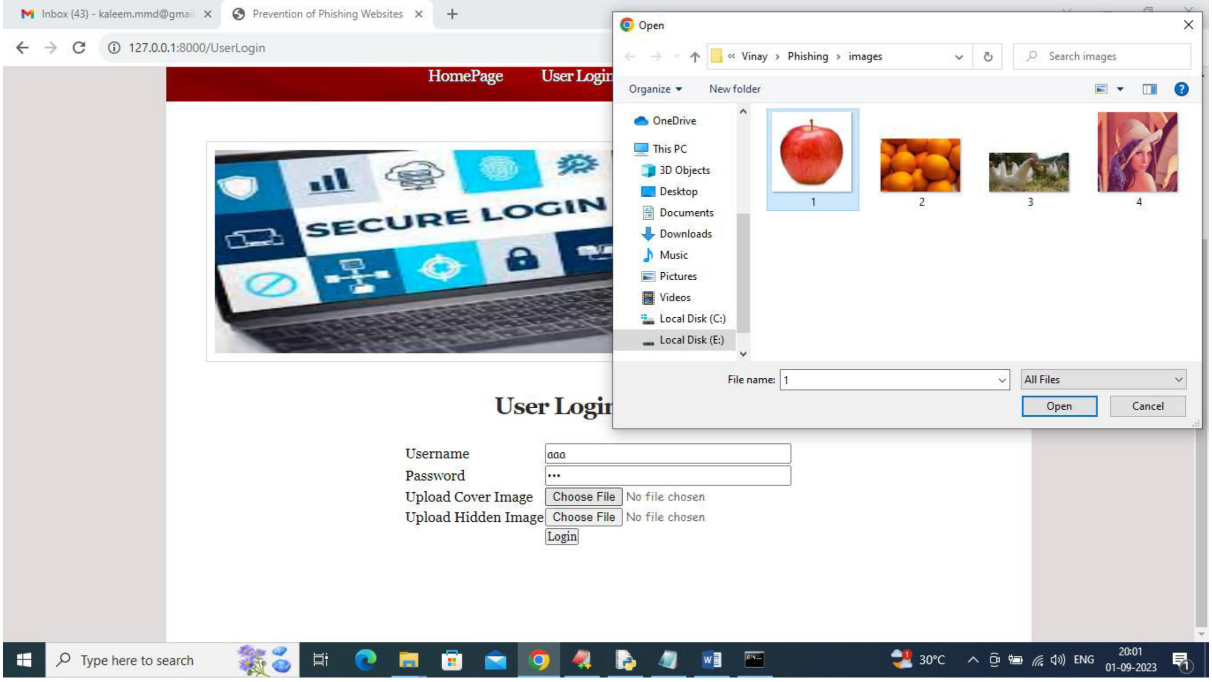
Inbox (43) - kaleem.mmd@gmail
Prevention of Phishing Websites
127.0.0.1:8000/SignupAction
SECURE LOGIN
Type here to search
30°C
ENG
20:01
01-09-2023

New User Signup Screen

Signup Process Completed

Username	
Password	
Contact No	
Email ID	
Address	
Upload Cover Image	Choose File No file chosen
Upload Hidden Image	Choose File No file chosen
	Submit

In above screen second user signup also completed and now click on ‘ User Login’ to login as user

