

*The Ministry of Higher Education and Scientific Research*

*University of Diyala*

*College of Engineering*

*Department of Computer and Software Engineering*



# *Secure the Stored Data by Preventing the Unauthorized Intranet Connection Access Using PHP and Java Script*

*A project*

*Submitted to the Department of (Computer and Software  
Engineering Dep.)University of Diyala – College of Engineering in  
Partial Fulfillment of the Requirements for the Degree of Bachelor's  
(Computer and Software )Engineering*

*Prepared by:-*

*Tiba Ghassan Mohammed*

*Marwa Ibrahim Faris*

*Noora Ghani Rahman*

*Under the Supervision of*

*Huda Mohammed Sal*

*1347/2016*

## *Abstract*

Web application security is the process of securing confidential data stored online from unauthorized access and modification. This Project is the approach to improve website security, we have shown attacks types and shown the solutions and countermeasures against vulnerabilities at the stage of software design and development. We will try to shed some light on making the Web applications more secure through design admin control panel to manage files and directories by using JAVA and PHP language implemented on Ubuntu V.14.04lts Linux operating system because of there are many benefits of Linux OS such as permissions scheme. Each file and directory on Linux system is assigned access rights for the owner of the file, the members of a group of related users, and everybody else. PHP is one of the most popular server side scripting languages running today. It is used for creating dynamic webpages that interact with the user offering customized information. PHP offers many advantages; it is fast, stable, secure, easy to use and open source.

In this work an attempt is made to design the admin control panel that built with robust security programming and tools. From the result which was done on some selected IP, a number of conclusion remarks was drawn: Easy to use for administration. Prevent unauthorized users gain access to sensitive data. Admin prevent the attacker that can used some attacks tools such as XSS, SQL injection and password crack to attack and access the admin control panel, and other benefits.

# *Chapter One*

## *Introduction*

## **1.1 Introduction**

Data security refers to protective privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is the main priority for organizations of every size and genre. Data security is also known as information security (IS) or computer security. A security mechanism may aim to prevent an attack, detect an attack, and respond to it. Prevention means that it is impossible to perpetrate a given attack in the presence of a given security mechanism. Detection aims to quickly and accurately detect the attack, i.e. to reduce the number of false positives, false negatives and to reduce the detection delay. A false positive is a case when detection occurs but there is no attack. A false negative is a case when there is an attack but detection does not occur. A response to an attack can be to tighten security mechanisms at the target, lodge a complaint on someone.[1]

So in this chapter discuss the main difference between security and protection and introduction about web application security, administrator, iptable and secure sell(SSH).

### **1.1.1 The Main Difference Between Security and Protection**

Security features include protection, but are more geared to defense of the system from external entities . Security ensures the authentication of system users to protect the integrity of the information stored in the system (both data and code), as well as the physical resources of the computer system. The security system prevents unauthorized access, malicious destruction or alteration of data, and accidental introduction of inconsistency.

Protection mechanisms are built into the operating system, and are utilized for control of access to files / accounts / data on a computer. Protection mechanisms control access to a system by limiting the types of file access permitted to users. In addition, protection must ensure that only processes that have gained proper authorization from the operating system can operate on memory segments, the CPU, and other resources.

The main difference between the two is that protection is internally focused while security has to deal with the environment as well.[2]

### **1.1.2 Web Application Security**

Web application security is the process of securing confidential data stored online from unauthorized access and modification. This is accomplished by enforcing stringent policy measures. Security threats can compromise the data stored by an organization is hackers with malicious intentions try to gain access to sensitive information.[3]

### **1.1.3 Administrator**

Administrator of organization's computing applications, be responsible for setting up and running a system that is critical to corporate mission and plan how to maximize the performance and high security in the work.[4]

### **1.1.4 IPtable**

Internet Protocol Address (or IP Address) is an unique address that computing devices used to identify itself and communicate with other devices in the Internet Protocol network. Any device connected to the IP network must

have an unique IP address within its network. An IP address is analogous to a street address or telephone number in that it is used to uniquely identify entity.

In order to maintain uniqueness within global namespace, the IP addresses are publicly registered with the Network Information Center (NIC) to avoid address conflicts. Devices that need to be publicly identified such as web or mail servers must have a globally unique IP address, and they are assigned a public IP address. Devices that do not require public access may be assigned a private IP address, and make it uniquely identifiable within one organization. For example, a network printer may be assigned a private IP address to prevent the world from printing from it. To allow organizations to freely assign private IP addresses, the NIC has reserved certain address blocks for private use.

The following IP blocks are reserved for private IP addresses:

Network and broadcast address, Default route, Loopback IPaddress, Link local address.

#### **1.1.4.1 loopback IPaddress**

The loopback IP address is the address used to access itself. The IPv4 designated 127.0.0.1 as the loopback address with the 255.0.0.0 subnet mask. A loopback interface is also known as a virtual IP, which does not associate with hardware interface. On Linux systems, the loopback interface is commonly called lo or loo. The corresponding hostname for this interface is called localhost .

The loopback address is used to test network software without physically installing a Network Interface Card (NIC), and without having to physically

connect the machine to a TCP/IP network. A good example of this is to access the web server running on itself by using `http://127.0.0.1` or `http://localhost`. [5]

## **1.5 Secure Shell**

Secure Shell is a protocol that provides authentication, encryption and data integrity to secure network communication. Implementation of secure shell offer the following capabilities: a secure command-shell, secure file transfer, and remote access to a variety of TCP/IP applications via a secure tunnel. Secure Shell client and server applications are widely available for most popular operating systems.

Secure Shell offers a good solution for the problem of securing data sent over a public network. For example, using Secure Shell and the Internet for securely transferring documents and work products electronically, rather than using a traditional overnight courier can provide a substantial cost savings. Using the Internet with Secure Shell to securely deliver his documents he could easily recoup the cost of Internet access with just one document transfer.

### **1.5.1 Functionality of Secure Shell**

Secure Shell provides three main capabilities, which open the door for many creative secure solutions.

- Secure command-shell.
- Secure file transfer.
- Port forwarding. [6]



## 1.6 website Security

There are two roads to accomplish excellent security:

**First option:** The admin will assign all of the resources needed to maintain constant alert to new security issues and he would ensure that all patches and updates are done at once, and have all of his existing applications reviewed for correct security, also he would maintain website from through a tight firewall, antivirus protection and run IPS/IDS.

**Second option:** The admin use a web scanning solution to test his existing equipment, applications and web site code to see if a known vulnerability actually exists. While firewalls, antivirus and IPS/IDS are all worthwhile,. Network and web site vulnerability scanning is the most efficient security investment of all. If someone want to walk in one of these roads, diligent wall building or vulnerability testing in fact will produce a safer website. This is proven by the number of web sites which get hacked every month.[7]

## 1.7 Since When does The User Need to Security

In this day and age, when the internet is vast and extends so far, there are annoying folks who want to be malicious. And that pretty much sums up he should secure everything. PHP security isn't just an option anymore; it's a necessity. Sites are hacked daily, and as he build a site using PHP, the user need to know how to keep its safe from the bad guys. PHP security is securing his site in PHP, to help prevent the bad guys from gaining unauthorized access to his site data. It helps him to keep his data's integrity and ensures availability as needed. he can start doing this in PHP with validating and sanitizing data on his site.[8]

## **1.8 The Aim of Project**

This Project will try to shed some light on making the Web applications more secure, since this area is mostly the responsibility of developer or is an effect of joint effort of developers and administrators.

## **1.9 Outlines of the Project.**

In addition to **Chapter One(Introduction to the project):-**That is Introduction of the project.

The project include three other **Chapters:-**

**Chapter Two:(Basic Concept of Website Security):-** Includes description for Hacker and Common Web application attacks types and ways to secure the website.

**Chapter Three:** Describes the project design and implementation in detail From the first step to the main interface with other contents.

**Chapter Four:** Includes conclusion and future work.

# **Chapter Two**

## **Basic concept of Website Security**

## **2.1 Introduction**

This chapter discusses the approaches to improve website security and we have shown attacks types and shown the solutions and countermeasures against vulnerabilities at the stage of software design and development.

### **2.1.1 Hackers**

A long time ago these were teenage hackers who attacked for bragging rights. While attacks were disruptive, there was no real malice and many times no large financial loss. Today, most attacks are perpetrated by organized criminal. There is a very active underground economy where people trade in stolen data, compromised machines and malicious code. Attacks occur mostly for financial reasons stolen data can be used for financial gain, denial of service can be used for extortion, spam can drive people to buy a shady product, ... Some attacks happen for personal or political reasons. This shift in attacker mix from hackers to organized criminal is significant because it means that attackers are much more motivated than before and capable of more sophisticated attacks. It is worth noting that the risk to the attacker from many attacks is very small. Attackers often use compromised machines that may be in some remote part of the world compared to the target. Most attacks do not last long or do not generate strong enough signal to be detected for most of their lifetime (e.g. intrusions). Even if one detects the attack and the end-machine involved there may be no traces there left of the attacker, or the machine may be in a foreign country that does not cooperate with investigation.[9]

### **2.1.2 Common Web Application Attacks Types**

Below is the list of some of the most common Web attack types:-

#### **1: SQL Injection**

The basic idea behind SQL Injection attack is abusing Web pages which allows users to enter text in form fields which are used for database queries. Hackers can enter a disguised SQL query, which changes the nature of the intended query. Hence the queries can be used to access the connected database and change or delete its data. Although protection from this kind of attack is very simple (especially using Microsoft.NET technologies), there is a big number of Internet systems which are vulnerable to this kind of attack. SQL query generated by concatenation of the static part of the query and values intended for form fields is the base of this attack.

