Development of an Intranet Based File Tranfer and Distribution System with Multi Security Layers Using Php Code

Aru Okereke Eze
Department Of Computer Engineering, Michael Okpara University Of Agriculture, Umudike Umuahia, Abia State-Nigeria.

Nnamdi Henry I.
Department Of Computer Engineering, Michael Okpara University Of Agriculture, Umudike Umuahia, Abia State-Nigeria.

Abstract
In this Article, an intranet based file transfer and distribution system was developed. With recent development in information security were hackers has developed sophisticated applications and program to hacked even seemingly secured systems, the need to build more security walls can never be overrated. This article focuses on developing an intranet based system that will have multi security layers of authentication before a user will have access to a shared file .In achieving this, organizations were under studied to possible points of loophole, identify necessary measures and strategies which were employed in the development of the design algorithm used in building the different modules . Being a module by module based software design the research was done with the water fall model which allows for stepwise development of these modules. The algorithm, system block diagram and system component description was done while the associated images were attached as figures in the appendix.
Keywords: Development, intranet, file transfer, distribution system, and multi security layer PHP codes.

I. Introduction

Information and Information Security

Network security is a big topic and is growing into a high profile (and often highly paid)

Information Technology (IT) specialty area (syngress.com, 2008).Currently, most enterprise intranet systems process user information for security and access authentication. However, unauthorized users often capture this information and may edit, modify, delete or otherwise corrupt this data(Malrey Lee et al 2011).Information is considered so valuable because it can affect behavior, a decision, or an outcome. For example, if a manager is told his/her company's net profit decreased in the past month, he/she may use the information as a reason to cut financial spending for the next month and apply other strategies to ensurethat the net profit rises back. Information security is of great importance and interest to everybody in the world of technology today, whetheryou are a mobile phone or a personal computer user, this is why information security is of the most importance in our everyday life, and in the IT technology fields, (Mohammed M. A, Alexander A. Q 2017).Since the inception of information and data security, organizations have deployed several strategies and layer(s) of security in order to checkmate illegal access to data and secure data from the hands of intruders, hackers and other unauthorized users. There have existed different layers of security before now, it started with the single layer security system of authentication, where a user is verified just by a single security factor, example the username and password for authentication. As time progressed, intruders and hackers developed sophisticated programs and software that has the ability to penetrate highly protected systems, it was observed that   these credentials (username and password) could easily be hacked by these intruders thereby compromising the integrity, authenticity and confidentiality of the data so easily; hence it was not seen as an optimum security system. Due to the observed lapses in the single layer security system, the double layer security layer was built. This system requires that a user successfully passes two layers of security, the first being the username and password.The password system must be able not only to prevent any access to the system by unauthorized users (i.e.prevent them from logging in at all), but it must also prevent users who are already logged in from doing things that they are not authorized to do (Robert Morris and Ken Thompson 2000).While the second layer might involve the use of biometrics. This system proved to be better than the single layer security system but still had some loop holes. The inefficiencies of these systems gave rise to the

---

need to have a multi layered security system which will give a better secured information/data transfer system by making the system very hard and difficult for a hacker to penetrate.

Information security has become a continuing concern in all areas of an organizational Information system. Security is neither a product nor software; it is a discipline that needs to be taken into consideration in any organizational decision. It is indeed true that there is no such thing as a completely secure system. But it is also correct that by increasing the security measures that protect your assets, you are making your system a much more difficult target for intruders, which, in turn, reduces the chances of becoming a victim when the right security technologies are in place. A possible hacker could target the communication channel and cause harm, obtain the data, decrypt it and re-insert a false message.(Mohammed M. A, Alexander A. Q 2017)

II.   Aim and Objectives of the Research

The aim of thisresearch work is to developan intranet based file exchange and distribution system with multi-layer security system. In achieving the goal of this research, the following research objectives are to be realized.
1. To investigate an organizational file sharing and management system in other to identify the loopholes responsible for the observed information security challenges.
2. To identify the necessary measures and strategies to be employed in combating this threat.
3. To develop an algorithm necessary for the designs of the different modules in the project.
4. To develop a Web base platform with Login module, a user's account creation and registration module, Upload and download panel module, develop a Captcha generation moduleall written with PHP.

