MIT | Academy of Engineering

School of Computer Engineering and Technology

Presentation for SY Minor Project Implementation Phase(Review 1)

Academic Year 2022-23

Graphical password representation

Students Name:

AYUSH KOUL (01)

VIRAJ RAINA (10)

AMEY SATONE (60)

DHEERAJ SINGH (84)

Guide:

Mrs NEHA HAJARE

Index

- **Introduction**
- **Problem Statement and Objectives**
- **Literature Review/Survey**
- **Proposed Block Diagram /design structure**
- **Methodology / Module-I(Project Work)**
- **Screenshot of Module -I**
- **Application**
- **Future work and Conclusion**
- **References**

Introduction

- User Authentication permits an individual to access network assets.
- Commonly textual passwords are the most used form.
- Textual passwords include special characters and numbers.
- Users may use only one password for multiple accounts.
- Textual passwords are considered strong enough to resist brute force attacks when we use passwords, comprising numbers, uppercase, and lowercase letters.
- **BUT** strong textual password are hard to remember.
- So user picks password that is short and is not strong enough, instead of irregular alphanumeric strings , which can be hacked easily.

continued

- Human actions such as selecting bad passwords for new accounts and inputting wrong passwords in an insecure way for later logins are regarded as the weakest link in the chain of authentication.
- Shouldersurfing occurs when someone watches over your shoulder to collect valuable or personal information such as your password, ATM PIN, or credit card number, as you key it into an electronic device.
- A strong textual password is hard to memorize and recollects. To avoiding such problems, we are presenting a secure graphical web-based authentication system that protects users from becoming victims of shoulder surfing attacks.
- Other than this, the password will be free from brute attacks and dictionary attacks.
- AICTE Hackathon statement 2022.

TEXTUAL REPRESENTATION

4 _ S @ t * 0 7 $ 1 A

DO YOU REMEMBER?

GRAPHICAL REPRESENTATION

DO YOU REMEMBER?

Problem statement

- GRAPHICAL PASSWORD AUTHENTICATION FOR WEB SERVICES.

Objectives to be achieved

1. **Graphical Passwords will be easy to remember.**
2. **Graphical Passwords are hard to crack by hackers.**
3. **Dictionary and Brute force attacks will not work against this system.**
4. **Vulnerabilities are less.**
5. **Shouldersurfing will be prevented.**

Lit Survey

- **Wantong Zheng** and **Chunfu Jia** proposed a method , called as **Combined PWD**. This scheme proposes an online secret phrase verification component, combined PWD, through embedding separators(e.g., spaces) into the passwords to make the password reached to hacker difficult but user himself find difficult to remember it.

- **Yang Jing boo** came up with the **one-time password** authentication schemes, which further can be divided into two types namely weak- password authentication schemes and strong-password authentication schemes he himself came-up with shortcoming in his own protocol and found that strong passwords have higher strength and easily guessing is not possible but are difficult for the user himself to remember it each time he/she need to login.

Lit Survey

- Graphical-based password methods such as recognition and recall-based have been proposed as an alternative to conventional password techniques. The main reason behind this is because graphic pictures are more easily recalled than text. This ease with which graphics are easily recalled has been widely referred to as “**Picture superiority effect**” by most of **researchers** around 2004. From 1994 to now, many of the attempt has been made in graphical authentication password.

Recognition-Based Technique

- **Pass-doodle:** This is a graphical password which is made up of handwritten designs or text that is normally drawn with a stylus onto a touch sensitive screen. According Jermyn et al. (1999) cracking the doodles is harder because they have a theoretically much larger number of possible doodle passwords than text passwords. Usability wise the Pass-doodle is not widely used because it has problems with recognition.

Lit Survey

Pure Recall-Based Technique

- **Draw A Secret (DAS):** This technique, presented in 1999, allowed the user to draw a simple picture onto a 2D grid as shown in Figure 2. The interface consisted of a rectangular grid of size G * G. Each cell in this grid was denoted by discrete rectangular coordinates (x, y).In this method the stroke is considered to be a sequence of cells on the grid which does not contain a pen up event. Thus the password is defined as a sequence of strokes, separated by pen up events. In order to be authenticated, the user is supposed to re-draw the picture by creating the stroke in the exact sequence that was used in the registration phase. In the event that the drawing touches the same grids as well as in the same sequence, then the user is successfully authenticated (Jermyn et al., 1999)