#### **2: OS Command Injection**

Web applications can be vulnerable in such a way that they allow a remote attacker to execute OS level commands via those applications. This issue is called “OS Command Injection vulnerability” and the attacking method exploiting this vulnerability is called “OS Command Injection attack”.

#### **3:Unchecked Path Parameter / Directory Traversal**

Some web applications allow to specify the name of files stored on the web server directly using external parameters. If such web application is not carefully programmed, attackers may specify an arbitrary file and have the web application execute unintended operations. This issue is called “Directory Traversal vulnerability” and one of the attacking methods exploiting this vulnerability is called “Directory Traversal attack”.

#### 4:Improper Session Management

Some web applications issue session ID, which is the information to identify the user, to manage sessions. If session ID is not created and managed properly, an attacker could steal the session ID of a legitimate user and gain unauthorized access to the services pretending to be the legitimate user. The attacking method exploiting this vulnerability in session management is called “Session Hijacking”.

#### 5: Cross-Site Scripting

CSS (Cross-Site Scripting) or XSS is possible with dynamic pages showing the input that is not properly validated. This allows the hacker to inject the malicious JavaScript code in a generated page and execute the script on a computer of any visitor of that Web site. Cross-site scripting could potentially impact any site that allows users to enter data.

This vulnerability is commonly seen on:

- Search engines that echo the search keyword that was entered,
- Error messages that echo the string that contained the error,
- Forms that are filled out where values are later presented to the use ,and
- Web message boards that allow users to post their own messages .

A hacker that successfully uses cross-site scripting can access sensitive data, steal or manipulate cookies, create HTTP requests which can be mistaken for those of a valid user, or execute malicious code on an end-user system.

## 6:Web Site Defacement

Occurs when a hacker breaks into a web server and alters the hosted website or creates one of his own.

## 7: Buffer Overflow

Hackers exploit buffer overflows by appending executable instructions to the end of data and causing that code to be run after it has entered memory.

## 8:HTTP Header Injection

Some web applications dynamically set the value of the HTTP response header fields based on the value passed by the external parameters. For example, HTTP redirection is implemented by setting a redirected-to URL specified in the parameter to the Location header field, or a web application may set the names entered in a bulletin board to the Set-Cookie header field. If the process of building an HTTP response header in such web applications has vulnerabilities, an attacker could add header fields, manipulate the response body and have the web application generate multiple responses. This issue is called “HTTP Header Injection vulnerability” and the attack method exploiting this vulnerability is called “HTTP Header Injection attack”. In particular, the attack that leads the web application to produce multiple responses is called “HTTP Response Splitting attack”.

## 9: Mail Header Injection

Some web applications provide a function that sends emails to the particular email addresses about, for example, the merchandise the users have purchased or survey replies. In general, these email addresses are pre- specified and only the web administrator can change. Depending on how it is implemented, however, an attacker may be able to set and change them to arbitrary email

addresses. This vulnerability is called “Mail Header Injection” and the attacking method exploiting this vulnerability is called “Mail Header Injection attack”.

#### 10: DOS (Denial Of Service)

An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted)

#### 11: Password Cracking

The process of recovering secret passwords from data that has been stored in or transmitted by a computer system, typically, by repeatedly verifying guesses for the password.[10]

### **2.1.3 Web Security Threats**

Table1 provides a summary of the types of security threats faced when using the Web. One way to group these threats is in terms of passive and active attacks Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted. Active attacks include impersonating another user, altering messages in transit between client and server, and altering information on a Web site Another way to classify Web security threats is in terms of the location of the threat: Web server, Web browser, and network traffic between browser of the location of the server.[11]



**Table1: Types of Security Threats.**

	Threats	Consequences	Countermeasures
<b>Integrity</b>	<ul style="list-style-type: none"><li>• Modification of user data</li><li>• Trojan horse browser</li><li>• Modification of memory</li><li>• Modification of message traffic in transit</li></ul>	<ul style="list-style-type: none"><li>• Loss of information</li><li>• Compromise of machine</li><li>• Vulnerability to all other threats</li></ul>	Cryptographic checksums
<b>Confidentiality</b>	<ul style="list-style-type: none"><li>• Eavesdropping on the net</li><li>• Theft of info from server</li><li>• Theft of data from client</li><li>• Info about network configuration</li><li>• Info about which client talks to server</li></ul>	<ul style="list-style-type: none"><li>• Loss of information</li><li>• Loss of privacy</li></ul>	Encryption, Web proxies
<b>Denial of Service</b>	<ul style="list-style-type: none"><li>• Killing of user threads</li><li>• Flooding machine with bogus requests</li><li>• Filling up disk or memory</li><li>• Isolating machine by DNS attacks</li></ul>	<ul style="list-style-type: none"><li>• Disruptive</li><li>• Annoying</li><li>• Prevent user from getting work done</li></ul>	Difficult to prevent
<b>Authentication</b>	<ul style="list-style-type: none"><li>• Impersonation of legitimate users</li><li>• Data forgery</li></ul>	<ul style="list-style-type: none"><li>• Misrepresentation of user</li><li>• Belief that false information is valid</li></ul>	Cryptographic techniques

#### **2.1.4 Ways to Secure Admin Website**

They have solutions and countermeasures against vulnerabilities at the stage of software design and development.

##### **1:Secure Web Server**

To safely operate a website, the administrator should not only secure web applications but also securely guard the web server. The admin can see if the web server's settings and operation are secure.

- Check OS and software vulnerability information constantly and take necessary actions accordingly.

- Implement an authentication mechanism other than using passwords for remote server access.
- When using password authentication, make sure to use a sufficiently complex string.
- Disable unused services and delete unnecessary accounts.
- Do not place a file the user do not intend to make public under the public directory on the web server.

## 2: Configure DNS Security

If the administrators are not careful in configuring and operating the domain names or the DNS servers they are using, malicious attackers could hijack their domain names. If domain names are hijacked, the visitors to the website can be directed to a phony website prepared by the attacker even though the visitors type in the correct URL. Domain name hijacking will affect not only website browsing but also emailing, and basically all Internet services. It may be a DNS issue but should be taken seriously for it will directly affect the website.

## 3: Protect Against Network Sniffing

The information to be exchanged between the website and the user may be leaked through network sniffing. If communication or data is unencrypted, captured information may be used for spoofing or other malicious purposes.

- If the website handles important information, encrypt communication.
- Do not send important information via email to notify the user and show it on the HTTPS encrypted web page instead.

#### 4: Use Strong Passwords

Most common way of implementing user authentication is to use a user ID/ password pair. If password management and processing by the website are inappropriate, the risk of a malicious attacker stealing user authentication information becomes higher. One way to wrongly obtain the user ID or password is guessing it. This is often tried for the websites with a simple password scheme full of easy-to-guess passwords. How you display a web page may give out even more hints for attackers to work on. If the website has an authentication mechanism, be careful about the following points.

- Set hard-to-guess default passwords.
- Require users to enter the current password to change password.
- Do not give away unnecessary hints in authentication error message.
- Mask password being entered in the password box.

#### 5: Keep Admin Applications Up to Date

Open source applications occupied a major part on the websites designing and development, these days a lot of people are hosting the open source CMS applications. They too encourage the admin to host them, but if he don't keep them up to date, that means definitely he are in trouble. Several times we try to warn he guys on this, but most of the time webmasters ignore this. They often try to send his email alerts about these security issues of using the old version of applications, but in most of the cases customers ignore. They request he to keep his application up to date, there are thousands of people working on the open source projects to keep them up to date and make them secure.

## 6: Secure Admin Pages With SSL Certificate

If the admin has any ecommerce type website must he know that having an SSL certificate for his SSL store is one of the most important thing to protect his customers valuable data and his reputation as well. Even if the admin has just a page which provide logins for his customers or members, then it is recommended to have an SSL certificate. This will ensure that all the information on his pages over the internet will be encrypted and almost impossible to read by any hackers.