III.   System development

The intranet based file transfer and distribution system with multilayer security is a web based platform that is hosted in a remote server .The remote server (XAMMP as used) provides the framework for the file upload, download, user account registration and validation processes. More so it creates a local connectivity as the system does not require internet to function.

Cross-Platform (X), Apache (A), MySQL (M), PHP (P) and Perl (P) (XAMPP)
XAMPP is a free and open source web server solution stack. It was used in this project to create a local web server used both for the testing and deployment purposes. It provides everything needed to set up a web server; server application (Apache), database (Maria DB), and scripting language (PHP) – is included in an extractable file. Other important components of the system are:

APTANA STUDIO: Aptana Studio is an open source integrated development environment (IDE) for building web applications. It was used in this project to supports the JavaScript, with code-completion, outlining, JavaScript debugging, error and warning notifications and integrated documentation.

BOOTSTRAP 3: Bootstrap is a free and open-source front-end web framework for designing websites and web applications. It was used in this project to beautify the front end of the design as it contains HTML- and CSS-based design templates for typography, forms, buttons, navigation and other interface components, as well as optional JavaScript extensions.

JQUERY: jQuery is a cross-platform JavaScript library designed to simplify the client-side scripting of HTML. It was used in this project for web navigation designs and in the creation of plug-in on top of the JavaScript.It also allowed the creation of powerful dynamic web pages

PHP (Hypertext Pre-processor) is currently one of the most popular programming languages, widely used in both the open source community and in industry to build large web-focused applicationsand application frameworks. It a flexible dynamic scripting language that executes in client browsers. (Ravi Chugh, Jeffrey A. Meister, et al 2009).

All the necessary modules that made up thus system as listed in the aims and objectiveswas written with the PHP code.PHP is currently one of the most popular programming languages, widely used in both the open source community and in industry to build large web-focused applications and application frameworks. (M. Hills and P. Klint, 2014) Eshkevar, Dos Santos, Cordy, &Antoniol also add that PHP is by far the most popular WEB scripting language, accounting for more than 80% of existing websites. (P. Kyriakakis and A. Chatzigeorgiou, 2014).

However, Scripting languages such as PHP have been criticized as inadequate for supporting maintenance of large scale software projects (P. Kyriakakis and A. Chatzigeorgiou, 2014). Kyriakakis et al attempt to provide insight into the way that PHP applications evolved over time. They examined several aspects of their history including the amount of unused code, the removal of functions, the use of libraries, the stability of their interfaces, the migration to object-orientation and the evolution of complexity.

This evolution is brought about because a web application (Build in PHP) evolve, new versions of programs, interactions and functionalities are added and existing ones are removed or modified. Web applications require configuration and programming attention to assure security, confidentiality, and trustiness

of the published information. During evolution of Web software, from one version to the next one, security flaws may be introduced, corrected, or ignored (E. Merloet el,) (Douglas Kunda and AlinasweSiame, 2017)

Systems design implies a systematic approach to the design of a system. It may take a bottom-up or top-down approach, but either way the process is systematic wherein it takes into account all related variables of the system that needs to be created from the architecture, to the required hardware and software, right down to the data and how it travels and transforms throughout its travel through the system. It overlaps with systems analysis, systems engineering and systems architecture. (Techopedia.com)

IV.   Design Model

This project being a purely software based project requires a model that will enable a step by step sequential develop from the scratch to the end of the project. With such consideration, the water fall model was employed in this design.

The waterfall model

The waterfall model is a popular version of the systems development life cycle model for software engineering. Often considered the classic approach to the systems development life cycle, the waterfall model describes a development method that is linear and sequential. Waterfall development has distinct goals for each phase of development. Once a phase of development is completed, the development proceeds to the next phase and there is no turning back.

