**INTRODUCTION**

1. **INTRODUCTION**

Phishing is a brand spoofing a variation on “phishing,” the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting. Phishing is a form of online criminal trick of stealing victims’ personal information by sending them spoofed emails urging them to visit a forged webpage that looks like a true one. Phishing is a form of onlineidentity theft associated with both social engineering and technical subterfuge. Specifically, phishers attempt to trick Internet users into revealing sensitive or private information, such as their bankaccount, credit-card numbers and passwords. Users are often lured to browse these web sites through spoofed email, and they might easily be convinced that fake pages with hijacked brand names.

Phishing is a form of online identity theft associated with both social engineering and technical subterfuge and a major threat to information security and personal privacy. Many anti-phishing solutions, such as content analysis and HTML code analysis, rely on this property to detect fake web pages. However, these techniques failed, as phishers are now composing phishing pages with no analyzable elements, such as images and flash objects. This paper proposes a new phishing detection scheme based on an URL domain identity & webpage image matching. At first, it identifies the similar authorized URL, using divide rule approach and approximate string matching algorithm. For this similar URL and input URL, the IP addresses will be identified. If their IP addresses doesn’t match with each other, then it could be phishing URL and phase-I phishing report will be generated. Then, this suspected URL’s webpage snapshot will be treated as an image during phase-II. In phase-II, keypoints will be detected and their features will be extracted. These features will be extracted using CCH descriptor. Then, match this suspected image features with the features of authorized webpage. If this matching crosses threshold value, then this webpage is phishing one. At last, final phishing report will be generated. As the combined approach of URL domain identity and webpage image matching used, it performs better than other existing tools.

This system proposes a new scheme for phishing page detection

based on two phases .

1. URL and Domain Identity

2. Image Based Webpage Matching

1. **URL and Domain Identity Verification**

Normally phishing is done via sending mails to thousands of users urging them to visit the fake website through the link or URL present in it. The input for proposed project is URLs for the detection process. These URLs are mostly similar to authorized URLs, with very minor variation which couldn’t observed by normal users. Using approximate string search algorithm similar authorized URLs will be searched which are stored in database that is often targeted by phishers. Then calculate the IP addresses of the similar URLs. If IP addresses of the Authorized URLs do not match with the IP address of entered (input) URL then this URL could be phishing one. This URL will be considered as input for next phase which are based on the webpage’s image matching.

1. **Image Based Webpage Matching**

In this phase, take a snapshot of a suspect webpage whose URL is detected as a suspected phishing URL in previous phase and treat it as an image throughout the detection process. The suspected webpage’s snapshot is taken from the URL detected as phishing in earlier URL and Domain identity phase. This scheme from first calculates certain number of key points in a suspected webpage image. (The key point is a point, it can be detected, though image undergoes through various changes, such as shifting, lighting variation etc.). Use descriptors to capture invariant information around discriminative key points on the suspect page. Then match the descriptors with those of authentic page’s descriptors’ which are already stored in descriptors database. Matching descriptors yields a similarity degree for a suspect page and an authentic page. Finally, we use the similarity degree between the two pages to determine whether the suspected page is a counterfeit. If the similarity degree between a suspected page and an authentic one is greater than a certain threshold, we consider the suspected page is a phishing page.

1. **Methods of Data Collection**

of websites and the snapshot of webpage’s of these URLs. Databases consist of authorized URLs and their webpage’s Proposed work mainly related to the financial services, payment services websites. In this project input data will be the URLs descriptors (features) as well as suspicious URLs and their webpage’s descriptors. So there are following possible ways to collect data from different sources

**1.1 PROJECT OVERVIEW**

PHISHING

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. The best way to protect yourself from phishing is to learn how to recognize a phish.

Phishing emails usually appear to come from a well-known organization and ask for your personal information — such as credit card number, social security number, account number or password. Often times phishing attempts appear to come from sites, services and companies with which you do not even have an account.

In order for Internet criminals to successfully "phish" your personal information, they must get you to go from an email to a website. Phishing emails will almost always tell you to click a link that takes you to a site where your personal information is requested

**1.Generic greeting.**Phishing emails are usually sent in large batches. To save time, Internet criminals use generic names like "First Generic Bank Customer" so they don't have to type all recipients' names out and send emails one-by-one. If you don't see your name, be suspicious.

**2.Forged link.** Even if a link has a name you recognize somewhere in it, it doesn't mean it links to the real organization. Roll your mouse over the link and see if it matches what appears in the email. If there is a discrepency, don't click on the link. Also, websites where it is safe to enter personal information begin with "https" — the "s" stands for secure. If you don't see "https" do not proceed.

**3.Requests personal information.** The point of sending phishing email is to trick you into providing your personal information. If you receive an email requesting your personal information, it is probably a phishing attempt.

**4.Sense of urgency.** Internet criminals want you to provide your personal information now. They do this by making you think something has happened that requires you to act fast. The faster they get your information, the faster they can move on to another victim.

**Similarity measures for image registration**

Image similarities are broadly used in [medical imaging](http://en.wikipedia.org/wiki/Medical_imaging). An image similarity measure quantifies the degree of similarity between intensity patterns in two images.[[2]](http://en.wikipedia.org/wiki/Image_registration#cite_note-AG-2) The choice of an image similarity measure depends on the modality of the images to be registered. Common examples of image similarity measures include [cross-correlation](http://en.wikipedia.org/wiki/Cross-correlation), [mutual information](http://en.wikipedia.org/wiki/Mutual_information), sum of squared intensity differences, and ratio image uniformity. Mutual information and normalized mutual information are the most popular image similarity measures for registration of multimodality images. Cross-correlation, sum of squared intensity differences and ratio image uniformity are commonly used for registration of images in the same modal

**Why Anti-Phishing Is Necessary Nowadays?**

Phishing has become one of the major issues in the recent times that have sent across a alarm for the internet users. The major reason for concern is the fact that phishing activity directly hit at us as it aims at securing our personal and sensitive information. In phishing, electronic mails or other form of communications are sent across to a specific targeted group of people asking for their credit card information, account details, usernames and passwords.

These mails generally look very professional and bear the looks of official ones. It is one of the most disturbing problems and makes use of large entities names. All of these types of mails asking for personal and significant information are fake ones and are not to be believed.

How does a phishing mail look?

Phishing mails are generally those which carry enticing or attractive announcement claiming that you have won a lottery for $10,000 or that you have won a holiday trip and so on. These mails will ask you to visit a particular link and once you do that, you will be asked to furnish your sensitive information like credit card number and account number. Make sure that you do not succumb to these fake campaigns. Many of these sites also directs you to make some payment to claim the gift amount and in the process they track down the information.

Things not to do to be safe:

* Do not respond to phishing mails
* Do not share your password or user names
* Never open the attachment of the phishing mails
* Do not provide your personal information

Be up to date

There are numerous types of phishing activities that are taking place and one need to put in some extra caution in this space as it is highly dangerous. There are different types and techniques of phishing exercised and this includes clone phishing, whaling and spear phishing. Some of the recent and advanced browsers come with the anti-phishing facility thereby, taking care of it in the initial stage itself. There have been several losses faced by people all over the world because of this fraudulent activity and the government has come with legislations in this regard.

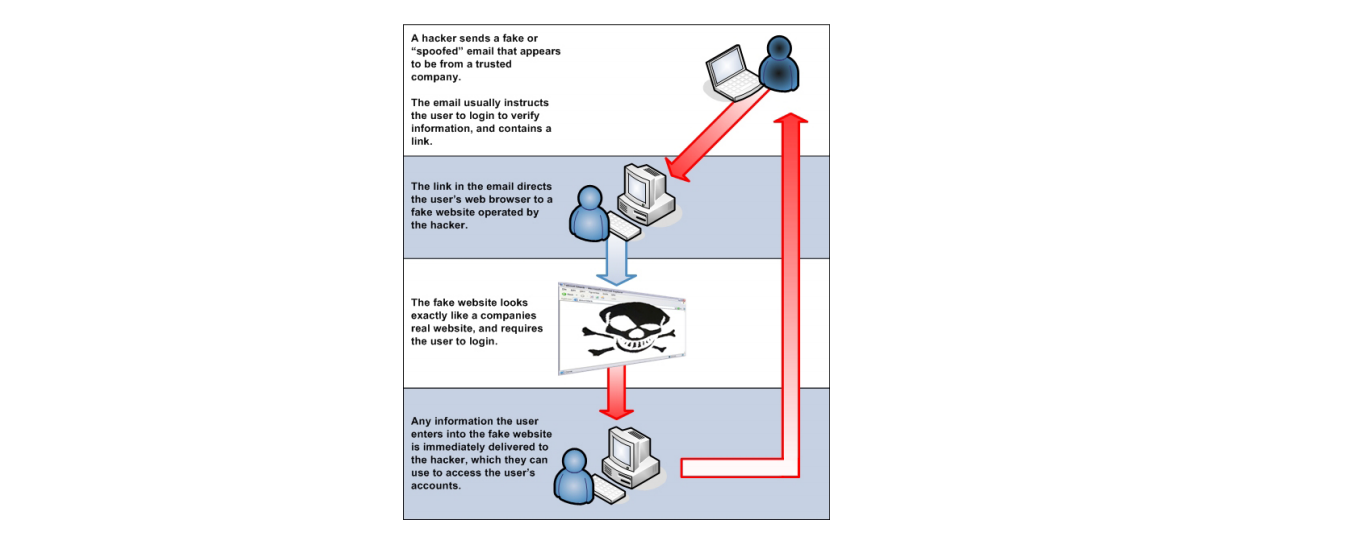
Protect yourself against phishing:

* Install an anti-virus as well as anti phishing software to the system
* Update the anti phishing software from time to time
* Register with the phishing detecting sites
* Use browsers that aids in detecting the phishing activities

These are some of the most basis measure that needs to be taken in order to prevent any phishing attacks on you. Make sure that you install the best of software and browsers so that the problem could be detected and rooted out at an early stage itself. It is better to prevent yourself from the attack rather than going for a corrective measure after the attack happened.

How phishing works

Several mediums are used by phishers. They are instance message, phone phishing, and pharming. However the most effective and universal way is sending email. So here we will describe how phishing mails works.



In general, phishing attacks are performed with the following four steps:

1) Phishers first create a faked web site in a web server. This web site would look

similar or even the same as the legitimate web site. Then they will apply for a domain

namewhich would have a very short survival time on some ISPs.

2) Using some tools, GroupMail is one example, they now send a lot of spoofed

e-mails to target users in the name of those legitimate companies and organizations,

trying to convince the potential victims to visit their Web sites.

3) Users receive the e-mails. When they open an e-mails there are some

hyperlinks waiting for them to click. If they do click on the spoofed hyperlink, the

link will direct them to a web page that is asking the users to input the required

information

4) Once the users input their information, the phishers will get them by email or

some other means. Then phishers can do anything they want with this information,

including drawing out the money from the users’ account.

In our anti-phishing system, we use several technologies to collect phishing

e-mails and analyzing them, and then we will take some actions to prevent the users

from being beguiled.

**SYSTEM ANALYSIS**

**2. SYSTEM ANALYSIS**

System analysis is the process of gathering and interpreting facts, diagnosing problems and using the facts to improve the system. Analysis is a detailed study of various operations performed by a system and their relationship within and outside of the system. This involves gathering information and using structured tools for analysis.

System analysis is the way of studying and studying a system with an eye on solving its problem-using computer. To analyze a system one has to study the working of the system in detail .The system analyst has to understand the functioning and concept of the system in detail ,before designing the appropriate computer based system that will meet all the requirements of the existing system.

**2.1 REQUIREMENT ANALYSIS**

Requirement analysis is done in order to understand the problem which should be solved by the software system. The problem could be automating an existing manual process, developing a new automated system or combination of two. For large systems have many features, and that need to perform many different tasks, understanding the requirements of the system is major task.

The emphasis in the requirement analysis is to for large system that have many features, and that need to perform many different tasks understanding the requirements of the system is major task.

This helps to identify what the users expect from the system, not how the system will achieve the goal. Since there are the clients and the developers, who manually don’t understand the limitations and needs, leads to inefficient system without analysis.

So before designing the system we analyse the user that answering the following questions

* Who will use our system?
* What they expect from the site?
* What there basic needs are?

The process of establishing the services the system should provide and the constraints under which it should operate called Requirement Analysis. System requirement should set out what the system must do rather than how it is done. A requirement definition is a statement, in natural language plus illustrations, which defines constraints under which the proposed system must operate. The document is also called functional specifications. It serves as a contract between the system buyer and the website developer.