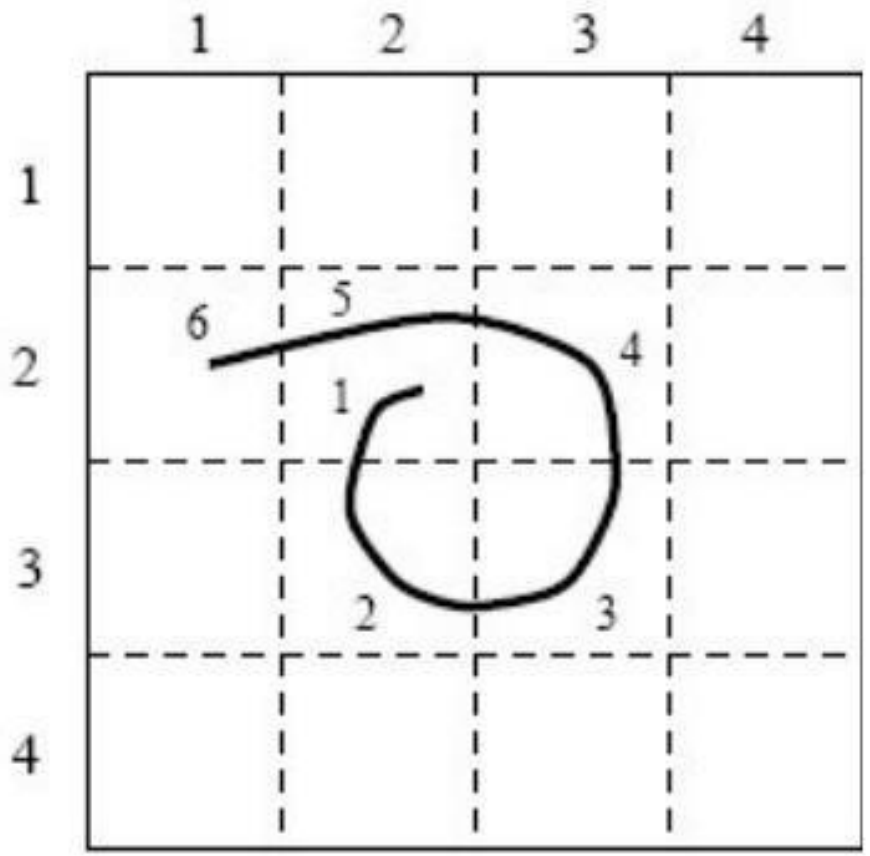


Figure 2. Draw a Secret (DAS) method on a 4*4 Grid.