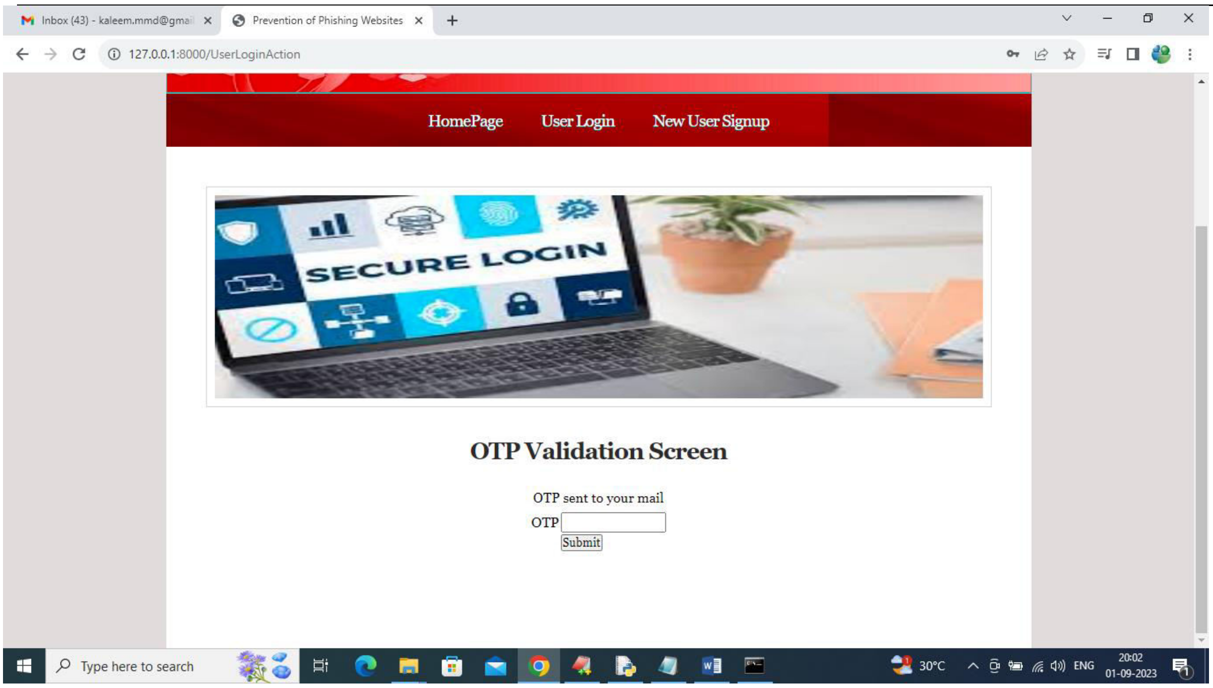


File name: 1

User Login

Username	aaa
Password	•••
Upload Cover Image	Choose File No file chosen
Upload Hidden Image	Choose File No file chosen
	Login

In above screen while login uploading same cover and hidden image and then press button to get below output


Inbox (43) - kaleem.mmd@gmai
Prevention of Phishing Websites
127.0.0.1:8000/UserLoginAction
HomePage
User Login
New User Signup
SECURE LOGIN
Type here to search
30°C
ENG
20:02
01-09-2023

