GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 10, Issue 6, June (2022)

SECURE E-BANKING

Mubashira Begom
Department of Computer Applications, Nirmala College For Women

J. S. Zeenath A.
Department of Computer Applications, Nirmala College For Women

ABSTRACT

The project entitled as "Secure E-Banking" is developed for the net banking users. There are number of users who purchase product online and make payment through E-banking. There are certain e-banking websites who ask user to provide sensitive data such as username, password or credit card details and personal information. They not only steal the bank information, but they will also take the money from the user and might steal the data to use them for future crimes. The concept used in this system is based on an end-host, the anti-phishing algorithm also known as link-guard algorithms. When the phisher sends the email or message to the user they can input the link in this algorithm, by evaluating the characteristics of the URL sent in that email it ranks how safe the site is and has various criteria that might put the threat at different levels. The Link Guard is based on URL characteristics so that it can detect and forestall unknown or new ones. This project is developed using PHP 5.1.3 as front end and MY SQL as back end

Keywords: My SQL , PHP

INTRODUCTION

The "Secure E-banking" is aimed to secure the user from online phishing. This is web based application to manage the personal details safe. In online, the attacker sends a link through a mail or message similar to legit but actually is not. It is a trap to take the information from the user. The user is attracted by the attacker as they are calling from their service provider like bank and ask to share the sensitive information which may be data or the transaction details. The attacker collects the information if the user enters it in the link. The phisher must duplicate the content of the target site, the hacker will use tools to (automatically) download the Web pages from the targeted site. It is therefore possible to detect this kind of download at the Web server and trace back to the phisher. Both approaches have shortcomings. For DNS scanning, it increases the overhead of the DNS systems and may cause problem for normal DNS queries, and furthermore, many phishing attacks simply do not require a DNS name. For phishing download detection, clever phishers may easily write tools which can mimic the behaviour of human beings to defeat the detection. Install online anti-phishing software in user's computers: Despite all the above efforts, it is still possible for the users to visit the spoofed Web sites. As a last defence, users can install anti-phishing tools in their computers. The anti-phishing tools in use today can be divided into two categories: blacklist/white list based and rule-based

LITERATURE REVIEW

Literature studies are the most critical element in every field of study as they present a description of the facts required for future research studies, policies and procedures(Andreini & Bettinelli, 2017). Systematic Literature Review (SLR) is a research method that critically appraises various studies and synthesizes both qualitative and quantitative findings(Burgers, Brugman, & Boeynaems, 2019). Its purpose is to investigate, categorize, evaluate and synthesize the prevailing literature relevant to specific topics or areas using a transparent, replicable process and applying inclusion and exclusion techniques (Kitchenham et al., 2009; Tranfield, Denyer, & Smart, 2003). It can be defined as "a reliable, scientific overview of extant research on a subject area of the topic (Petticrew & Roberts, 2008). It provides a transparent, replicable and auditable trail of the reviewer's decision, procedure and conclusion. The literature review is carried out in three key steps: planning, conducting and reporting as adopted by the existing study.

METHODOLOGY

ADMIN MODULE

Login
Registration
Add to blacklist
Logout

USER MODULE

Login
Registration
Check website
Send feedback
Logout

ADMINISTRATOR MODULE

LOGIN

Login In this module, Admin can access their account through this page. After successful login, this page was redirected to the home page. If the admin doesn't have an account registers the account through registration page.

REGISTRATION

In this module, every new admin has to register their details. After register the admin can login.

