

WEB SECURITY: SETTING UP STUNGEYE BLOG SOFTWARE

RRC Polytech
Full Stack Web Development
Winnipeg, MB Canada

Motivation

- Hackers are (or could be) actually good, pleasant and extremely intelligent people who could keep computer criminals on the run (run away, escaping).

Ankit Fadia

How to setup **StungEye Blog** software?

Download blog software

- Download the “blog” software from the “Learn”
- Unzip the file and put in your Software folder

Table of Contents

321

Course Overview

11

Tips and Fixes

12

Module 1 - Ethical Hacking

12

Module 2 - VM Setup

40

Module 3 - SQL/XSS Injection

23

SQL Injections and Login Scripts

10

Add a description...

New ▾

Add Existing Activities ▾

Bulk Edit

blog

Zip Compressed File

Database Security

PowerPoint Presentation



Database Security

PowerPoint Presentation



PHP MairaDB login script with encryption tutorial

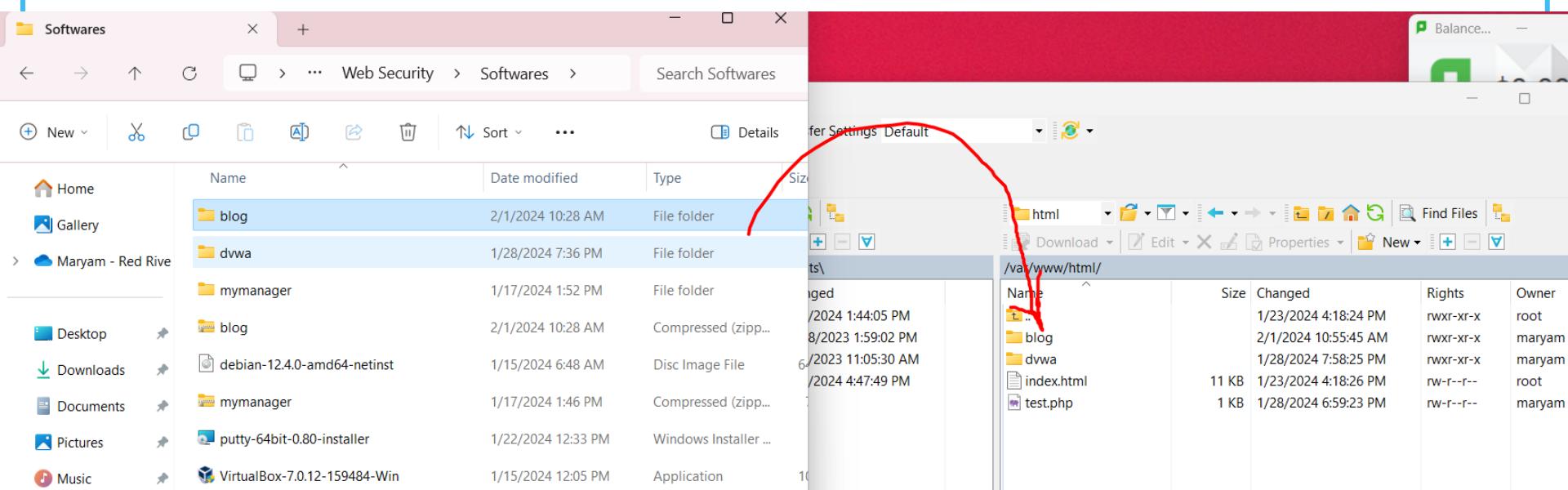
Word Document

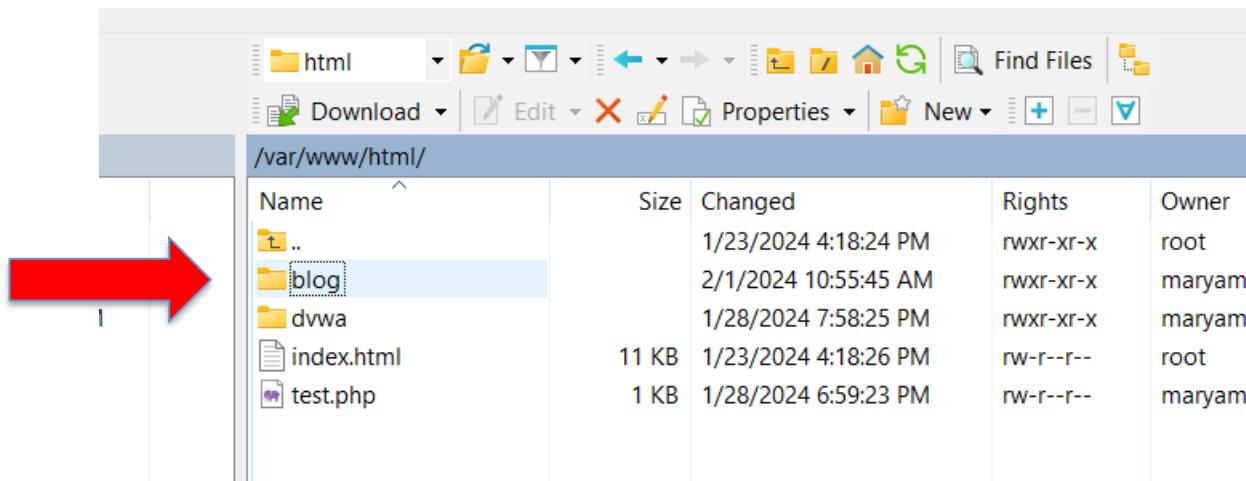


Database Security

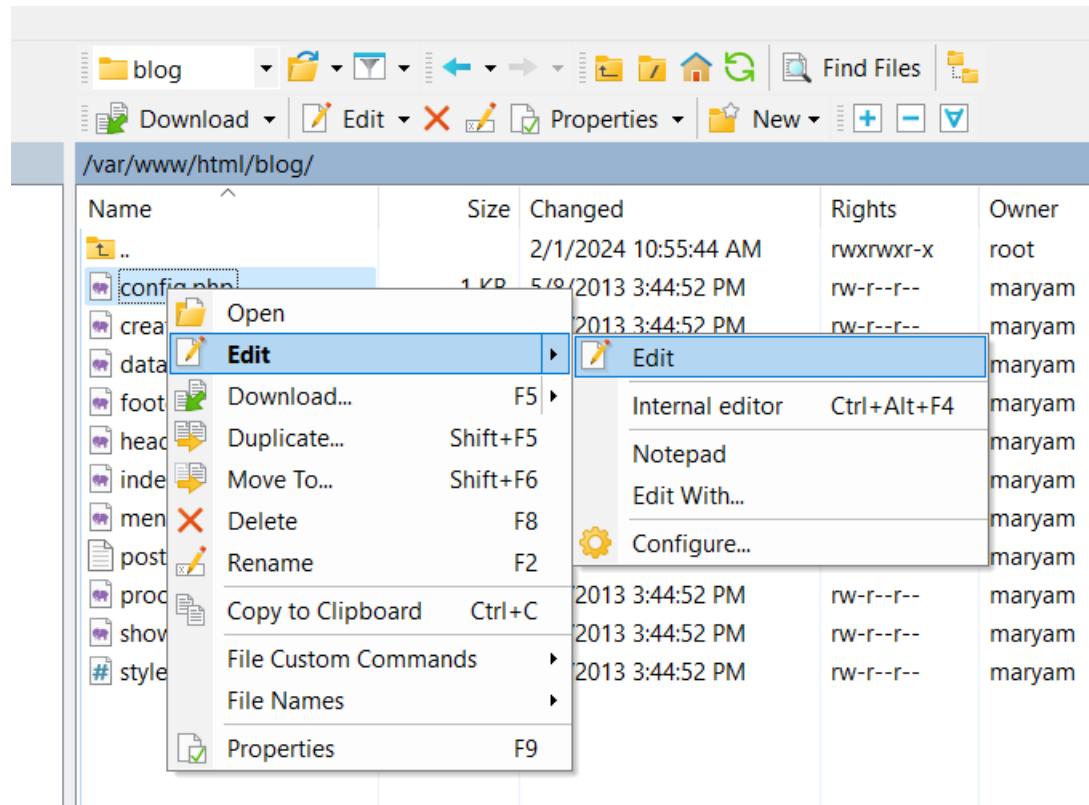