Firstly a requirement definition is written and then it is expanded to requirement specification. The website design is based directly on the requirement specifications. The requirement specification document must specify all functional and performance requirements.

**2.2. EXISTING SYSTEM**

Existing approaches to Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. Despite the vulnerabilities, it’s the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks. Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks. The strong system-assigned passwords are difficult for users to remember.

**2.3 .PROPOSED SYSTEM**

Now-a-days, all business, government, and academic organizations are investing a lot of money, time and computer memory for the security of information. Online password guessing attacks have been known since the early days of the Internet, there is little academic literature on prevention techniques. This project deals with guessing attacks like brute force attacks and dictionary attacks.

This project proposes a click-based graphical password system. During password creation, there is a small view port area that is randomly positioned on the image. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess.

Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. Automated Turing Tests (ATTs) continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users.

This project proposes a new Password Guessing Resistant Protocol (PGRP), derived upon revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT.

This proposed system also provides protection against key logger spy ware. Since, computer mouse is used rather than the keyboard to enter our graphical password; this protects the password from key loggers.

**2.4. FEASIBILITY STUDY**

A feasibility study is a general examination of the potential of an idea to be converted into a business . This study focussed largely on the entrepreneur to convert the idea into business enterprise. Feasibility study is procedure that identifies, describes and evaluates candidates systems and selects the best system for the job. An estimate is made of whether the identified user needs may be satisfied using current software and hardware technologies. The study will decide if the proposed system will be cost effective from the business view of point and if it can be developed given existing budgetary constraints. The key considerations involved in the feasibility analysis are economical, technical, behavioural and operational.

**2.4.1 Economical Feasibility**

Economical analysis is the most frequently used method for evaluating the effectiveness of a candidates system. The economical analysis is to determines the benefits and savings that are expected from a candidates system and compare with costs. The system is economically feasible, as the organization processes the hardware and software resources required for the functioning of the system. Any additional resources, if required, can also be easily acquired.

**2.4.2 Technical Feasibility**

Technical Feasibility centre on the existing computer system and to add what extent it can support the proposed addition. Since the minimum requirements of the system like IIS on the server and a browser on the client, are met by any average user.

* + 1. **Operational Feasibility**

The system operation is the longest phase in the development life cycle of a system. So, operational feasibility should be given much importance. The users of the system don’t need through training on the system. All they are expected to know to operate the system is the basic netsurfing knowledge. It has a user- friendly interface.

* + 1. **Behavioural Feasibility**

The behaviour of the site plays an important role in the number of users accessing the website. This is due to the fact that is a simple site is very easy and convenient to use as compared to complex ones.

**2.5 SYSTEM SPECIFICATION**

**HARDWARE SPECIFICATION**

System : Pentium IV 2.4 GHz.

Hard Disk : 40 GB.

Floppy Drive : 1.44 Mb.

Monitor : 14’ Colour Monitor.

Mouse : Optical Mouse.

Ram : 512 Mb.

Keyboard : 101 Keyboard.

**SOFTWARE SPECIFICATION**

Operating system : Windows XP.

Coding Language : PHP

Data Base : SQL Server 2005.

Front end : Adobe Dreamweaver CS4 10.0

Back end : MySql server.

Web server : XAMPP 1.7.7

**2.6 SOFTWARE REQUIREMENT SPECIFICATION :**

**2.6.1 Customer Requirements :**

Customer requirements define system properties and constraints. Examples of system properties are reliability, response time and store occupancy. Examples of constraints are the capabilities of the i/o devices attached to the system and the data representations used by other systems connected to the required system. Customer requirements can be classified into:

**2.6.2 Product Requirements :**

These are requirement, which result from the need for the delivered product to behave in a particular way. For this system the memory requirement is minimum 128MB RAM and 20GB of secondary store and 56KBPS/LAN card.

**2.6.3 Organizational Requirements :**

These are requirements, which are consequences of organizational policies and procedures.

**2.6.4 External Requirements :**

This covers all the factors external to the system and its development.

**2.6.5 Functional Requirements :**

* The website should be able to connect over the internet.
* The website should be able to manage the tasks specified from the user.
* The Administrator has the power to accept reject a user request.
* The Administrator has the power to add users and product.
* The Administrator can view account details of both admin and registered users**.**

**SYSTEM DESIGN**

**3. SYSTEM DESIGN**

The most creative and challenging phase of the system life cycle is system design . The term design describes the final system and the process by which it is developed.

The first step in design is to determine how the output is to be produced and in what format . Second the formats of input screens are to be determined. The input data and the master files have to be designed to meet the requirements of the proposed output.

Input Design :

This provides details like the type of input data medium arrangement or coding of data guidance to provide input data to the users ,data items and transactions that need validation to detect errors and methods for performing input validation and steps to follow when an error occurs.

Inaccurate input data are most common cause of errors in data processing. Errors entered by data entry operators can be controlled by input design. Input design is the process of converting user-oriented inputs to a computer-based format. Input data are collected and organized into groups of similar data.

The goal of designing input data is to make data entry easy, logical and free from errors as possible. In the design of input the following steps must be considered.

* The allocated space for each field.
* Field sequence, which must match that in the source document.
* The format in which data fields are entered

We have to keep in mind the following things to design the system

* What data to input
* What medium to use

Input design is a part of overall system design which requires very careful attention. Often the collection of input data is the most expensive part of the system, in terms of the equipment used; it is the point of most contact for the users with the computer system; and it is prone to error. If data going into the system is incorrect, then the processing and output will magnify these errors. Thus the designer has a number of clear objectives in input design.

Output Design :

One of the most important features if the system for users is the output it produces. Output design should improve the system relationship with the user.

The objective of output design is to define the control and formats of all printed , documented, reports and screens produced by the system. Output generally refers to the results that are generated by the system.

**3.1 PROJECT MODULES**

The project is divided into four modules

* User Registration
* User Login
* Password Creation
* AddS Module

**User Registration Module :**

A registered user is one who uses a program or a website and provides his/her credentials, effectively proving his/her identity.Generally speaking, any person can become a registered user by providing some credentials, usually in the form of a username (or email) and password. After that, one can access information and privileges unavailable to non-registered users, usually referred to simply as guests. The action of providing the proper credentials for a website is called logging in, or signing in.

Since the site knows about the identity of persona using the page, it can Display personalized data (the simplest way is saying "Hello, John!"),Switch to personalized settings (e.g., "Disable pictures" or change site language),Let the user perform actions from his identity (like post in a forum using his nickname),Access private data (like email or pm),Control automated edits, also known as spamming,Allows the Web Developers to email registered users with updates on their site.

This module deals with user registration. New users have to register to create an account. User should register with his\her Username, Password, Phonenumber, Email. This information is store in our database.After the successful registration user can use the account with the user name and password provided at the time of registration.

**User Login Module**

In computer security, a login or logon refers to the credentials required to obtain access to a computer system or other restricted area. Logging in or on and signing in or on is the process by which individual access to a computer system is controlled by identifying and authenticating the user through the credentials presented by the user.

Once a user has logged in, they can then log out or log off when access is no longer needed. To log out is to close off one's access to a computer system after having previously logged in.

Logging in is usually used to enter a specific page, which trespassers cannot see. Once the user is logged in, the login token may be used to track what actions the user has taken while connected to the site. Logging out may be performed explicitly by the user taking some action, such as entering the appropriate command, or clicking a website link labeled as such. It can also be done implicitly, such as by the user powering off his or her workstation, closing a web browser window, leaving a website, or not refreshing a webpage within a defined period.

In the case of web sites that use cookies to track sessions, when the user logs out, session-only cookies from that site will usually be deleted from the user's computer. In addition, the server invalidates any associations with the session, making any session-handle in the user's cookie store useless. This feature comes in handy if the user is using a public computer or a computer that is using a public wireless connection. As a security precaution, one should not rely on implicit means of logging out of a system, especially not on a public computer, instead one should explicitly log out and wait for the confirmation that this request has taken place.

Logging out of a computer when leaving it is a common security practice, preventing unauthorized users from tampering with it. There are also people who choose to have a password-protected screensaver set to activate after some period of inactivity, requiring the user to re-enter his or her login credentials to unlock the screensaver and gain access to the system. There can be different methods of logging in that may be via image, fingerprints, eye scan, password (oral or textual input), etc.

In this system first user should provide the username then he/she should select the thumbil image which is chosen as password at the time of enrolment .User should select the defined click points to verify the identity.After the successful verification user can use their account.

**Password creation**

Password creation means choosing a strong memorable password.Passwords can be either Knowledge based or token based or biometric based.Knowledge base systems include text and graphical passwords.

In this system we use graphical passwords. Graphical passwords can be implemented using two methods such as recognition based and recall based methods.Recall based mechanism use passpoints and cued click points.In this project a combination of recall based technique is used for password creation.

For password creation user should choose a thumbil image either predefined image or user select image.The image is processed and converting into a fixed size by cropping.Then user have to select sequential five click point on the image which is treated as the password.

The click point is captured by listening the mouse event.Mouse click action on the image is saved to store the password click points.

**AddS Module**

Additional security module include extra security actions to the imagepassword system.Number of Loginattempt , Login count check is check each time before providing access to the account.If check count is greater than two User will be in blocked state.

Recently login machine detail check is also done to ensure that the user is the authenticated person. If the system found any unusual activity on the account then a verification code is send to the mobile of the user.Then the verification code must be entered to gain access to his/her account.

**3.2 DATA FLOW DIAGRAM**

Data flow diagram is used to define the flow of the system and its resource such as information Data flow diagrams are a way of expressing system requirements in graphical manner. Data flow diagrams represent one of the most ingenious tools used for structured analysis. A data flow diagram or DFD as it is called bubble chart. It has purpose of clarifying system requirements and identifying major transformations that will become programs in system design. It is the major starting point in the system design phase that functionally decomposes the requirement specifications down to the lowest level of detail.

A DFD consists of a series of bubbles by joined by lines. The bubbles represent data transformations and lines represent flow in the system.

A DFD has 4 major symbols they are follows

Square, this defines source or destination of data.

Arrow, this shows flow of data

Oval, this represents a process that transforms incoming outgoing flow.

Rectangle, this represents data store and this also represents static data

too.

**3.3 TABLE DESIGN**

Table design means how data should be organized around user requirements. How data are organized depends on the data and response requirements that determine hardware configurations. An integrated approach to file design is the data base. The general theme around in the database is to handle information as an integrated whole.

Database is a collection of inter related data stored together data with control redundancy to serve one or more application .A program now request the data through database system(DBMS),which determines the data sharing. The general objectives are to make information access easy, quick, efficient, inexperience and flexible for the user.

In the backend we use database named “imagepassword” to store all information in the table.

**3.3.1 Signup Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Field** | **Type** | **Null** | **Key** | **Default** | **Extra** |
| ID | Integer(11) | No | PRI | NULL |  |
| username | Varchar(30) | No | Unique | NULL |  |
| password | Varchar(500) | No |  | NULL |  |
| imagename | Varchar(30) | No |  | NULL |  |
| Email | Varchar(30) | No |  | NULL |  |
| phonenumber | Bigint(10) | No |  | NULL |  |
| Textpassword | Varchar(30) | No |  | NULL |  |
| Blockedto | Datetime | No |  | NULL |  |

Table 3.3.1. Signup Table

**3.3.2 Blocked Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Field** | **Type** | **Null** | **Key** | **Default** | **Extra** |
| username | Varchar(100) | No | PRI | NULL |  |

Table 3.3.2. Blocked Table

**3.3.3 Reset Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Field** | **Type** | **Null** | **Key** | **Default** | **Extra** |
| Email | Varchar(100) | No | PRI | NULL |  |
| Code | Varchar(100) | No | Unique | NULL |  |
| Username | Varchar(100) | No |  | NULL |  |

Table 3.3.3.Reset Table

**SYSTEM IMPLEMENTATION**

**4 .SYSTEM IMPLEMENTATION**

Implementation is the stage in the project where the theoretical design is turned into working system and is giving confidence on the new system for the users that it will work efficiently and effectively. It involves careful planning, investigation of the current system and its constraints on implementation, design of methods to achieve the change over, an evaluation of change over methods. Apart from planning major task of preparing the implementation are education and training of users. The more complex system is being implemented, the more involved will be the system analysis and design effort required just for implementation.

An implementation co-ordination committee based on politics of individual organization has been appointed. The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to

be carried out, discussions made regarding the equipment and resources and the additional equipment has to be acquired to implement the new system.