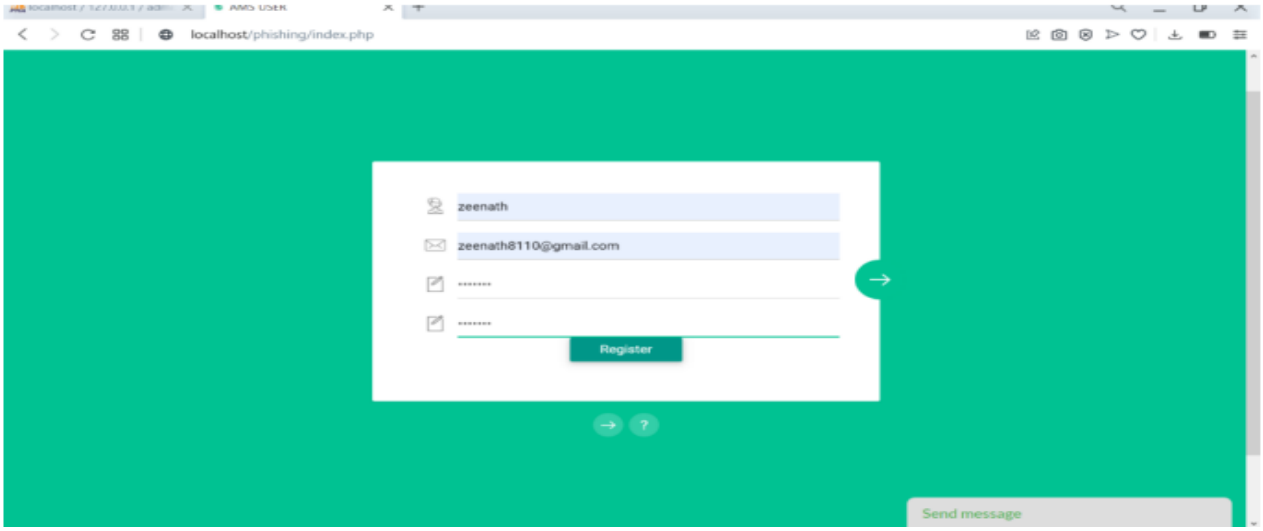
ADD TO BLACK LIST

Admin can add a website to blacklisted site when admin received a request or verifying it from the IP or its DNS

LOGOUT

This module was used for the admin to logout the account. Once logged out the account no one will access the account without the knowledge of username and password.

USER MODULE



LOGIN

User can access the account through they logged in. The Login Module is allowed to enter the User Name and Password to log in. If the user doesn't have an account, the user register their details on registration page.

REGISTRATION