Zip Compressed File

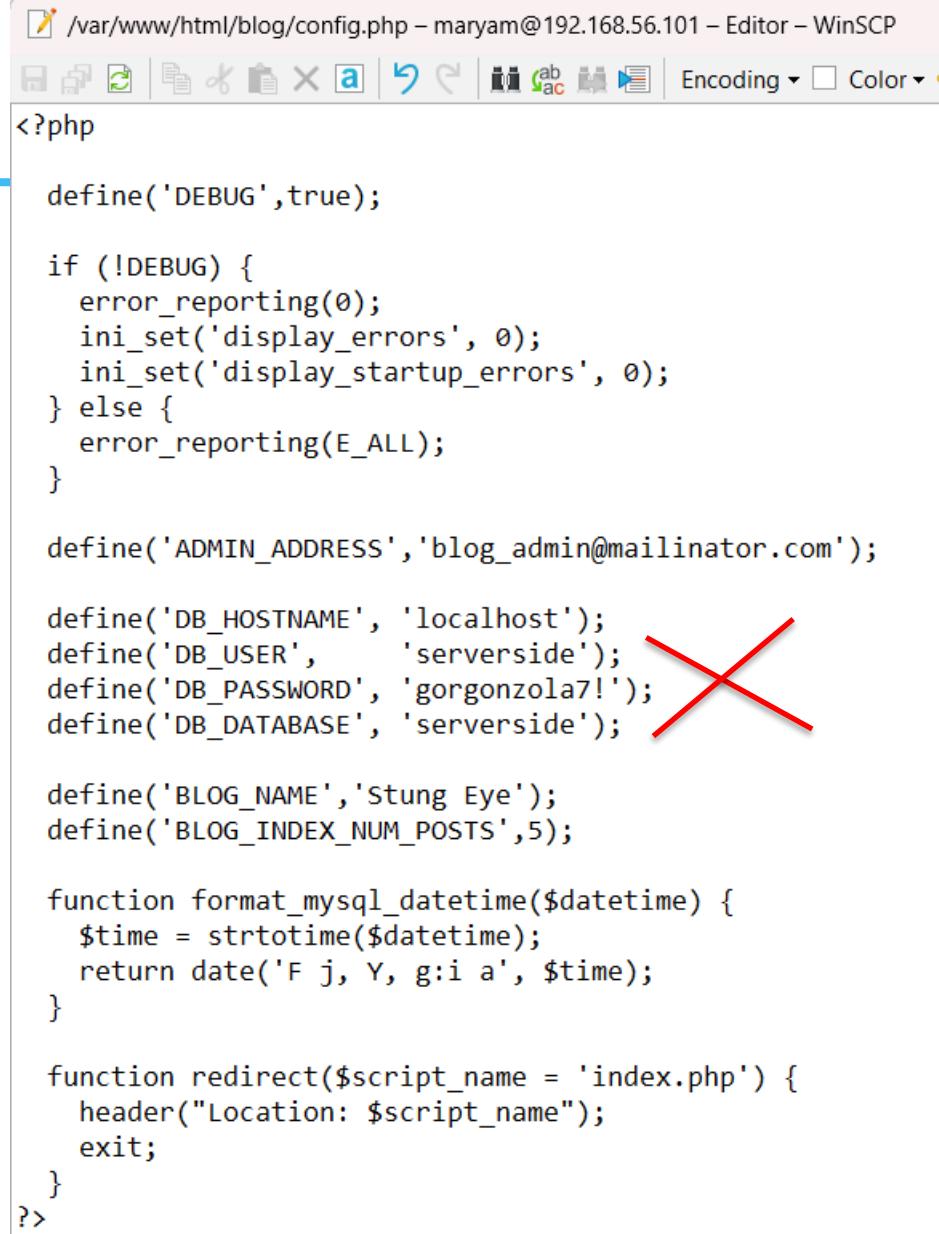
Drag the folder to WinSCP in html directory





Connect blog to Debian Server





The screenshot shows a WinSCP Editor window displaying a PHP configuration file named config.php. The file contains various defines and functions. A large red 'X' is drawn over the database connection definitions.

```
<?php

define('DEBUG',true);

if (!DEBUG) {
    error_reporting(0);
    ini_set('display_errors', 0);
    ini_set('display_startup_errors', 0);
} else {
    error_reporting(E_ALL);
}

define('ADMIN_ADDRESS','blog_admin@mailinator.com');

define('DB_HOSTNAME', 'localhost');
define('DB_USER',      'serverside');
define('DB_PASSWORD',  'gorgonzola7!');
define('DB_DATABASE',  'serverside'); X

define('BLOG_NAME','Stung Eye');
define('BLOG_INDEX_NUM_POSTS',5);

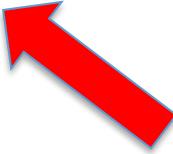
function format_mysql_datetime($datetime) {
    $time = strtotime($datetime);
    return date('F j, Y, g:i a', $time);
}

function redirect($script_name = 'index.php') {
    header("Location: $script_name");
    exit;
}
?>
```

Edit and Save

```
define('ADMIN_ADDRESS', 'blog_admin@mailinator.com');

define('DB_HOSTNAME', 'localhost');
define('DB_USER', 'bloguser');
define('DB_PASSWORD', 'password');
define('DB_DATABASE', 'blog');
```



It is important



Name	Size	Changed	Rights	Owner
..		2/1/2024 10:55:44 AM	rwxrwxr-x	root
config.php	1 KB	2/1/2024 11:22:54 AM	rw-r--r--	maryam
create.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
database.php	2 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
footer.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
header.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
index.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
menu.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
posts.sql	2 KB	5/8/2013 3:45:42 PM	rw-r--r--	maryam
process_post.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
show.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
style.css	2 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam

Open the Word File

- Download and open “PHP MairaDB login script with encryption tutorial.doc” file

Module 1 - Ethical
Hacking 12

Module 2 - VM Setup 37

Module 3 - SQL/XSS
Injection 23

SQL Injections and
Login Scripts 10

Database/XSS
Security 13

Module 4 - Privacy &
Secure Storage 36

Module 5 - Risks 75

Module 6 -
Pentesting 55



- blog Zip Compressed File ✓
- Database Security PowerPoint Presentation ✓
- Database Security PowerPoint Presentation ✓
- PHP MairaDB login script with encryption tutorial Word Document ✓
- Database Security Zip Compressed File ✓
- setup SQL File ✓
- php_login Zip Compressed File ✓

Debian (or PuTTY)

- In your command type (to prompt to root password)
 - ~\$ su –
 - Enter your password

```
maryam@deb:~$ su -  
Password:  
root@deb:~#
```



Step 1: Configure Database and Create Database and User If Necessary

➤ In PuTTY, login as **root**

➤ Type:

```
nano /etc/mysql/mariadb.conf.d/50-server.cnf
```

➤ press the **downward** key from keyboard

 maryam@deb: ~



The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Thu Feb 1 07:55:05 2024 from 192.168.56.1

maryam@deb:~\$ su -

Password:

root@deb:~# whoami

root

root@deb:~# nano /etc/mysql/mariadb.conf.d/50-server.cnf

```
GNU nano 7.2          /etc/mysql/mariadb.conf.d/50-server.cnf
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address        = 127.0.0.1

#
# * Fine Tuning
#
```

- nano /etc/mysql/mariadb.conf.d/50-server.cnf
- bind-address = 0.0.0.0

```
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address          = 0.0.0.0
#
# * Fine Tuning
#
```

Save (^ + o)

```
# When running under systemd, error logging goes via stdout/stderr to journald  
# and when running legacy init error logging goes to syslog due to  
Save modified buffer?  
Y Yes  
N No          ^C Cancel
```

Exit (^ + x)

```
GNU nano 7.2          /etc/mysql/mariadb.conf.d/50-server.cnf

# * Basic Settings
#
#user                  = mysql
pid-file              = /run/mysqld/mysqld.pid
basedir                = /usr
#datadir               = /var/lib/mysql
#tmpdir                = /tmp

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address           = 0.0.0.0

#
# * Fine Tuning

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line
```

```
root@deb:~# systemctl restart mysql.service
```

```
root@deb:~# systemctl restart mariadb.service
```

Use PuTTY

```
|root@deb:~# mysql -u root
```

```
MariaDB [(none)]> create database blog;  
Query OK, 1 row affected (0.002 sec)
```

Create Two Users “admin” & “user” and



Table of Contents > Module 3 - SQL/XSS Injection > SQL Injections and Login Scripts > PHP MairaDB login script with encryption tutorial

PHP MairaDB login script with encryption tutorial

A screenshot of a document editor or PDF viewer. On the left, there's a sidebar with a table of contents for a "PHP Login script tutorial" containing 13 items. The main content area shows a text block followed by several code snippets in a monospaced font. The code includes MySQL commands for logging in, creating a database, and granting privileges to users "bloguser" and "blogadmin".

that goes with it.

Log into the command line version of mysql:

```
mysql -u root
```

Once in MySQL command line utility (or more specifically, MariaDB), create a database with:

```
create database blog;
```

Next we need to create two users, a localhost account for database connections within the application, and one to allow network connectivity to manage through something like SQLManager

```
grant all privileges on blog.* to 'bloguser'@'localhost' identified by 'password';
```

```
grant all privileges on blog.* to 'blogadmin'@'%' identified by 'password';
```

Create Two Users “admin” & “user” and Grant them Access

```
MariaDB [(none)]> grant all privileges on blog.* to 'bloguser'@'localhost' identified by 'password';  
Query OK, 0 rows affected (0.008 sec)
```

```
MariaDB [(none)]> grant all privileges on blog.* to 'blogadmin'@'%'' identified by 'password';  
Query OK, 0 rows affected (0.025 sec)
```