Implementation is the final and important phase. The system can be implemented only after through testing is done and it is found to working according to the specification. This method also offers the greatest security since the old system can take over if the errors are found or inability to handle certain type of transactions while using the new system.

The implementation plan includes a description of all activities that must occur to implement the system and to put it into operation. It indicates the personal respossible

for the activities and prepares a time chart for implementing the system, The implementation plan consists of the following step.

* List all files required for implementation.
* Identify all data required to build new files during the implementation.
* List all new documents and procedures that go into the new system.

The implemented system has the following features:

* Reduced data redundancy.
* Ease of use.
* Controlled flow.
* Simplifies the management activities.

**Security Technologies And Policies:**

Security involves both policies and mechanisms to protect the data and ensures that it is not accessed, altered or deleted without proper authorization. There are two dimensions for the protection of data in the data base. The logged user can only perform the operations. This ensures that the confidentiality of the data is maintained, second, the data must be protected from accidental or intentional corruption or destruction.

The security features are considered while developing the system, so as to avoid the errors and omissions that may lead to serious problems. The system may have to face the unwanted events called threats. A threat to a computer system is any events that adversely affect the one or more assets or resources, which make up the system. An event can be any of the following:

* Interruption of communication.
* Destruction of hardware.
* Modification of software.
* Removal of programs.
* Disclosure of information.

There are many methods for handling a threat.

* Avoid it by altering the design.
* Threat retention.
* Threat reduction that is the frequency of occurrence of a threat is reduced.

The security measures of a computer system should be specified at an early stage in the design of the system. During the system operation each user should understand the procedures required to keep the system secure.

There are many possible threats to the security and integrity of any system where more than one user is associated with the system. Software integrity has become increasingly important. The attribute measures a system’s ability to withstand attacks, both accidental and intentional on its security. Attacks can be made on all the three components of software: programs date and documents.

In this project the data security, data validation checking methods are applied using a password authentication. All the data, which is entered by the administrator, will be validated.

**Maintenance :**

The maintenance is an important phase of any system. Maintenance of the system should be done accurately and with specific care for proper running of the system.

Maintenance involves the software industry captive, typing up the system resources. It means restoring something to its original condition. Maintenance involves a wide range of activities including correcting, coding and design errors, updating documentation and test data and upgrading user support. Maintenance is continued till the product is re-engineered or deployed to another platform. Maintenance is also done based on fixing the problems reported, changing the interface with other software or hardware enhancing the software.

Any system developed should be secured and protected against possible hazards. The system should be maintained and upgraded according to the technological advancements. It ensures the data integrity, data control and security. The system must be protected from fire and other natural calamities. The backup copies of data must be maintained daily so that to prevent the loss of data due to various reasons. Security measures are provided to prevent unauthorized access of the database at various levels.

Software maintenance is divided into the following three categories :

* Corrective maintenance
* Adaptive maintenance
* Perfective maintenance

Corrective maintenance has to do with the removal of residual errors present in the product when it is delivered as well as errors introduced into the software during its maintenance.

Adaptive maintenance modifies the software to keep it up to date with its operative environment. It may be needed because of changes in the user requirements, changes in target platforms, or changes in external interfaces.

Perfective maintenance involves changing the software to improve some of its qualities. The request to perfective maintenance may come directly from the software engineer, in order to improve the status of the product on the market, or they may come.Administrator manages the GUI that helps the users to easily use the system without difficulty.

Here we implement the side that is directly in contact with the users. A user is allowed to enter the system after authentication of that particular user. The users of the system have to provide user name and password .If a particular user is not in the login table, then he can’t access the system. In this module the administrator can upload new image to the database and delete images from that. The users can select image to store the password. The user select a point in image to store long term password.

**4.1 DETAILS OF SOFTWARE USED :**

**4.1.1 phpMyAdmin :**

phpMyAdmin is a free software tool written in [PHP](http://php.net/), intended to handle the administration of [MySQL](http://mysql.com/) over the World Wide Web. phpMyAdmin supports a wide range of operations with MySQL. The most frequently used operations are supported by the user interface (managing databases, tables, fields, relations, indexes, users, permissions, etc), while you still have the ability to directly execute any SQL statement.

phpMyAdmin comes with a wide range of [documentation](http://www.phpmyadmin.net/home_page/docs.php) and users are welcome to update [our wiki pages](http://wiki.phpmyadmin.net/) to share ideas and howto use for various operations. The [phpMyAdmin team](http://www.phpmyadmin.net/home_page/team.php) will try to help you if you face any problem; you can use a [variety of support channels](http://www.phpmyadmin.net/home_page/support.php) to get help.phpMyAdmin is also very deeply documented in a book writtenby one of the developers – [Mastering phpMyAdmin for Effective MySQL Management](http://link.packtpub.com/XJdqZr), which is available in English and [Spanish](http://www.phpmyadmin.net/home_page/docs.php#books).

To ease usage to a wide range of people, phpMyAdmin is being translated into [69 languages](http://www.phpmyadmin.net/home_page/translations.php) and supports both LTR and RTL languages.

Since version 3.0.0, phpMyAdmin joined the GoPHP5 initiative and dropped compatibility code for older PHP and MySQL versions; version 3 and later requires at least PHP 5.2 and MySQL 5.phpMyAdmin has won several [awards](http://www.phpmyadmin.net/home_page/awards.php). Among others, it was chosen as the best PHP application in various awards and has won every year the SourceForge.net Community Choice Awards as "Best Tool or Utility for SysAdmins”.phpMyAdmin is a fourteen-year-old project with a stable and flexible code base, to find out more about the project and its history see this [separate page](http://www.phpmyadmin.net/home_page/about.php).

**4.1.2 Dreamweaver:**

Adobe Dreamweaver is a[proprietary](http://en.wikipedia.org/wiki/Proprietary_software) [webdevelopment](http://en.wikipedia.org/wiki/Web_development) [application](http://en.wikipedia.org/wiki/Application_software) developed by [Adobe Systems](http://en.wikipedia.org/wiki/Adobe_Systems). Dreamweaver was originally developed by [Macromedia](http://en.wikipedia.org/wiki/Macromedia) in 1997 and was maintained by them until Macromedia was acquired by Adobe Systems in 2005.Adobe Dreamweaver is available for both [Mac](http://en.wikipedia.org/wiki/Mac_OS_X) and [Windows](http://en.wikipedia.org/wiki/Microsoft_Windows) [operating systems](http://en.wikipedia.org/wiki/Operating_system).

Following Adobe's acquisition of the Macromedia product suite, releases of Dreamweaver subsequent to version 8.0 have been more compliant with [W3C](http://en.wikipedia.org/wiki/World_Wide_Web_Consortium)standards. Recent versions have improved support for [Web](http://en.wikipedia.org/wiki/World_Wide_Web) technologies such as [CSS](http://en.wikipedia.org/wiki/Cascading_Style_Sheets), [JavaScript](http://en.wikipedia.org/wiki/JavaScript), and various [server-side scripting](http://en.wikipedia.org/wiki/Server-side_scripting) [languages](http://en.wikipedia.org/wiki/Programming_language) and[frameworks](http://en.wikipedia.org/wiki/Software_framework) including [ASP](http://en.wikipedia.org/wiki/Active_Server_Pages) (ASP JavaScript, ASP VBScript, ASP.NET C#, ASP.NET VB), [ColdFusion](http://en.wikipedia.org/wiki/ColdFusion), [Scriptlet](http://en.wikipedia.org/wiki/Scriptlet), and [PHP](http://en.wikipedia.org/wiki/PHP). Adobe Dreamweaver is a web design and development application that provides a visual [WYSIWYG](http://en.wikipedia.org/wiki/WYSIWYG) editor (colloquially referred to as the Design view) and a code editor with standard features such as [syntax highlighting](http://en.wikipedia.org/wiki/Syntax_highlighting), [code completion](http://en.wikipedia.org/wiki/Autocomplete#In_source_code_editors), and code collapsing as well as more sophisticated features such as real-time [syntax checking](http://en.wikipedia.org/wiki/Syntax_analysis#Programming_languages) and code introspection for generating code hints to assist the user in writing code. The Design view facilitates rapid layout design and [code generation](http://en.wikipedia.org/wiki/Automatic_programming#Source_code_generation)as it allows users to quickly create and manipulate the layout of [HTML](http://en.wikipedia.org/wiki/HTML) elements. Dreamweaver features an integrated browser for previewing developed webpages in the program's own preview pane in addition to allowing content to be open in locally installed web browsers. It provides transfer and synchronization features, the ability to find and replace lines of text or code by search terms or regular expressions across the entire site, and a templating feature that allows single-source update of shared code and layout across entire sites without server-side includes or scripting. The behaviors panel also enables use of basic JavaScript without any coding knowledge, and integration with Adobe's Spry Ajax framework offers easy access to dynamically-generated content and interfaces.

Dreamweaver can use third-party "Extensions" to extend core functionality of the application, which any web developer can write (largely in [HTML](http://en.wikipedia.org/wiki/HTML) and [JavaScript](http://en.wikipedia.org/wiki/JavaScript)). Dreamweaver is supported by a large community of extension developers who make extensions available (both commercial and free) for most web development tasks from simple rollover effects to full-featured shopping carts.Dreamweaver, like [other HTML editors](http://en.wikipedia.org/wiki/Comparison_of_WYSIWYG_HTML_editors#Editor_features), edits [files](http://en.wikipedia.org/wiki/Computer_file) locally then uploads them to the remote web server using [FTP](http://en.wikipedia.org/wiki/File_Transfer_Protocol), [SFTP](http://en.wikipedia.org/wiki/SSH_file_transfer_protocol).

**4.1.3 XAMPP :**

XAMPP requirees only one [zip](http://en.wikipedia.org/wiki/ZIP_%28file_format%29), [tar](http://en.wikipedia.org/wiki/Tar_%28file_format%29), [7z](http://en.wikipedia.org/wiki/7z), or [exe](http://en.wikipedia.org/wiki/EXE) file to be downloaded and run, and little or no configuration of the various components that make up the web server is required. XAMPP is regularly updated to incorporate the latest releases of [Apache](http://en.wikipedia.org/wiki/Apache_HTTP_Server)/[MySQL](http://en.wikipedia.org/wiki/MySQL)/[PHP](http://en.wikipedia.org/wiki/PHP) and [Perl](http://en.wikipedia.org/wiki/Perl). It also comes with a number of other modules including [OpenSSL](http://en.wikipedia.org/wiki/OpenSSL) and [phpMyAdmin](http://en.wikipedia.org/wiki/PhpMyAdmin).

Self-contained, multiple instances of XAMPP can exist on a single computer, and any given instance can be copied from one computer to another.It is offered in both a full, standard version and a smaller version.

Officially, XAMPP's designers intended it for use only as a development tool, to allow website designers and programmers to test their work on their own computers without any access to the Internet. To make this as easy as possible, many important security features are disabled by default. In practice, however, XAMPP is sometimes used to actually serve web pages on the [World Wide Web](http://en.wikipedia.org/wiki/World_Wide_Web). A special tool is provided to password-protect the most important parts of the package. XAMPP also provides support for creating and manipulating databases in [MySQL](http://en.wikipedia.org/wiki/MySQL) and [SQLite](http://en.wikipedia.org/wiki/SQLite) among others.

Once XAMPP is installed, it is possible to treat a [localhost](http://en.wikipedia.org/wiki/Localhost) like a remote host by connecting using an [FTP](http://en.wikipedia.org/wiki/File_Transfer_Protocol) client. Using a program like [FileZilla](http://en.wikipedia.org/wiki/FileZilla) has many advantages when installing a [content management system](http://en.wikipedia.org/wiki/Content_management_system) (CMS) like [Joomla](http://en.wikipedia.org/wiki/Joomla). It is also possible to connect to localhost via FTP with an [HTML editor](http://en.wikipedia.org/wiki/HTML_editor).

**4.1.4JAVA SCRIPT:**

JavaScript is use for validation purposes usually at the client-side, which do not require the server. It is a programming language integrated with HTML. JavaScript facilitates the developer with properties related to document windows, frames, forms, loaded documents and links. This scripting language also traps user events so programs can be developed for such events. This is an interpreter-based language and source code files are directly executed at runtime. Javascript includes built-in objects related to the current windows and documents as well as objects such as Math, String, Date functions respectively. Since JavaScript is an object-based language, it supports instances, methods and properties.

The browsers support JavaScript. In JavaScript, the document object refers to ‘whatever web page the reader is currently looking through’ – which is also the document that contains the JavaScript code. The links are objects within the document object. Date, button, checkbox, elements array from password are the other objects available.JavaScript statements are used to build loops into the script so that commands can be executed several times.