In this module, every new user has to register their details, such as name, address, mobile number, email details. After registration, only users get user account. It's a Onetime registration, later by getting the Admin approval the user can login to the home page.

CHECK WEBSITE

User can check a website or URL link, when the hacker hacked the information. Then the user can send to admin as it seems to be phishing website or URL. Name Check Login Check User Register.

SEND FEEDBACK

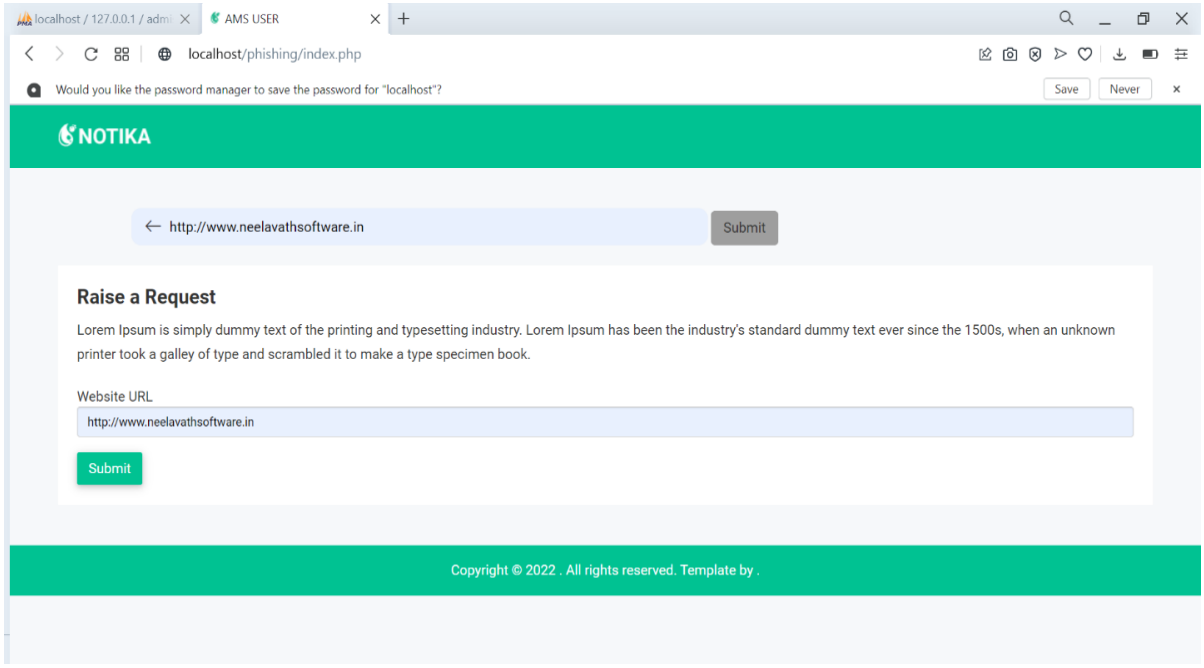
In this module user send the feedback about the website and its information.

