

KLE Society's
KLE Technological University



Information Security Course Project Report
On

Web Security Using SSL, OTP And CAPTCHA

Submitted By

TEAM NUMBER - 09

SHREEYA GOGGI	01FE19BCS045
RASHMI KIRAGI	01FE19BCS057
RENUKA TALWAR	01FE19BCS068
SAHANA BHASME	01FE19BCS072

School of Computer Science and Engineering

,
Vidyangar, Hubballi – 580031, India.

Academic year 2022-2023

ABSTRACT

Today, digitalization decisively penetrates all the sides of modern society. When we refer to the Web applications and portals then the security is at a higher stake since there is an increase in transactions and sharing of information through web portals and applications. Hence data security is of utmost importance, to prevent infiltration and illegal access to data by hackers. The statistics also reveal that 15 million people across the United States become a victim of Identity Theft, online. There is a collective loss of \$50 billion. 100 million Americans faced problems due to these online data thefts or Identity Thefts. This project discusses web security using CAPTCHA and OTP for user authentication and also web security through the implementation of SSL.

Contents

ABSTRACT.....	2
1. INTRODUCTION	4
PROBLEM STATEMENT	4
OBJECTIVES	4
2. LITERATURE SURVEY	5
3. PROPOSED WORK	6
4. RESULTS AND DISCUSSION	7
TOOLS USED	7
5. CONCLUSION.....	10
6. REFERENCES.....	11

1. INTRODUCTION

In the post-password world, strong web security relies on a dynamic approach built from a variety of tools and policies. It's important to never rely on any single method for comprehensive protection. That means two things firstly if you're currently relying on passwords alone, it's time to evolve, and using two factor authentication is a solid first step and secondly two factor authentication is an essential security tool, but it becomes even more effective when it's used as part of a coordinated strategy of security applications and policies

And more important thing in information security SSL which keeps internet connections secure and prevents criminals from reading or modifying information transferred between two systems. When you see a padlock icon next to the URL in the address bar, that means SSL protects the website you are visiting.

PROBLEM STATEMENT

To Integrate OTP, CAPTCHA and SSL in web application to authenticate the user and secure the data exchange between server and user.

OBJECTIVES

- To design web portal to capture user registration details.
- To authenticate user through OTP and CAPTCHA to login.
- To implement SSL to secure the data exchange between user and server.

2. LITERATURE SURVEY

In [1], the authors present identity verification using the “Bundled CAPTCHA OTP” instead of using the traditional password. The Bundled CAPTCHA OTP which is the unique random parameter for any login will be used instead of a traditional password. We use an e-mail as the way to receive client-side the Bundled CAPTCHA OTP because it is easier to apply without any problems compare to using mobile phones. The system is designed to process simple step-by-step authentication. It uses less resources, operates quickly.

In [2], the authors discussed application of the encryption and decryption algorithms studied in order to increase security in networks by preventing hackers from infiltrating. As a result, a reliable and secure communication system between members of a network can be provided by preventing additional traffic in the website environment in order to increase speed, accuracy and security in the network and web systems of data sharing. The obtained results proved the reliability and capabilities of the developed software in the study which can be used in the internet.

In [3], the authors propose a authentication model by implementing two-factor authentication (2FA) over email or phone. The paper then shows how the authentication scheme can be extended to provide a secure session through a methodology similar to an SSL/TLS handshake. Proposed model does not sacrifice processing speed as it provides a more secure communications. It can be easily and flexibly integrated with other schemes to combat other cyber-attacks. This scheme out-performed other prototypes.

In [4], the authors discussed text-based captcha that is recommended with crypto hash functions preventing multiple accessing attacks. Proposed security system involves 3 layers: captcha, encryption (AES) and hashing. Comparison of 10 login authentication techniques over ten years on: passwords cryptography, hashing adaptability, anti-robot captcha usages, login encryption technique utilization and integration complexity of system. Proposed integration of captcha crypto hash functions system has an effective improvement of about 30% over old systems.

In [5], the authors emphasizes that the secured access to web contents and the interaction with web application are becoming one of the most important issues in the context of Internet. HTTP protocol which uses plain text transmission is employed for data communication over Internet. Secure Socket Layer (SSL) certificates over HTTP evolve into HTTPS protocol which is one of most used solutions that provide security. A combination of different algorithms are considered to provide confidentiality and integrity foreach level of security. The proposed approach is experimented with a prototype inhealthcare domain.