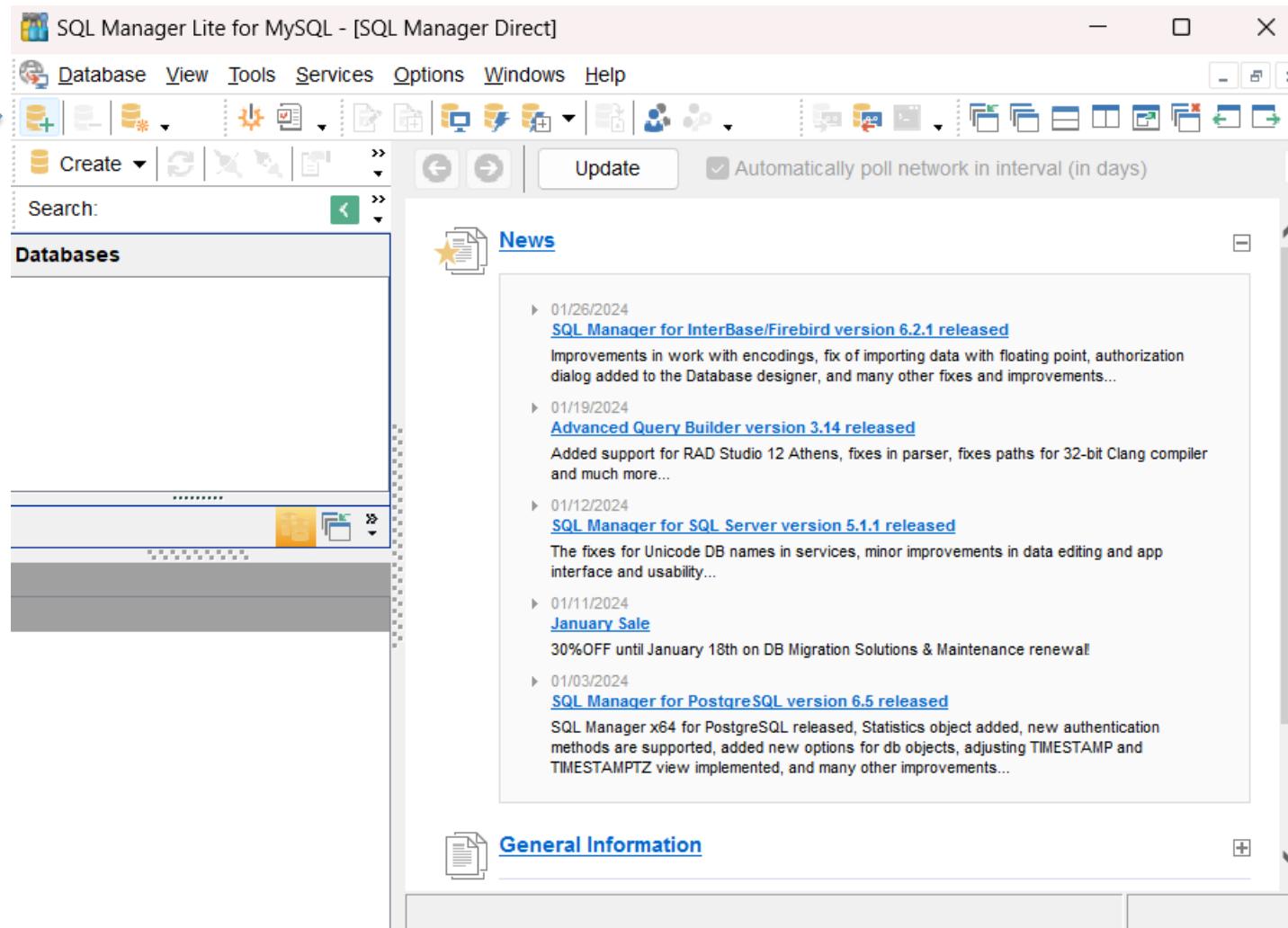
```
MariaDB [(none)]> flush privileges;  
Query OK, 0 rows affected (0.001 sec)
```

```
MariaDB [(none)]> exit  
Bye
```

- grant all privileges on blog.*
to 'bloguser'@'localhost'
identified by 'password';
- grant all privileges on blog.*
to 'blogadmin'@'%' identified by
'password';

Launch MySQL

Select menu item Database: Register Database

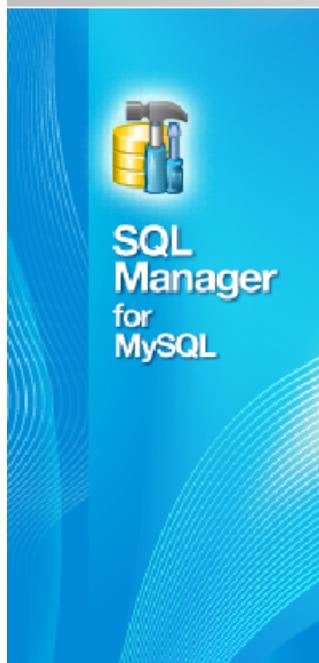


Register Database Wizard

X

Register Database

Specify the connection parameters



Welcome to the Register Database Wizard!

