**Phishing Website Detector**

**Project Synopsis**

Major Project (MCA465)

Degree

**MASTER OF COMPUTER APPLICATION**

**(MCA)**

|  |  |
| --- | --- |
| PROJECT GUIDE:  **Mr. Gaurav Rajput** | SUBMITTED BY:  **Toshika Ahlawat (TCA2163099)**  **Utkarsh Gupta (TCA2163100)** |



**FACULTY OF ENGINEERING & COMPUTING SCIENCES**

**TEERTHANKER MAHAVEER UNIVERSITY, MORADABAD**

Table of Contents

[1 Project Title 3](#_Toc117152972)

[2 Domain 3](#_Toc117152973)

[3 Problem Statement 3](#_Toc117152974)

[4 Project Description 3](#_Toc117152975)

[4.1 Scope of the Work 4](#_Toc117152976)

[4.2 Project Modules 4](#_Toc117152977)

[5 Implementation Methodology 4](#_Toc117152978)

[6 Technologies to be used 5](#_Toc117152979)

[6.1 Software Platform – Microsoft Visual Studio 2019. 5](#_Toc117152980)

[6.2 Hardware Platform 5](#_Toc117152981)

[6.3 Tools 6](#_Toc117152982)

[7 Advantages of this Project 6](#_Toc117152983)

[8 Team Details 6](#_Toc117152984)

[9 Conclusion 6](#_Toc117152985)

# Project Title

**Phishing Website Detector**

# Domain

A phishing website detector using PHP is a tool that can analyze a given URL or domain name and determine if it is likely to be a phishing website. Phishing websites are fraudulent websites designed to steal sensitive information such as usernames, passwords, and credit card numbers. These websites are often designed to look like legitimate websites and may use social engineering tactics to trick users into entering their personal information.

It can help protect users from falling victim to these types of scams by analyzing the domain name or URL for indicators of a phishing attempt. This may include checking for similarities to well-known brands, looking for multiple hyphens or numbers in the domain name, analyzing the length of the domain name, and more.

In addition to analyzing the domain name, it can also use machine learning techniques to analyze the website content and other factors to determine if a website is likely to be a phishing website.

The final product should be a user-friendly tool that can accurately and reliably identify potentially fraudulent websites and help users protect themselves from the harmful consequences of online scams and fraud. The scope of the work for a phishing website detector using PHP may also include additional features such as user authentication and authorization, data storage and retrieval, user education, and threat intelligence integration, among others. Overall, it can be an effective tool for protecting users from phishing scams and other types of online fraud.

# Problem Statement

Phishing attacks have become a serious threat to internet users and organizations. Attackers use fake websites to steal sensitive information from unsuspecting victims, leading to financial losses, identity theft, and other serious consequences. Although there are several anti-phishing tools available, most of them are either expensive or complex to use. Therefore, there is a need for a simple and effective tool that can detect phishing websites and alert users in real-time.

The project "Phishing Website Detector using PHP" aims to address this problem by developing a web application that can identify and flag potentially malicious websites using machine learning algorithms. The application will use features such as URL structure, domain age, SSL certificate, and website content to detect phishing attempts. It will also maintain a database of known phishing websites and provide real-time alerts to users if they attempt to visit such sites.

The project will be developed using PHP, a widely used server-side scripting language, and will be compatible with most web servers. The application will be user-friendly and accessible to both technical and non-technical users. By developing an effective and easy-to-use tool to detect phishing websites, the project will help users protect their sensitive information and mitigate the risks associated with online attacks.

# Project Description

Phishing attacks are a common threat to internet users. Cybercriminals create fake websites that mimic legitimate websites in order to steal sensitive information such as login credentials, credit card numbers, and other personal data. The aim of this project is to develop a phishing website detector using PHP that can help users identify potentially malicious websites and prevent them from falling victim to phishing attacks.

The phishing website detector will use a combination of machine learning algorithms and heuristics to analyze the structure, content, and behavior of websites in order to determine whether they are legitimate or not. The system will be trained on a large dataset of known phishing websites and will use this knowledge to identify new phishing websites in real-time.

The system will be built using the PHP programming language, which is widely used for web development. The user interface will be designed using HTML, CSS, and JavaScript to provide a user-friendly experience. The system will be able to analyze websites from different platforms such as desktop and mobile browsers.

The project will consist of the following modules:

**URL analysis:** The detector will analyze the URL of the website to determine if it is legitimate or not. It will check for common phishing indicators such as fake domains, subdomains, and misspellings.