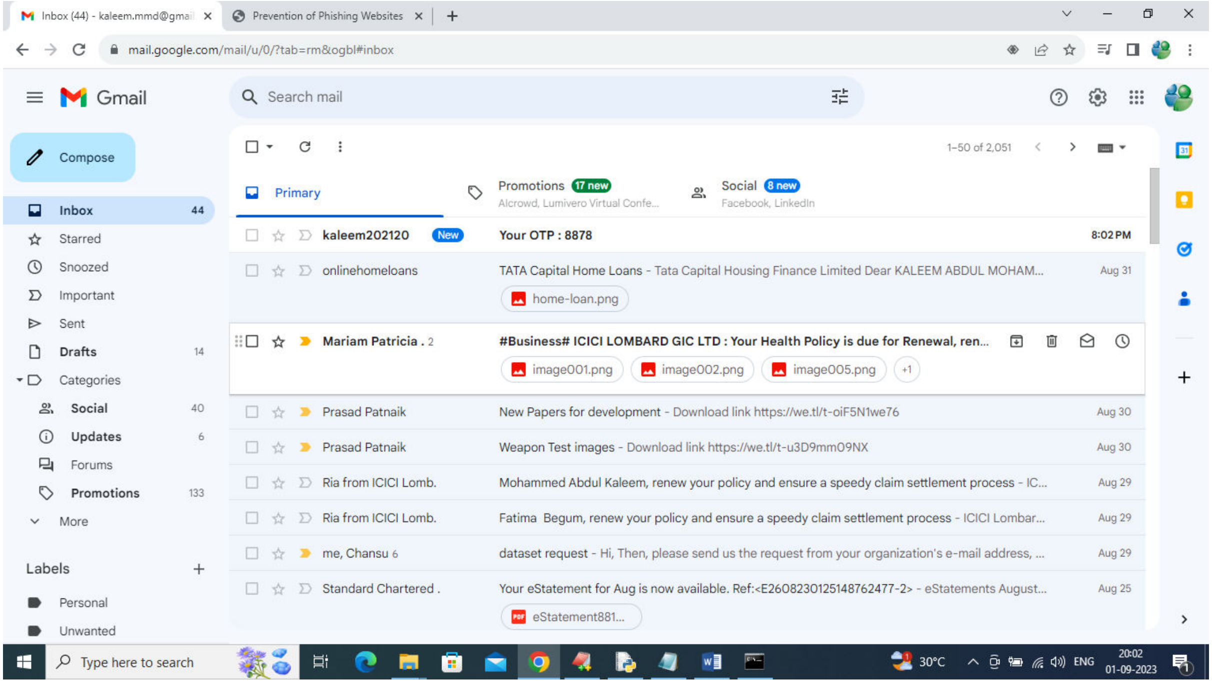
OTP Validation Screen

OTP sent to your mail

OTP

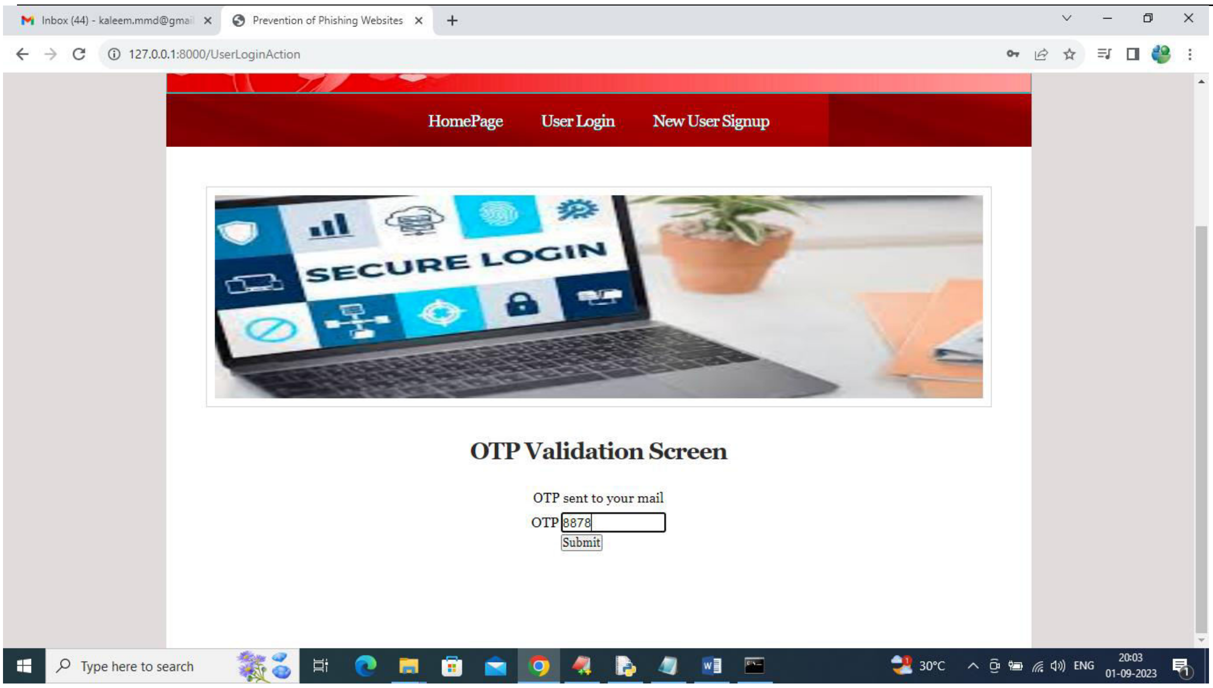
Submit

In above screen OTP sent to mail which we can see in below screen



kaleem202120 New	Your OTP : 8878	8:02 PM
onlinehomeloans	TATA Capital Home Loans - Tata Capital Housing Finance Limited Dear KALEEM ABDUL MOHAM... home-loan.png	Aug 31
Mariam Patricia . 2	#Business# ICICI LOMBARD GIC LTD : Your Health Policy is due for Renewal, ren... image001.png image002.png image005.png +1	
Prasad Patnaik	New Papers for development - Download link https://we.tl/t-oiF5N1we76	Aug 30
Prasad Patnaik	Weapon Test images - Download link https://we.tl/t-u3D9mm09NX	Aug 30
Ria from ICICI Lomb.	Mohammed Abdul Kaleem, renew your policy and ensure a speedy claim settlement process - IC...	Aug 29
Ria from ICICI Lomb.	Fatima Begum, renew your policy and ensure a speedy claim settlement process - ICICI Lombar...	Aug 29
me, Chansu 6	dataset request - Hi, Then, please send us the request from your organization's e-mail address, ...	Aug 29
Standard Chartered .	Your eStatement for Aug is now available. Ref:<E2608230125148762477-2> - eStatements August... eStatement881...	Aug 25

