

# **TITLE OF YOUR PROJECT**

**Parul Institute of Computer Applications**

**Semester 2 Project -1**

**2022-23**

**Team members**

1. < 2205101110145> <Asmi Veer> <C>
2. < 2205101110129> <Sneha Dhanawade><C>
3. < 2205101110119> <Vrunda kotecha><C>

# INDEX

- Abstract
- Tools and Technology Used
- Features of Proposed System
- Limitation of Proposed System
- Users and their role description
- System Flow Diagram
- Data Flow Diagram ( All Levels)
- Use Case Diagram
- Data Dictionary
- Screenshots of Development Phase 1 ( Designing of your Project)
- Screenshots of Development Phase 2 ( Features Implementation)



# ABSTRACT

- An approach to detection of phishing WebPages based on visual similarity is proposed, which can be utilized as a part of an enterprise solution for anti-phishing.
- Phishing is a form of identity theft in which a combination of social engineering and web site spoofing techniques are used to trick a user into revealing confidential information with economic value. In a typical phishing attack, a large number of spoofed e-mails are sent to random users.



# TOOLS AND TECHNOLOGY USED

- Programming language: PHP
- Web development framework: Laravel
- Database management system: MySQL
- Front-end technologies: HTML, CSS, JavaScript, Bootstrap
- Other tools:
  - Github
  - Composer for package management
  - PHPUnit for testing
  - Apache server for deployment



# FEATURES OF PROPOSED SYSTEM

- User authentication and authorization
- Phishing link detection
- Link analysis



# LIMITATION OF PROPOSED SYSTEM

- ❑ The accuracy of the system may not be 100%, as phishing techniques are constantly evolving and becoming more sophisticated.
- ❑ The system may not be able to detect phishing attempts in real-time, as it may require some time to analyze incoming emails and URLs.
- ❑ The system may not be effective against social engineering attacks.
- ❑ The system may not be able to prevent users from clicking on phishing links or entering sensitive information, as it can only provide warnings and alerts.



# USERS AND THEIR ROLE DESCRIPTION

Admin :

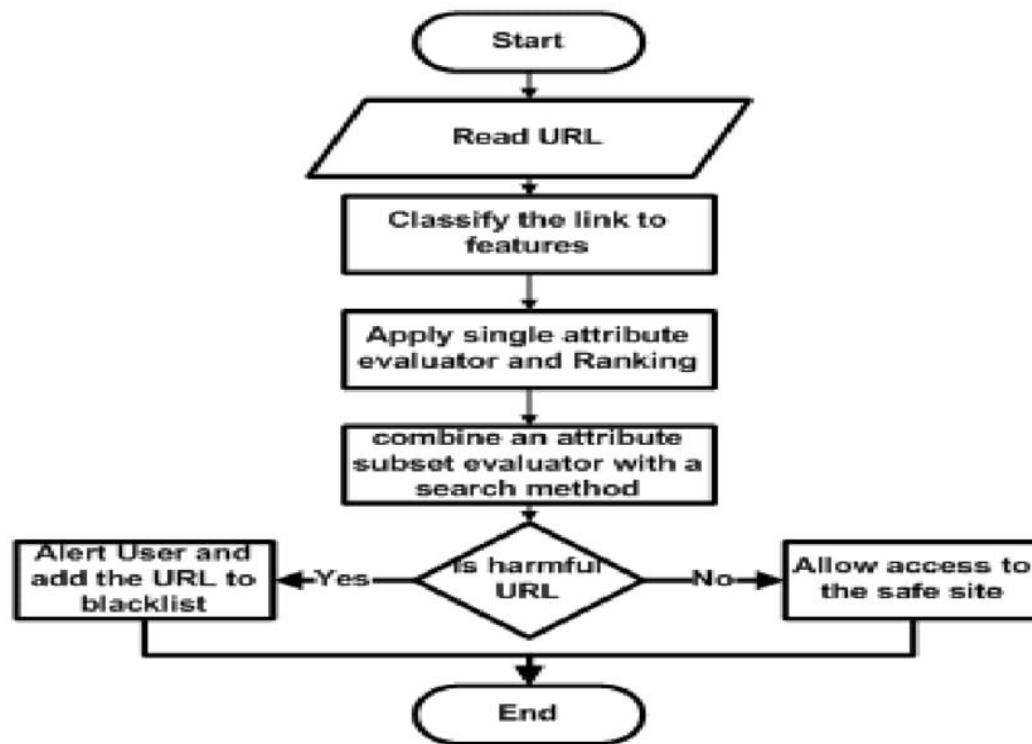
The admin user will have full access to the system and will be responsible for managing user accounts, adding or removing features, and monitoring the system's overall performance.