3. PROPOSED WORK

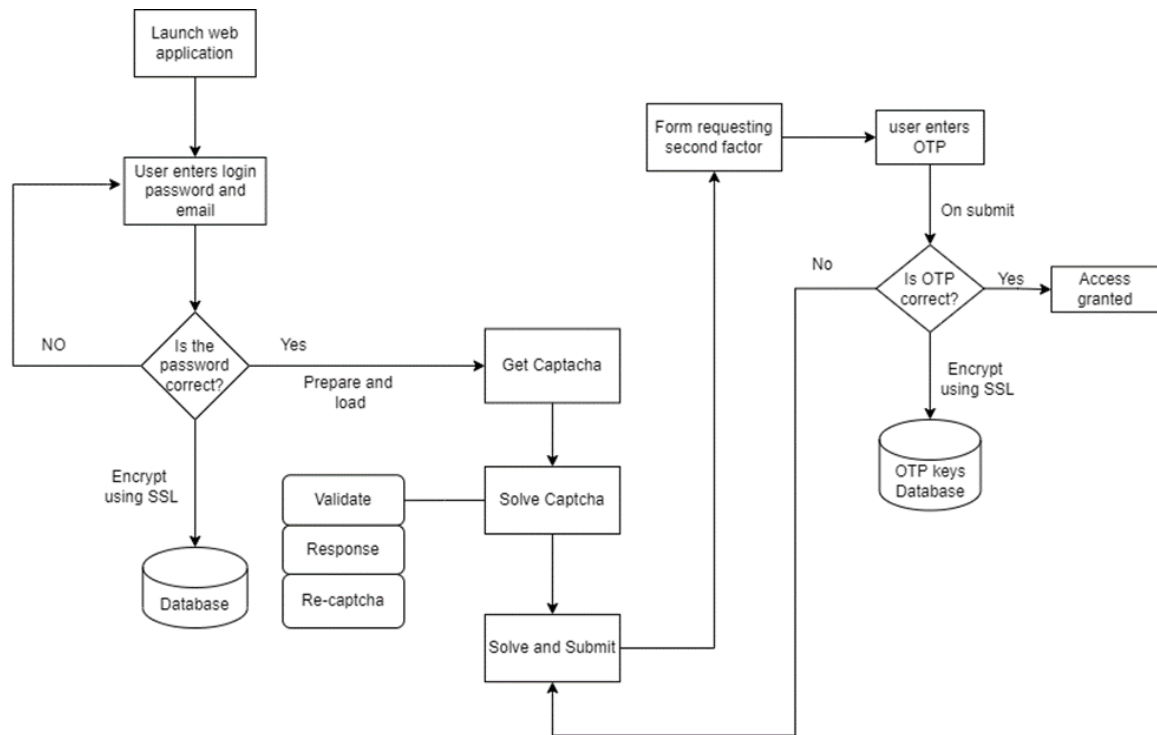


Fig. 3.1. Flowchart of proposed work.