This model was useful in this project because it allowed departmentalization in terms of module by module development and managerial control. A schedule can be set with deadlines for each stage of development and a product can proceed through the development process, and theoretically. The development moved from concept, through design, implementation, testing, installation, troubleshooting, and ends up at operation and maintenance. Each phase of this development proceeds in strict order, without any overlapping oriterative steps.

The observed disadvantage of waterfall development in this project is that it does not allow for much reflection or revision. Once a module is in the testing stage, it is very difficult to go back and change something that was not well-thought out in the concept stage.
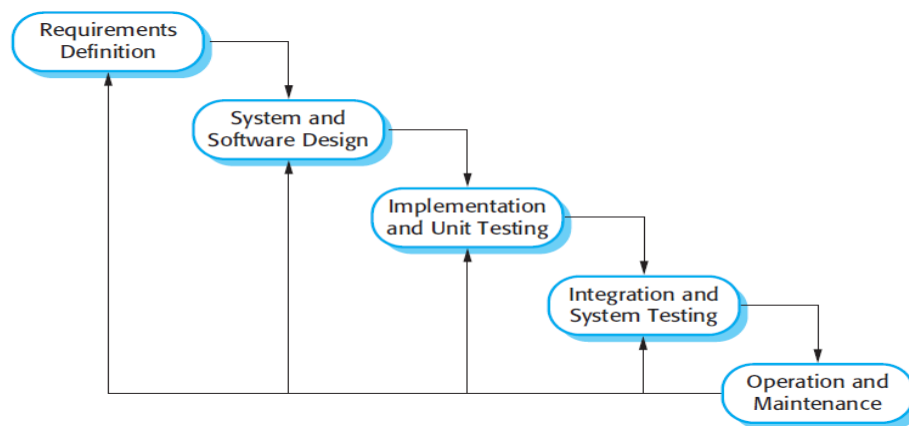

Fig.1 The waterfall design model (softwarekno.blogspot.com/2016/09/waterfall-model.html)
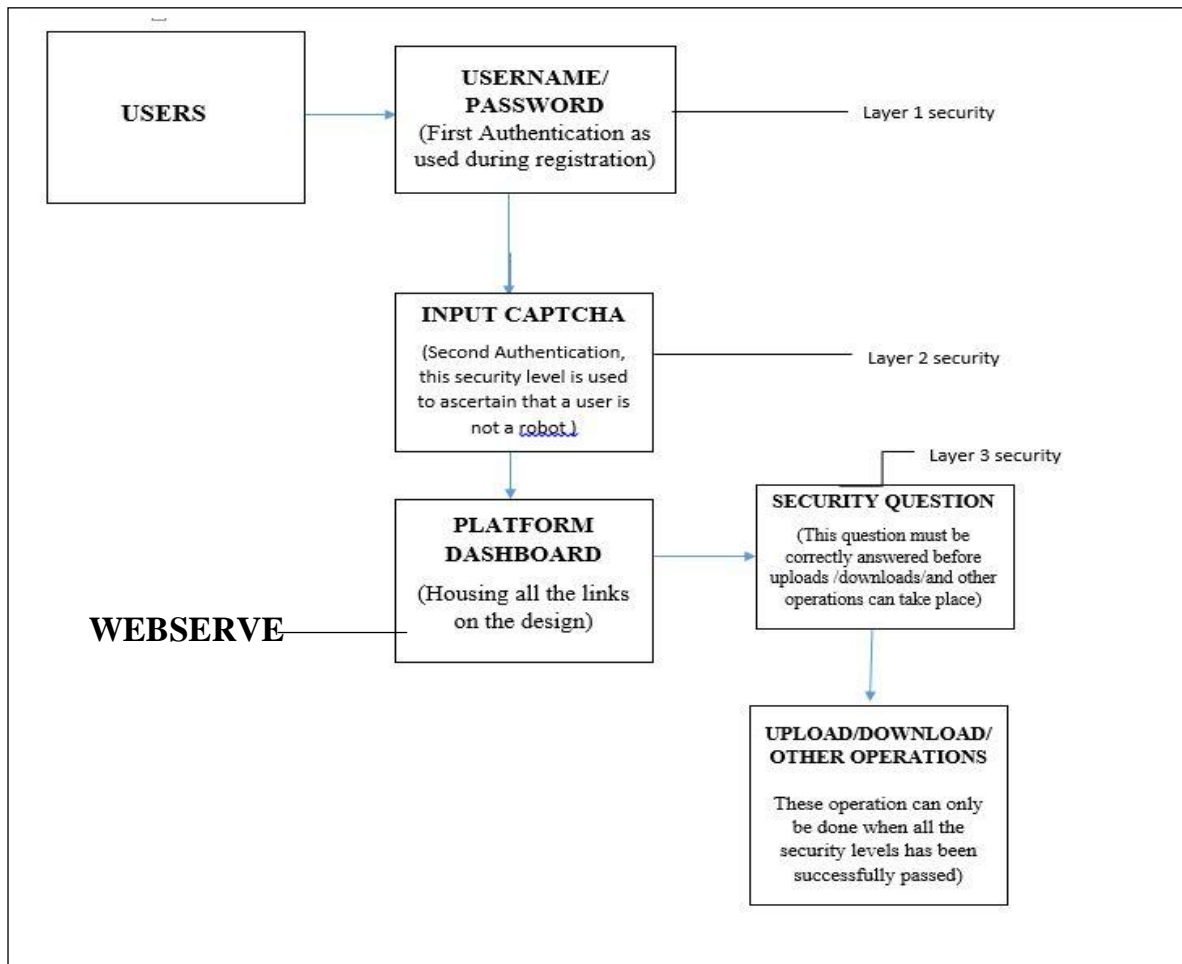
Fig. 2The Process Design Diagram