This wizard allows you to set the connection parameters for the selected databases only once, giving you the possibility to connect them quickly afterwards.

This wizard will guide you through the process of setting the connection parameters, selecting databases, and customizing their specific options.

Host name

localhost

Port

3306

User name

root

Password

Named pipe

Method

Direct

Help

< Back

Next >

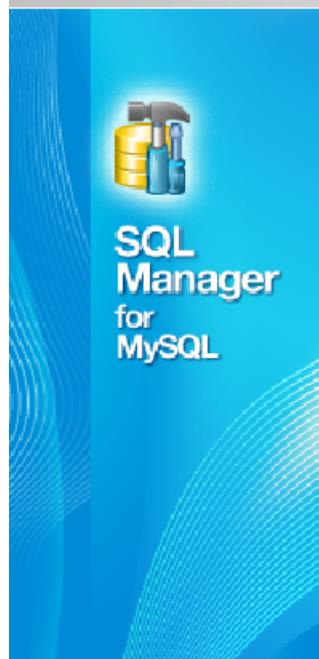
Cancel



Register Database Wizard

Register Database

Specify the connection parameters



Welcome to the Register Database Wizard!

This wizard allows you to set the connection parameters for the selected databases only once, giving you the possibility to connect them quickly afterwards.

This wizard will guide you through the process of setting the connection parameters, selecting databases, and customizing their specific options.

<u>Host name</u>	<input type="text" value="192.168.56.101"/>	<u>Port</u>	<input type="text" value="3306"/>
<u>User name</u>	<input type="text" value="blogadmin"/>		
<u>Password</u>	<input type="password" value="*****"/>		
<u>Named pipe</u>	<input type="text"/>		
<u>Method</u>	<input type="text" value="Direct"/>		

[Help](#)

[Back](#)

[Next >](#)

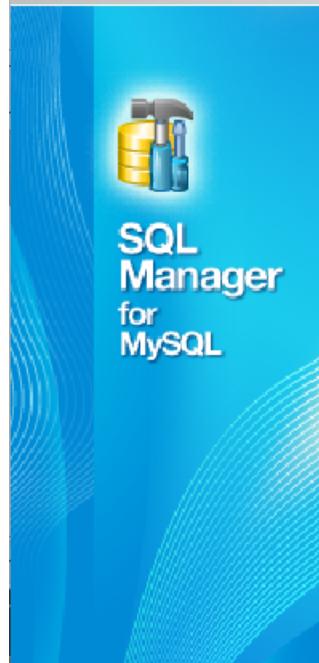
[Cancel](#)

Register Database Wizard

X

Register Database

Set some specific options for registered database(s) and click the Finish button



Database name

blog

Database alias

blog on 192.168.56.101

Refresh objects on connection

Interactive mode

Login prompt before connection

Quote identifiers

Use compression protocol

Autoconnect at startup

Help

< Back

Finish

Cancel

SQL Manager Lite for MySQL - [SQL Manager Direct]

Database View Tools Services Options Windows Help

Create Update Automatically poll network in interval (in days)

Search:

Databases

- + 192.168.56.101

blog on 192.168.56.101 (SSL)