In above mail received OTP and now user same for OTP validation in below screen



Inbox (44) - kaleem.mmd@gmail
Prevention of Phishing Websites
127.0.0.1:8000/UserLoginAction
HomePage
User Login
New User Signup
SECURE LOGIN
Type here to search
30°C
ENG
20:03
01-09-2023

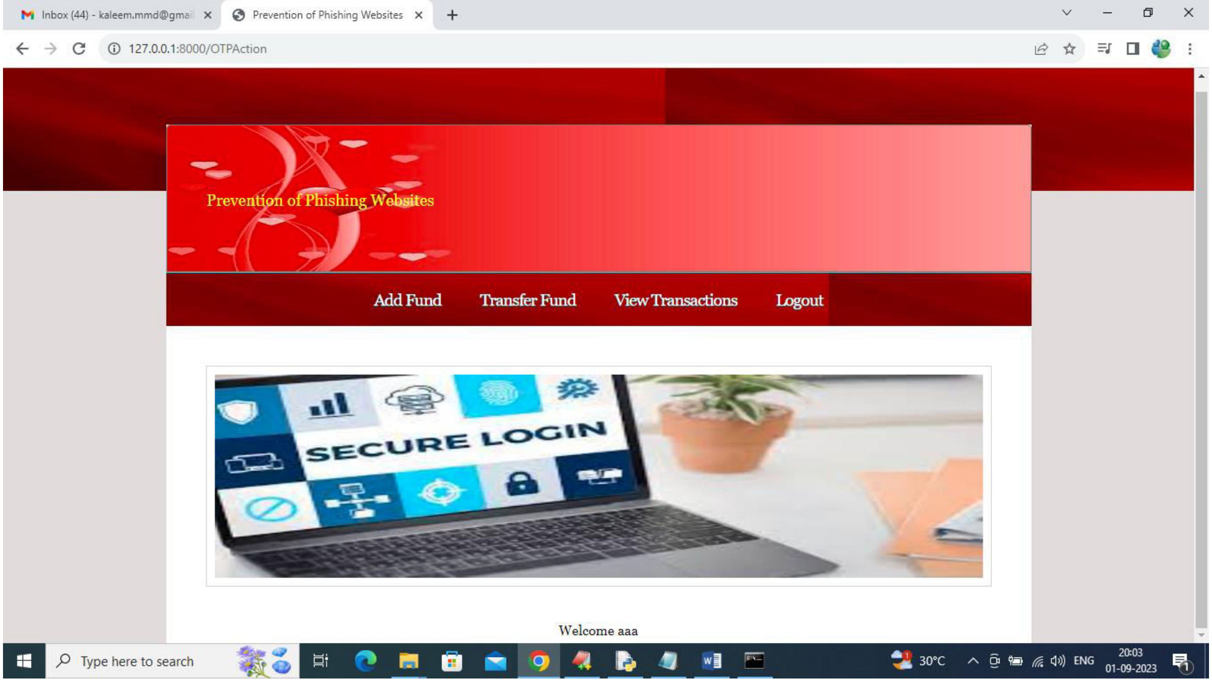
OTP Validation Screen

OTP sent to your mail

OTP 8878

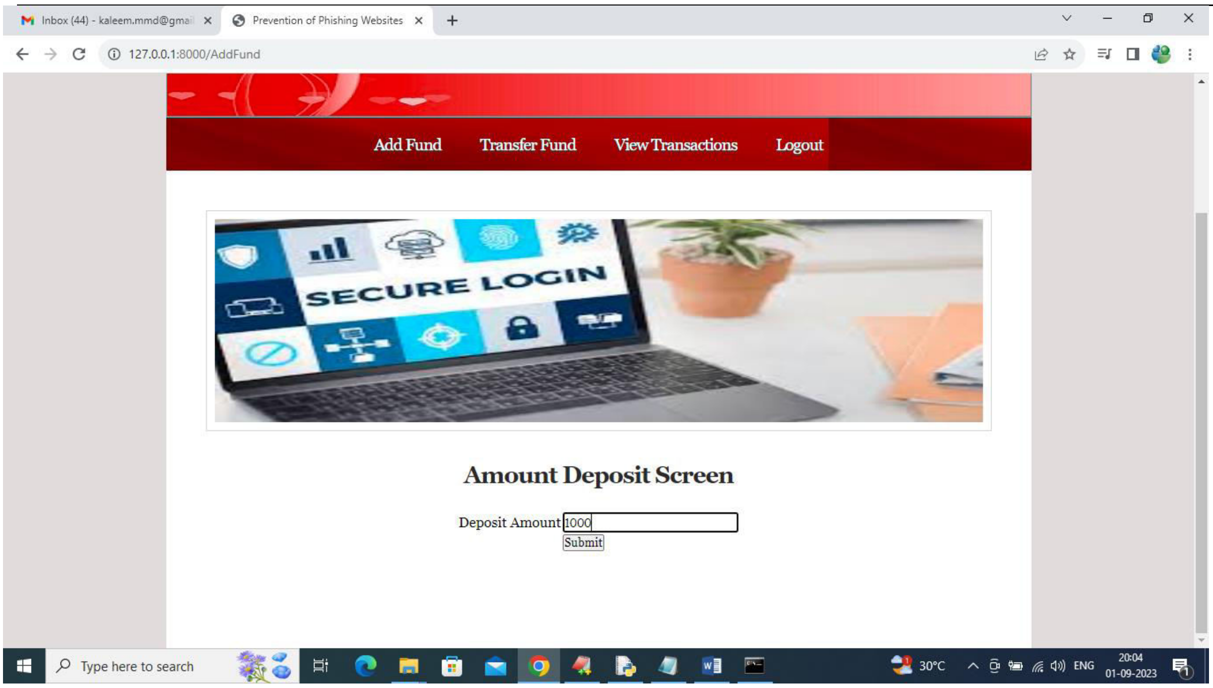
Submit

Inabove screen entered OTP and press button to get below user home page



Welcome aaa

Inabove screen user logged in successfully and now click on ‘ Add Fund’ link to add some deposit