Event handlers are those parts of language that tell JavaScript to send or to carry out some actions. The event handlers go into regular HTML tags.

* Can display custom dialog boxes on the screen, i.e. alert (), confirm () and prompt ().
* Have two data types – Numbers and Strings.
* JavaScript has custom functions and allows user to write code to have user-defined functions.

**4.1.5 HTML**

HTML stands for Hyper Text Markup Language, which is an application of Standard Generalized Markup Language (SGML). It is a simple language used to define and describe the layout of a web page.HTML supports Multimedia and document links.

HTML consists of special codes which when embedded in text, adds formatting. The special characters which separate HTML from ordinary text are the left and right brackets (<>). These brackets contain instructions known as TAGS which are not case sensitive.HTML, similar to a computer programming language or a script language requires you to express your thoughts in a specific structure; its purpose is to transmit the structure of documents between the users.

HTML was developed to force you to think about document structure rather than document appearance because of the Web’s focus on being a cross platform.

Advantages ofhtml:

HTML files are compatible with any web browser. That is HTML documents are system-independent, and they can be displayed on any computer that supports HTML.

HTML is based on structure rather than on appearance. So an HTML author can define a numbered list, and the users can specify whether they wish to view that list with Roman or Arabic numerals. This provides users with more flexibility in how a document is viewed.

HTML files are small. The tags used to describe an HTML file have little overhead. Tags are instructions to the browser software that tell how to display text and are easy to learn.

**4.1.6 My SQL:**

MySQL database has become the world's most popular Open source database because of its consistency, fast performance, high reliability and ease of use. It has also become the database of choice for a new generation of applications built on the LAMP stack (Linux, Apache, MySQL, PHP / Perl / Python). MySQL runs on more than 20 platforms including Linux, Windows, OS/X, HP-UX, AIX, Netware, giving you the kind of flexibility that puts you in control. MySQL offers a comprehensive range of certified software, support, training and consulting.

MySQL is a multithreaded, multi-user SQL Database Management System. My SQL's implementation of a relational database is an abstraction on top of a computer’s file system. The relational database abstraction allows collection of data items to be organized as a set of formally described tables. Data can be accessed or reassembled from these tables in many different ways, which do not require any reorganization of the database tables themselves.

Relational database speak SQL (Structured Query Language). SQL is a standard interactive programming language for getting information from and updating a relational database. Although SQL itself is both an ANSI and an ISO standard, many database products support SQL with proprietary extensions to the standard language. MySQL's extensions to SQL are not proprietary, since MySQL's code is kept free (as in the user's library to use hte code) by the GPL. SQL queries take the form of a command language that lets you select, insert, update, find out the location of data, and so forth.

My SQL Features

* Very fast and much reliable for any type of application.
* Very lightweight application.
* Command line tool is very powerful and can be used to run SQL queries against database.
* Supports indexing and binary objects.
* Allows changing the structure of table while server is running.
* It has a wide user base.
* It is a very fast thread-based memory allocation system.

My SQL Database Server

MySQL database has become the world's most popular Open source database because of its consistency, fast performance, high reliability and ease of use. It has also become the database of choice for a new generation of applications built on the LAMP stack (Linux, Apache, MySQL, PHP / Perl / Python). MySQL runs on more than 20 platforms including Linux, Windows, OS/X, HP-UX, AIX, Netware, giving you the kind of flexibility that puts you in control. MySQL offers a comprehensive range of certified software, support, training and consulting.

MySQL is a multithreaded, multi-user SQL Database Management System. My SQL's implementation of a relational database is an abstraction on top of a computer’s file system. The relational database abstraction allows collection of data items to be organized as a set of formally described tables. Data can be accessed or reassembled from these tables in many different ways, which do not require any reorganization of the database tables themselves. Relational database speak SQL (Structured Query Language). SQL is a standard interactive programming language for getting information from and updating a relational database. Although SQL itself is both an ANSI and an ISO standard, many database products support SQL with proprietary extensions to the standard language. MySQL's extensions to SQL are not proprietary, since MySQL's code is kept free (as in the user's library to use hte code) by the GPL. SQL queries take the form of a command language that lets you select, insert, update, find out the location of data, and so forth.