## 7: Protect Admin Htaccess File

Htaccess file is one of the most important yet most powerful file, which can control the behavior of his website and possess the power to even redirect his entire website to a different one. This type of attacks becomes more popular these days, in this attack a malicious hacker will inject a redirection code to a malicious website. It is simple, as we said earlier do not assign full permissions to his htaccess file or he can write this below piece of code in his htaccess file which do not let any others access your htaccess file.

```
Files ~ “^.*.([Hh][Tt][Aa])”>
```

```
order allow, deny
```

```
deny from all
```

```
satisfy all
```

```
</Files>
```

The above code will protect his htaccess file from being accessed by others and will not let hackers inject any malicious code.

## 8: Keep Admin Home or Office PC Secure

In a recent survey it is disclosed that 30 to 40% of the malicious files are uploaded by the webmasters themselves. If his system is infected with the virus then obviously the next job of that virus to make sure that it will inject the malicious code in his web pages while the user are trying to upload them or send his login credentials to the remote hacker so he can take care of the rest. So always keep his PC clean and scan it daily with an updated antivirus program. Check for any unusual behavior before uploading his files.

#### 9: Secure Admin Private and Admin Areas with IP Restrictions

It is always recommended to secure his private areas with IP restrictions or at least with an SSL encryption. IP restriction is a bit way advanced yet effective method to stop the unauthorized personnel to access a particular area of his website. If the user have a static IP at his home or office PC, it is recommend to set IP restrictions with .htaccess rule, so only his home or office PC can only access that particular area. Here is an example htaccess code to IP restrict the access to a particular location.

```
# ALLOW USER BY IP
```

```
<Limit GET POST>
```

```
order deny,allow
```

```
deny from all
```

```
allow from 1.2.3.4
```

```
</Limit>
```

The above code restrict all other users from accessing a particular area except that allowed IP (ex: 1.2.3.4). he can replace that IP address with his and place that htaccess in the folder which he want to restrict from public access.

## 10: Change Admin Database Table Prefix

If the admin have a dynamic website with back-end database support, then it is recommended to use a different table prefix than a default one comes with his application. Also if he have a raw tables without any prefixes then it is important to add a prefix which hard to guess, this will ensure that no one can able to guess what is his database username, so there is no point of hacking the password. they also recommend he to please use strong passwords for his database users, do not use same password for all the users. Make sure that each of his password is unique and absolutely strong.

## 11: Try to have Admin Own Virtual Private Server

Having his own virtual private server (VPS) is always an added advantage, The admin can define his own rules and he will have his own server with the choice of his own OS like Windows VPS and Linux VPS. This will enable additional layer of security and make all his data placed in his own server. This may not be a security measure, but worth trying. Because he will get a lot of advantages like writing his own rules installing all type of security applications etc. [10][12]

## 2.2 The Secure Shell (SSH)

SSH, the Secure Shell, is a popular, powerful, software-based approach to network security. Whenever data is sent by a computer to the network, SSH automatically encrypts it. When the data reaches its intended recipient, SSH automatically decrypts (unscrambles) it.

The result is transparent encryption: users can work normally, unaware that their communications are safely encrypted on the network. In addition, SSH

uses modern, secure encryption algorithms and is effective enough to be found within mission-critical applications at major corporations.

"SSH" is pronounced by spelling it aloud: S-S-H. You might find the name "Secure Shell" a little puzzling, because it is not, in fact, a shell at all. The name was coined from the existing rsh utility, a ubiquitous Unix program that also provides remote logins but is very insecure.

SSH has a client/server architecture, as shown in Figure 2-1. An SSH server program, typically installed and run by a system administrator, accepts or rejects incoming connections to its host computer. Users then run SSH client programs, typically on other computers, to make requests of the SSH server, such as "Please log me in," "Please send me a file," or "Please execute this command." All communications between clients and servers are securely encrypted and protected from modification.[12]

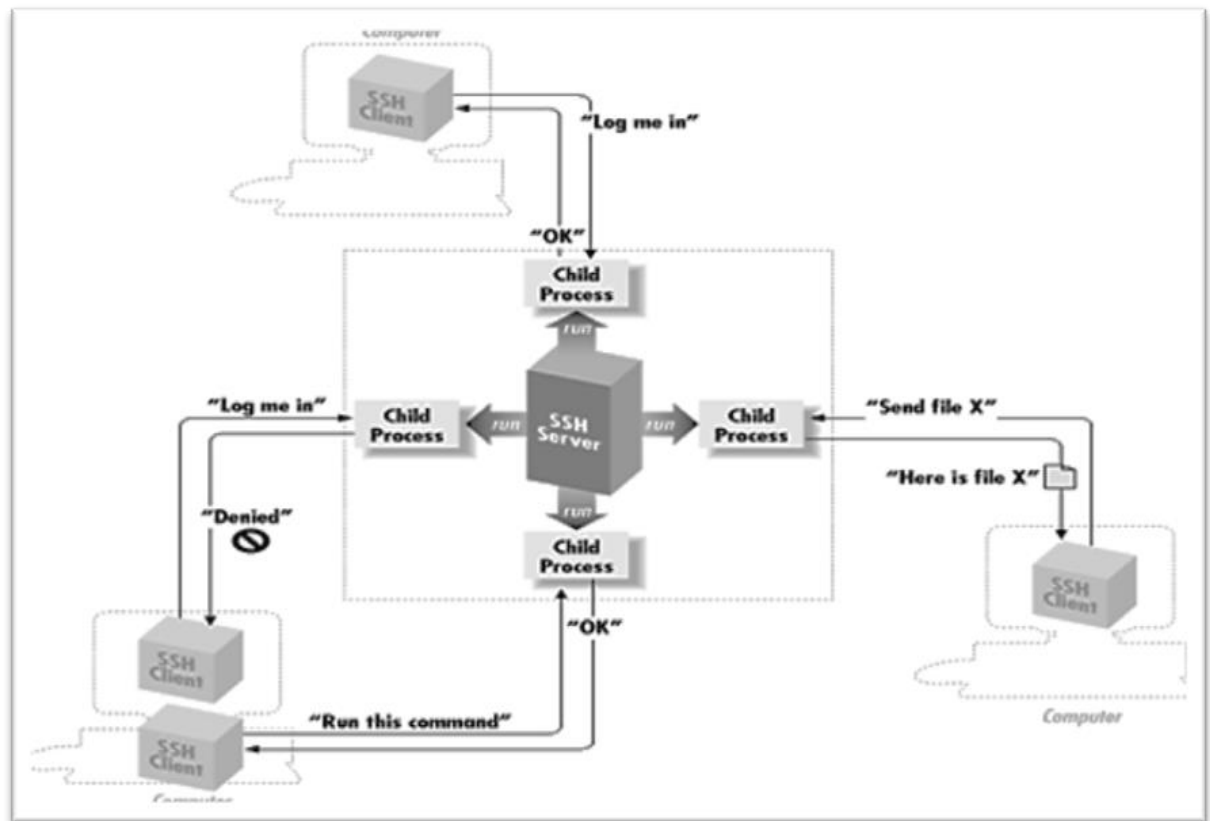


Figure 2-1. SSH Architecture

### 2.2.1 The SSH Protocol

SSH is a protocol, not a product. It is a specification of how to conduct secure communication over a network. Although we say "the SSH protocol," there are actually two incompatible versions of the protocols in common use: SSH-1 and SSH-2. The SSH protocol covers authentication, encryption, and the integrity of data transmitted over a network, as shown in Figure 2-2. Let's define these terms:

- **Authentication**

Reliably determines someone's identity. If the user try to log into an account on a remote computer, SSH asks for digital proof of his identity. If he pass the test, he may log in; otherwise SSH rejects the connection.



- Encryption

Scrambles data so it is unintelligible except to the intended recipients. This protects user data as it passes over the network.

- Integrity

Guarantees the data traveling over the network arrives unaltered. If a third party captures and modifies his data in transit, SSH detects this fact.