V. Block Diagram'sComponent Explanation

Web server

The web server being a locally hosted server is accessed just within the internal connection using the LAN, or the Wi-Fi-Hotspot technology as the case may be.

Web serverin this design is a computer where the web content is stored, that is, uploaded files from registered users are stored in the web server. On the other hand, registered users only can be able to access the uploaded files and be able to view and download after successfully passing the different layers of authentications and validations.

Web server working

The Web server responds to the client request in either of the following two ways:

1.   Sending the file to the client associated with the requested URL.

2.   Generating response by invoking a script and communicating with database

In this design, Xampp v3.2.2 is used to provide the remote server that permits the sharing of this platform with users that are remotely connected to the network. It holds the database (.sql) that keeps a user's credentials (username, password and security question) and validates a user trying to log into the system.

The User: The user of the system is the human ware involved in a file sharing and distribution operation. He/she might either be the sender or the receiver of the file on transit. Access is granted to the user after a successful authentication or validation of the different security layers in the system.

Layer 1 Security

From the block diagram, the first layer in the system is the user's initial credential verification interface. The initial credential in this case is the username and password. Input data is accepted from the logging page of the server. When you input the correct username and password for authentication, your script sends an HTTP header to the server during API function calls. This allows the script to effectively log in as the desired user before the function.

Layer 2 Security
The second security layer in this system is the Captcha validation process.
After successful validation of the first security layer, you will now be required to embark on the Captcha validation. Captcha generator generates randomly fixed length of alphanumeric which a user must have to input back into the system for validation. The Captcha validation process is used to ascertain that it is actually a human user trying to access the platform and not a robot system.