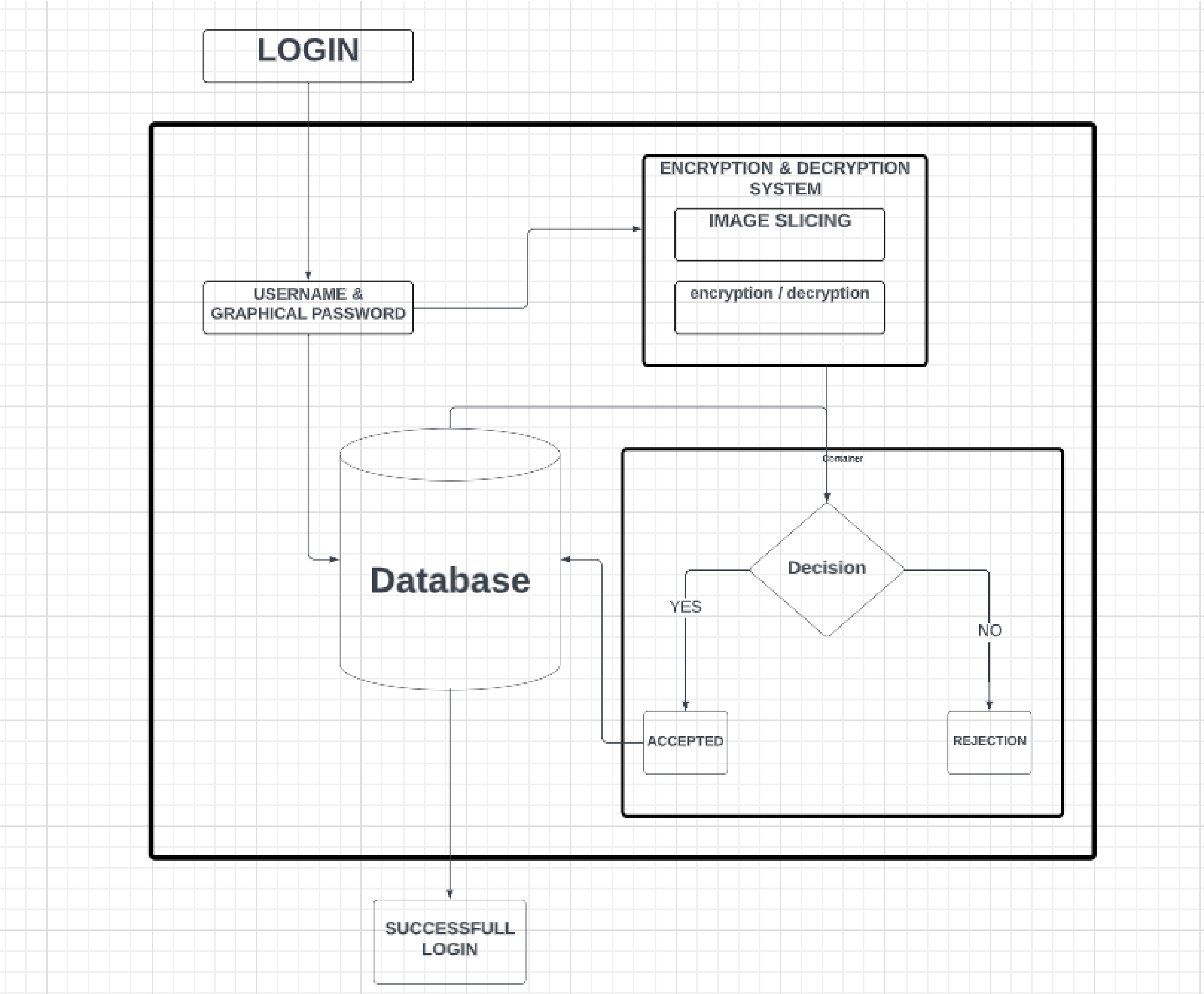
Lit Survey

- **Captcha:**- Manuel Blum in 2003 along with team of researcher invented it. It is also a type of graphical authentication of password. mainly two types textual and graphical ,but it has short-coming that it is easy recognized even by the bot and cracked by hacker.

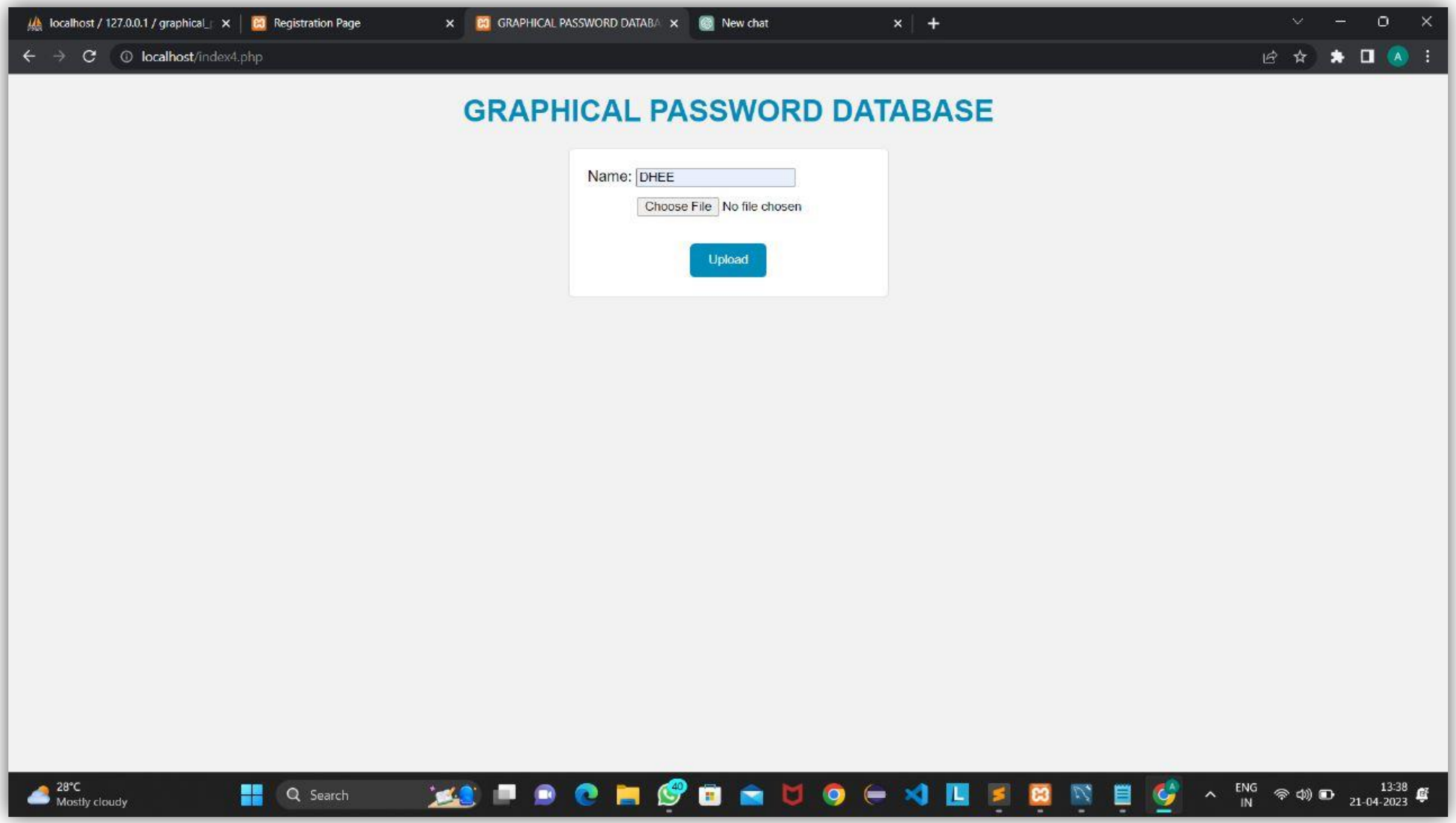
- **Two Step verification :-**Then researcher came with up use of a picture password for the second authentication. So, no need for complex textual passwords. Users can use any basic textual password at first and then secondly with graph authentication but it was observer that it time consuming and not much safer process.