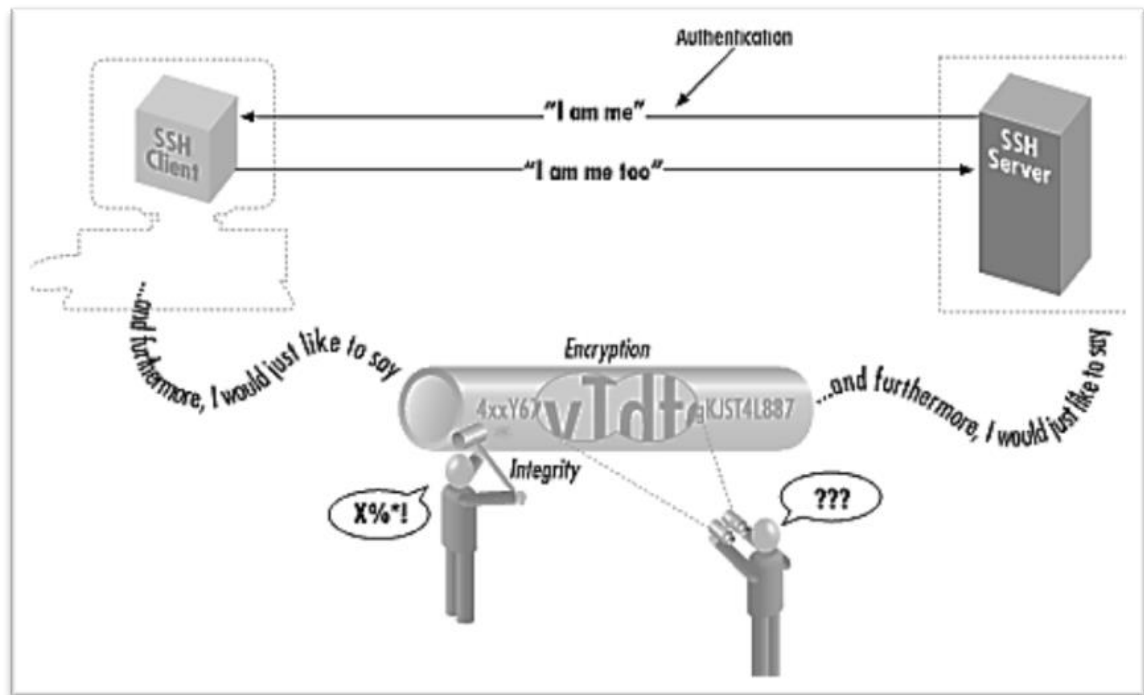


Figure 2-2. Authentication, Encryption, and Integrity

In short, SSH makes network connections between computers, with strong guarantees that the parties on both ends of the connection are genuine. It also ensures that any data passing over these connections arrives unmodified and unread by eavesdroppers.[13]

### **2.2.2 SSH and IP tables**

With SSH and IPtables, you have two easy ways to access hosts and services inside your network from the outside world without exposing them directly. First, The admin can run SSH on the firewall and use SSH's port forwarding feature to access internal hosts and services from the outside, without exposing them directly to the outside. Second, he can use IPtables Destination Network Address Translation to expose SSH for multiple servers as distinct ports on the firewall's public IPaddress, with the connections forwarded to the individual hosts inside the network.

### **2.3 IPaddress**


An IP address consists of four numbers, each of which contains one to three digits, with a single dot (.) separating each number or set of digits. Each of the four numbers can range from 0 to 255. Here's an example of what an IP address might look like: 78.125.0.209. This innocuous-looking group of four numbers is the key that empowers the user to send and retrieve data over the Internet connections, ensuring that their messages, as well as our requests for data and the data they've requested, will reach their correct Internet destinations. Without this numeric protocol, sending and receiving data over the World Wide Web would be impossible.

IP addresses can be either static or dynamic. Static IP addresses never change. They serve as a permanent Internet address and provide a simple and reliable way for remote computers to contact he. Static IP addresses reveal such information as the continent, country, region, and city in which a computer is located; the ISP (Internet Service Provider) that services that particular computer; and such technical information as the precise latitude and longitude of the country, as well as the locale, of the computer. Dynamic IP addressing

assigns a different IP address each time the ISP customer logs on to their computer, but this is dependent upon the Internet Service Provider (ISP) because some ISP's only change the IP address as they deem it necessary. The biggest advantages of Dynamic IP Addressing are less security risk as the computer is assigned a new IP address each time the customer logs on, they are cost effective and there is automatic network configuration (the less human intervention with network configuration the better). Dynamic addressing is usually used by ISP's so that one IP address can be assigned to several users, however some ISP's use Sticky Dynamic IP Addressing and do not change the IP address very often. Dynamic IP Addressing can be used by families with several computers or by a small business owner who has a home office.[14]

## **2.4 Firewall**

A firewall can help prevent hackers or malicious software (such as worms) from gaining access to his computer through a network or the Internet. A firewall can also help stop his computer from sending malicious software to other computers. The admin can customize four settings for each type of network location in windows firewall. To find these settings, follow these steps:

- Open Windows Firewall by clicking the Start button  of the Start button, and then clicking Control Panel. In the search box, type firewall, and then click Windows Firewall. In the left pane, click Turn Windows Firewall on or off. Administrator permission required If the user is prompted for an administrator password or confirmation, type the password or provide confirmation.

Here's what the settings do and when The admin should use them.

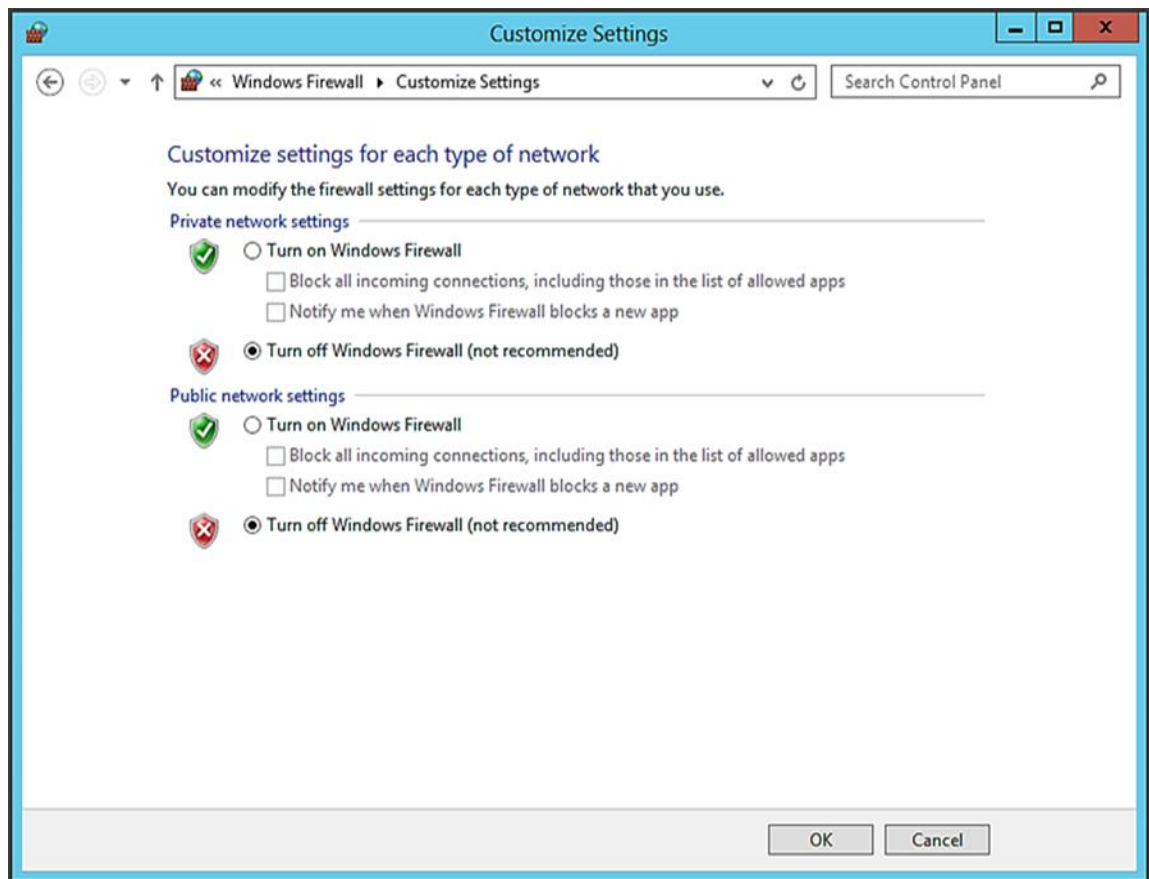


Figure 2-3 Customize Setting for Firewall

- Turn on Windows Firewall

This setting is selected by default. When Windows Firewall is on, most programs are blocked from communicating through the firewall. If the admin want to allow a program to communicate through the firewall, he can add it to the list of allowed programs. For example, he might not be able to send photos in an instant message until he add the instant messaging program to the list of allowed programs. To add a program to the list, see Allow a program to communicate through Windows Firewall.

- Block all incoming connections, including those in the list of allowed programs

This setting blocks all unsolicited attempts to connect to his computer. Use this setting when the user need maximum protection for his computer, such as when he connect to a public network in a hotel or airport, or when a computer worm is spreading over the Internet. With this setting, he isn't notified when Windows Firewall blocks programs, and programs in the list of allowed programs are ignored. When he block all incoming connections, he can still view most webpages, send and receive e-mail, and send and receive instant messages.

- Notify his when Windows Firewall blocks a new program

If the admin select this check box, Windows Firewall will inform he when it blocks a new program and give he the option of unblocking that program.

- Turn off Windows Firewall (not recommended)

Avoid using this setting unless admin has another firewall running on his computer. Turning off Windows Firewall might make his computer (and his network, if he have one) more vulnerable to damage from hackers and malicious software.[15]

## **2.5 Administration**

Only authorized administrators can log into the Admin Interface. An authorized administrator is a user who has the admin role. Authorized administrators have access to all administrative tasks in website; therefore, authorized administrators are trusted personnel and are assumed to be non-hostile, appropriately trained, and follow proper administrative procedures. To access the Admin Interface, complete the following procedure:

1. Open the following URL in a browser:

http://localhost:8001/

Note: If user are not accessing the Admin Interface from the same system on which Website is running, he will have to use the IP address or domain name of the server instead of localhost.