Layer 3 Security
Once a user is successful in the first and second layer that is the initial credentials (username and password) and the Captcha verification, the next security layer will me meet at the dashboard when files are either to be uploaded or downloaded. This security question is one of the strongest security check on this plat form, a user while registering selects and answers a security question. This question is save in one table in the excel database as one of the tables and must be answered correctly before an upload or download operation can be carried out in this platform.
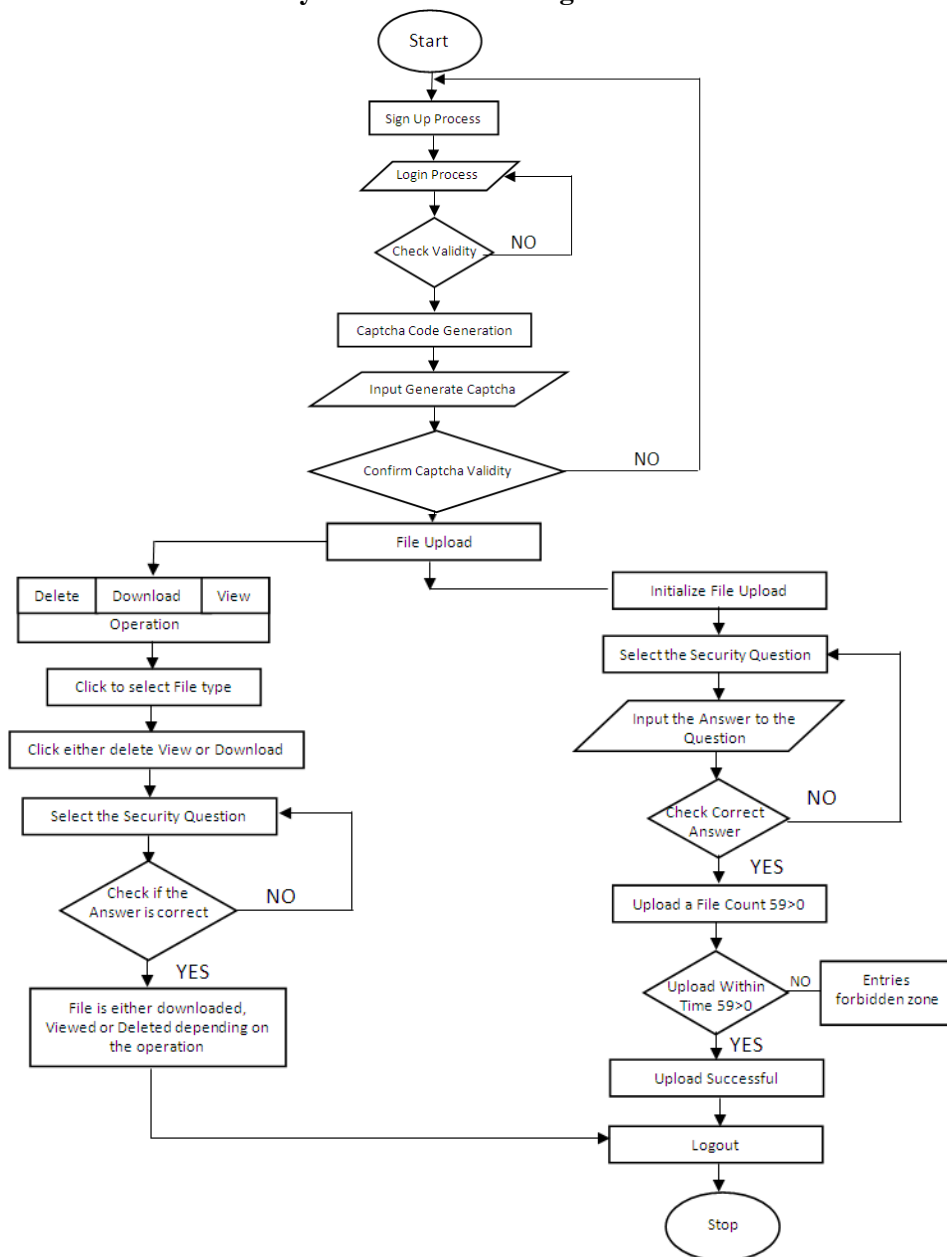
VI. System Flowchart Diagram

Fig 3 Design flowchart of the system

VII.   The System Design Algorithm

Step1.   Start
Step2.   Sign up
Step3.   Login into the platform using the created username and password
Step4.   IF Username and password is Correct
                    Then goto step5
                    Else goto Step2
Step5.   Input the generated captcha code
Step6.   IF captcha is correct
Then goto Step7
Else goto step2
Step7.   Select upload
Step8.   Answer security question proceeding step2
Step9.   IF Security question is correct
                    Then goto Step10
                    Else goto Step9.
Step10   Select the file and then upload.
To download, Delete, View.
Step11.   Select from the upload file types (All file)
Step12   Click on the required file operation (Download, Delete, and View)
Step13   Answer the security question as provided during the step2
Step14   IF security question is correct
Then goto Step15
Else goto step14
Step15   File is either downloaded, Deleted or viewed depending on step12
Step16   Click on logout tab
Step17   Stop