- Then finally we came up with idea which is safer, easier and effective to remember and also time saving , making the password authentication process **text-less** and **completely graphical**.

Block diagram



Methodology /Module-I

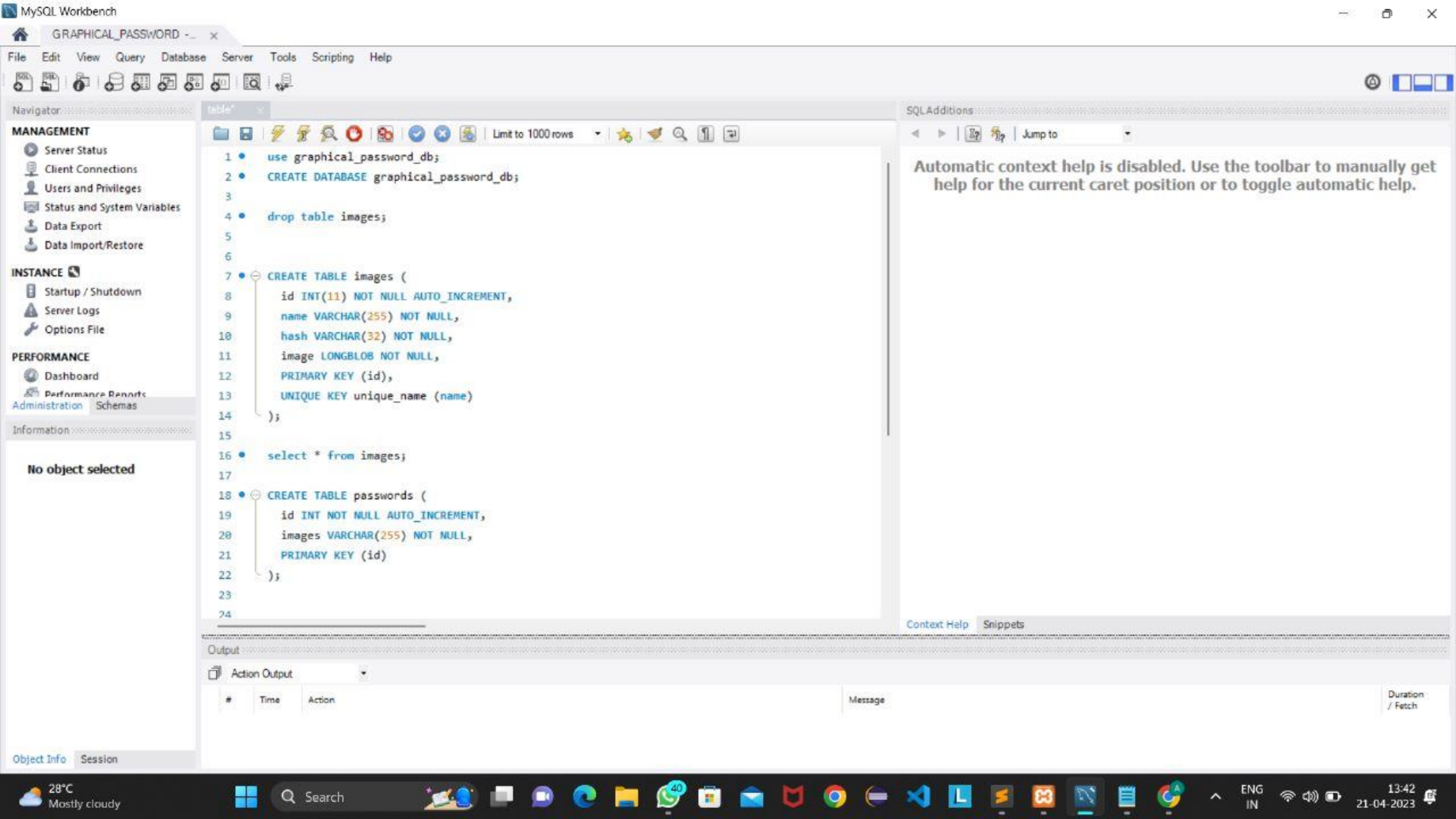


GRAPHICAL PASSWORD DATABASE

Name: DHEE

Choose File No file chosen

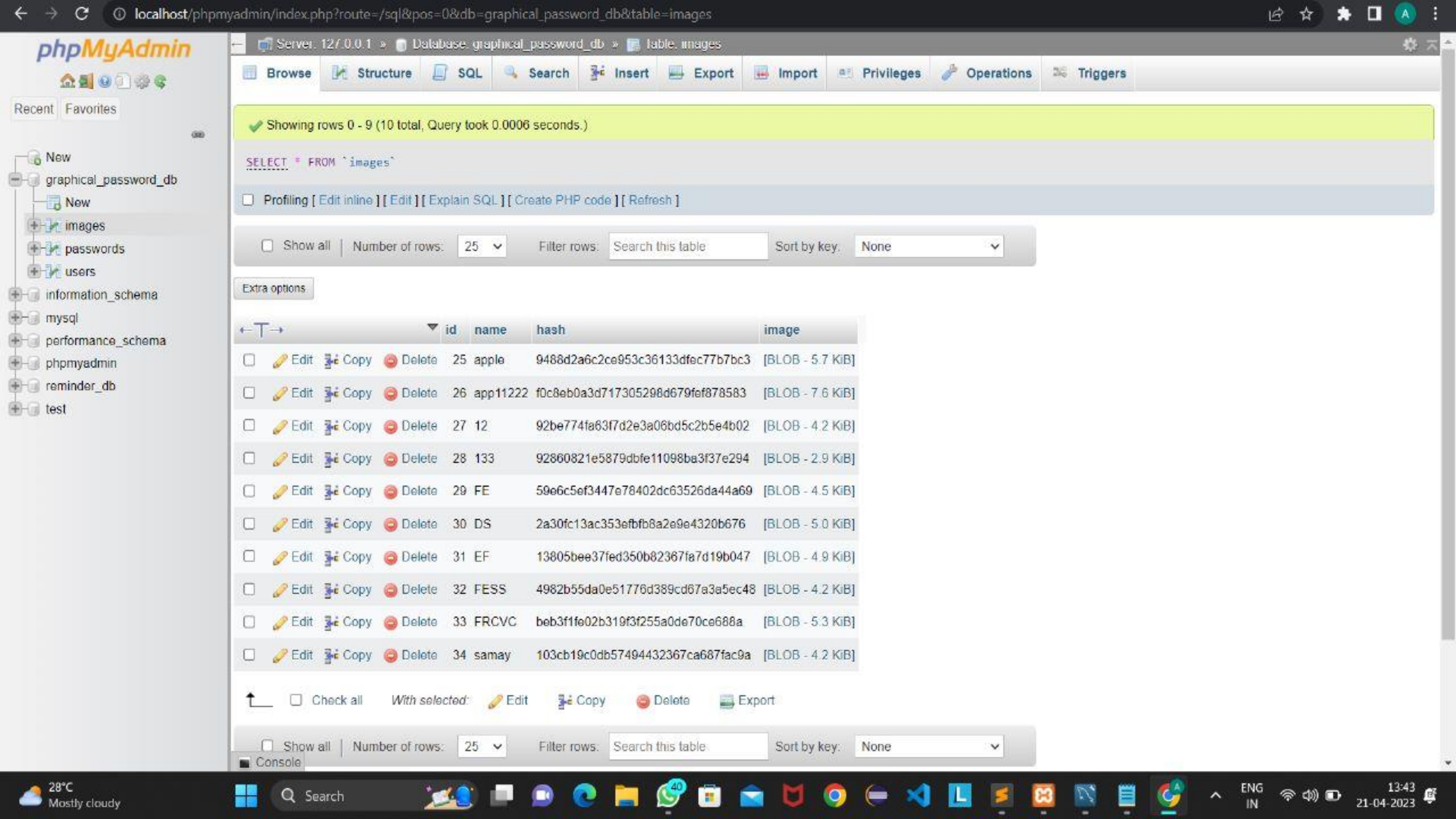
Upload



```sql
use graphical_password_db;
CREATE DATABASE graphical_password_db;

drop table images;


CREATE TABLE images (
  id INT(11) NOT NULL AUTO_INCREMENT,
  name VARCHAR(255) NOT NULL,
  hash VARCHAR(32) NOT NULL,
  image LONGBLOB NOT NULL,
  PRIMARY KEY (id),
  UNIQUE KEY unique_name (name)
);

select * from images;

CREATE TABLE passwords (
  id INT NOT NULL AUTO_INCREMENT,
  images VARCHAR(255) NOT NULL,
  PRIMARY KEY (id)
);

```

Automatic context help is disabled. Use the toolbar to manually get help for the current caret position or to toggle automatic help.