Regular User :

The regular user will have limited access to the system and will be able to use the phishing link detection feature.

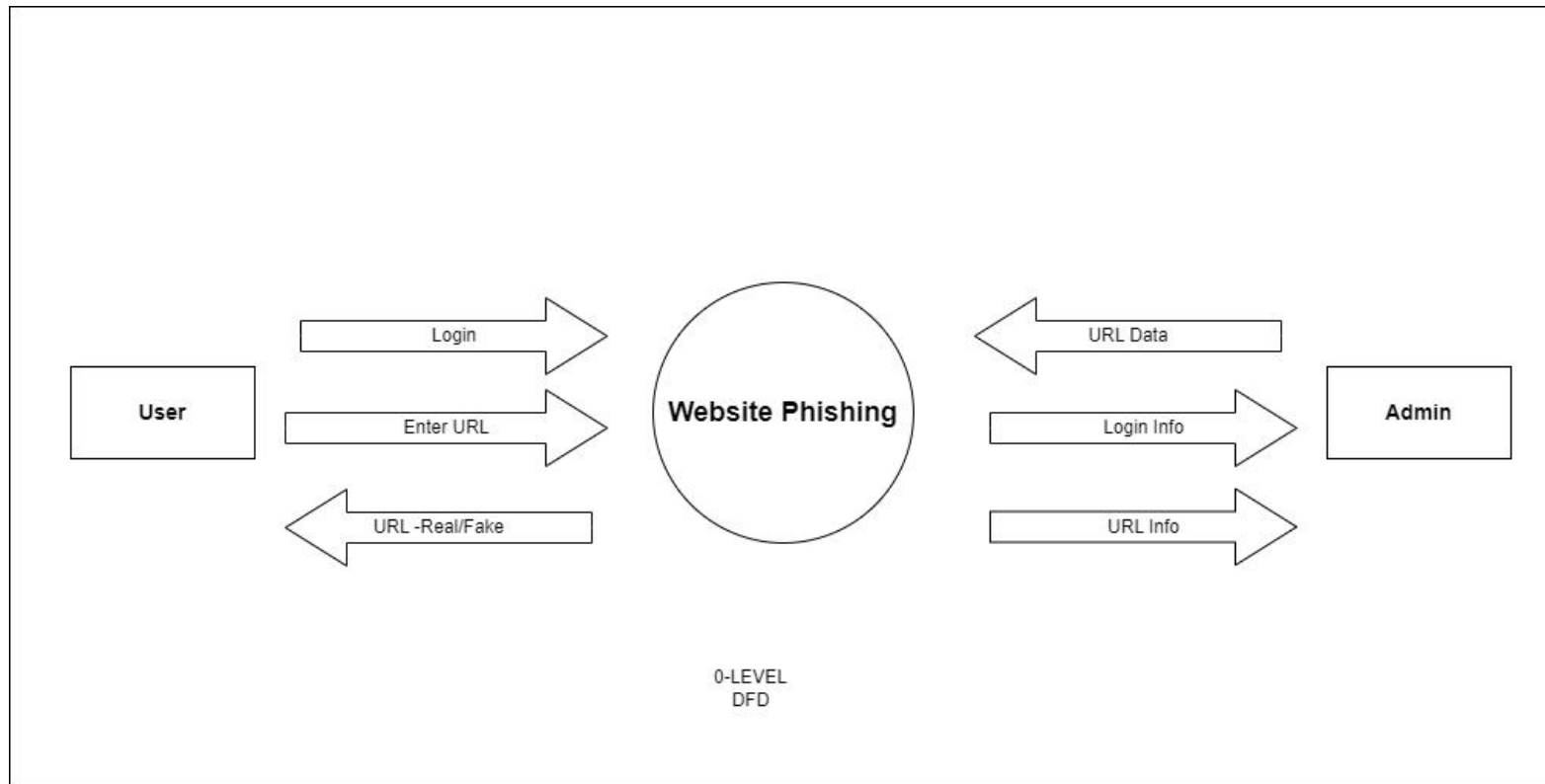


# SYSTEM FLOW DIAGRAM

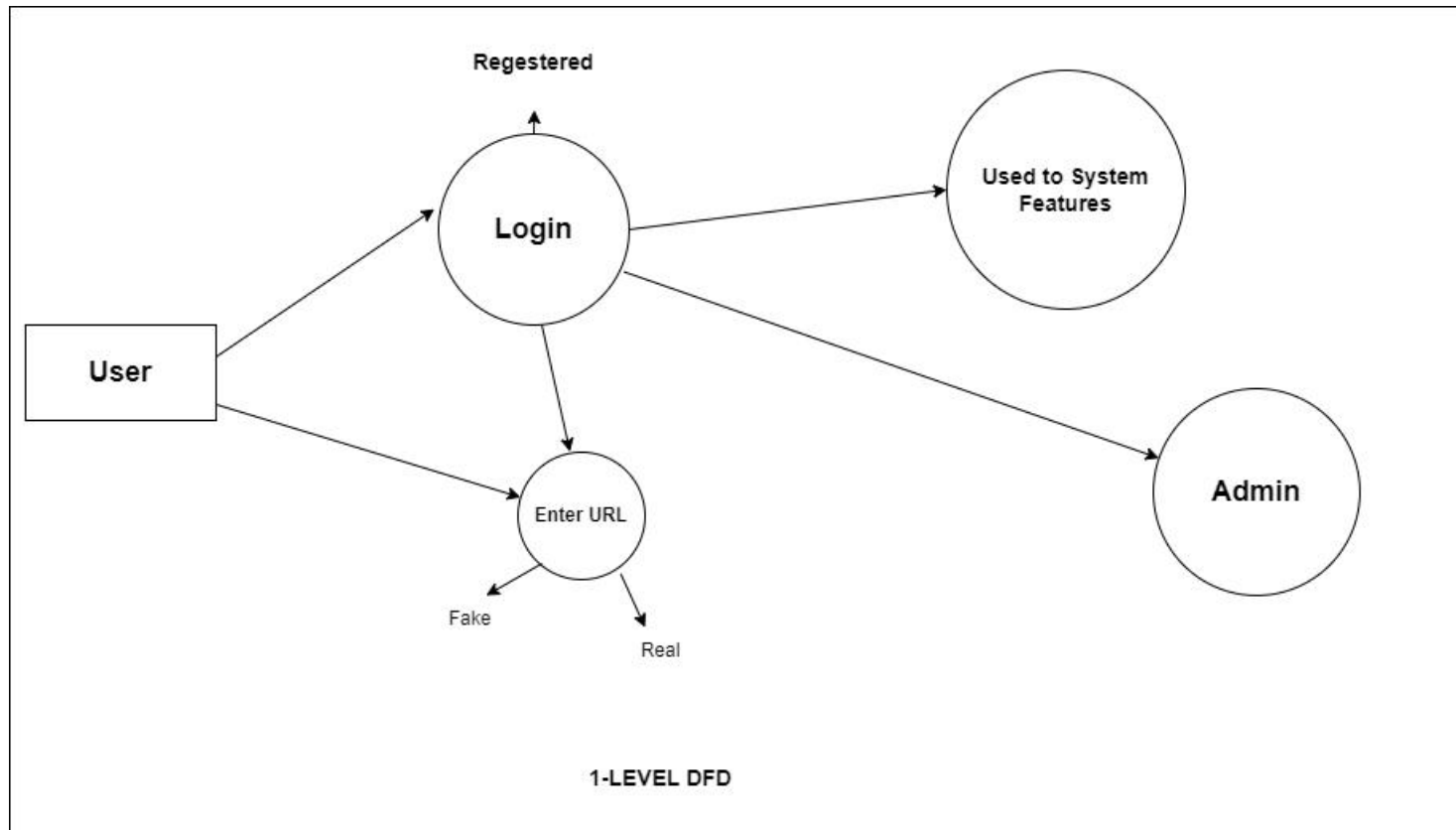