2. Log in with his admin user name and password. The summary screen for the Admin Interface displays.

Note: If he has already logged on as an admin user during this session, he do not have to log in again.

### **2.5.1 Overview of the Admin Interface**

With the Admin Interface, the user can complete any of the following tasks:

- Manage basic software configuration.
- Create and configure groups.
- Create and manage databases.
- Create and manage new forests.
- Backup and restore forest content.
- Create and manage new web server and Java-language access paths.
- Create and manage security configurations.
- Tune system performance.
- Configure namespaces and schemas.
- Check the status of resources on his systems.[16]

## 2.6 Web Traffic Security Approaches

A number of approaches to providing Web security are possible. The various approaches that have been considered are similar in the services they provide and to some extent, in the mechanisms that they use, but they differ with respect to their scope of applicability and their relative location within the TCP/IP protocol stack. Figure 1 illustrates this difference. One way to provide Web security is to use IP security (IPsec) (Figure 2-4). The advantage of using IPsec is that it is transparent to end users and applications and provides a general-purpose solution. Furthermore, IPsec includes a filtering capability so that only selected traffic need incur the overhead of IPsec processing.[11]

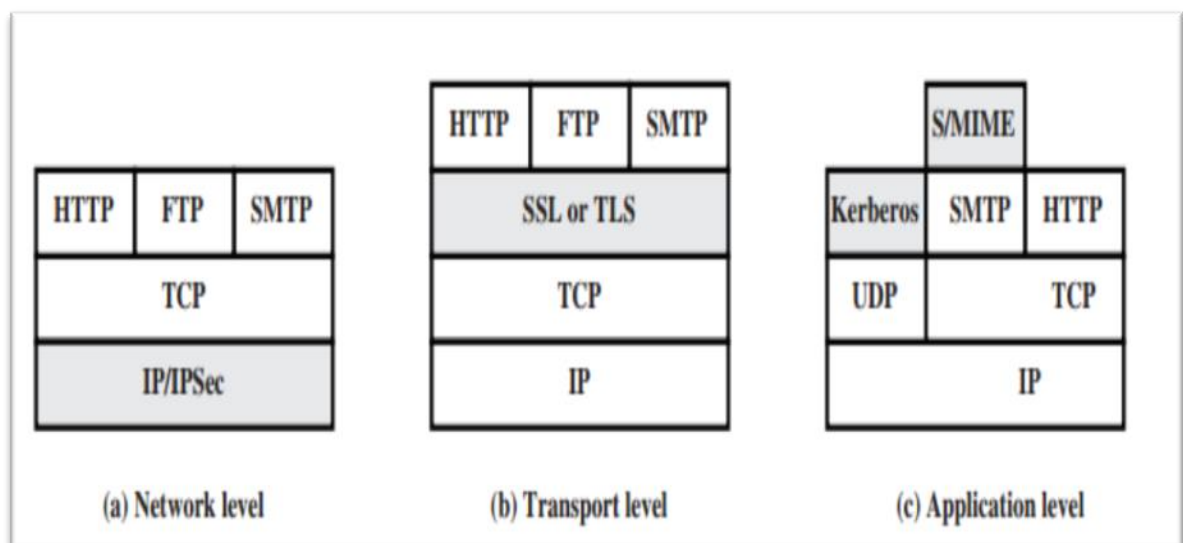


Figure 2-4 Relative Location of Security Facilities in the TCP/IP Protocol Stack.

*Chapter Three*

*Project Design and  
Implementation*



### **3.1 Introduction**

This chapter presents the results of the project, and how will design control panel to protect the files contained within the website to prevent unauthorized access to it and how to protect access to the Control Panel by creating a login form design using lamp open source software package with Ubuntu operating system version 14.04lts.

### **3.2 Design Admin Login Script with PHP and MySQL**

We will design login form for admin to enter to the admin panel control and secure this login form against various attackers.

#### **3.2.1 Requirements for Design Login Webpage**

- HTML
- CSS
- PHP
- MySQL
- LAMP Server

#### **3.2.2 Topics on Which This Design Touches**

##### **1- Security Topics**

- How to prevent SQL injection exploits when using user-supplied data in a SQL query.
- How to prevent XSS attacks when displaying user-supplied data on a web page.
- How to securely store passwords in a database.
- How to securely redirect a user to another web page.

## 2-Database Interaction Topics

- How to connect to a MySQL database using PHP
- How to insert a new row of data in the database (INSERT query)
- How to fetch a list of data from the database and display it in a table (SELECT query)
- How to check whether a particular value already exists in the database

## 3 -Login System Specific Topics

- How to check whether an admin is logged in or not, and force them to be logged in to view a particular page.
- How to build a login form.

### 3.2.3 Step of Design Login Webpage

#### Step 1: Create Login.php

This file contains html form with three input box which will take admin name and password and confirm password entered by admin and then after submitting the form, the php code will match that admin name and password combination in database and when it finds both results in table then it will allow admin to access home page else it will show appropriate message.

```
<html>
<head>
<title>
noor
</title>
<link rel="stylesheet" type="text/css" href="style.css">
</head>
<body>
<div id="main">
<div id="login">
<h2>Login Form</h2>
<form action="" method="POST">
<label>AdminName :</label>
<input id="name" name="admin" placeholder="username" type="text">
<label>Password :</label>
<input id="password" name="pass" placeholder="*****" type="password">
<label>conf:</label>
<input id="password" name="conf" placeholder="*****" type="password"> <br />
<input name="log" type="submit" value=" sign-in " />
</form>
</div>
</div>
</body>
</html>
```

Figure (3-1): HTML Code of Login Form.

**Login Form**

AdminName :  Password :  conf:

Figure (3-2): Login Webpage output

## Step2: Style.css

Use CSS style on the webpage to create some attraction to login webpage.

```
#main {
width:960px;
margin:50px auto;
font-family:raleway;
}

h2 {
background-color:#FEFFED;
text-align:center;
border-radius:10px 10px 0 0;
margin:-10px -40px;
padding:15px;
}

#login {
width:300px;
float:left;
border-radius:10px;
font-family:raleway;
border:2px solid #ccc;
padding:10px 40px 25px;
margin-top:70px;
}
```

Figure (3-3): CSS Code of Login Form

**Login Form**

AdminName :

Password :

conf:

Figure (3-4): Login Webpage after Applying CSS Style .

### Step 3: Creating Table in Database of Login Form

#	Name	Type	Collation	Attributes	Null	Default	Extra	Action
1	adminName	varchar(250)			No	None		Change  Drop  Primary  Unique  Index  Spatial  More
2	password	varchar(250)			No	None		Change  Drop  Primary  Unique  Index  Spatial  More
3	conf	varchar(250)			No	None		Change  Drop  Primary  Unique  Index  Spatial  More

Figure (3-5): Create Table

### Step 4: Inserting Data to the Table

adminName	password	conf
noor	cb57ecb84e74770b86295c2245543f63b2b22ec4202cb962ac...	cb57ecb84e74770b86295c2245543f63b2b22ec4202cb962ac...

Figure (3-6): Insert Data to the Table

### Step 5: Create Database Connection

Connection database with login form to check admin name and password.

```
$connectdb=mysql_connect("127.0.0.1","root","");  
mysql_select_db("loggg") or die("cannot connect");
```

Figure (3-7): Database Connection Code.

### Step 6: Check login.PHP

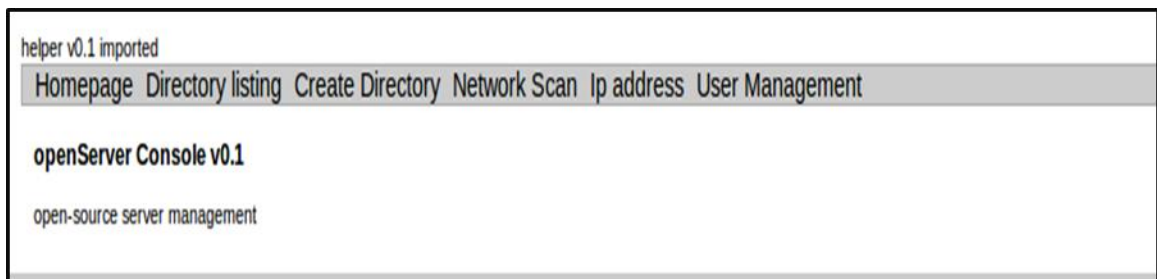
When an admin submit their admin name and password, PHP code in checklogin.php as shown in figure (3-8) will check the admin name and password. If the admin has the right admin name and password, it will allow admin to access home page show in figure (3-9), if admin name or password is wrong the system will then show a message as in figure (3-10), if the admin enters a password not equal confirm will then show a message as in figure (3-

11) and also when the admin forget one of fields empty will then show a message as in figure (3-12).