No object selected

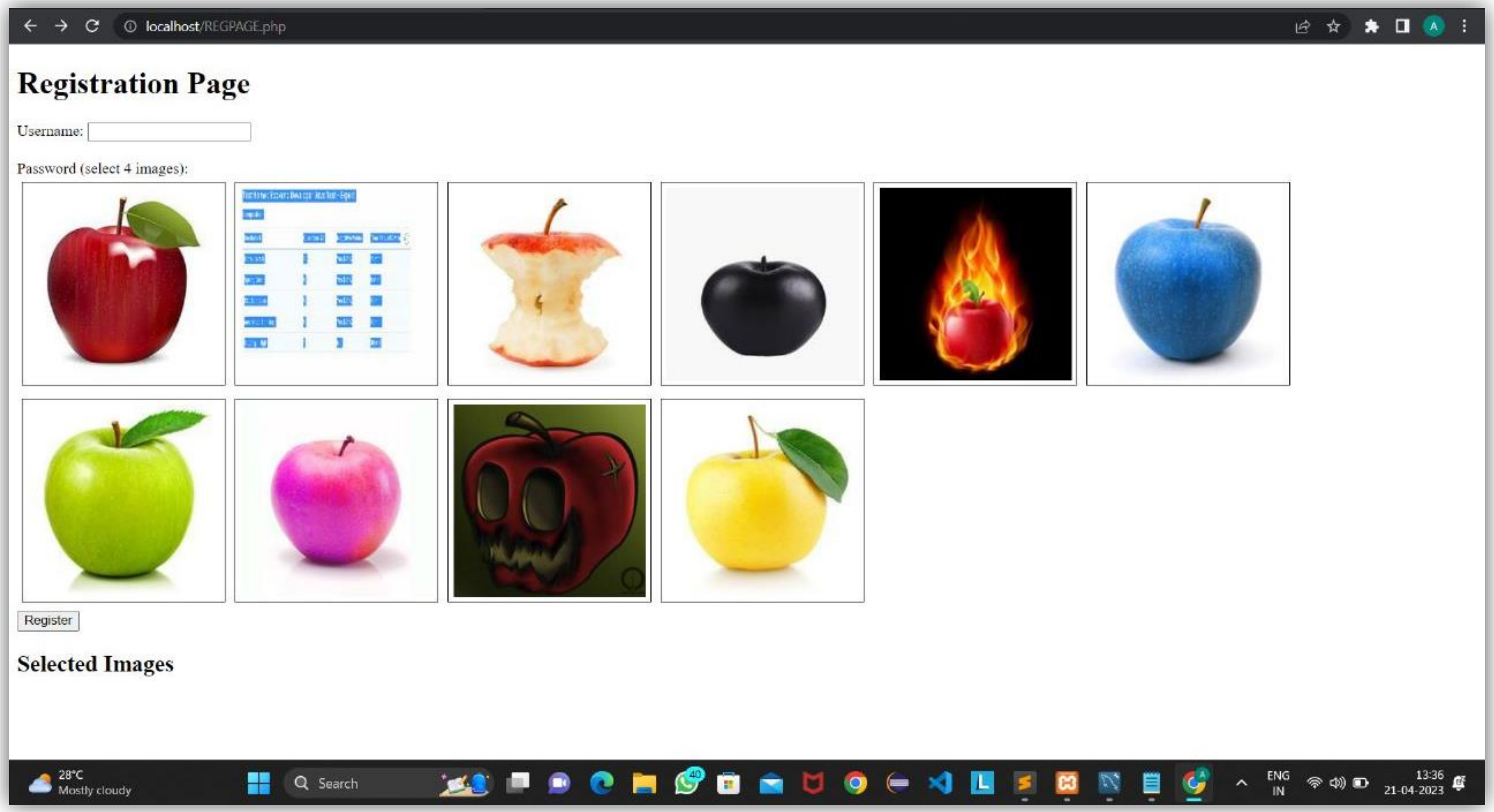


Showing rows 0 - 9 (10 total, Query took 0.0006 seconds.)

```
SELECT * FROM `images`
```