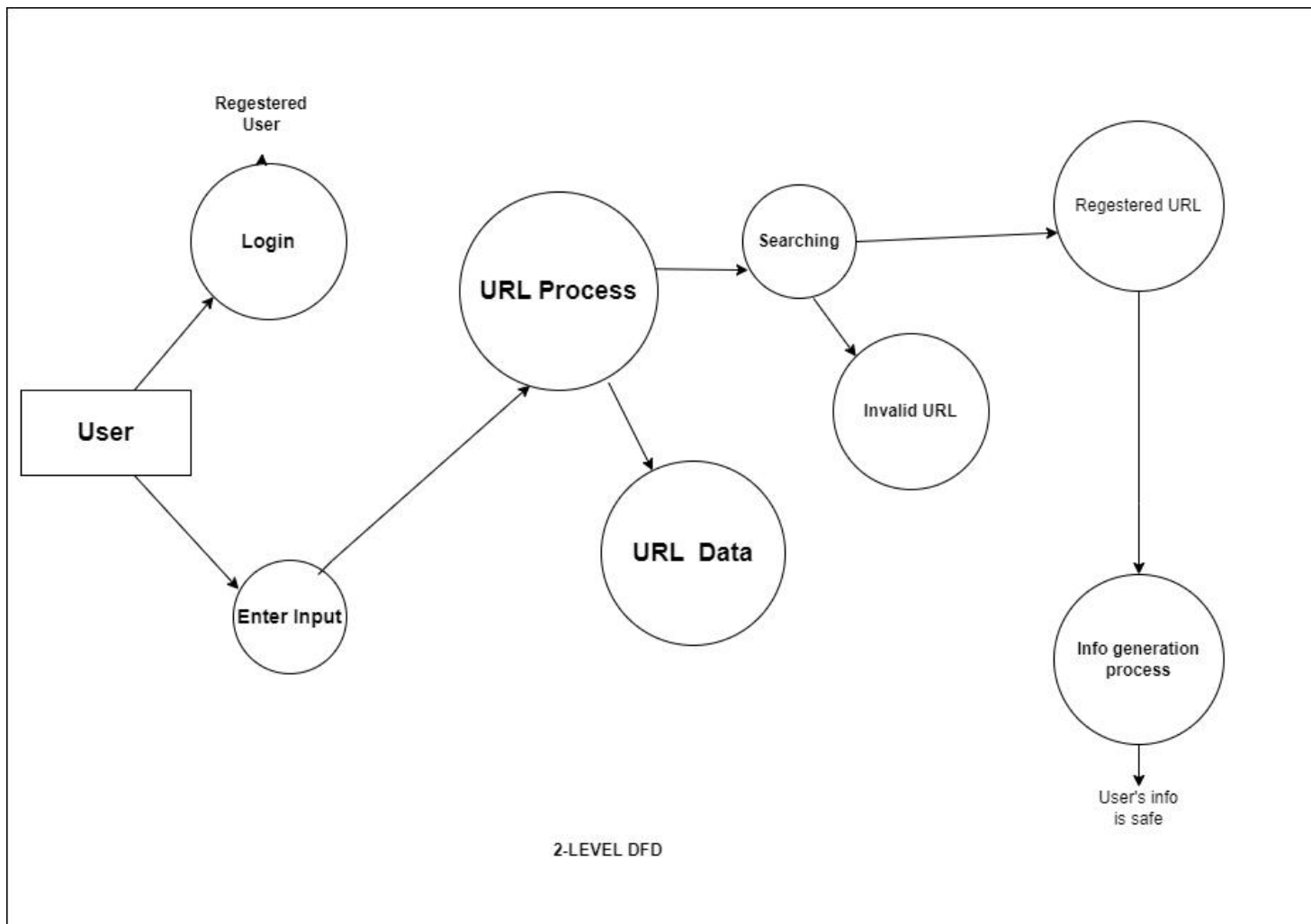
# DATA FLOW DIAGRAM



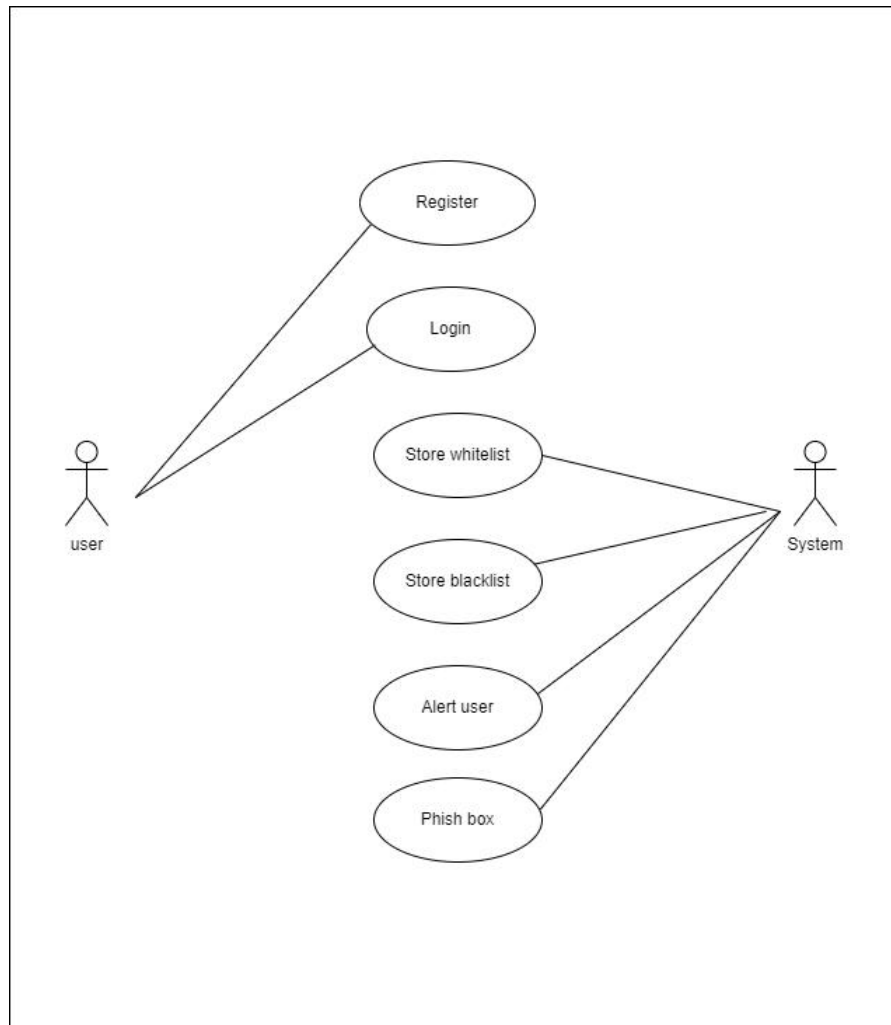
# DATA FLOW DIAGRAM



# DATA FLOW DIAGRAM



# USE CASE DIAGRAM



# DATA DICTIONARY

Sr. No.	Field Name	Data Type	Size	Constraint	Description	Example
1	Id	int	11	Primary key		1,2,3...
2	First name	varchar	20	-		Nirmeet
3	Last name	Varchar	20	-		Patel
4	User name	Varchar	20	Foreign key		nirmeet_123
5	Email	Varchar	50	-		Example123@gmail.com
6	Password	Varchar	250	-		123#456
7	Contact	Double	-	-		9182736405
8	User type	Varchar	20	-		
9	Forgot pass identity	Varchar	32	-		
10	Created	Datetime	-	-		
11	Modified	datetime	-	-		