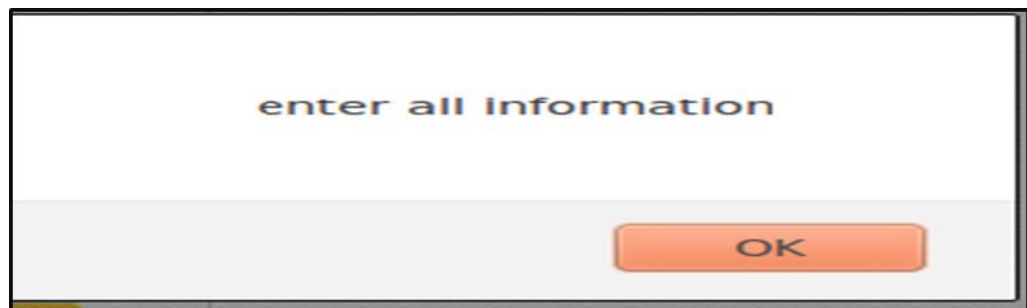
The image shows a login form titled "Login Form" in a yellow header. Below the header, there are three input fields. The first is labeled "AdminName :" and contains the text "noor". The second is labeled "Password :" and contains three dots. The third is labeled "conf:" and contains three dots and a vertical bar. Below these fields is a yellow button labeled "sign-in".

Figure (3-8): Check Login.



The image shows a web application interface. At the top, it says "helper v0.1 imported". Below that is a navigation bar with links: "Homepage", "Directory listing", "Create Directory", "Network Scan", "Ip address", and "User Management". Below the navigation bar, it says "openServer Console v0.1" and "open-source server management".

Figure (3-9): Homepage Admin Panel.



The image shows a dialog box with the text "enter all Information" in the center. At the bottom right, there is an orange button labeled "OK".

Figure (3-10): Enter all Information.

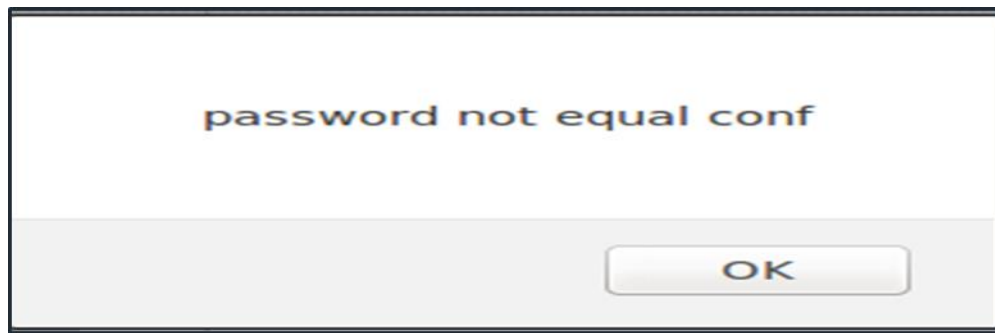


Figure (3-11): Password not Equal Confirm



Figure (3-12): Wrong Admin Name and Password

### **3.3 The Admin Panel Modules.**

Design admin panel control contain many forms (listing directory, create directory, scan network and IP address) design as forms making easy work and correction error if happen in some place.

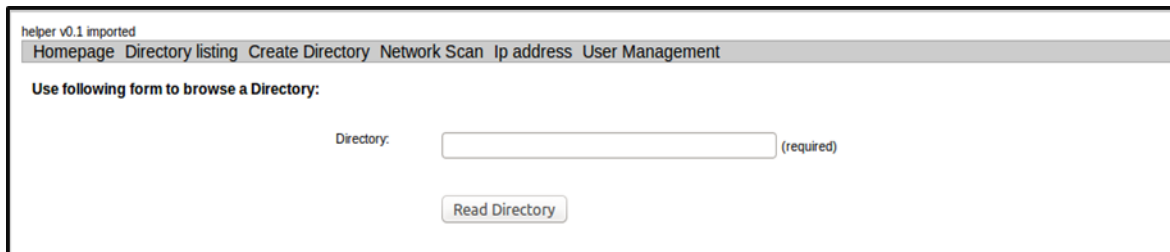
#### **3.3.1 Requirements for Design Admin Panel Control:**

- HTML
- CS
- PHP
- LAMP server

### 3.2.3 Step of Design Admin Panel Control

#### Step 1: Create Directory Listing Form.

This form lists directory contents of files and directories with (ls command), is a Linux shell command. Directory listing form show in figure (3-13), when admin enter directory list all the file and directory of path /var/www/html show in figure (3-14), when admin not enter directory will show message in figure(3-15) ,also when admin enter error directory will show message in figure (3-16). There are other ls command options show in figure (3-17).



helper v0.1 imported

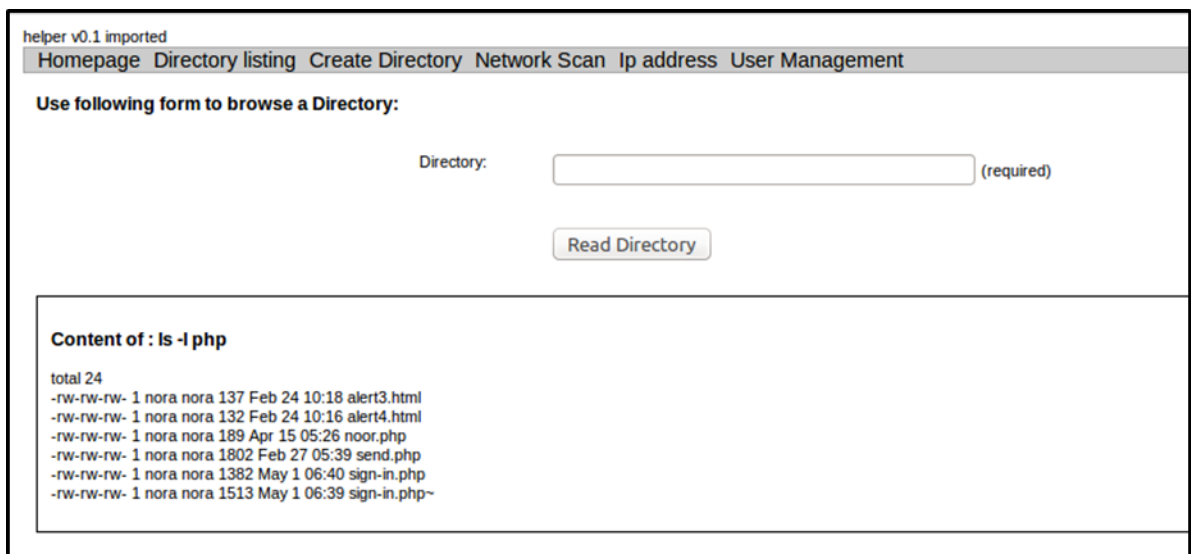
Homepage Directory listing Create Directory Network Scan Ip address User Management

Use following form to browse a Directory:

Directory:  (required)

Read Directory

Figure(3- 13): Directory Listing Form.



helper v0.1 imported

Homepage Directory listing Create Directory Network Scan Ip address User Management

Use following form to browse a Directory:

Directory:  (required)

Read Directory

Content of : ls -l php

```
total 24
-rw-rw-rw- 1 nora nora 137 Feb 24 10:18 alert3.html
-rw-rw-rw- 1 nora nora 132 Feb 24 10:16 alert4.html
-rw-rw-rw- 1 nora nora 189 Apr 15 05:26 noor.php
-rw-rw-rw- 1 nora nora 1802 Feb 27 05:39 send.php
-rw-rw-rw- 1 nora nora 1382 May 1 06:40 sign-in.php
-rw-rw-rw- 1 nora nora 1513 May 1 06:39 sign-in.php~
```

Figure (3-14): Content of Directory.

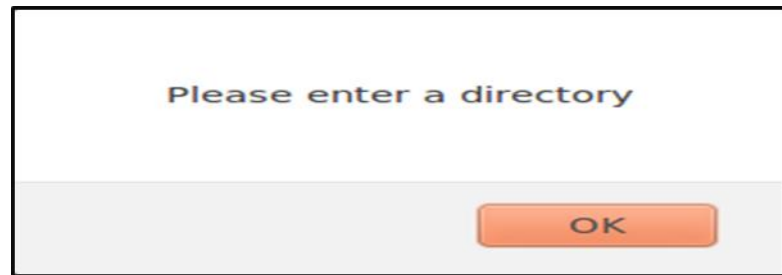


Figure (3-15): Enter Directory



Figure (3-16): System Error Message.