**Content analysis:** The detector will analyze the content of the website to identify any suspicious elements such as fake logos, forms, and links. It will also scan for hidden code and scripts that are commonly used in phishing attacks.

**Machine learning model:** This module will use the extracted features to classify websites as either legitimate or phishing.

**Browser integration**: The detector will be integrated with popular web browsers such as Google Chrome and Mozilla Firefox. It will display a warning message if the user attempts to visit a potentially phishing website.

**Standalone application:** The detector will also be designed to work as a standalone application that can be installed on desktops and mobile devices. It will offer real-time protection against phishing attacks, even when the user is not using a web browser.

**User interface:** This module will provide a user-friendly interface for users to input website URLs and receive a report on whether the website is legitimate or not.

The phishing website detector project will help users to protect themselves from phishing attacks by providing a reliable and easy-to-use tool for identifying potentially malicious websites.

## Scope of the Work

**1.Research and Analysis:**

* Conduct research to identify existing PHP libraries or frameworks that can be used to develop the phishing website detector.
* Analyse the requirements and specifications of the project, including the user interface, functionality, and performance.
* Study the different types of phishing attacks and techniques used by attackers to create phishing websites.

**2.Development of the System:**

* Develop the system architecture and design based on the requirements and specifications.
* Implement the user interface design and functionality using PHP, HTML, CSS, and JavaScript.
* Develop the backend server-side scripts using PHP to process and analyze the input data from the user.
* Integrate different APIs, libraries, and frameworks to enhance the functionality of the system, such as email validation APIs, domain validation APIs, and machine learning libraries.

**3.Testing and Quality Assurance:**

* Conduct rigorous testing to ensure the system is free of bugs and errors.
* Perform stress testing to determine the system's performance under heavy traffic and load.
* Test the system's security features and verify that it is capable of detecting phishing websites accurately.

**4.Deployment and Maintenance:**

* Deploy the system on a web server, such as Apache or Nginx.
* Develop a backup and recovery strategy to ensure the system's availability in case of any failures or disasters.
* Provide ongoing maintenance and support to ensure the system's smooth operation and to address any issues or bugs that may arise.

## Project Modules

some possible project modules for the phishing website detector using PHP:

**User Interface:** This module will be responsible for creating a user-friendly interface for users to interact with the system. It will include features such as user registration, login, and account management.

**URL Scanner:** This module will scan the URLs submitted by the users to determine if they are phishing websites or not. It will utilize various techniques such as web page analysis, blacklisting, and machine learning algorithms to detect phishing websites.

**Blacklist Management:** This module will maintain a list of known phishing websites and will use this list to compare URLs submitted by users. The module will also update the blacklist regularly to ensure that the system is up-to-date with the latest phishing websites.

**Machine Learning:** This module will use machine learning algorithms to detect patterns in URLs that may indicate a phishing website. It will use a variety of techniques such as natural language processing, neural networks, and decision trees to analyze URLs and determine their legitimacy.

**Reporting**: This module will generate reports for users and administrators to view the status of the URLs submitted to the system. Reports will include information such as the URL status, the date of submission, and the user who submitted the URL.

**Email Notification:** This module will send email notifications to users and administrators when a phishing website is detected. The module will also provide instructions on how to handle the situation and prevent further damage.

**Admin Panel:** This module will provide an interface for administrators to manage the system. It will include features such as user management, blacklist management, and system configuration.

**Database Management:** This module will handle the storage and retrieval of data for the system. It will include features such as data backup, data restoration, and database optimization.

**API Integration:** This module will provide an API for third-party applications to integrate with the phishing website detector. The API will allow external applications to scan URLs and receive reports on the status of the URLs.

# Implementation Methodology

**The implementation methodology for the project phishing website detector using PHP can be divided into several stages:**

**Requirement Gathering:** In this stage, the requirements for the project are gathered by the project manager or developer. This includes understanding the purpose of the project, the functionalities it should offer, and the constraints of the project.

**Design:** In this stage, the system is designed according to the requirements gathered in the previous stage. The design includes the database schema, the user interface, and the algorithms to detect phishing websites.

**Development:** In this stage, the project is developed using PHP. The database schema is implemented, the user interface is designed, and the algorithms are coded. The development phase is an iterative process that involves frequent testing and bug fixing.