**4.2 SCREENSHOTS**

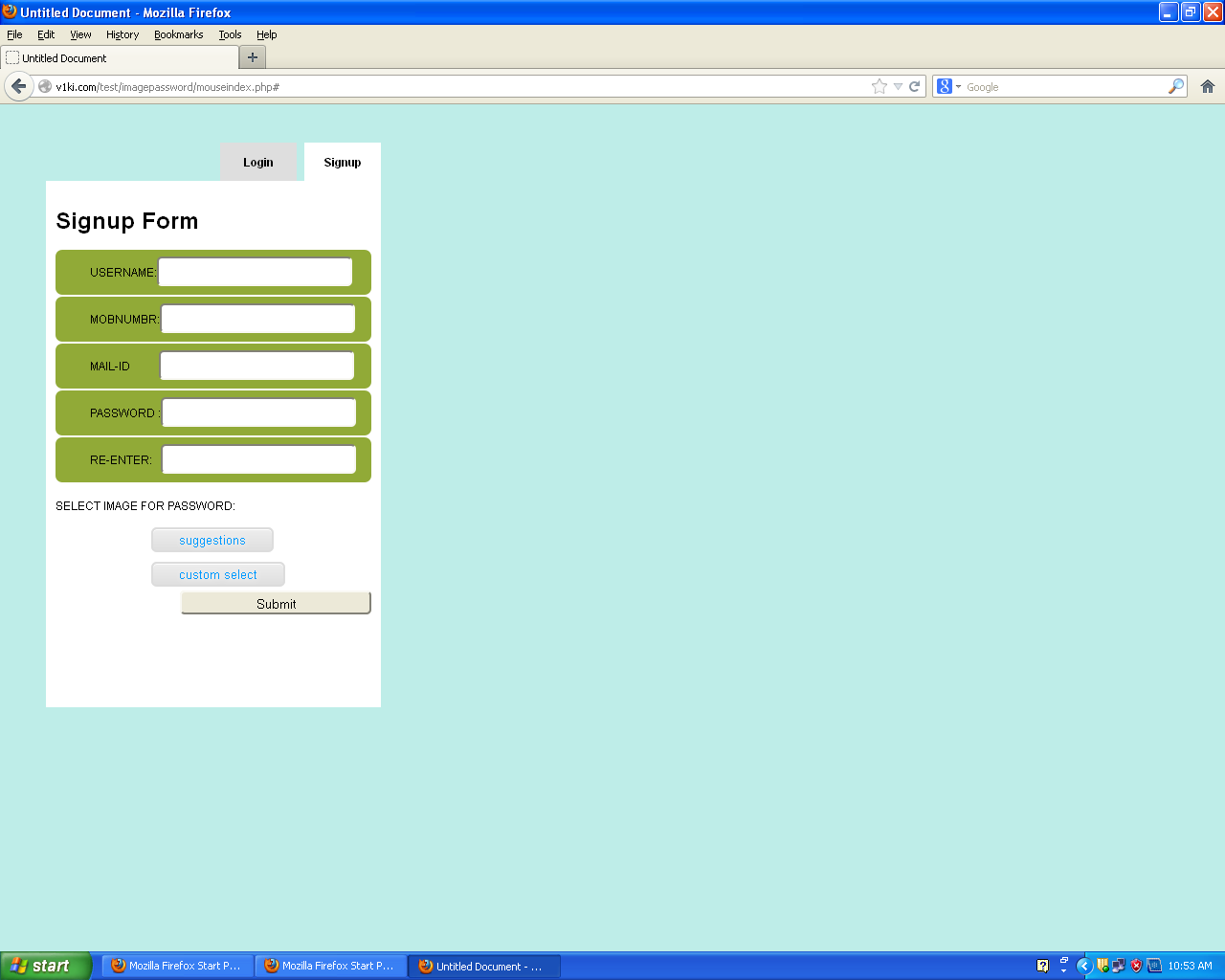


Figure 4.2.1.Signup view

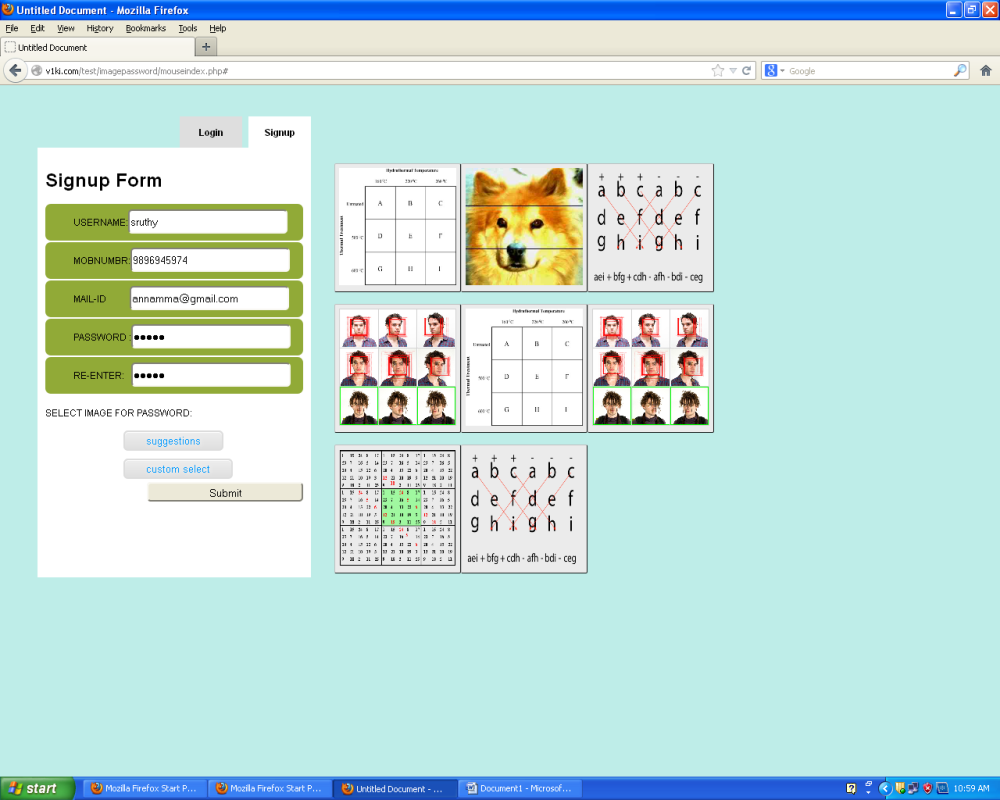


Figure 4.2.2.Signup image selection

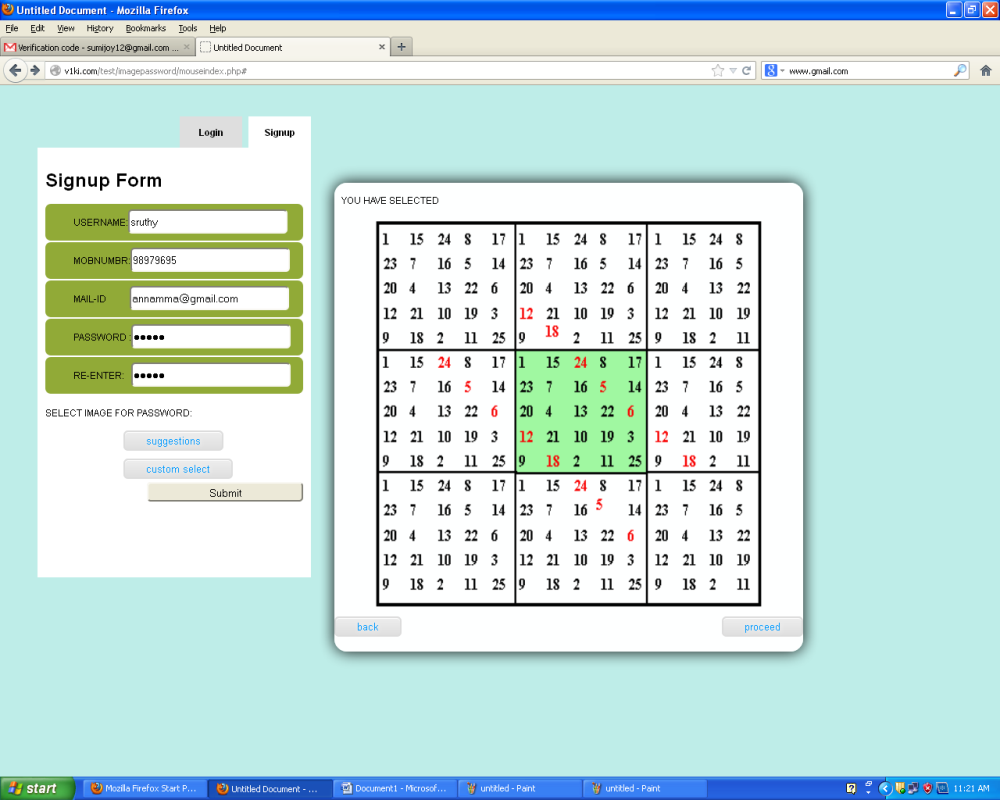


Figure 4.2.3.Signup selected image

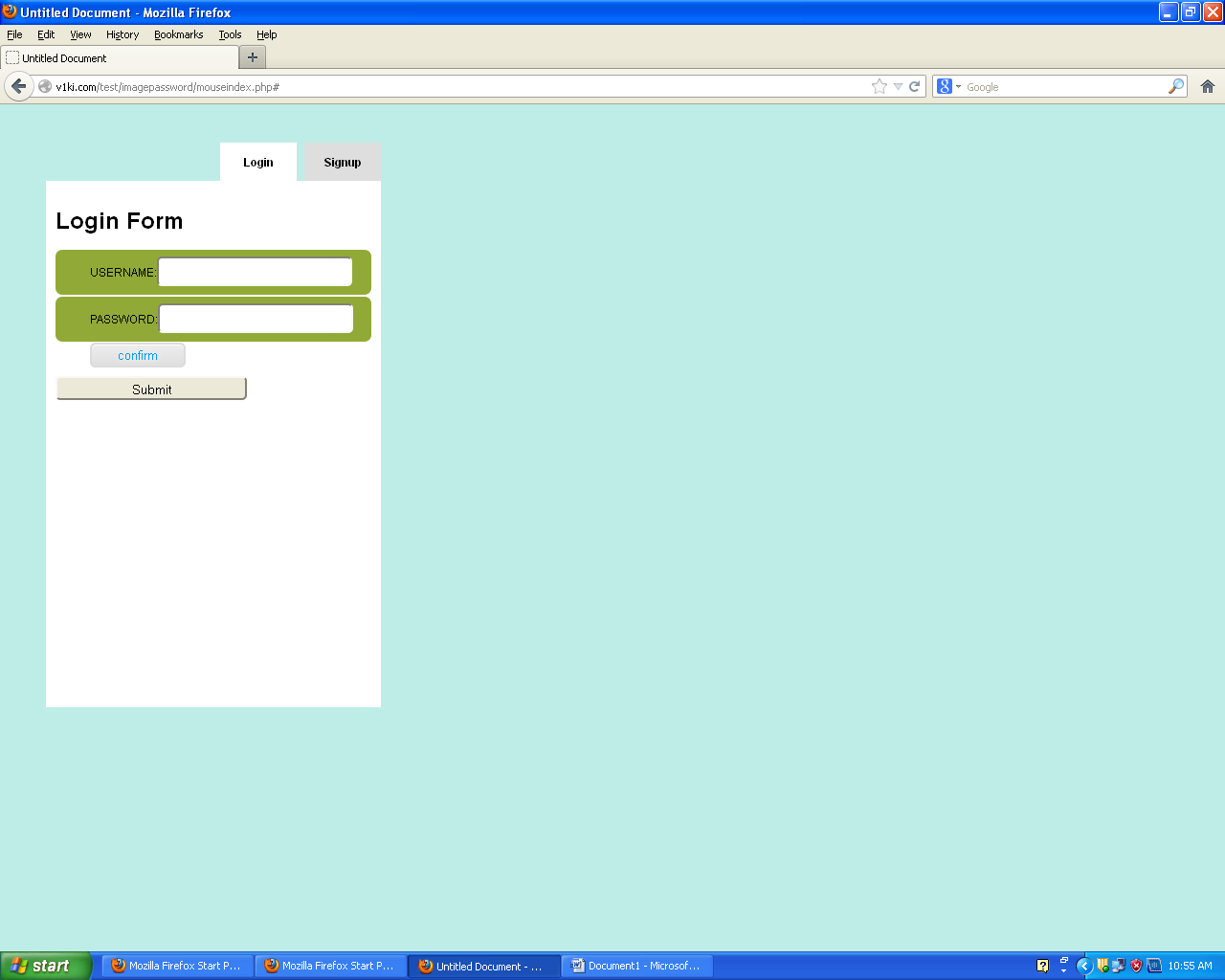


Figure 4.2.4.Login view

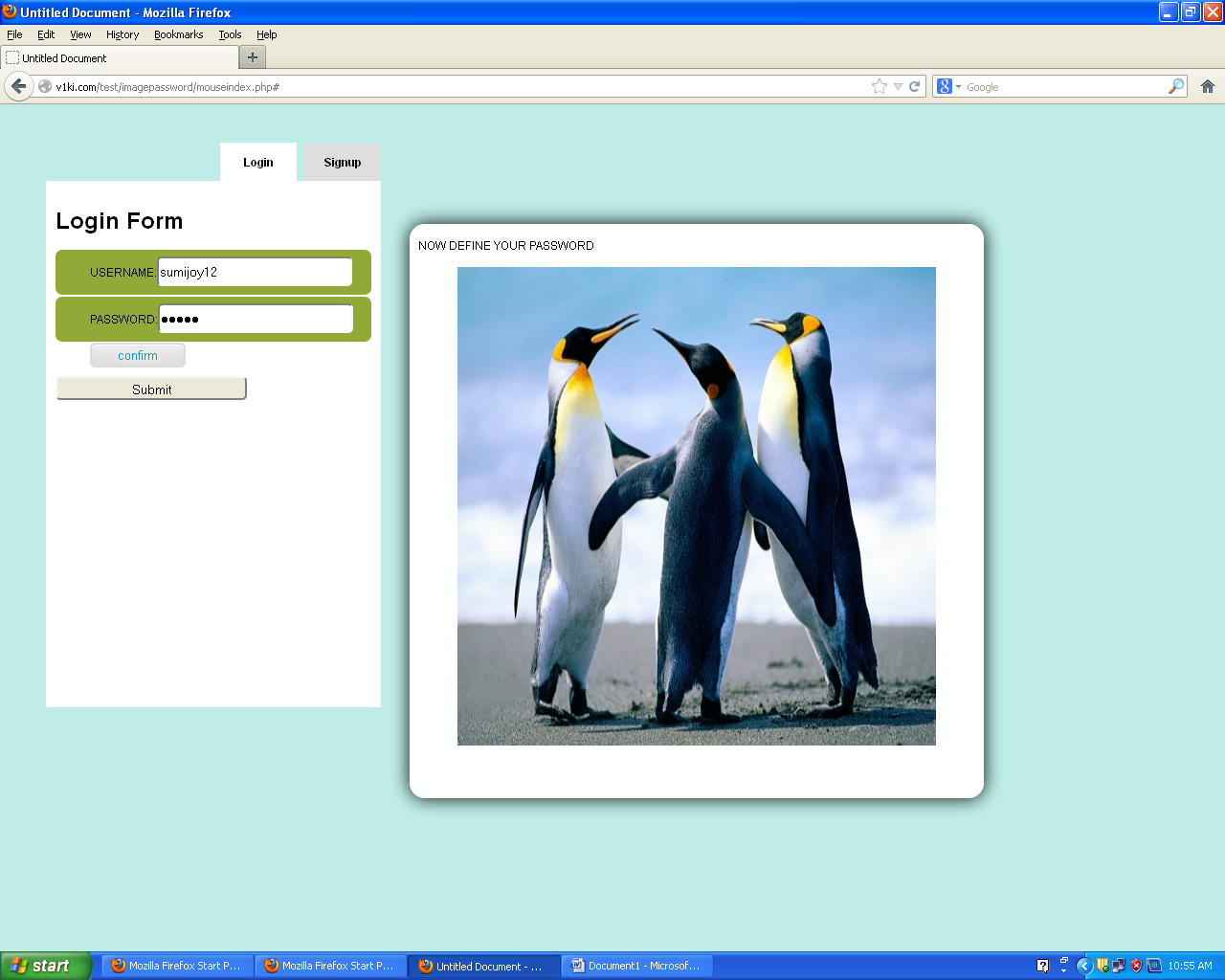


Figure 4.2.5.Login conformed image

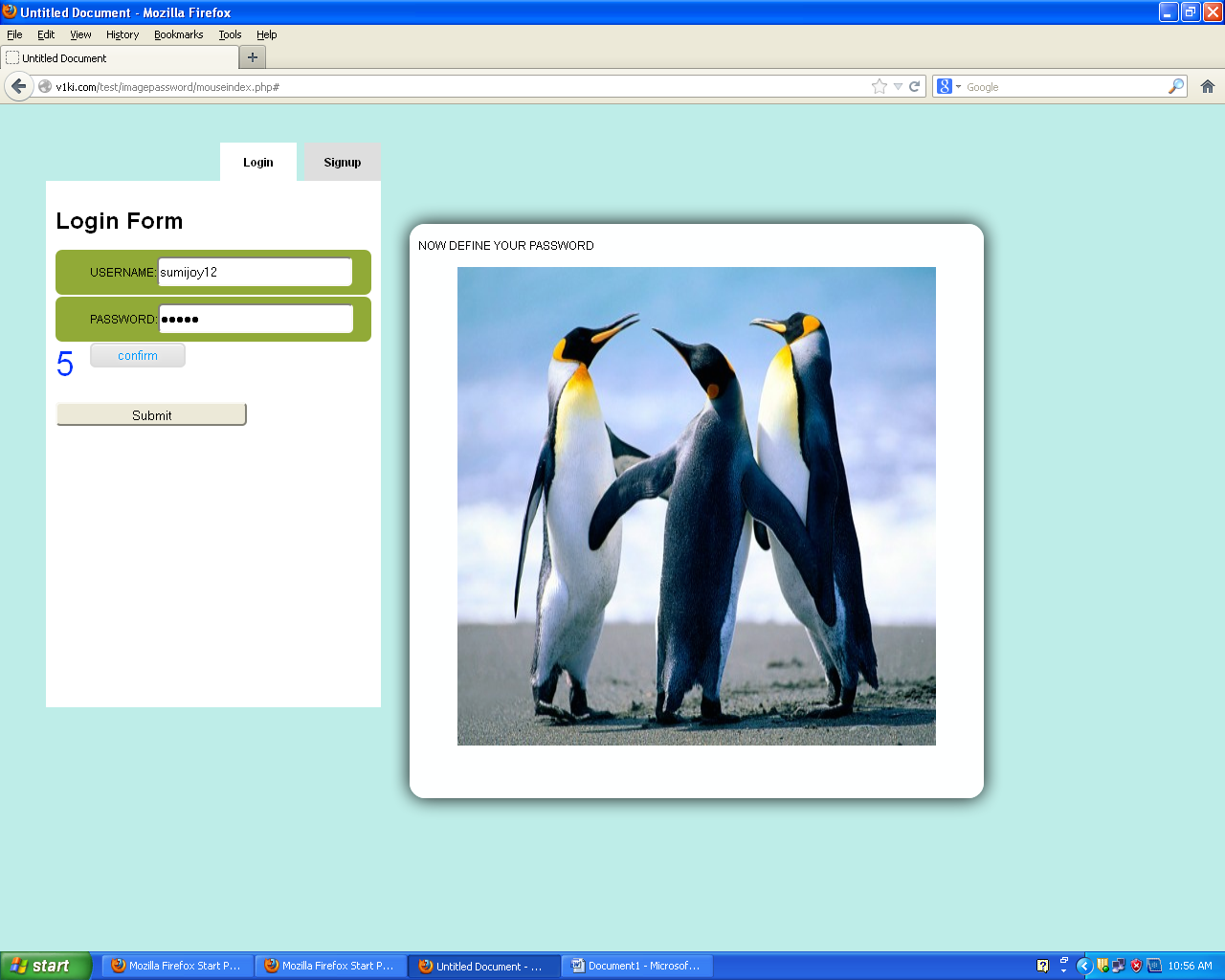


Figure 4.2.6.Defining click points for Login

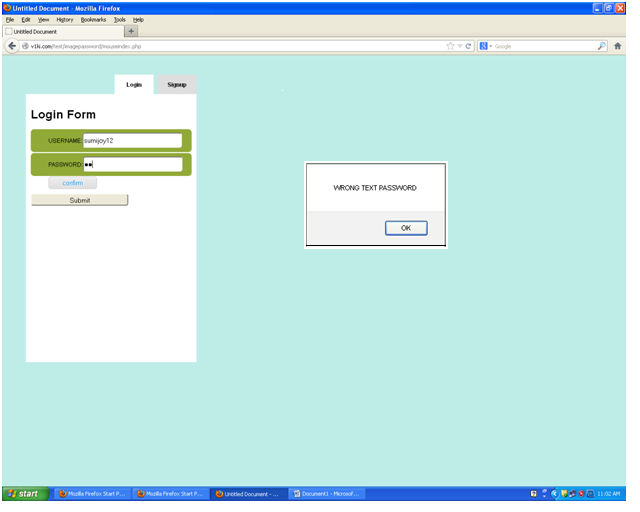


Figure 4.2.7. Login validation

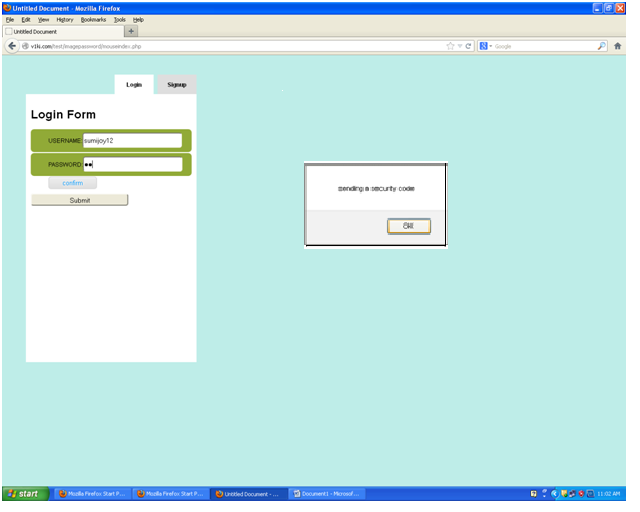


Figure 4.2.8.Security code sending

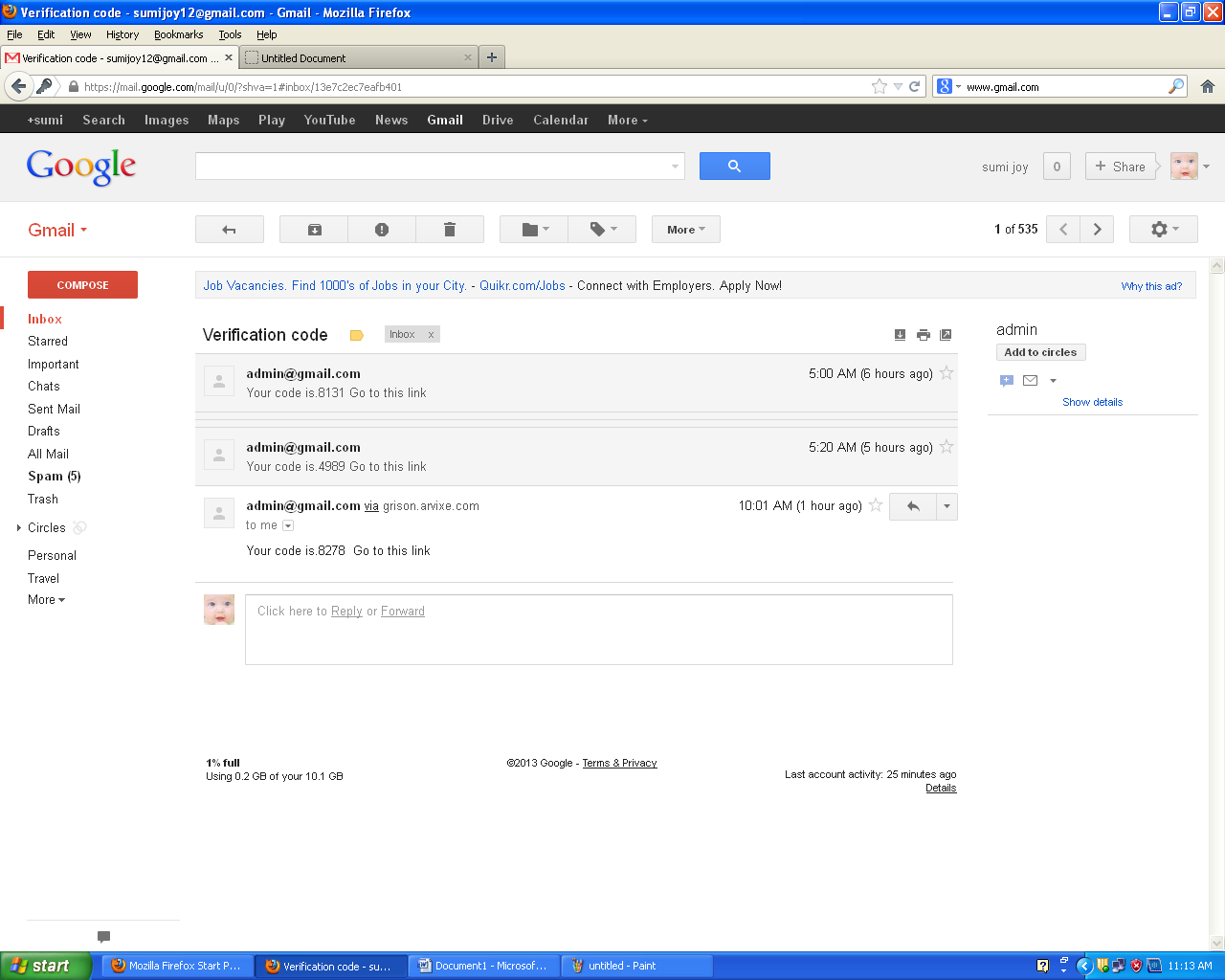


Figure 4.2.9.Verifing security code on user mail account

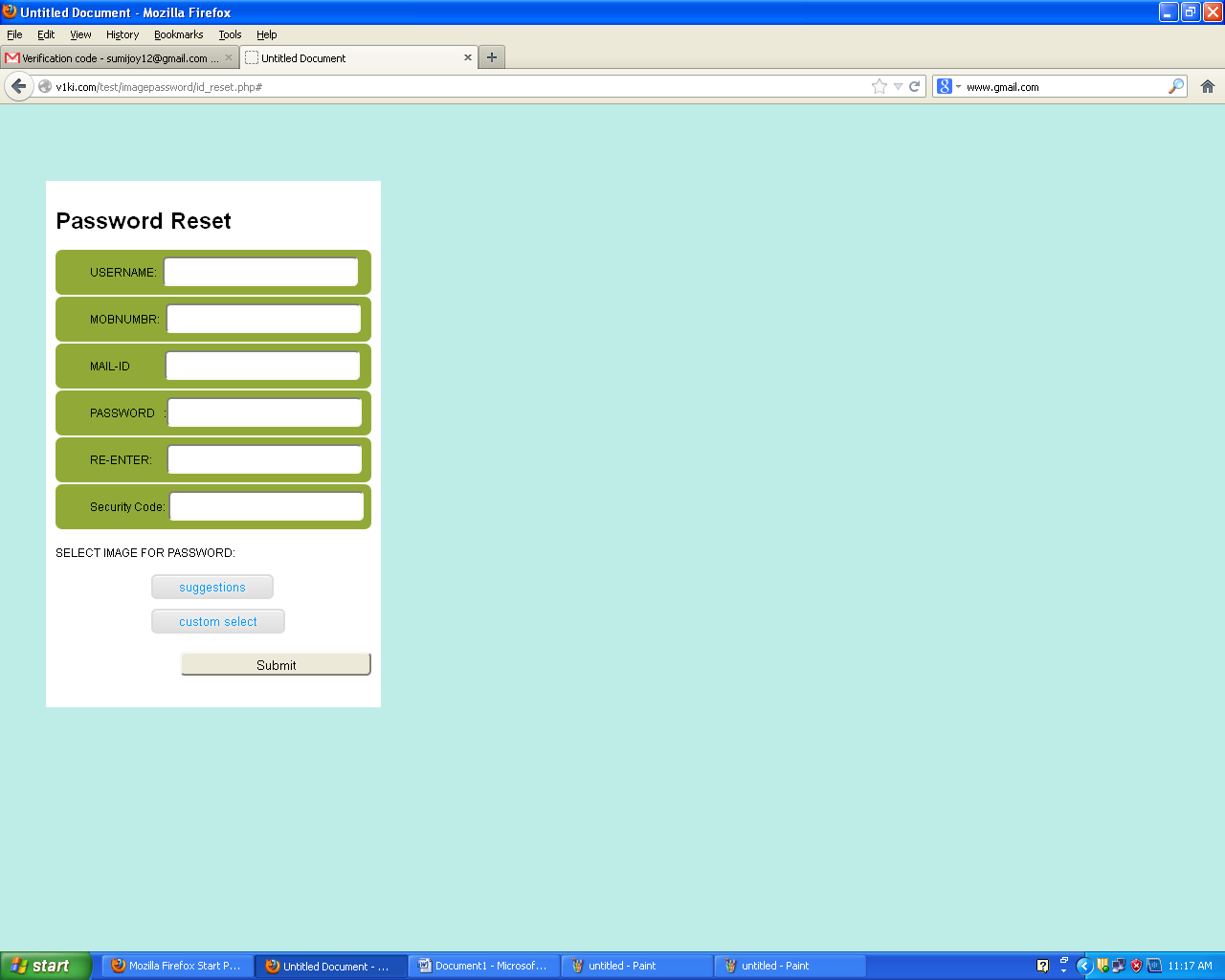


Figure 4.2.10.Password resetting by entering security code

**4.3 SYSTEM TESTING**

System testing of software or hardware is testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. System testing falls within the scope of black box testing, and as such, should require no knowledge of the inner design of the code or logic.

As a rule, system testing takes, as its input, all of the "integrated" software components that have successfully passed integration testing and also the software system itself integrated with any applicable hardware system(s). The purpose of integration testing is to detect any inconsistencies between the software units that are integrated together (called assemblages) or between any of the assemblages and the hardware. System testing is a more limiting type of testing; it seeks to detect defects both within the "inter-assemblages" and also within the system as a whole. Entire system is tested as per the requirements. Black-box type testing that is based on overall requirements specifications, covers all combined parts of a system.

**4.3.1 Software Testing**

Software testing is an important phase in the development of the system. Generally, system testing involves testing integration of each module in the system. The objective while testing the system is to test the discrepancies between the system and the original objective. The quality of an information system depends on its design, development, implementation and design.

Testing is the most important activity in the development phase. Testing is the process of finding errors or bugs in the system. Testing ensure that the user needs are satisfied. In other words it is a process by which one detects the defects in the system.