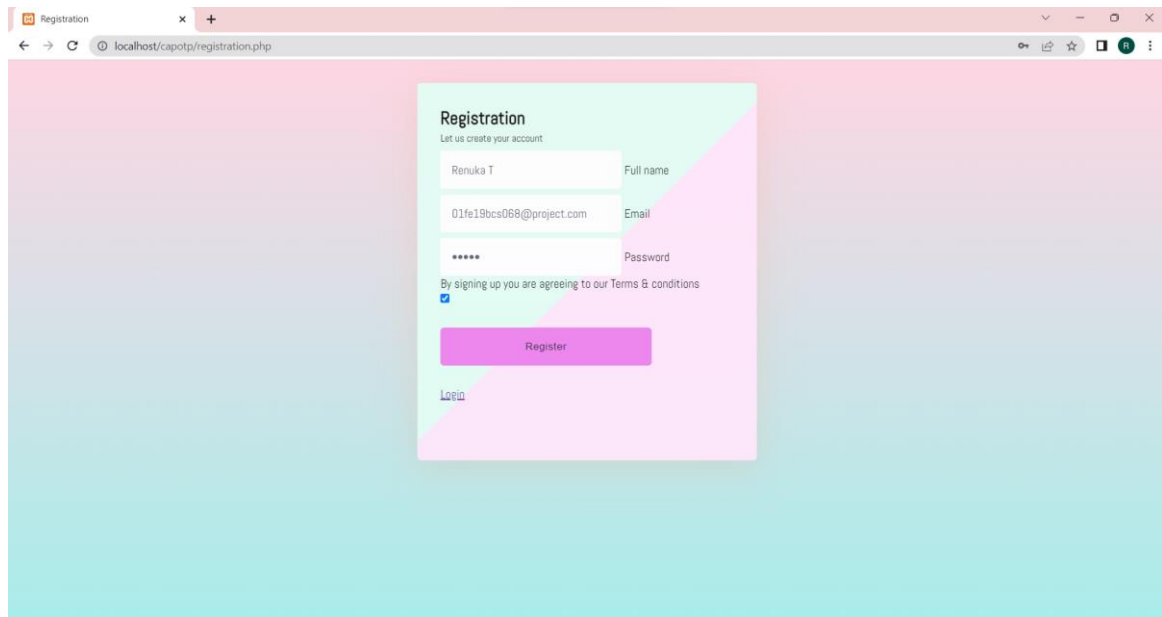
The user first Registers to website by providing his details such as full name, email address and password then click on agreement button and submit the details. Now if the user wants to login to the website he can enter his login credentials which are full name, email address, password and CAPTCHA that he is allocated with then if user exists he will be directed to home page of the site. If the user do not remember his password he has another way to login that is through OTP where user enters his full name and email address if that user exists in the database then the otp will be sent to that email which user can enter in the OTP field then OTP is validated if matched, the user is authenticated and redirects to the website home page.

4. RESULTS AND DISCUSSION

TOOLS USED

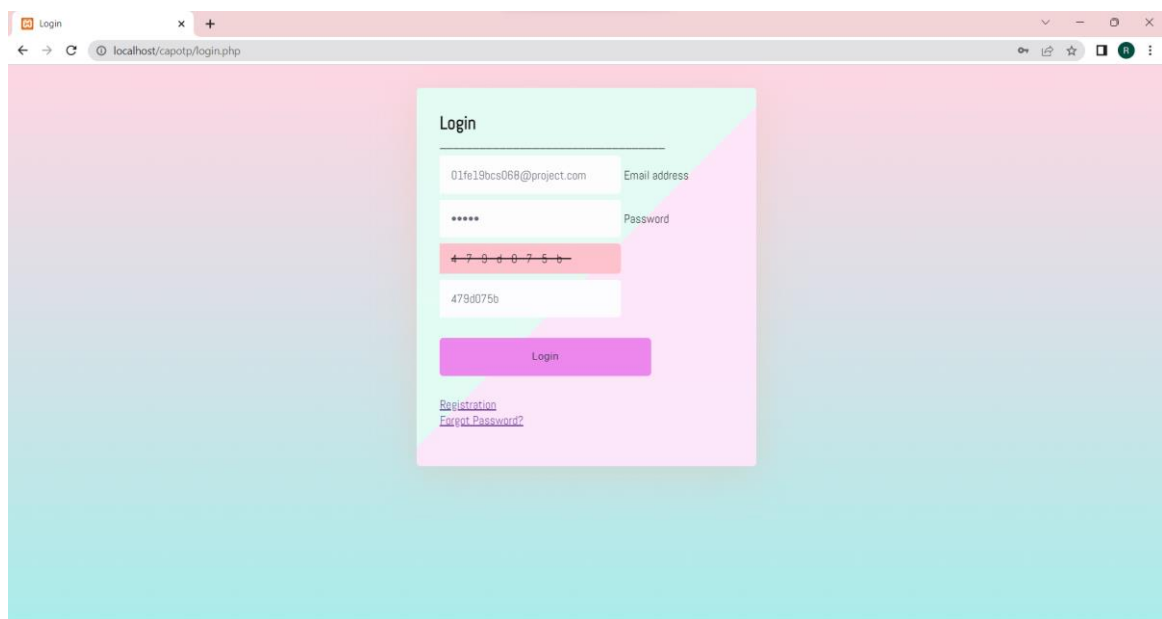
- XAMPP server with PHP and Mysql
- Hmail server
- EmClient and Thunderbird mail.