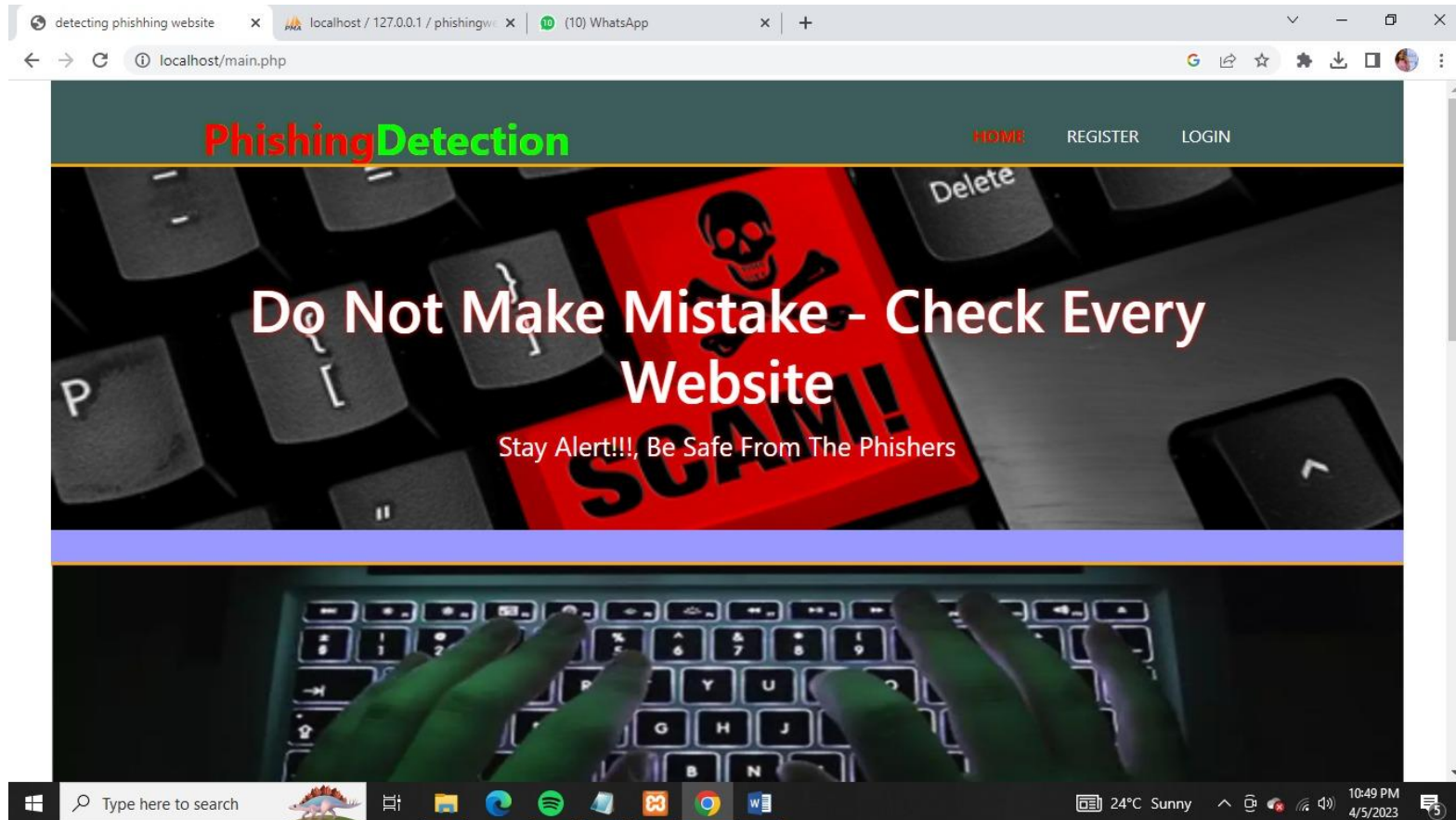
# DATA DICTIONERY

Sr. No.	Field Name	Data Type	Size	Constraint	Description	Example
1	Uid	Int	11	Primary key		1,2,3,4..
2	url	Varchar	200	-		<a href="https://www.instagram.com/credicard/">https://www.instagram.com/credicard/</a>
3	type	int	11	-		-1

Sr. No.	Field Name	Data Type	Size	Constraint	Description	Example
1	F id	Int	11	Primary key		1,2,3,4..
2	Rate	Varchar	10	-		Average, good
3	name	Varchar	20	-		Sandeep Sharma, Krishna....
4	Email	Varchar	30	-		
5	comment	text	-	-		It's good, I like this system ,etc