VIII.   Modules Description

This platform designed with PHP has Top-gym/fitness template (html) integrated into the system which gives it the animated motion background as found in the initial authentication pages of the application

1.   The Sign Up/Registration Module
This module written with the PHP code and enhanced with the Bootstrap and JQuery enables a user to register/sign up into the platform.When a new user visits the platform, he /she is required to register/sign up on to the platform, during registration he/she is expected to supply his email ,password and answer one of the security question. This security question is very important to note as it serves as another security layer at the upload and download panel. Fig A on the Appendix showsa picture of the sign up page of the design.

2.   The Login Module
This login module was also written with the php code and enhanced with the Bootstrap and JQuery. It enables an existing user to login into the platform once he/she has provided the matching login credential as validated against the details on the server as provided during registration.Note the credentials must be provided exactly as it was inputted at the registration stage (same case style) for a successful validation.Fig B on the Appendix shows the picture of the sign in/login page of the design.

3.   The Captcha Module
The captcha generator is a random code generator designed to generate different codes each time it's triggered. The captcha was used in this project to create a security level in other to ensure that a user is human and not a robot.
After a successful provision of the first authentication, i.e. the username and password, the user is expected to pass the second authentication level. This level requires that the user enters the generated captcha and submit it using the "sign in" button as found in the image below. Fig Cin the appendix the diagram of the Captcha page

4.   The Dashboard Module
         The dashboard module of this design is a page which serves as the home page for this application. The dashboard is reached after a successful passage of the authentication levels. This page houses the links to different modules/panels in this project like the upload module, the All-file module, logout module and the different file type links.Fig D on the appendix shows the picture of the platforms dashboard.
         Now once a particular file type is to be shared between users in this platform, a sender logs in and uploads after successfully providing the answer to the security question he answered during the sign up stage,

while the receiver logs in, clicks on the file type from the all-file module and downloads after providing the correct answer to the security question he answered at the sign up stage. The sender and the receiver must be connected with an intranet based connection and the application is hosted in a remote server.

It is important to note that the upload process is timed, once you click to initialize file upload process, the timer system counts down from sixty seconds to zero and enters the forbidden zone (warning page) and you will be required to answer the security question again before you can continue.

This check is designed to be another form of security that will ensure that an intruder did not upload into the hub in a situation where the right user initializes an upload sequence but had to leave his system to attend to something else. The system will enter into the warning zone to protect the platform.

When a user wants to download a file, he clicks at the "All File" tab at the left hand side of the dashboard, he/she then and clicks from the drop down the kind of file he wishes to download and then selects the action he/she wants to take, either to download, delete or view the file. Note the action a user can take is determined by the role assigned to the user by the super admin.

Create Admin

Another additional module in this system is the Create Admin Module: This module was designed in other to allow for the assigning of roles and privileges on the platform.The super admin of this system has the right and power to view users on the platform, assign roles and responsibilities to the users of the system, hence the extent of one's operation on the platform is determined by the role assigned to him by the super admin. A user can either be a super admin (can manage other admins), an admin (can delete a file from the hub) or an Editor (can hide a file on the hub though not from a super admin or admin).Fig E on the appendix shows the diagram of the role control module (Create admin).