		id	name	hash	image
□	Edit Copy Delete	25	apple	9488d2a6c2ce953c36133dfec77b7bc3	[BLOB - 5.7 KiB]
□	Edit Copy Delete	26	app11222	f0c8eb0a3d717305298d679fef878583	[BLOB - 7.6 KiB]
□	Edit Copy Delete	27	12	92be774fa63f7d2e3a06bd5c2b5e4b02	[BLOB - 4.2 KiB]
□	Edit Copy Delete	28	133	92860821e5879dbfe11098ba3f37e294	[BLOB - 2.9 KiB]
□	Edit Copy Delete	29	FE	59e6c5ef3447e78402dc63526da44a69	[BLOB - 4.5 KiB]
□	Edit Copy Delete	30	DS	2a30fc13ac353efbfb8a2e9e4320b676	[BLOB - 5.0 KiB]
□	Edit Copy Delete	31	EF	13805bee37fed350b82367fa7d19b047	[BLOB - 4.9 KiB]
□	Edit Copy Delete	32	FESS	4982b55da0e51776d389cd67a3a5ec48	[BLOB - 4.2 KiB]
□	Edit Copy Delete	33	FRCVC	beb3f1fe02b319f3f255a0de70ce688a	[BLOB - 5.3 KiB]
□	Edit Copy Delete	34	samay	103cb19c0db57494432367ca687fac9a	[BLOB - 4.2 KiB]

Screenshot of Module _I



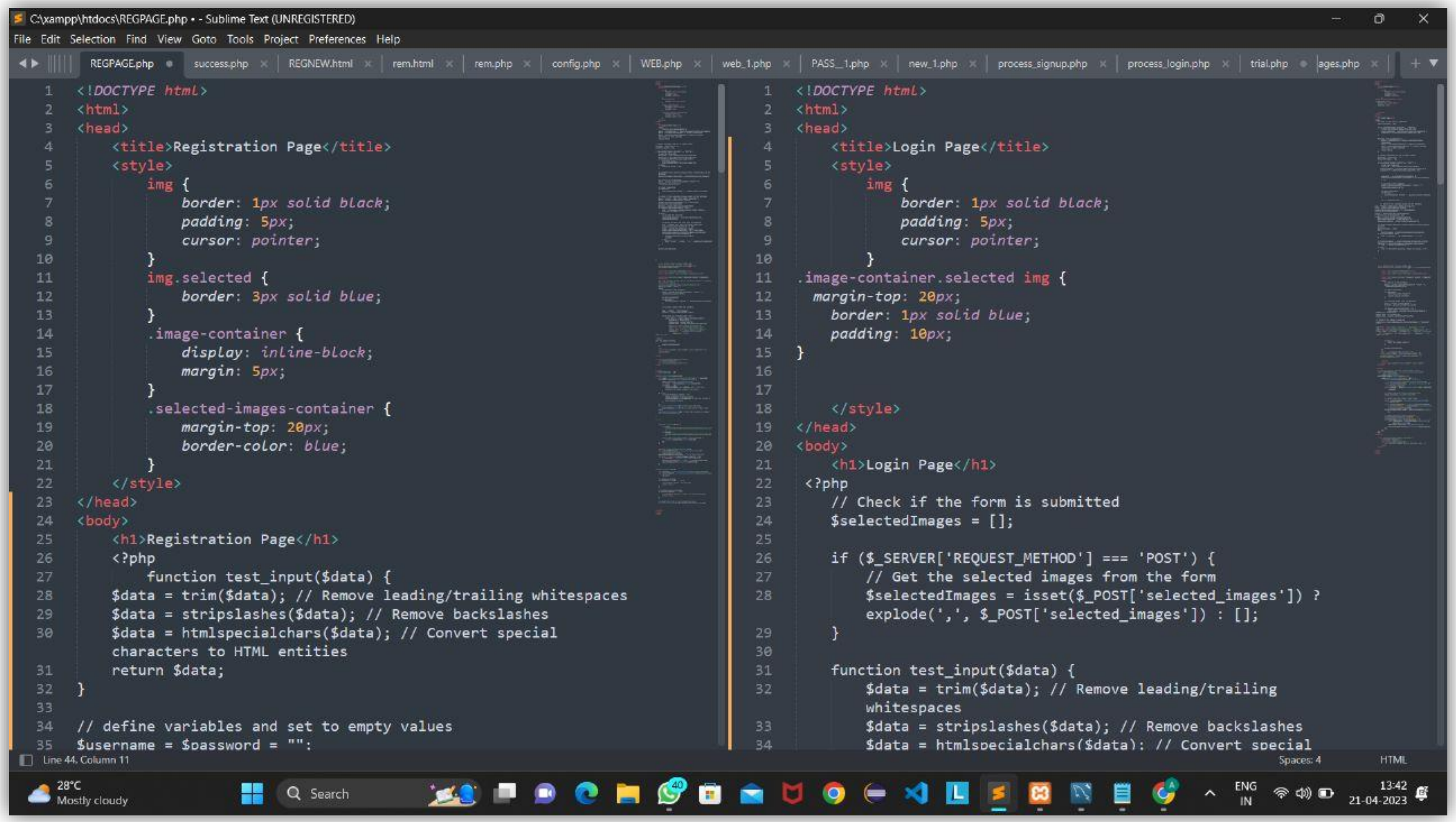
Registration Page

Username:

Password (select 4 images):

Selected Images

Code



```
<!DOCTYPE html>
<html>
<head>
    <title>Registration Page</title>
    <style>
        img {
            border: 1px solid black;
            padding: 5px;
            cursor: pointer;
        }
        img.selected {
            border: 3px solid blue;
        }
        .image-container {
            display: inline-block;
            margin: 5px;
        }
        .selected-images-container {
            margin-top: 20px;
            border-color: blue;
        }
    </style>
</head>
<body>
    <h1>Registration Page</h1>
    <?php
        function test_input($data) {
    $data = trim($data); // Remove leading/trailing whitespaces
    $data = stripslashes($data); // Remove backslashes
    $data = htmlspecialchars($data); // Convert special
    characters to HTML entities
    return $data;
}

// define variables and set to empty values
$username = $password = "";
```

```
<!DOCTYPE html>
<html>
<head>
    <title>Login Page</title>
    <style>
        img {
            border: 1px solid black;
            padding: 5px;
            cursor: pointer;
        }
.image-container.selected img {
  margin-top: 20px;
    border: 1px solid blue;
    padding: 10px;
}


    </style>
</head>
<body>
    <h1>Login Page</h1>
 <?php
    // Check if the form is submitted
    $selectedImages = [];

    if ($_SERVER['REQUEST_METHOD'] === 'POST') {
        // Get the selected images from the form
        $selectedImages = isset($_POST['selected_images']) ?
        explode(',', $_POST['selected_images']) : [];
    }

    function test_input($data) {
        $data = trim($data); // Remove leading/trailing
        whitespaces
        $data = stripslashes($data); // Remove backslashes
        $data = htmlspecialchars($data); // Convert special
```

Applications

- Web applications: Graphical password authentication can be used to secure online accounts and web applications, providing an alternative to text-based passwords.
- Mobile devices: Graphical password authentication can be used to secure smartphones, tablets, and other mobile devices, providing an alternative to text-based passcodes or fingerprints.
- Computer systems: Graphical password authentication can be used to secure computer systems and networks, providing an alternative to text-based passwords or biometrics.
- Banking and financial services: Graphical password authentication can be used to secure online banking and financial services, providing an additional layer of security for sensitive transactions.
- Government and military: Graphical password authentication can be used to secure sensitive government and military systems, providing an additional layer of security for classified information.

Conclusion

- Everyone wants safer, easier and effective way to remember a password.

- Each of the above mentioned need will be fulfilled if and only if the password is textless.

- So , as a solution to this we came up an idea of **GRAPHICAL AUTHENTICATION.**

Selected References

1. Wantong zheng, Chunfu Jia, CombinedPWD: A New Password Authentication Mechanism Using SeparatorsBetween Keystrokes: 2017 13th International Conference on Computational Intelligence and Security (CIS)
1. Salisu Ibrahim Yusuf, Moussa Mahamat Boukar, User Define Time Based Change Pattern Dynamic Password AuthenticationScheme, 2018 14th InternationalConference on Electronics Computer
1. Yang Jingbo, Shen Pingping, A secure strong password authentiction protocol, 2010 2nd International Conference on Software Technology and Engineering
1. Hua Wang, Yao Guo, Xiangqun Chen, DPAC: A Reuse-Oriented Password Authentication Framework for Improving Password Security, 2008 11th IEEE High Assurance Systems Engineering Symposium
1. Salah Refish, PAC-RMPN: Password Authentication Code Based RMPN, 2018 International Conference on AdvancedScience and Engineering (ICOASE)
1. M Hamza Zaki, Adil Husain, M Sarosh Secure pattern-key based password authentication scheme2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT)
1. Vasundhara R Pagar, Rohini G Pise, Strengthening password security through honeyword and Honey encryptiontechnique, 2017 International Conference on Trends in Electronics and Informatics (ICEI)
1. S. Sood, A. Sarje, and K. Singh, Cryptanalysis of password authentication schemes: Current status and key issues, in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 17..
9. S. Gurav, L. Gawade, P. Rane, and N. Khochare, Graphical password authentication: Cloud securing scheme, in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014International Conference on, Jan 2014, pp. 479483
10. A. Bianchi, I. Oakley, and D.S. Kwon, The secure haptic keypad: A tactile password system, in Proceedings of the SIGCHI Conference on Human Factors in Computing System. CHI 10. New York, NY, USA: ACM, 2010, 10891092.
11. E. von Zezschwitz, A. De Luca, and H. Hussmann, Honey, shrunk the keys: Influences of mobile devices on password composition and authentication performance, in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI 14. New York, NY, USA: ACM, 2014, pp. 461470.

Thank You!!

Any questions.