# SCREENSHOTS OF DEVELOPMENT PHASE 1 ( DESIGNING OF YOUR PROJECT)



# SCREENSHOTS OF DEVELOPMENT PHASE 2 ( FEATURES IMPLEMENTATION)

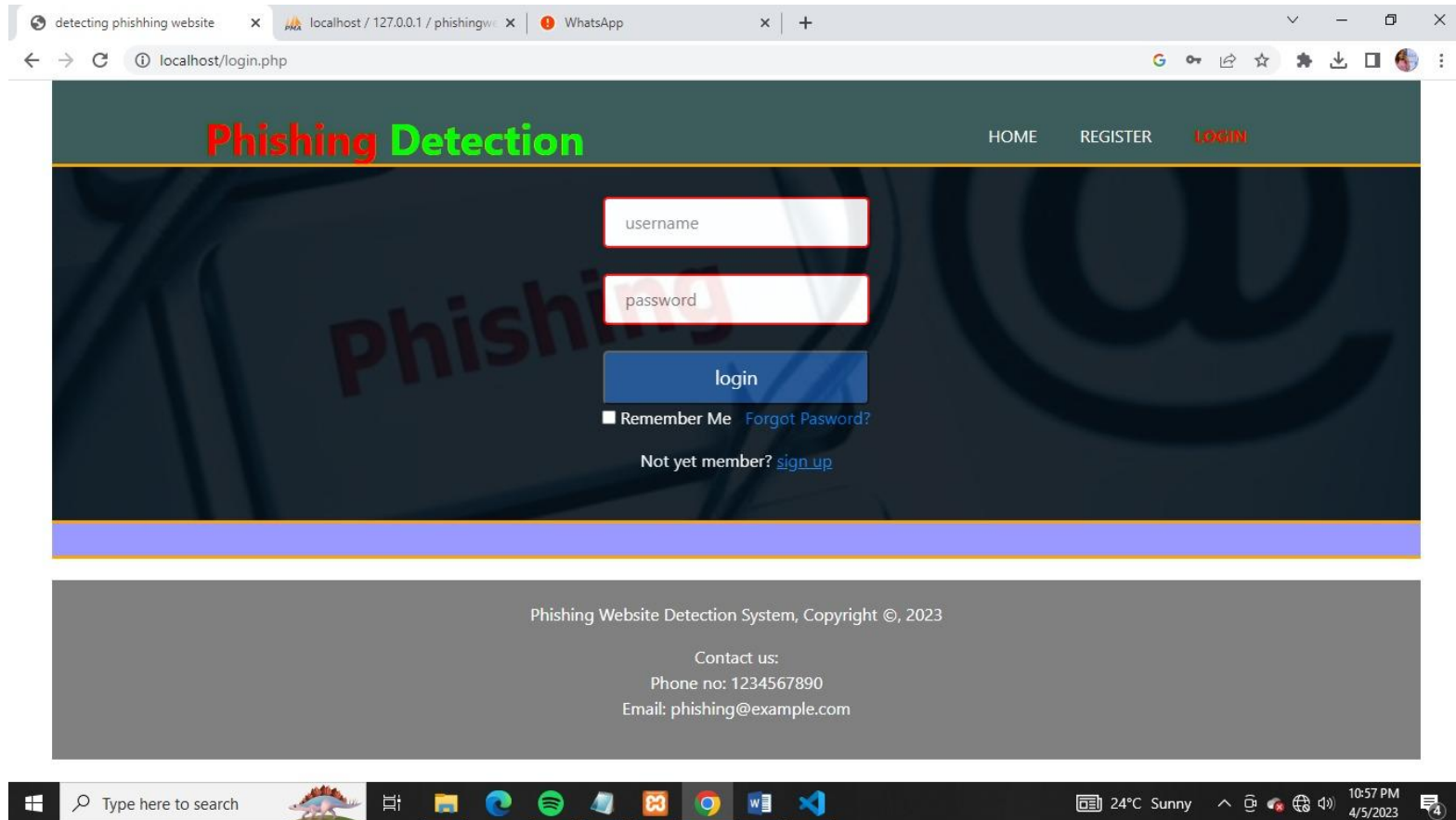
The screenshot displays a web browser window with the address bar showing 'localhost/register.php'. The page title is 'Phishing Detection'. The navigation bar includes links for 'HOME', 'REGISTER', and 'LOGIN'. The main content area features a registration form with the following fields:

- first name
- last name
- username
- email
- password
- confirm password (with a green 'Matching' status indicator)
- phone number (with a dropdown arrow icon)

A blue 'register' button is located at the bottom of the form. The background of the page is dark with a large, faint watermark of a padlock and the word 'phishing'.



# SCREENSHOTS OF DEVELOPMENT PHASE 2 ( FEATURES IMPLEMENTATION)



THANK YOU !!!