Software testing methods are traditionally divided into black box testing and white box testing. These two approaches are used to describe the point of view that a test engineer takes when designing test cases.

Black box testing treats the software as a black-box without any understanding of internal behavior. It aims to test the functionality according to the requirements. Thus, the tester inputs data and only sees the output from the test object. This level of testing usually requires thorough test cases to be provided to the tester who then can simply verify that for a given input, the output value (or behavior), is the same as the expected value specified in the test case. Black box testing methods include: equivalence partitioning , boundary value analysis, all-pairs testing, fuzz testing, model-based testing, traceability matrix etc.

White box testing, however, is when the tester has access to the internal data structures, code, and algorithms. White box testing methods include creating tests to satisfy some code coverage criteria. For example, the test designer can create tests to cause all statements in the program to be executed at least once. Other examples of white box testing are mutation testing and fault injection methods. White box testing includes all static testing. This testing is based on knowledge of the internal logic of an application’s code. Also known as Glass box Testing. Internal software and code working should be known for this type of testing. Tests are based on coverage of code statements, branches, paths, conditions.

There are many approaches to software testing. Reviews, walkthroughs or inspections are considered as static testing, whereas actually running the program with a given set of test cases in a given development stage is referred to as dynamic testing.

Software testing is used in association with verification and validation:

* Verification: Have we built the software right
* Validation:Have we built the right software

The different types of testing are:

* Unit Testing
* Integration Testing
* Validation Testing
* System Testing
* Output Testing

**Unit Testing**

In computer programming, unit testing is a procedure used to validate that individual units of source code are working properly. A unit is the smallest testable part of an application. In procedural programming a unit may be an individual program, function, procedure, etc., while in object-oriented programming, the smallest unit is a method, which may belong to a base/super class, abstract class or derived/child class.