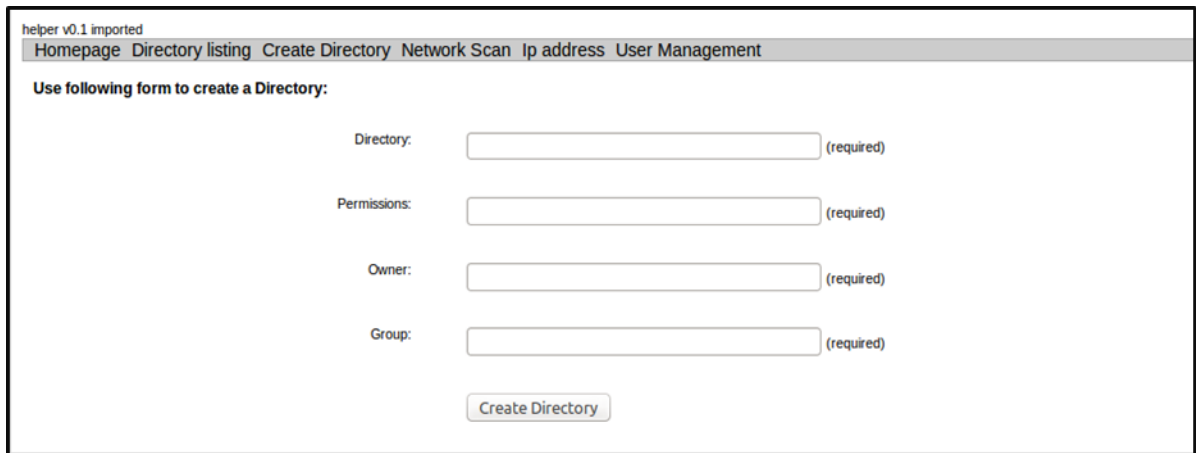
option	description
<code>ls -a</code>	list all files including hidden file starting with '.'
<code>ls --color</code>	colored list [=always/never/auto]
<code>ls -d</code>	list directories - with ' */'
<code>ls -F</code>	add one char of */=>@  to enteries
<code>ls -i</code>	list file's inode index number
<code>ls -l</code>	list with long format - show permissions
<code>ls -la</code>	list long format including hidden files
<code>ls -lh</code>	list long format with readable file size
<code>ls -ls</code>	list with long format with file size
<code>ls -r</code>	list in reverse order
<code>ls -R</code>	list recursively directory tree
<code>ls -s</code>	list file size
<code>ls -S</code>	sort by file size
<code>ls -t</code>	sort by time & date
<code>ls -X</code>	sort by extension name

Figure (3-17): ls Command Options [17].



## Step 2: Create Directory Form.

In this form creating a new directory and determining permissions and add user and group to this directory. Create directory form shown in figure (3-18) when an admin enter correct information of directory as in figure (3-19) show the output (created directory) in figure (3-20), when an admin enter error information will show message in figure (3-21) and also if admin forget one of fields empty will show message in figure (3-22).



The screenshot shows a web application interface for creating a directory. At the top, there is a navigation bar with the following links: [Homepage](#), [Directory listing](#), [Create Directory](#), [Network Scan](#), [Ip address](#), and [User Management](#). Below the navigation bar, the text "Use following form to create a Directory:" is displayed. The form consists of four labeled input fields, each followed by "(required)":

- Directory:
- Permissions:
- Owner:
- Group:

At the bottom of the form, there is a button labeled "Create Directory".

Figure (3- 18): Create Directory Form.

helper v0.1 imported

Homepage Directory listing Create Directory Network Scan Ip address User Management

Use following form to create a Directory:

Directory:  (required)

Permissions:  (required)

Owner:  (required)

Group:  (required)

Figure (3-19): Directory Information.

helper v0.1 imported

Homepage Directory listing Create Directory Network Scan Ip address User Management

Use following form to create a Directory:

Directory:  (required)

Permissions:  (required)

Owner:  (required)

Group:  (required)

Directory created :noor

Figure (3-20): Directory Created.

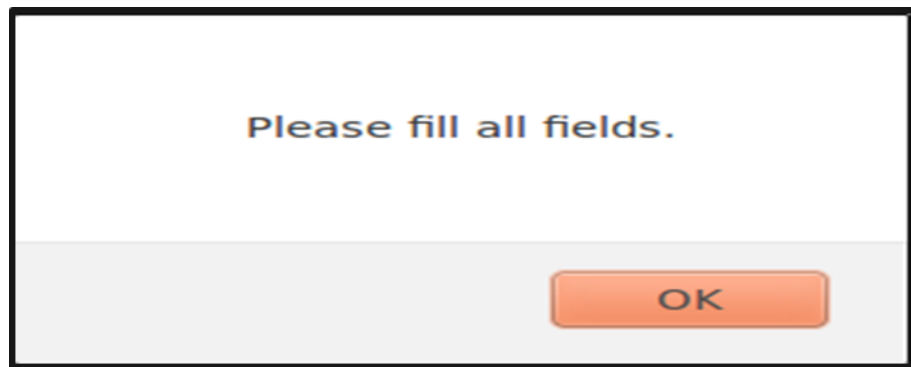


Figure (3-21): POP Message for Invalid Directory Information.



Figure (3-22): Error Message.

### **File Permissions.**

Linux uses the same permissions scheme as UNIX. Each file and directory on your system is assigned access rights for the owner of the file, the members of a group of related users, and everybody else. Rights can be assigned to read a file, to write a file, and to execute a file (i.e., run the file as a program) [18]. In the diagram show in figure (3-23) we see how the first portion of the listing is interpreted. It consists of a character indicating the file type, followed by three sets of three characters that convey the reading, writing and execution permission for the owner, group, and everybody else [19].

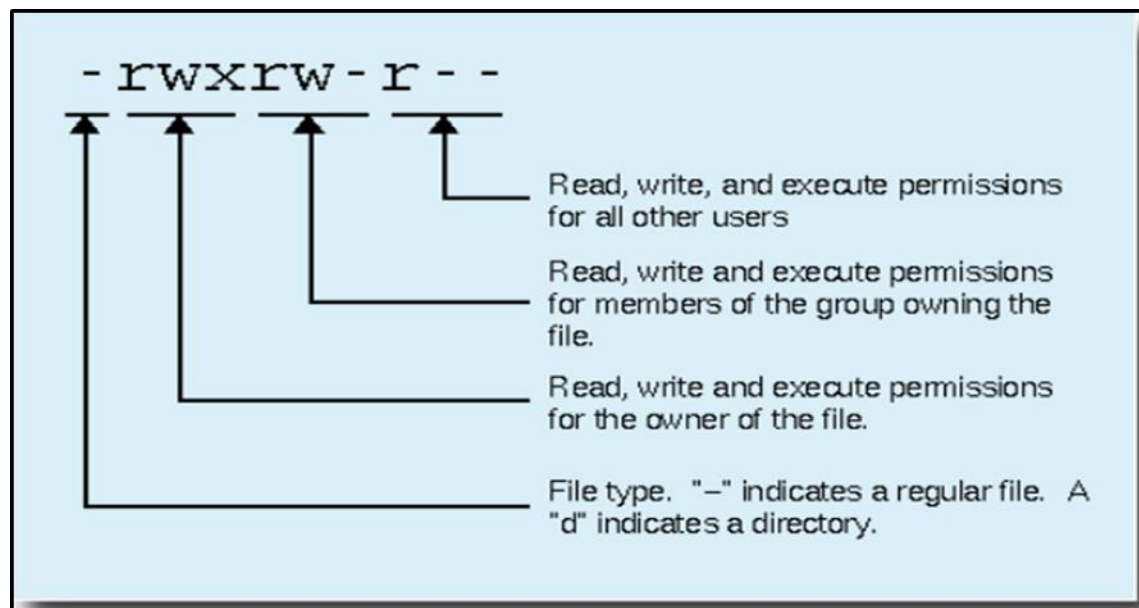


Figure (3-23): File Permission.

### User and Group.


Linux/Unix operating systems have the ability to multitask in a manner similar to other operating systems. However, Linux's major difference from other operating systems is its ability to have multiple users. Linux was designed to allow more than one user to have access to the system at the same time. In order for this multiuser design to work properly, there needs to be a method to protect users from each other. This is where permissions come in to play [20].

### Step 3: Create Network Scan Form

This form scan network for live hosts using Nmap Network exploration tool and security scanner. Network scan form shown in figure (3-24). When admin enter IP network and netmask as in figure (3-25) show the output of host connection on the network in figure (3- 26) and also if admin forget one of fields empty will show message in figure (3-27).