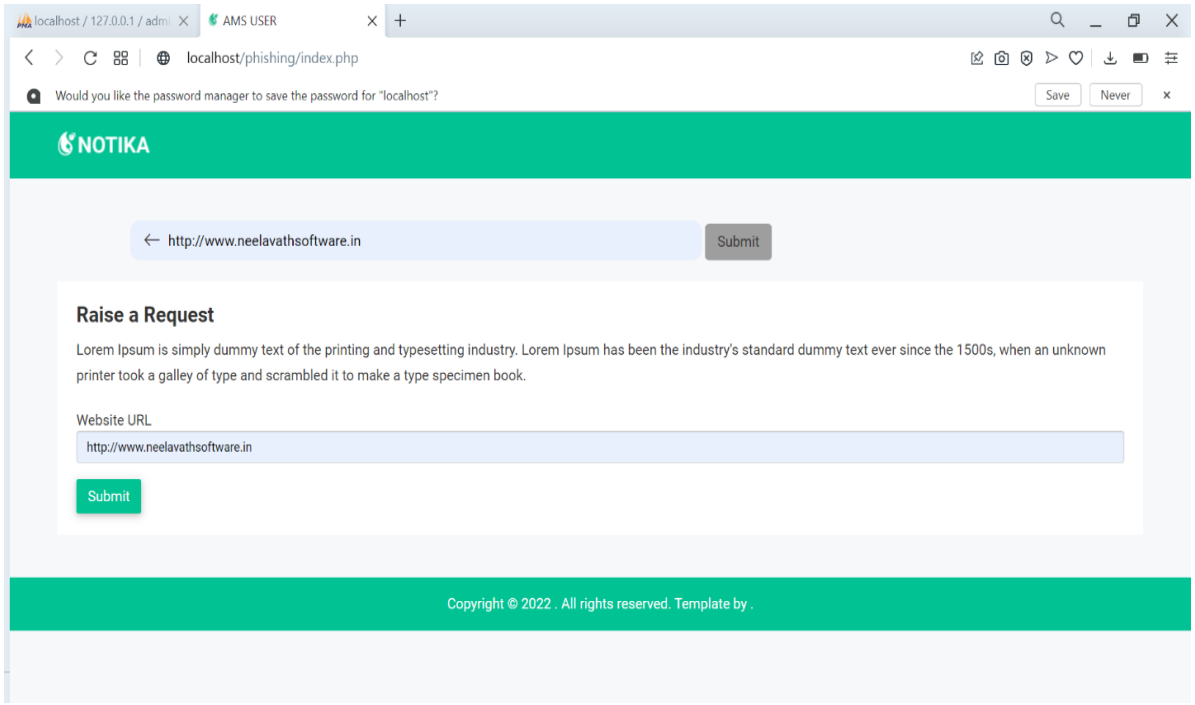
LOGOUT

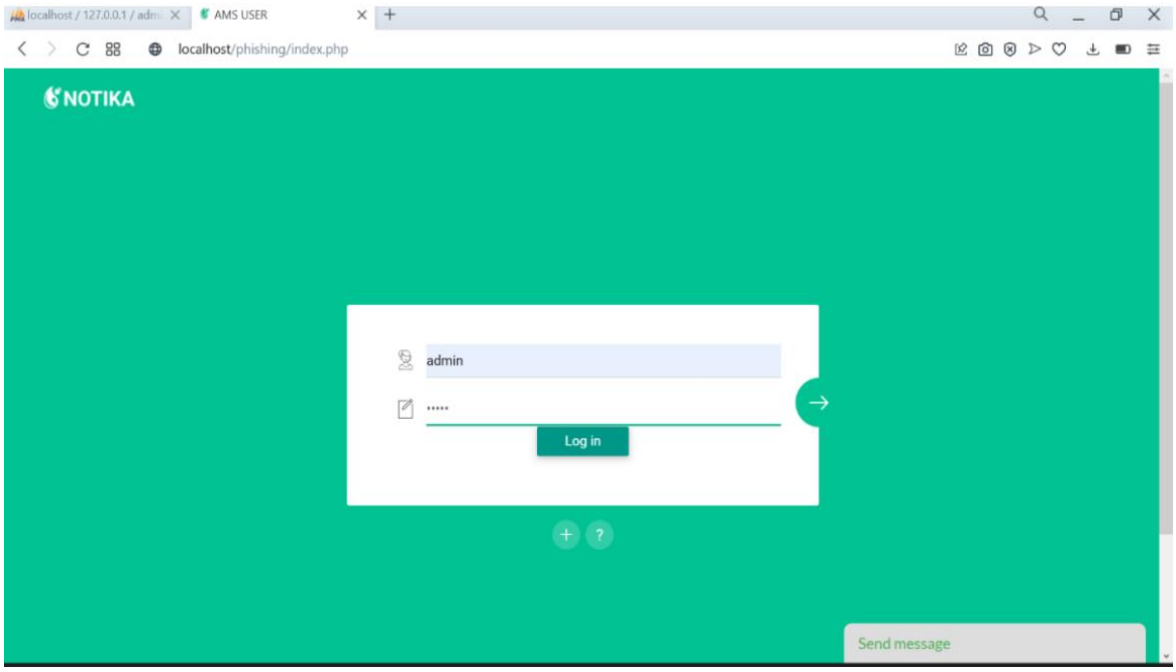
This module was used for the user to log out the account. Once logged out no one can access the user account without the knowledge of the username and password