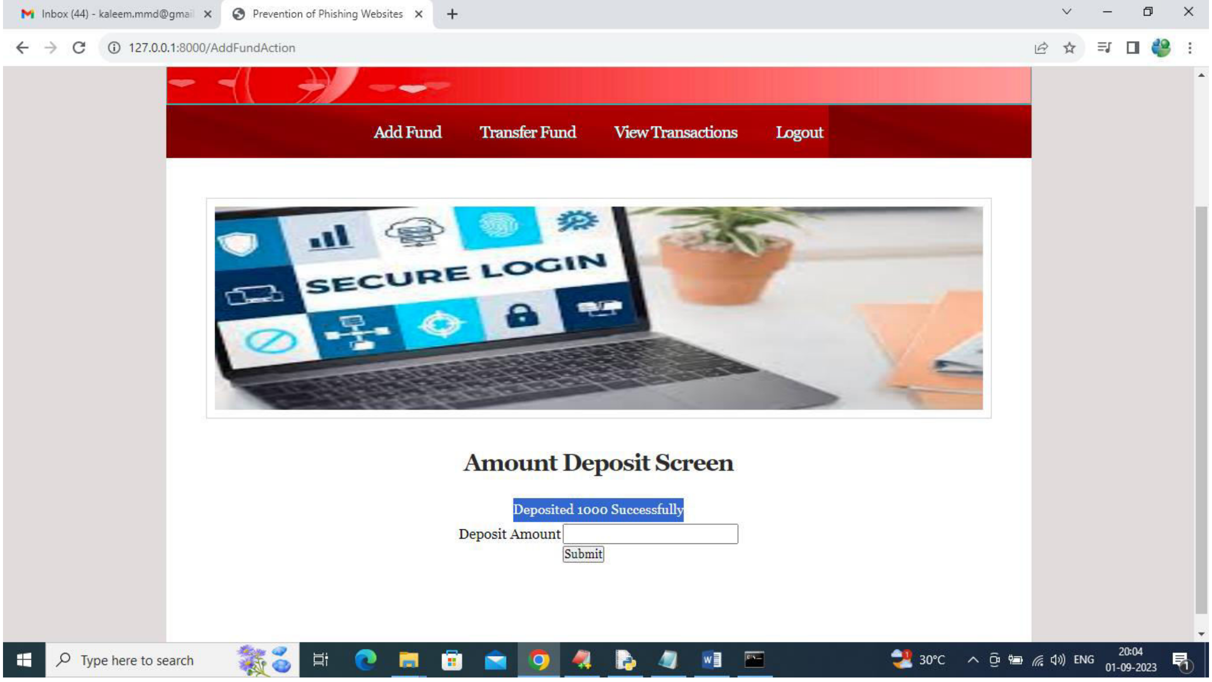


Amount Deposit Screen

Deposit Amount 1000

Submit

Inabove screen adding some amount and press button to get below page



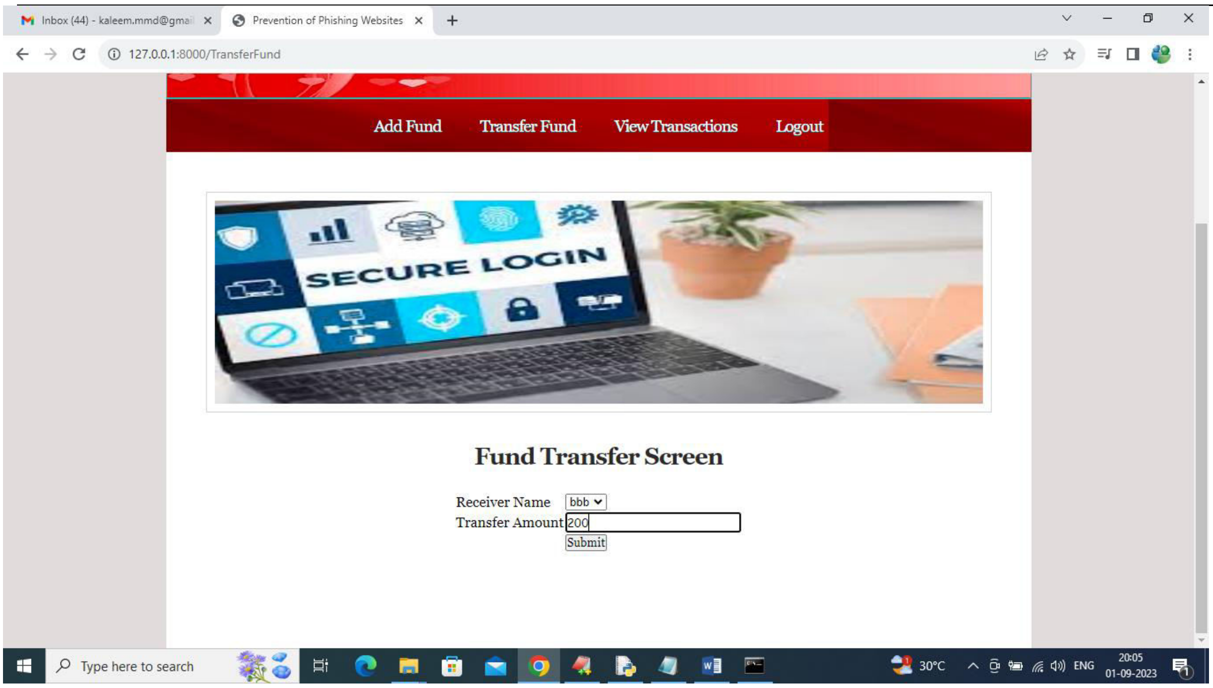
Amount Deposit Screen

Deposited 1000 Successfully

Deposit Amount

Submit

Inabove screen in blue colour text amount added and now click on ‘ Transfer Fund’ link to get below page


Inbox (44) - kaleem.mmd@gmail
Prevention of Phishing Websites
127.0.0.1:8000/TransferFund
Add Fund
Transfer Fund
View Transactions
Logout
SECURE LOGIN