Ideally, each test case is independent from the others; mock or fake objects as well as test harnesses can be used to assist testing a module in isolation. Unit testing is typically done by software developers to ensure that the code they have written meets software requirements and behaves as the developer intended.

In this we test each module individually but not integrate the whole system. It focuses verification efforts even in the smallest unit of software design in each module. This is also known as “Module Testing”. The testing is carried out in the programming style itself. In this testing each module is focused to work satisfactorily as regard to the expected output from the module. There are some validation checks for the fields

In this test focus on each modules meandering User Management, Web Services, Mail, SMS, Feedback of the system individually, ensuring that it function properly as an individual unit according to solve the requirement of a particular module. In unit testing control path are tested to uncover errors in the boundary of the module.

.

**Integration Testing**

Integration testing (sometimes called Integration and Testing, abbreviated I&T) is the phase of software testing in which individual software modules are combined and tested as a group. It follows unit testing and precedes system testing.Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing.

Data can be lost across an interface, one module can have adverse effect on the other sub-functions, when combined may not produce the desired functions.

Integration testing is the systematic testing to uncover the errors within the interface. This testing is done with simple data .The need for an integrated system is to find the overall performance.

The purpose of integration testing is to verify functional, performance and reliability requirements placed on major design items. These "design items", i.e. assemblages (or groups of units), are exercised through their interfaces using black box testing, success and error cases being simulated via appropriate parameter and data inputs. Simulated usage of shared data areas and inter-process communication is tested and individual subsystems are exercised through their input interface. Test cases are constructed to test that all components within assemblages interact correctly, for example across procedure calls or process activations, and this is done after testing individual modules, i.e. unit testing.

Here this Integration testing is done by assembling Web Services, Mail, SMS together. This Systematic technique for constructing the program structure while at the same time conducting test to uncover errors to associate with interfacing.

1. **Validation Testing**

At the culmination of black box testing (Here the structure of the program is not considered), software is completely assembled as a package .Interface errors have been uncovered and correct and final series of tests, i.e., and validation test begins. The customer defines validation with a simple definition and validation succeeds When the software functions in manner than can be reasonably accepted.

**Recovery testing**

In this test method we are concerned with the software’s ability to retrieve lost data or to make sure that software does not loose any data during the updating of the database. We will be mainly looking at transaction processing when we talk about the recovering testing. In transaction protection we will be testing the software to make sure that when it saves any thing it will save all of it or none of it. This is necessary to avoid existence of corrupt data in database.

**Security testing**

In this testing section we are concerned about the security of the software. We will be testing the software to see if unauthorized users are able to access sensitive parts of the software. We have divided the security section in three stages

.

* Password Login

We will try to log in using invalid user name or valid user name and invalid password. We will also test the software to see if it allows access without any identification what so ever. We will also test the software so that password is not saved in any way within computer for others to view.

* Modular Access

Our software identifies the user and allows him or her to access only certain modules. We will test to see if the software restricts unauthorized users from accessing certain modules of the software. In particular we want to make sure that user cannot access modules for the administrator.

* Priority Access

Priority access is not of a serious concern since this system is only used by the administrator who has the sole ownership of the system.

**Stress testing**

In this test method we are concerned with the software’s ability to allow concurrent transaction. Too much of the work at the same time may cause system shutdown or frees. We want to test and to make sure that this does not happen. As test procedure we will try to create as much traffic for the software as we can by opening several applications concurrently. We should not have any trouble in achieving our goal in this section of the test since our product is not at the large-scale software products and does not generate too much traffic either.

**White Box Testing**

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are required and used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT).

While white-box testing can be applied at the unit, integration and system levels of the software testing process, it is usually done at the unit level. It can test paths within a unit, paths between units during integration, and between subsystems during a system level test. Though this method of test design can uncover many errors or problems, it might not detect unimplemented parts of the specification or missing requirements.

**White-box test design techniques include :**

* Control flow testing
* Data flow testing
* Branch testing
* Path testing
* Unit test cases

In this method of testing we will test the smallest unit of software called modules. We will be testing all the important paths to find any errors within the boundary of module. So here white box search is applied. We will be testing parts of the software rather than the entire software. The modules are as follows.

**Blackbox Testing**



Figure 4.3.1.Black box testing

Black-box testing is a method of software testing that tests the functionality of an application as opposed to its internal structures or workings (see white-box testing). Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. Test cases are built around specifications and requirements, i.e., what the application is supposed to do. It uses external descriptions of the software, including specifications, requirements, and designs to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid inputs and determines the correct output. There is no knowledge of the test object's internal structure.

This method of test can be applied to all levels of software testing: unit, integration, functional, system and acceptance. It typically comprises most if not all testing at higher levels, but can also dominate unit testing as well.

**Typical black-box test design techniques include :**

* Decision table testing
* All-pairs testing
* State transition tables
* Equivalence partitioning
* Boundary value analysis.

**System Testing :**

When a system is developed it is hoped that it performs properly. In practice however some errors always occur. The main purpose of testing an information system is to find the errors and correct them. A successful test is one which finds an error. The main objectives of the system testing are:

* To ensure during operation the system will perform as per specification.
* To make sure that the system meets user requirements during operation.
* To verify that the controls incorporated in the system function as intended.
* To see that when correct inputs are fed to the system and the outputs are correct.
* To make sure that during operation incorrect input processing and output will be deleted.

Software testing is a critical element of software quality assurance and represents the ultimate review of specification , design and coding . If the testing conducted successfully, it will uncover errors in the software. As a secondary benefit, testing demonstrates that the software functions appear to be working according to specification and that performance requirements appear to have been made.

The scope of the system test should include both manual operations and computer operations system testing is comprehensive evaluation of the programs manual procedures, computer operations and control.

System testing is the process of checking if the developed system is working according to the original objectives and requirements. All the testing needs to be conducted in accordance to the test conditions specified earlier.

**CONCLUSION AND FUTURE WORK**

**5. CONCLUSION**

A major advantage of Persuasive cued click point scheme is its large password space over alphanumeric passwords. There is a growing interest for Graphical passwords since they are better than Text based passwords, although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. Online password guessing attacks on password-only systems have been observed for decades. Present-day attackers targeting such systems are empowered by having control of thousand to million node boot nets. In previous ATT-based login protocols, there exists a security-usability trade-off with respect to the number of free failed login attempts (i.e., with no ATTs) versus user login convenience (e.g., less ATTs and other requirements). In contrast, PGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. PGRP is apparently more effective in preventing password guessing attacks (without answering ATT challenges), it also offers more convenient login experience, e.g., fewer ATT challenges for legitimate users. PGRP appears suitable for organizations of both small and large number of user accounts.

**6. REFERENCES**

[01]Chippy.T and R.Nagendran,“Defenses against large scale onlinePassword guessing attacks by usingPersuasive click points “.

[02] Sonia Chiasson, P.C.vanOorschot, and Robert Biddle,“GraphicalPassword Authentication Using Cued Click Points”.

[03] Manu Kumar, Tal Garfinkel, Dan Boneh andTerry Winograd, “Reducing Shoulder-urfing byUsing Gazebased Password Entry”

[04] Zhi Li, Qibin Sun, Yong Lian, and D. D.Giusto, „An association-based graphicalpassword design resistant to shoulder surfingattack‟.

[05] R. Dhamija and A. Perrig, "Deja Vu: A UserStudy Using Images for Authentication".

[06] S. Akula and V. Devisetty, "Image BasedRegistration and Authentication System".

[07] L. Sobrado and J.-C.Birget, "Graphicalpasswords”.

[08] I. Jermyn, A. Mayer, F. Monrose, M. K.Reiter, and A.D. Rubin, "The Design andAnalysis of Graphical Passwords,"

[ 09] <http://w3schools.com/php/default.asp>

[10] <http://w3schools.com/js/default.asp>

**7. APPENDIX**

|  |  |  |
| --- | --- | --- |
| Sl. No | Content | Pg No. |
|  | **Appendix I : List of Tables** |  |
| 1 | Signup Table | 21 |
| 2 | Blocked Table | 22 |
| 3 | Reset Table | 22 |

**Appendix II : List of Figures**

|  |  |  |
| --- | --- | --- |
| Figure No. | Figure | Pg No. |
| 3.2.1 | 0-Level DFD | 19 |
| 3.2.2 | 1-Level DFD | 20 |
| 4.2.1 | Signup view | 33 |
| 4.2.2 | Signup image selection | 33 |
| 4.2.3 | Signup selected image | 34 |
| 4.2.4 | Login view | 34 |
| 4.2.5 | Login conformed image view | 35 |
| 4.2.6 | Defining click point for login | 35 |
| 4.2.7 | Login validation | 36 |
| 4.2.8 | Security code sending | 36 |
| 4.2.9 | Verifing security code on user mail account | 37 |
| 4.2.10 | Password resetting by entering security code | 37 |
| 4.4.10.1 | Black box testing | 43 |

**Appendix III : Code**

//mouseindex.php.....Login and registration tab.

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>Untitled Document</title>

</head>

<link rel="stylesheet" type="text/css" href="css/style.css"/>

<script type="text/javascript" src="js/scriptsfunctions.js"></script>

<script type="text/javascript" src="http://ajax.googleapis.com/

ajax/libs/jquery/1.5/jquery.min.js"></script>

<script type="application/javascript">

$(document).ready(function()

{

$(".tab").click(function()

{

var X=$(this).attr('id');

if(X=='signup')

{

//document.getElementById('imagesuggestions').style.visibility='hidden';

$("#login").removeClass('select');

$("#signup").addClass('select');

$("#loginbox").slideUp();

$("#signupbox").slideDown();

}

else

{

document.getElementById('imagesuggestions').style.visibility='hidden';

document.getElementById('imageupload').innerHTML='';

$("#signup").removeClass('select');

$("#login").addClass('select');

$("#signupbox").slideUp();

$("#loginbox").slideDown();

}

});

});

</script>

<script type="text/javascript" src="js/jquery.form.js"></script>

<script type="text/javascript">

$(document).ready(function()

{

$('#photoimg').live('change', function()

{

//document.getElementById('imagesuggestions').style.visibility='visible';

$("#preview").html('');

$("#preview").html('wait........');

$("#imageform").ajaxForm(

{

target: '#imageupload'

}).submit();

});

});

</script>

<body onload="ints()" onmousemove="capmouse(event)">

<div style="margin:40px">

<div id="container">

<div id="tabbox">

<a href="#" id="signup" class="tab signup">Signup</a>

<a href="#" id="login" class="tab select">Login</a>

</div>

<div id="panel">

<div class="box" id="loginbox"><h1>Login Form</h1>

<form method="post" action="checklogin.php">

<ul>

<li>

USERNAME:<input type="text" name="lusername" id="lusername"" required/>

<a class="butn" id="confirmbtn" onclick="showpasswordimages()">confirm</a>

</li>

<li id="ltextpassword">

PASSWORD:<input type="text" name="ltextpassword" required/>

</li>

</ul>

<input type="hidden" id="lselectedimagename" name="lselectedimagename">

<input type="hidden" id="limageclicks" name="limageclicks">

<span id="clickcount" value="" class="clickcount"></span>

<br><br><input id="sbmtbtn" type="submit" value="Submit">

</form>

</div>

<div class="box" id="signupbox"><h1>Singup Form</h1>

<form action="signup.php" method="post" id="signup" onsubmit="return validateForm();">

<ul>

<li>USERNAME:<input type="text" name="username" id="username" /></li>

<li>MOBNUMBR:<input type="text" name="mobnum" id="mobnum" /></li>

<li>MAIL-ID&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="text" name="mailid" id="mailid" /></li>

<li>PASSWORD&nbsp;:<input type="password" name="textpassword" id="textpassword" /></li>

<li>RE-ENTER:<input type="password" name="retextpassword" id="retextpassword" /></li>

<input type="hidden" id="selectedimagename" name="selectedimagename">

<input type="hidden" id="imageclicks" name="imageclicks">

<span id="lclickcount" class="clickcount"></span>

</ul>

<br><br><br>SELECT IMAGE FOR PASSWORD:

<div id="imgslct" class="imgslct">

<a class="butn" onclick="showsuuggestion()">suggestions</a>

<a class="butn" onclick="showuploadselection()">custom select</a>

</div>

<div class="floatright">

<input type="submit" value="Submit">

</div>

</form>

</div>

<div id="imageupload" clas="imagesuggestions">

</div>

<div class="imagesuggestions" id="imagesuggestions">

<?php

$imgDir = "images";

//$thumbDir = "/images/";

$images = scandir($imgDir);