Logout Module

The users are expected to logout of the platform after a successful sharing of file in other to avoid an intruder having access to the platform from his logged account.
Another primary security level that is worthy of being noted is the system administrative password of the server system which a user must provide before having access to the server.
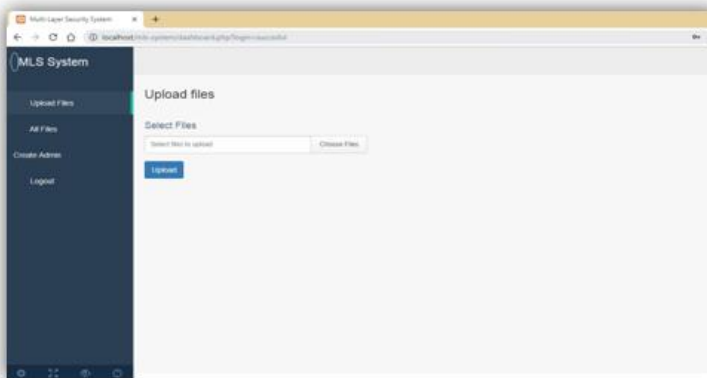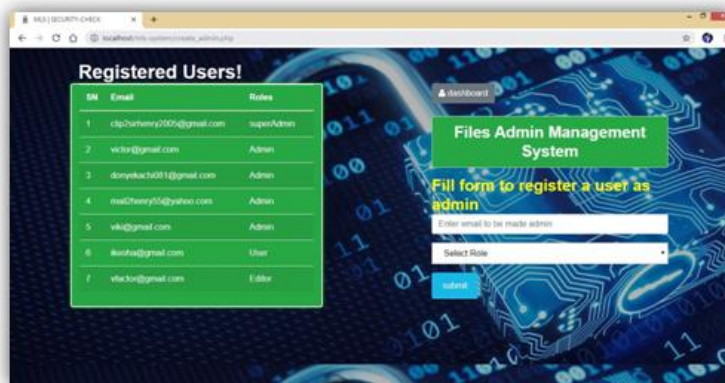
Appendix

Fig A
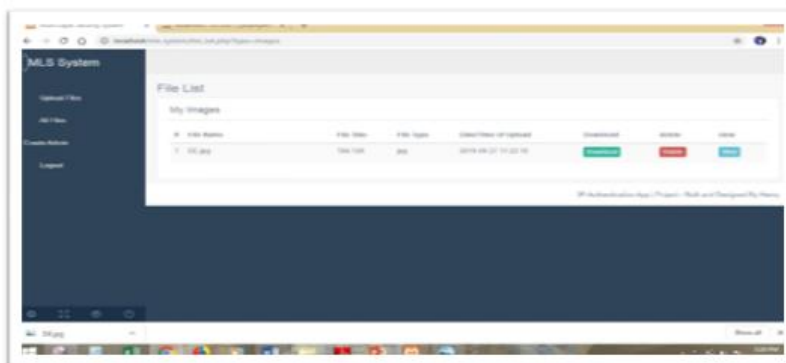

Fig B

Fig C

Fig E

Fig D

Fig F

Reference

[1].   Douglas Kunda and AlinasweSiame,(2017)"Evolution of PHP Applications: A Systematic Literature Review" Mulungushi University, Kabwe, Zambia.
[2].   E. Merlo, D. Letarte and G. Antoniol, "SQL-Injection Security Evolution Analysis in PHP," IEEE, pp. 45-49, 2007. https://doi.org/10.1109/wse.2007.4380243

[3].   M. Hills and P. Klint (2014) "PHP AiR: Analyzing PHP Systems with Rascal," IEEE, pp. 454- 457, 2014.
[4].   Malrey Lee et al (2011) "Design and implementation of an intranet Security and access control system In ubi-com" Computing and Informatics, Vol. 30.
[5].   Mohammed M. A* , Alexander A Q (2017) "Information Security in an Organization" International Journal of Computer (IJC)
[6].   P. Kyriakakis and A. Chatzigeorgiou, "Maintenance Patterns of large-scale PHP Web Applications," IEEE International Conference on Software Maintenance and Evolution, pp. 381-390, 2014.
[7].   Ravi Chugh, Jeffrey A. Meister, et al (2009). "Staged information flow for JavaScript". Programming Language Design and Implementation. (PLDI)
[8].   Robert Morris and Ken Thompson (2000) "Password Security: A Case History" Bell Laboratories
[9].   Techopedia Explains System Designhttps://www.techopedia.com/definition/29998/system-design
        www.syngress.com(2008).Network Security Basics • Chapter 1.
        http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Network-Security-Basics.pdf