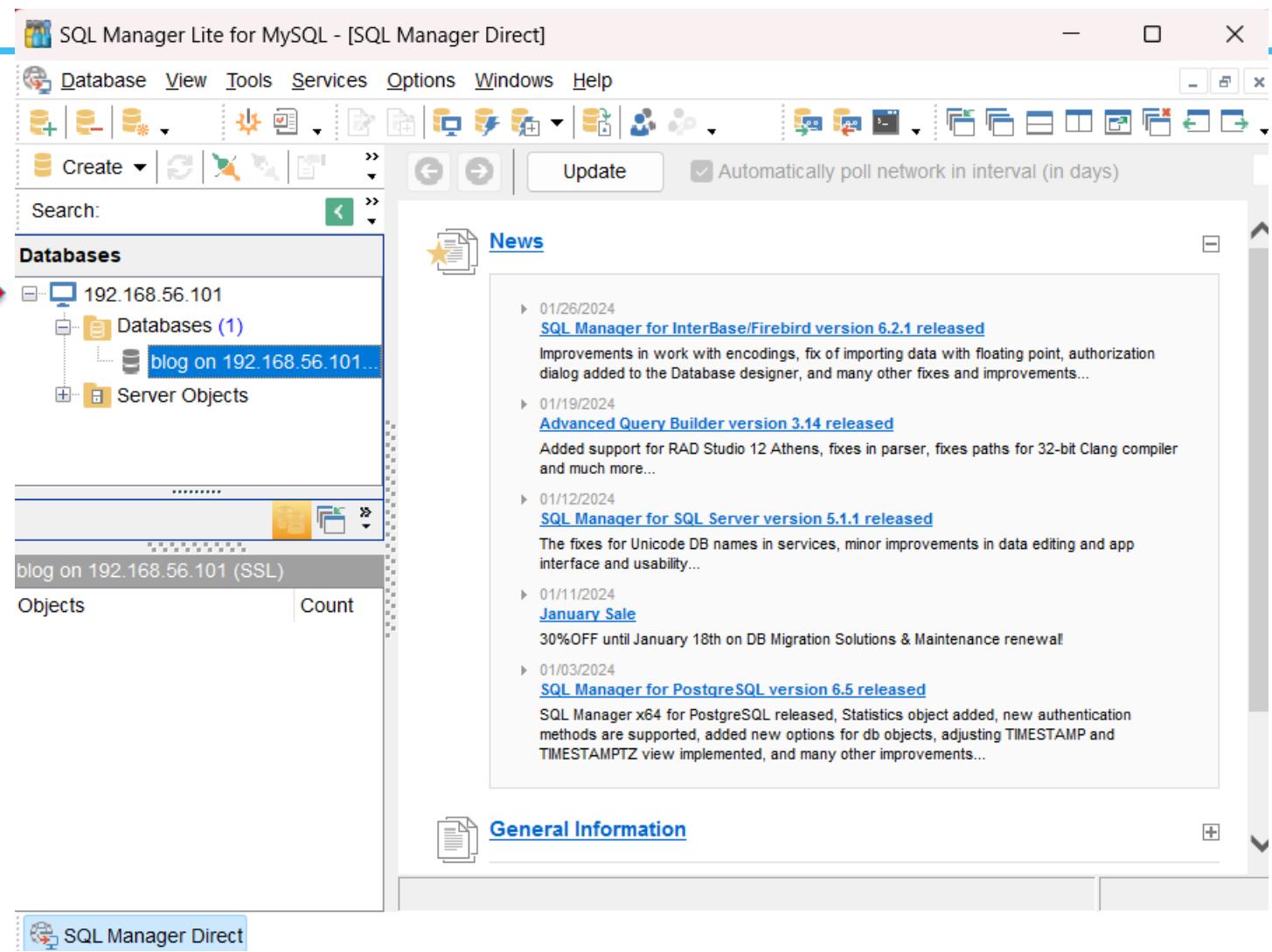
Objects Count

News

- 01/26/2024 [SQL Manager for InterBase/Firebird version 6.2.1 released](#)
Improvements in work with encodings, fix of importing data with floating point, authorization dialog added to the Database designer, and many other fixes and improvements...
- 01/19/2024 [Advanced Query Builder version 3.14 released](#)
Added support for RAD Studio 12 Athens, fixes in parser, fixes paths for 32-bit Clang compiler and much more...
- 01/12/2024 [SQL Manager for SQL Server version 5.1.1 released](#)
The fixes for Unicode DB names in services, minor improvements in data editing and app interface and usability...
- 01/11/2024 [January Sale](#)
30% OFF until January 18th on DB Migration Solutions & Maintenance renewal!
- 01/03/2024 [SQL Manager for PostgreSQL version 6.5 released](#)
SQL Manager x64 for PostgreSQL released, Statistics object added, new authentication methods are supported, added new options for db objects, adjusting TIMESTAMP and TIMESTAMPTZ view implemented, and many other improvements...

General Information

SQL Manager Direct



New SQL Editor

SQL Manager Lite for MySQL - [SQL Editor - [blog on 192.168.56.101]]

Database View Tools Services Options Windows Help



Search:

Databases

- 192.168.56.101
 - Databases (1)
 - blog on 192.168.56.10...
 - Tables
 - Views
 - Procedures
 - Functions
 - UDFs
 - Scheduled Events
 - Triggers
 - Favorite Queries
 - Favorite Objects
 - Local Scripts
 - Server Objects (1)
 - Federated servers