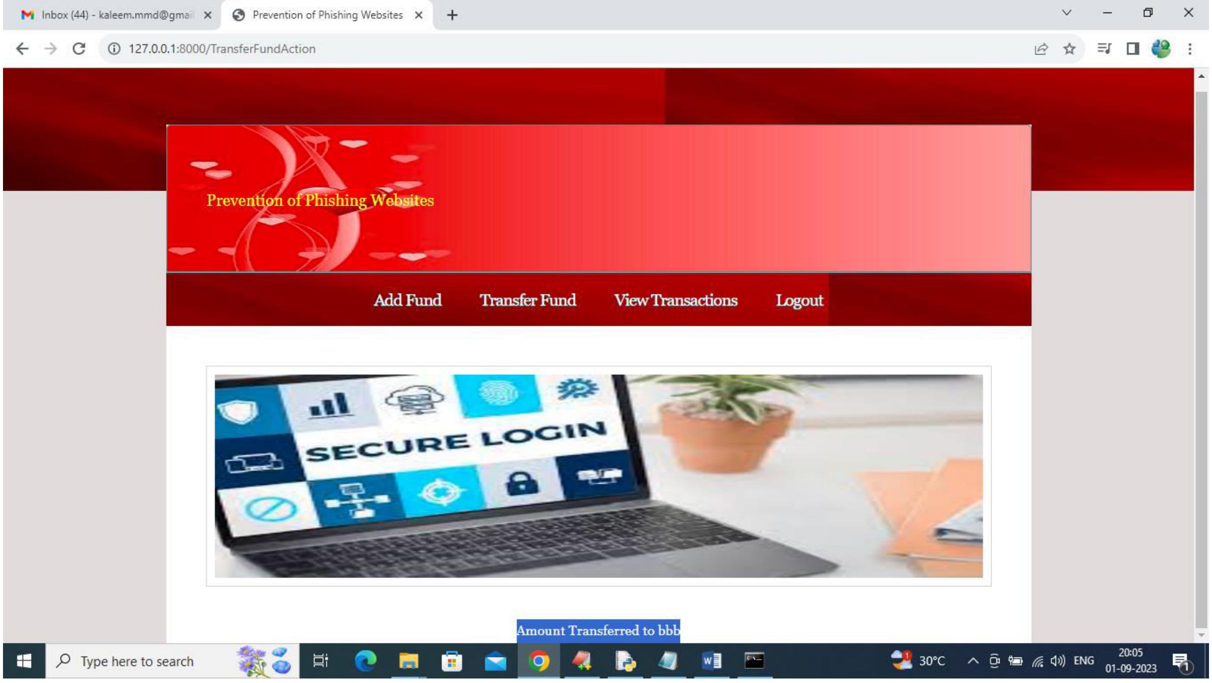
Fund Transfer Screen

Receiver Name bbb

Transfer Amount 200

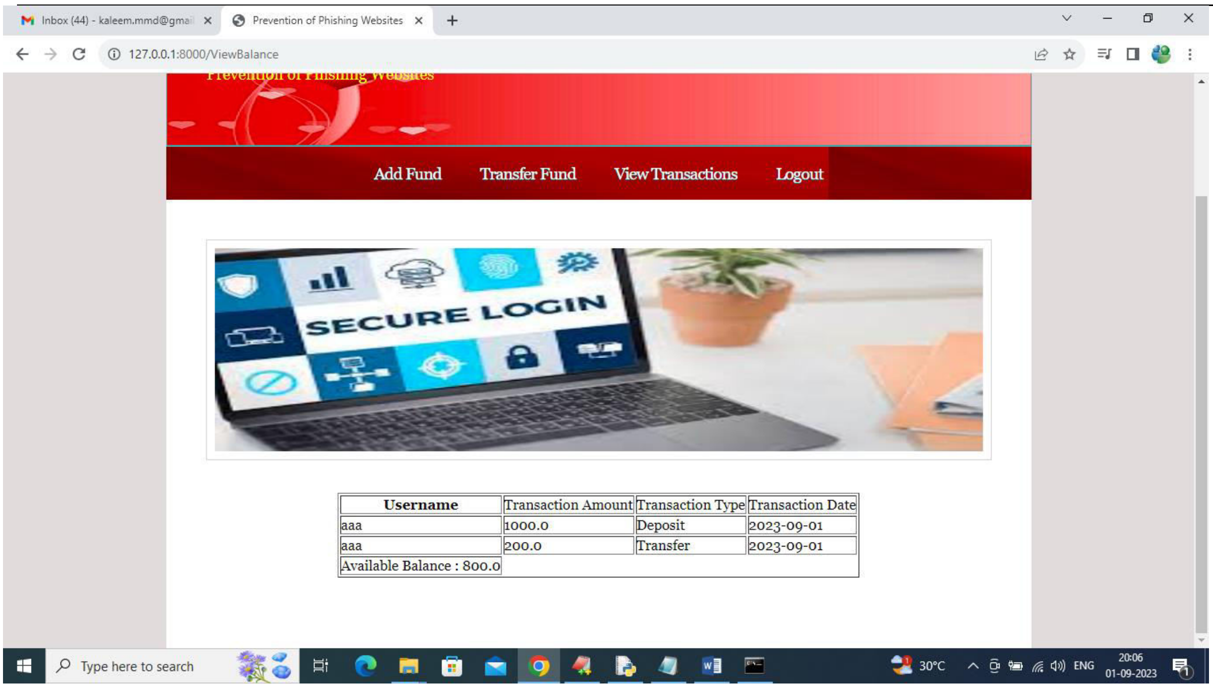
Submit

In above screen selecting Receiver and then entering transferring amount and press button to get below page