REGISTRATION



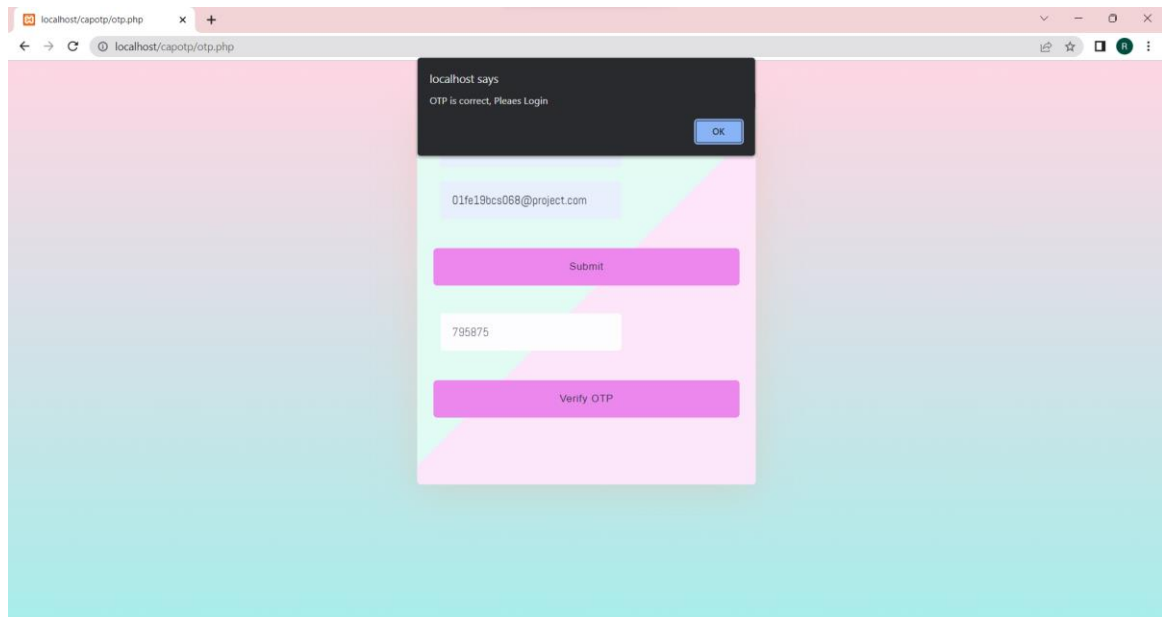
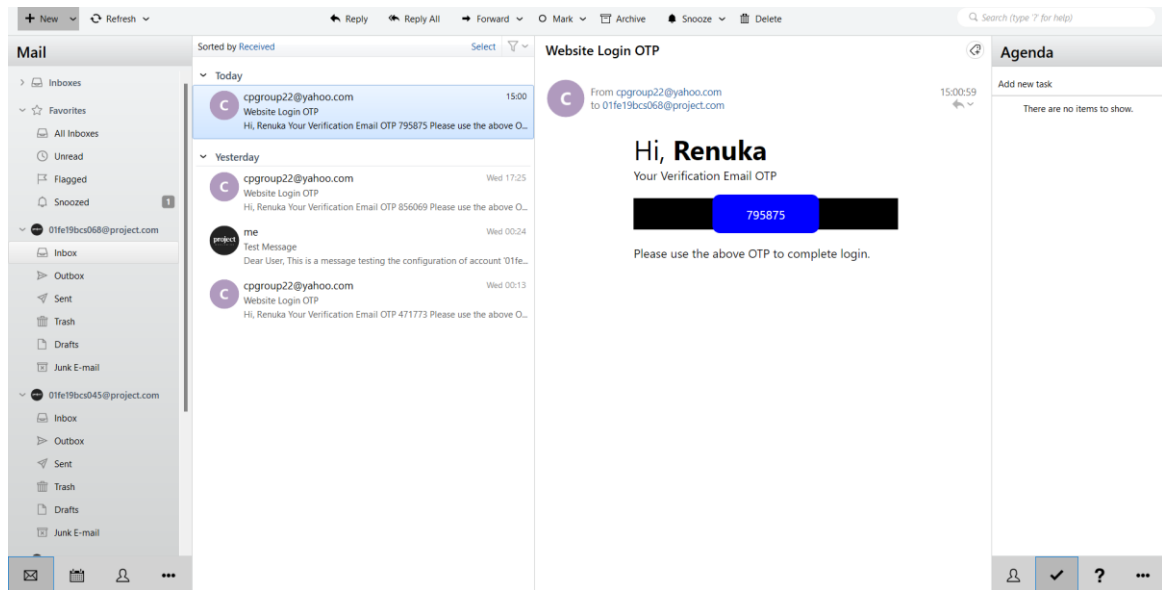
The screenshot shows a web browser window with the address bar displaying "localhost/capotp/registration.php". The page features a registration form titled "Registration" with the subtitle "Let us create your account". The form includes input fields for "Full name" (containing "Renuka T"), "Email" (containing "01fe19bcs068@project.com"), and "Password" (displayed as "*****"). Below these fields is a checkbox labeled "By signing up you are agreeing to our Terms & conditions" which is checked. A purple "Register" button is positioned below the checkbox. At the bottom left of the form, there is a link labeled "Login". The background of the page is a light blue gradient.