RESULT

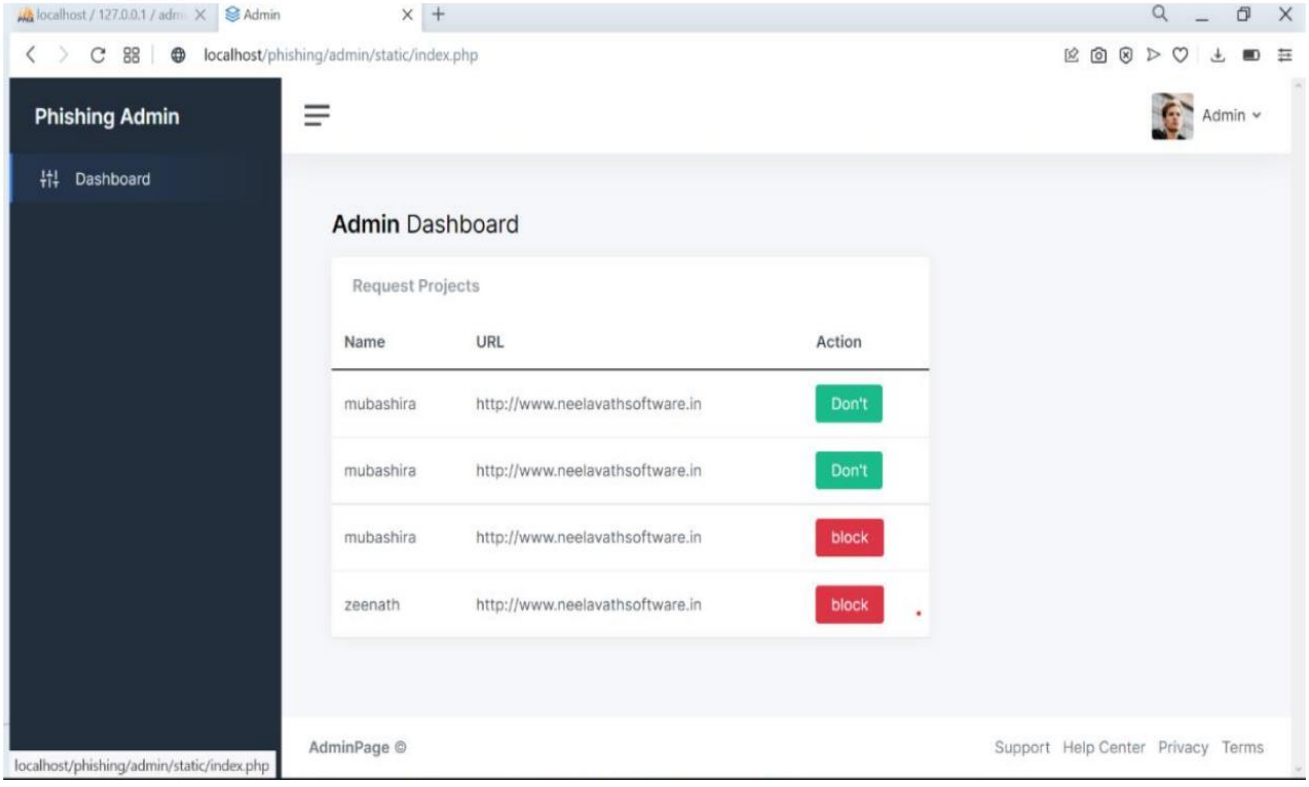
- ✓ USER REGISTER
- ✓ REQUEST
- ✓ ADMIN LOGIN







✓ BLOCKING LIST



CONCLUSION AND FUTURE WORK

Phishing is an appalling threat in the web security domain. In this attack, the user inputs the personal information to a fake website which looks like a legitimate one. We have presented a survey on phishing detection approaches based on visual similarity. This survey provides a better understanding of phishing website, various solution, and future scope in phishing detection.

Many approaches are discussed in this paper for phishing detection. Most of the approaches still have limitations like accuracy, the counter measure against new phishing websites, failing to detect embedded objects, and so forth. These approaches use various features of a webpage to detect phishing attacks, such as text similarity, font colour, font size, and images present in the webpage.

Text based similarity approaches are relatively fast, but they are unable to detect phishing attack if the text is replaced with some image. Image processing based approaches have high accuracy rate while they are complex in nature and are time-consuming. Furthermore, most of the work is done offline. These involve data collection and profile-creation phases to be completed first.

A comparative table is prepared for easy glancing at the advantages and drawbacks of the available approaches. No single technique is enough for adopting it for phishing detection purposes. Detection of phishing websites with high accuracy is still an open challenge for further research and development

A future work will focus on collecting phishing and non-phishing web-sites that are currently accessible in the web and extract a list of features

REFERENCES

1. M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: a literature survey," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091–2121, 2013.View at: Publisher Site | Google Scholar
2. R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 324–335, 2013.View at: Publisher Site | Google Scholar
3. A. K. Jain and B. B. Gupta, "Comparative analysis of features based machine learning approaches for phishing detection," in Proceedings of the 10th INDIA-COM, New Delhi, India, 2016.View at: Google Scholar.

WEBSITES

1. https://www.sciencedirect.com/topics/computer-science/phishing-detection
2. https://romisatriawahono.net/lecture/rm/survey/network%20security/khonji520-%20phishing%20detection%20