**Testing:** In this stage, the project is tested to ensure that it meets the requirements and is functioning as expected. The testing can be done through manual testing or automated testing. The testing phase includes functional testing, integration testing, and system testing.

**Deployment:** In this stage, the project is deployed on the web server. This includes uploading the PHP files, configuring the database, and setting up the server environment. The deployment phase is critical to ensure that the project is accessible and running smoothly.

**Maintenance:** In this stage, the project is maintained by the development team. This includes fixing bugs, adding new features, and updating the system to ensure it is up-to-date with the latest security protocols.

**Data Flow Diagram: -**

**IIIINPUT URLS**

**DIVIDE INTO SUB-STRINGS**

**AUTHORIZED URL DATABASE**

**PHISHING REPORT**

**INPUT URLS**

**CONVERT INTO IP**

**AUTHORIZED IP'S DATABASE**

**PHISHING REPORT**

# Technologies to be used

**Software Technologies:**

* PHP: PHP is the primary programming language used to develop the project. It is a server-side scripting language that can be used to create dynamic web pages and web applications. PHP is widely used for its flexibility, speed, and ease of use.
* MySQL: MySQL is a relational database management system that can be used to store and retrieve data. It is widely used for its high performance, scalability, and reliability. MySQL can be integrated with PHP to create dynamic web applications.
* HTML/CSS/JavaScript: These technologies are used to create the user interface and the front-end of the web application. HTML is used for creating the structure of web pages, CSS is used for styling and designing the web pages, and JavaScript is used for adding interactivity to the web pages.
* Web Server: A web server is required to run the PHP scripts and serve the web pages to the user. Apache is a popular web server that can be used for this project.

**Hardware Technologies:**

* Computer
* Internet Connection
* Server
* Firewall

# Advantages of this Project

There are several advantages to implementing this project, including:

1. Increased Security: One of the primary advantages of using a phishing website detector is increased security. By detecting potential phishing sites, users can avoid sharing their sensitive information on such sites, thereby reducing the risk of identity theft and financial fraud.
2. Easy to Use: Another advantage of this project is its ease of use. The website can be easily accessed by anyone with an internet connection, and the detection process is simple and straightforward.
3. Cost-Effective: Implementing a phishing website detector using PHP is a cost-effective solution for detecting phishing sites. This is because the PHP programming language is open-source, which means that it is free to use, and there are many resources available online for learning how to use it.
4. Customizable: PHP is a highly customizable programming language, which means that the phishing website detector can be tailored to suit the specific needs of the user. This allows users to add additional features or modify the existing ones to suit their preferences.
5. Scalable: The project phishing website detector using PHP is also scalable, which means that it can be easily adapted to handle larger volumes of data and traffic as the user base grows.
6. Overall, implementing a project phishing website detector using PHP provides several benefits, including increased security, ease of use, cost-effectiveness, customizability, and scalability.

# Team Details

| **Project Name & ID** | **Course Name** | **Student ID** | **Student Name** | **Role** | **Signature** |
| --- | --- | --- | --- | --- | --- |
| Phishing Website Detector |  | Tca2163099 | Toshika Ahlawat |  |  |
| Tca2163100 | Utkarsh Gupta |  |  |

# Conclusion

In conclusion, the project "Phishing Website Detector using PHP" has been successfully implemented and achieved its goals. The project aimed to develop a web-based application that could identify phishing websites and provide users with warnings to avoid visiting them.

The project used several technologies such as PHP, HTML, CSS, and JavaScript, which allowed us to create a user-friendly interface that is easy to navigate. The application was designed to detect phishing websites by analyzing various attributes of the website such as URL, SSL certificate, page content, etc. The project also implemented an email notification system that alerts users when they encounter a potentially harmful website.

One of the strengths of this project is its ability to continuously update its database of known phishing websites, which ensures that users are provided with the most up-to-date information. Additionally, the project's user-friendly interface and clear warning messages make it accessible to a wide range of users, regardless of their technical expertise.

The project does have some limitations, such as the reliance on user reports to detect new phishing websites, which may lead to delays in identifying new threats. Additionally, the project may not be able to detect phishing websites that are designed to evade detection techniques.

Overall, the "Phishing Website Detector using PHP" project provides a valuable tool for users to protect themselves from phishing attacks. By detecting and warning users about potentially harmful websites, this project can help prevent the theft of personal and sensitive information. Future enhancements to the project could include the integration of machine learning techniques to improve detection accuracy and reduce false positives.