CAPTCHA

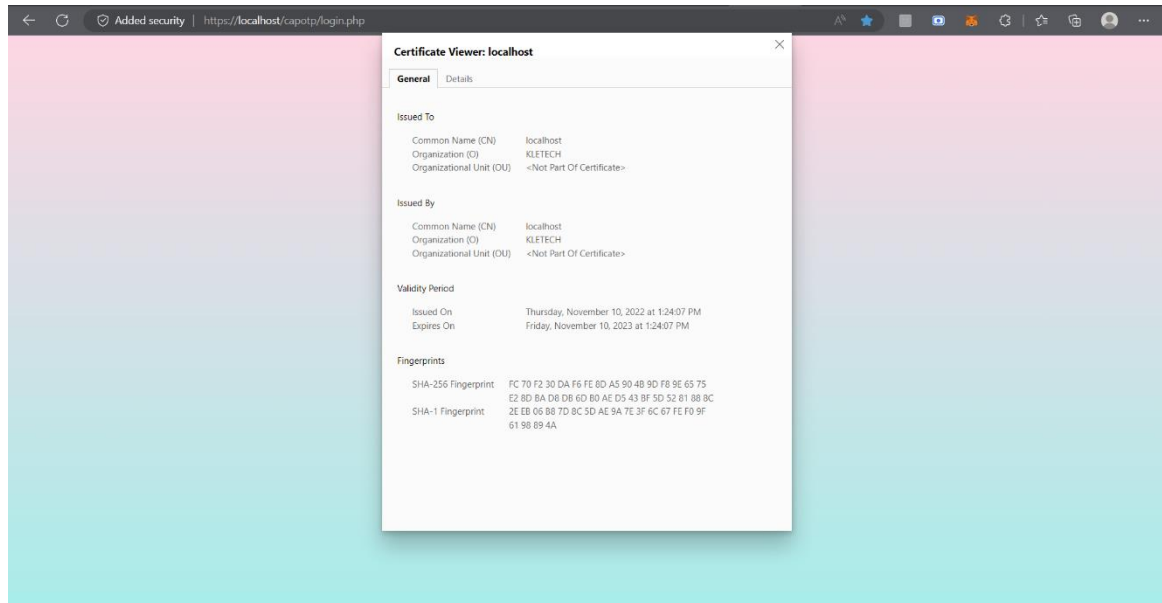


The screenshot shows a web browser window with the address bar displaying "localhost/capotp/login.php". The page features a login form titled "Login". The form includes input fields for "Email address" (containing "01fe19bcs068@project.com") and "Password" (displayed as "*****"). Below the password field is a CAPTCHA image showing the numbers "4 7 9 4 0 7 5 6". Below the CAPTCHA is an input field containing the text "479d075b". A purple "Login" button is positioned below the input fields. At the bottom left of the form, there are two links: "Registration" and "Forgot Password?". The background of the page is a light blue gradient.