//$ignore = array( ".", ".." );

$allowedExts = array("jpg", "jpeg", "gif", "png");

// print\_r($images);

echo '<ul>';

for($i = 0,$j=0; $i< count($images); $i++)

{

$extension = pathinfo($images[$i]);

if(in\_array($extension['extension'], $allowedExts))

{

$j++;

print('<li><a onclick='."selectmouseimage('$images[$i]')".' ><imgsrc="images/'.$images[$i].'" width="150" height="150" alt="suggested" /></a></li>');

if($j%3==0)print('<br>');

}

}

echo '</ul>';

?>

</div>

</body>

</html>

//dbConnect.php

<?php

$mysql\_hostname = "localhost";

$mysql\_user = "root";

$mysql\_password = "";

$mysql\_database = "imagepassword";

$bd = mysql\_connect($mysql\_hostname, $mysql\_user, $mysql\_password)

or die("Oppssome thing went wrong");

mysql\_select\_db($mysql\_database, $bd) or die("Oppssome thing went wrong");

?>

//checklogin.php

<?phperror\_reporting (E\_ALL ^ E\_NOTICE); ?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>Untitled Document</title>

</head>

<script type="text/javascript" src="js/scriptsfunctions.js"></script>

<body>

<?php

include('dbConnect.php');

$lusername = $\_POST['lusername'];

$limagename = $\_POST['lselectedimagename'];

$limageclicks = $\_POST['limageclicks'];

$textpswd = $\_POST['ltextpassword'];

$sql = "SELECT `imagename`, `password`, `blockedto`, `textpassword` FROM `signup` WHERE `username`='$lusername'";

$result = mysql\_query($sql);

$row = mysql\_fetch\_array($result);

$imagename = $row['imagename'];

$password = $row['password'];

$blockedto = $row['blockedto'];

$textpassword = $row['textpassword'];

$date = date('Y-m-d H:i:s');

if(md5($textpswd)!=$textpassword)

{

?>

<script>

alert(md5($textpswd));

alert($textpassword);

alert('WRONG TEXT PASSWORD');

window.location = 'mouseindex.php';

</script>

<?php

}

if($blockedto>$date)

{

?>

<script>

alert('BLOCKED ACCOUNT');

window.location = 'mouseindex.php';

</script>

<?php

}

$passwordarray = explode("@", $password);

$limageclicksarray = explode("@", $limageclicks);

for($i=0;$i<5;$i++)

{

list($passwordx, $passwordy ) = split(',', $passwordarray[$i]);

list($imageclickx, $imageclicky ) = split(',', $limageclicksarray[$i]);

$x=$passwordx-$imageclickx;

$y=$passwordy-$imageclicky;

$x=sqrt($x\*$x);

$y=sqrt($y\*$y);

if($x>50||$y>50)

{?>

<script>

var attempt = getCookie('<?php echo $lusername.'attempt';?>');

if(attempt) {attempt = parseInt(attempt) +1;}else{attempt=1;}

setCookie('<?php echo $lusername.'attempt';?>',attempt,3600\*1000);

if(attempt>5)

{

varlogcheck = getCookie('<?php echo $lusername.'logged';?>');

if(logcheck!='imagepassword')

{

alert('send a security code');

window.location='sendsecuritycode.php?username=<?php echo $lusername; ?>';

}else if(attempt>15)

{

alert('this account has been blocked temporarly');

setCookie('<?php echo $lusername.'attempt';?>','0',3600\*1000);

window.location = "blockaccount.php";

}

}else{

alert('login failed');

window.location="mouseindex.phpx";

}

</script>

<?php }

} ?>

<script>

setCookie('<?php echo $lusername.'logged'; ?>','imagepassword');

window.location = "loginsuccess.php";

</script>

</body>

</html>

//signup.php

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>Untitled Document</title>

</head>

<body>

<?php

include('dbConnect.php');

$username = $\_POST['username'];

$mobnum = $\_POST['mobnum'];

$mailid = $\_POST['mailid'];

$selectedimagename = $\_POST['selectedimagename'];

$imageclicks = $\_POST['imageclicks'];

$textpassword = md5($\_POST['textpassword']);

$sql = "INSERT INTO `signup`( `username`, `mobnum`, `mailid`,`textpassword`, `imagename`, `password`) VALUES ('$username','$mobnum','$mailid','$textpassword','$selectedimagename','$imageclicks' )";

if(mysql\_query($sql))

{?>

<script>

alert("registration was successfull");

window.location="mouseindex.php";

</script>

<?php }

?>

</body>

</html>

// JavaScript Document

varposx;varposy;varimageclicks='';

varclickcount = 0;

functioncapmouse(e){

// captures the mouse position

posx = 0; posy = 0;

if (!e){var e = window.event;}

if (e.pageX || e.pageY){

posx = e.pageX;

posy = e.pageY;

}

else if (e.clientX || e.clientY){

posx = e.clientX;

posy = e.clientY;

}

}

functionshowP(){

//alert('X mouse is: '+posx+' Y mouse is: '+posy);

if(imageclicks=='')

{imageclicks = posx+','+posy;}

else{imageclicks = imageclicks+'@'+posx+','+posy;}

document.getElementById('imageclicks').value=imageclicks;

clickcount++;

document.getElementById('lclickcount').innerHTML=clickcount;

//alert(document.getElementById('imageclicks').value);

}

functionimagefiled()

{

imgname = document.getElementById('fileimage').value;

if(imgname=='')

{alert('select an image to next');}

else{document.getElementById('imagesuggestions').style.visibility = 'visible';}

}

function test()

{

//alert('tset');

}

functiongetselect(m)

{

alert('YOU HAVE SELECTED:::'+m);

}

function map()

{

var m=1;

var map = '<map name="mappassword">';

w=100;

h=100;

for(r=0;r<5;r++)

{

for(c=0;c<5;c++,m++)

{

map+='<area shape="rect" coords="'+(r\*w)+','+(c\*h)+','+((r+1)\*w)+','+((c+1)\*h)+'" onclick="getselect('+m+')" />';

}

}

map+='</map>';

document.getElementById('maping').innerHTML = map;

}

functionselectimage(str)

{

document.getElementById('imagesuggestions').innerHTML = '<div class="ibox"><br>&nbsp;&nbsp;&nbsp;YOU HAVE SELECTED<br><br><div class="img"><imgsrc="images/'+str+'" width="500" height="500" alt="suggested" /></img></div><a class="butn" onclick="showsuuggestion()"/>back</a><div class="floatright"><a class="butn" onclick="mapselected('+"'"+str+"'"+');"/>proceed </a></div>';

}

functionmapselected(str)

{

document.getElementById('imagesuggestions').innerHTML = '<div class="ibox"><br>&nbsp;&nbsp;&nbsp;NOW DEFINE YOUR PASSWORD<br><br><div class="img"><imgsrc="images/'+str+'" width="500" height="500" alt="suggested" usemap="#mappassword"/></img></div><div id="maping" class="maping"></div><div class="floatright"><a class="butn" onclick="test();"/>shuffle </a></div>';

map();

}

functionselectmouseimage(str)

{

document.getElementById('imagesuggestions').innerHTML = '<div class="ibox"><br>&nbsp;&nbsp;&nbsp;YOU HAVE SELECTED<br><br><div class="img"><imgsrc="images/'+str+'" width="500" height="500" alt="suggested" /></img></div><a class="butn" onclick="showsuuggestion()"/>back</a><div class="floatright"><a class="butn" onclick="mouseselected('+"'"+str+"'"+');"/>proceed</a></div>';

}

functionuserselected(str)

{

//alert(str);

document.getElementById('selectedimagename').value = 'uploads/'+str;

document.getElementById('imagesuggestions').innerHTML = '<div class="ibox"><br>&nbsp;&nbsp;&nbsp;NOW DEFINE YOUR PASSWORD<br><br><div class="img"><imgsrc="uploads/'+str+'" width="500" height="500" alt="suggested" onclick="showP()"/></img></div><div id="maping" class="maping"></div><div class="floatright"><a class="butn" onclick="test();"/>shuffle </a></div>';

document.getElementById('imageupload').style.visibility='hidden';

document.getElementById('imagesuggestions').style.visibility='visible';

}

functionmouseselected(str)

{

document.getElementById('selectedimagename').value = 'images/'+str;

document.getElementById('imagesuggestions').innerHTML = '<div class="ibox"><br>&nbsp;&nbsp;&nbsp;NOW DEFINE YOUR PASSWORD<br><br><div class="img"><imgsrc="images/'+str+'" width="500" height="500" alt="suggested" onclick="showP()"/></img></div><div id="maping" class="maping"></div><div class="floatright"><a class="butn" onclick="test();"/>shuffle </a></div>';

}

functionshowpasswordimages()

{

//alert();

var username = document.getElementById('lusername').value;

//alert(username);

varxmlhttp;

if (username=="")

{

document.getElementById("imagesuggestion").innerHTML="no images found for you";

return;

}

if (window.XMLHttpRequest)

{// code for IE7+, Firefox, Chrome, Opera, Safari

xmlhttp=new XMLHttpRequest();

}

else

{// code for IE6, IE5

xmlhttp=new ActiveXObject("Microsoft.XMLHTTP");

}

xmlhttp.onreadystatechange=function()

{

if (xmlhttp.readyState==4 &&xmlhttp.status==200)

{

//alert(xmlhttp.responseText);

//document.getElementById("imagesuggestions").innerHTML=xmlhttp.responseText;

showpasswordimage(xmlhttp.responseText);

}

}

xmlhttp.open("GET","getpasswordimages.php?username="+username,true);

xmlhttp.send();

}

functionshowpasswordimage(imagename)

{

//alert(imagename);

//document.getElementById("imagesuggestion").innerHTML='';

//document.getElementById('passwordsuggestedlist').innerHTML='<?php echo passwordsuggesteds($'+imagename+'); ?>';

document.getElementById('lselectedimagename').value = imagename;

document.getElementById('imagesuggestions').innerHTML = '<div class="ibox"><br>&nbsp;&nbsp;&nbsp;NOW DEFINE YOUR PASSWORD<br><br><div class="img"><imgsrc="'+imagename+'" width="500" height="500" alt="suggested" onclick="getP()"/></img></div>';

document.getElementById("imagesuggestions").style.visibility='visible';

}

functiongetP(){

//alert('X mouse is: '+posx+' Y mouse is: '+posy);

clickcount++;

if(imageclicks=='')

{imageclicks = posx+','+posy;}

else{imageclicks = imageclicks+'@'+posx+','+posy;}

document.getElementById('limageclicks').value=imageclicks;

document.getElementById('clickcount').innerHTML=clickcount;

}

functionshowsuuggestion()

{

document.getElementById('imageupload').innerHTML='';

if((document.getElementById('imagesuggestions').style.visibility)=='hidden')

{document.getElementById('imagesuggestions').style.visibility = 'visible';}

else{document.getElementById('imagesuggestions').style.visibility = 'visible';}

}

functionvalidateForm()

{

var username=document.forms["signup"]["username"].value;

varmobnum=document.forms["signup"]["mobnum"].value;

varmailid=document.forms["signup"]["mailid"].value;

var selectedimage=document.forms["signup"]["selectedimagename"].value;

varimageclicks=document.getElementById('lclickcount').innerHTML;

//alert(limageclicks);

varatpos=mailid.indexOf("@");

vardotpos=mailid.lastIndexOf(".");

if(username=='')

{alert("username not enterd");return false;}

else if (atpos<1 || dotpos<atpos+2 || dotpos+2>=x.length)

{

alert("Not a valid e-mail address");

return false;

}

else if(isNaN(mobnum))

{

alert("Enter the valid Mobile Number(Like : 999999999)");

return false;

}

else if(imageclicks!='5')

{

alert('image password not defined properly');

return false;

}

}

functionshowuploadselection()

{

document.getElementById('imageupload').innerHTML = '<div class="floatleft"><form id="imageform" method="post" enctype="multipart/form-data" action="uploadimage.php">Upload image <input type="file" name="photoimg" id="photoimg" /></form><div id="preview"></div></div>';

document.getElementById('imagesuggestions').style.visibility='hidden';

}

//mapimage.php

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>Untitled Document</title>

<script type="text/javascript" src="js/scriptsfunctions.js"></script>

</head>

<body onload="map();">

<body onmousemove="capmouse(event)">

<imgsrc="images/sample.gif" width="300" height="300" onclick="showP()">

<imgsrc="images/sample.gif" width="300" height="300" usemap="#mappassword">

<div id="maping" class="maping"></div>

</body>

</html></html>