Inbox (44) - kaleem.mmd@gmail
Prevention of Phishing Websites
127.0.0.1:8000/TransferFundAction
Prevention of Phishing Websites
Add Fund
Transfer Fund
View Transactions
Logout
SECURE LOGIN

Amount Transferred to bbb

Inabove screen transferred successfully done and now can click on ‘ View Transactions’ to view balance sheet


Inbox (44) - kaleem.mmd@gmai
Prevention of Phishing Websites
127.0.0.1:8000/ViewBalance
Prevention of Phishing Websites
Add Fund
Transfer Fund
View Transactions
Logout
SECURE LOGIN
Type here to search
30°C
ENG
20:06
01-09-2023

Username	Transaction Amount	Transaction Type	Transaction Date
aaa	1000.0	Deposit	2023-09-01
aaa	200.0	Transfer	2023-09-01
Available Balance : 800.0			

In above screen user can view deposited and transferred amount with available balance. Similarly by following above screens you can login as second user and do same operations

6. CONCLUSION AND FUTURE WORK

CONCLUSION

Phishing attacks remain a persistent and evolving threat in the digital landscape, targeting individuals, businesses, and institutions to steal sensitive information. The limitations of traditional prevention systems—reliance on blacklists, static heuristic rules, and challenges in machine learning implementations—underscore the need for a more comprehensive and adaptive approach.The proposed system addresses these limitations by integrating advanced machine learning models, dynamic heuristic analysis, and a real-time threat intelligence network. This multi-layered defense mechanism significantly enhances the detection accuracy and adaptability of phishing prevention efforts. By leveraging continuous learning and real-time data updates, the system can swiftly respond to emerging phishing tactics, providing robust protection against both known and novel threats.Furthermore, the inclusion of an interactive user education module emphasizes the importance of user awareness and empowerment in phishing prevention. Through gamified learning techniques and regular phishing simulations, users are better equipped to recognize and avoid phishing attempts, thus serving as an essential line of defense.In conclusion, the proposed system offers a holistic solution that combines technological advancements with proactive user education to effectively combat phishing attacks. By addressing the existing system's drawbacks and introducing a dynamic, collaborative, and user-centric approach, this system aims to significantly reduce the incidence and impact of phishing websites. Continued innovation and collaboration among stakeholders will be crucial in maintaining and enhancing the effectiveness of phishing prevention strategies, ensuring a safer online environment for all users.

7. REFRENCES

1. Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. Expert Systems with Applications, 37(12), 7913-7921.
2. Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006). Phishing email detection based on structural properties. Proceedings of the 9th Annual NYS Cyber Security Conference.
3. Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). A framework for detection and measurement of phishing attacks. Proceedings of the 2007 ACM workshop on Recurring malcode.
4. Hara, T., Yamada, A., & Misue, K. (2009). Preventing phishing attacks using visual similarity based on earth mover's distance. Proceedings of the 6th International Conference on Soft Computing and Intelligent Systems.
5. Jain, A. K., & Gupta, B. B. (2018). Phishing detection: Analysis of visual similarity based approaches. Journal of Information Security and Applications, 40, 1-19.
6. Marchal, S., Francois, J., State, R., & Engel, T. (2014). PhishStorm: Detecting phishing with streaming analytics. IEEE Transactions on Network and Service Management, 11(4), 458-471.
7. Moghimi, M., & Varjani, A. Y. (2016). New rule-based phishing detection method. Expert Systems with Applications, 53, 231-242.
8. Patil, P. M., & Patil, P. V. (2017). A novel approach for detection of phishing websites. International Journal of Computer Applications, 166(5), 22-26.
9. Prakash, P., Kumar, M., Kompella, R. R., & Gupta, M. (2010). PhishNet: Predictive blacklisting to detect phishing attacks. IEEE INFOCOM 2010.
10. Ramesh, S., & Raj, S. C. (2018). A novel approach for detecting phishing websites using random forest classifier. International Journal of Pure and Applied Mathematics, 119(15), 875-884.