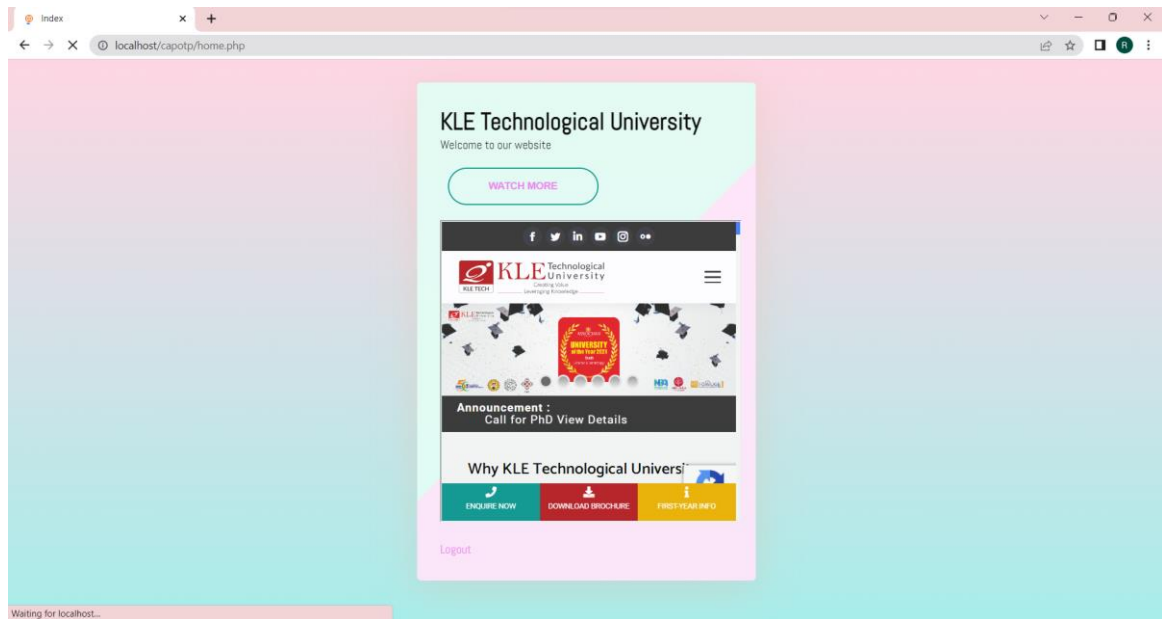
OTP



SSL



HOME PAGE



5. CONCLUSION

A need for web portal security is of prime importance because of increasing number of transactions and sharing of information that are taking place through web portals. There are various methods to secure the web page among these SSL, CAPTCHA and OTP are popular methods when it comes to secure the data exchange between web portal and the server, authentication of the user. With plain HTTP, that information is vulnerable to attacks. But when you use HTTP over SSL or TLS (HTTPS), you encrypt and authenticate that data during transport, which makes it secure. CAPTCHA offers protection from remote digital entry by making sure only a human being with the right password can access your account. CAPTCHA works because computers can create a distorted image and process a response, but they can't read or solve the problem the way a human must to pass the test. The OTP feature prevents some forms of identity theft by making sure that a captured user name/password pair cannot be used a second time. The user's login name stays the same, and the one-time password changes with each login. All three increase the strength of security provided to web portals.

6. REFERENCES

- [1] Thivanon Kaunsuwan, Thawatchai Chomsiri
“Authentication Model using the Bundled CAPTCHA OTP Instead of Traditional Password”, 2019

- [2] Roza Dastres, Mohsen Soori,
“Secure Socket Layer in the Network and Web Security”, 2020

- [3] Muath Obaidt, Joselph Brown, Suhaib Obeidat, Majdi Rawashdeh,
“A Hybrid Dynamic Encryption Scheme for Multi-Factor Verification”, 2020

- [4] Nafisah Kheshaifaty , Adnan Gutub,
“Preventing Multiple Accessing Attacks via Efficient Integration of Captcha Crypto Hash Functions”, 2022

- [5] Maheswaran A, Kanchana Rajaram,
“Web Application Security Using SSL Certificates”, 2018