## Nmap:

(Network Mapper) is a security scanner originally written by Gordon Lyon used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses [21].



helper v0.1 imported

Homepage Directory listing Create Directory Network Scan Ip address User Management

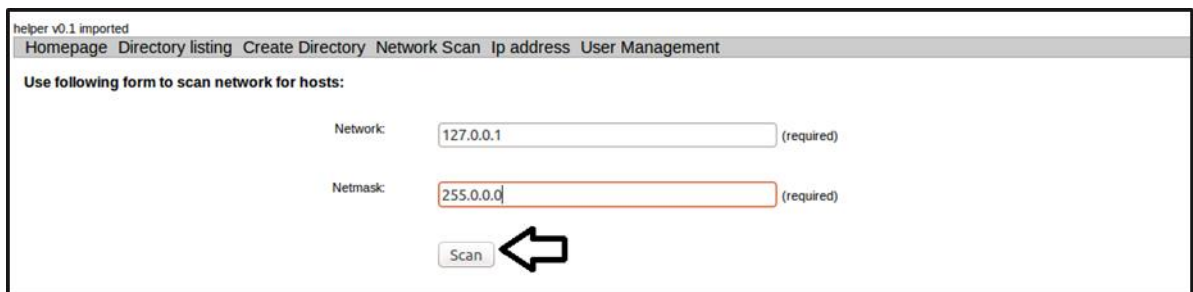
Use following form to scan network for hosts:

Network:  (required)

Netmask:  (required)

Scan

Figure (3-24): Network Scan Form.



helper v0.1 imported

Homepage Directory listing Create Directory Network Scan Ip address User Management

Use following form to scan network for hosts:

Network:  (required)

Netmask:  (required)

Scan

Figure (3-25): Netmask Scan.

Figure (3-26): Results of Netmask Scan.

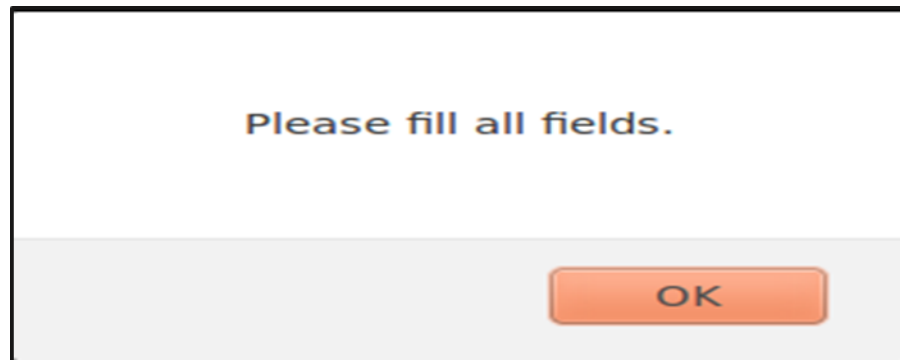


Figure (3-27): POP Message for Invalid Input Scan.

### Step 3: Create IP Address Form

This form is used for packet filtering using filter table to redirect IP address Input, drop IP or accept IP or forward it. IP address form show in figure (3-28). Admin use INPUT chain to accept packet coming into the system, the admin enter the IP as figure (3-29) and click button accept the output allow to IP address to exist in admin system as figure (3-30) and admin use INPUT chain to drop packet coming into the system, the admin enter the IP as figure (3-31) and if he click button drop that mean the system cannot accept or forward this IP as figure (3-32) and also Admin accept packet and forward packet the admin enter the IP as figure (3-33) and click button

forward the output forward the IP to other net as figure (3-34) and if admin enter corrupt IP will show error message that content notification for admin to enter the IP in figure(3-35).

The screenshot shows a web application interface with a header bar containing the text "helper v0.1 imported" and a navigation menu with links: "Homepage", "Directory listing", "Create Directory", "Network Scan", "Ip address", and "User Management". The "Ip address" link is highlighted. Below the header, there is a label "IP address:" followed by an empty text input field and the text "(required)". At the bottom, there are three buttons: "DROP", "ACCEPT", and "FORWORD".

Figure (3-28): IP Address Form.

This screenshot is similar to the previous one, but the text input field now contains the IP address "202.54.1.1". The "ACCEPT" button is highlighted with a red border, indicating it has been selected.

Figure (3-29): The IP Accept.

This screenshot shows the same interface, but with a message box at the bottom that reads "the ip accept : 202.54.1.1". The "ACCEPT" button remains highlighted.

Figure (3-30):.The Result of IP Accept.

helper v0.1 imported

Homepage Directory listing Create Directory Network Scan Ip address User Management

IP address:  (required)

Figure (3-31): The IP Drop.

helper v0.1 imported

Homepage Directory listing Create Directory Network Scan Ip address User Management

IP address:  (required)

the ip drop : 10.10.10.10

Figure (3-32): The Result of IP Drop.

helper v0.1 imported

Homepage Directory listing Create Directory Network Scan Ip address User Management

IP address:  (required)

Figure (3-33): The IP Forward.

helper v0.1 imported

Homepage Directory listing Create Directory Network Scan Ip address User Management

IP address:  (required)

the ip forward : 192.168.0.0



Figure (3-34): The Result of IP Forward.

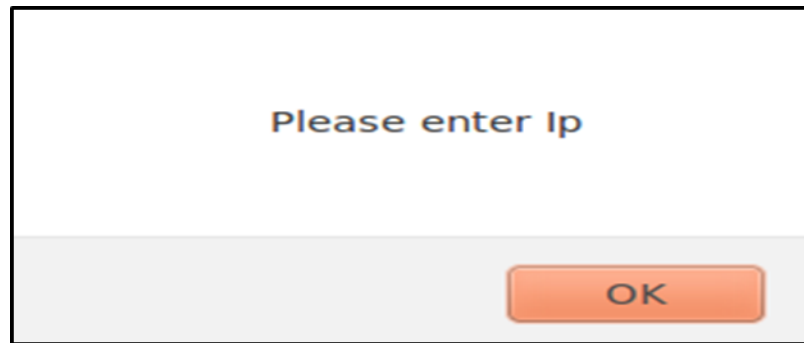


Figure (3-35): Notification For Admin to Enter IP.

# *Chapter Four*

## *Conclusion and Future Work*

## 4-1 Conclusion

We conclude from our work:

In this work an attempt is made to design the admin control panel that built with robust security programming and tools. From the result which was done on some selected IP, a number of conclusion remarks Were drawn:

- 1-Easy to use for administration.
- 2- Prevent unauthorized users gain access to the sensitive data.
- 3- The Admin prevents the attacker that can used some attacks tools such as XSS, SQL injection and password crack to attack and access the admin control panel .
- 4- Create new directories, determine permissions, add user and group to this directories to prevent other owner to have full permission on this file.
- 5-Scan network button allow admin to search in the network about the numbers of IP, IP types and the times of IP that try to connection to the website. This button is useful for admin to do the search process to choose which IP is accept and which is been drop that mean not allow to exist in the system.
- 6- The admin can take the advantage of IP address button to specify which IP address that may be cause harm to the system, and then the admin could be drop the IP that try to connect with system for many times.

#### **4-2 Suggestion and Future work:**

The following are our recommendation for the future work:

Our suggestion for the future students is to design this system (Admin control panel system) by using WAMP (Windows, Apache, MySQL, PHP) that depending on windows operating system.

## References

1. <https://www.techopedia.com/definition/26464/data-security> .
2. <http://homeworkstarter.com/2014/08/25/protection-vs-security/> .
3. [www.techopedia.com/definition/24377/web-application-security](http://www.techopedia.com/definition/24377/web-application-security) .
4. [docs.oracle.com/cd/E13211\\_01/wle/admin/intro.htm](http://docs.oracle.com/cd/E13211_01/wle/admin/intro.htm).
5. <https://www.iplocation.net/ip-address> .
6. Ssh- An Overview of the Secure Shell (SSH), 4848 tramway ridge dr. ne suite 101 Albuquerque, nm 87111.,2008.
7. <http://www.beyondsecurity.com/web-security-and-web-scanning.html> .
8. <https://www.dreamhost.com/blog/2013/05/22/php-security-user-validation-and-sanitization-for-the-beginner/> .
9. <http://ccss.usc.edu/499/lecture1.html> .
10. "How to Secure Your Website", 5th Edition, It Security Center (ISEC), April 2011, Japan.
11. "Cryptography and Network Security Principles and Practice ", William Stallings, FIFTH Edition, 2011.
12. <https://www.hostdepartment.com/blog/2013/06/06/top-10-ways-to-secure-your-website/> .
13. [http://docstore.mik.ua/orelly/networking\\_2ndEd/ssh/ch01\\_01.htm#ch0185](http://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch01_01.htm#ch0185)  
138 .
14. <http://whatismyipaddress.com/ip-address> .

15. <http://windows.microsoft.com/en-us/windows/understanding-firewall-settings#1TC=windows-7> .

16. Administrator's Guide Mark Logic, 8 February, Last Revised: 8.0-3, June, 2015.

17. <http://www.rapidtables.com/code/linux/ls.htm> .

18. <https://www.linode.com/docs/tools-reference/linux-users-and-groups> .

19. <http://linuxcommand.org/lts0070.php>.

20. <https://www.linode.com/docs/tools-reference/linux-users-and-groups> .

21. <https://en.wikipedia.org/wiki/Nmap> .