Database blog on 192.168.56.101

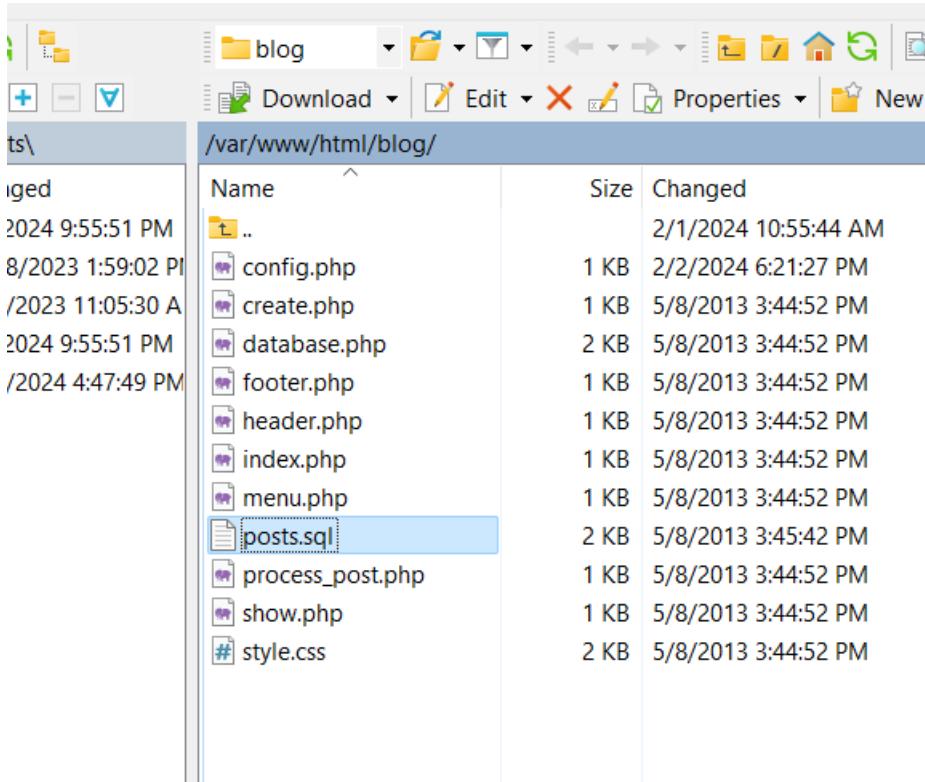
- General
- Execute
 - Execute under Cursor
 - Explain query
 - SQL Editor options
 - Results on Edit tab
 - Disable all code features

- Queries
- Add new query
 - Rename current query
 - Delete current query
 - Delete all queries
 - Add to Favorite Queries

- Edit

Edit Logs

WinSCP



The screenshot shows a Windows-style file explorer window. The address bar indicates the path is `/var/www/html/blog/`. The left pane shows a tree view with a folder icon, a plus sign, a minus sign, and a triangle icon. The right pane is a grid view displaying files. The columns are labeled "Name", "Size", and "Changed". The "Name" column lists files: .., config.php, create.php, database.php, footer.php, header.php, index.php, menu.php, posts.sql, process_post.php, show.php, and style.css. The "Size" column shows sizes like 1 KB, 2 KB, and 1 KB. The "Changed" column shows dates like 2/1/2024 10:55:44 AM and 5/8/2013 3:44:52 PM. The file "posts.sql" is highlighted with a blue selection bar.

Name	Size	Changed
..	1 KB	2/1/2024 10:55:44 AM
config.php	1 KB	2/2/2024 6:21:27 PM
create.php	1 KB	5/8/2013 3:44:52 PM
database.php	2 KB	5/8/2013 3:44:52 PM
footer.php	1 KB	5/8/2013 3:44:52 PM
header.php	1 KB	5/8/2013 3:44:52 PM
index.php	1 KB	5/8/2013 3:44:52 PM
menu.php	1 KB	5/8/2013 3:44:52 PM
posts.sql	2 KB	5/8/2013 3:45:42 PM
process_post.php	1 KB	5/8/2013 3:44:52 PM
show.php	1 KB	5/8/2013 3:44:52 PM
style.css	2 KB	5/8/2013 3:44:52 PM

Sample Posts

```
/var/www/html/blog/posts.sql - maryam@192.168.56.101 - Editor - WinSCP
File Edit View Insert Tools Options Help Encoding Color ? 

-- 
-- Table structure for table `posts`
-- 

CREATE TABLE IF NOT EXISTS `posts` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `title` varchar(255) NOT NULL,
  `content` text NOT NULL,
  `created_at` timestamp NOT NULL DEFAULT '0000-00-00 00:00:00',
  `updated_at` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=5 ;

-- 
-- Dumping data for table `posts`
-- 

INSERT INTO `posts` (`id`, `title`, `content`, `created_at`, `updated_at`) VALUES
(1, 'Luctus Metus Libero', 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus hendrerit', '2013-05-08 19:01:07', '2013-05-08 19:01:07'),
(2, 'Consectetuer Adipiscing', 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec odio. Qu', '2013-05-08 19:01:07', '2013-05-08 19:01:07'),
(4, 'New Post', 'This is some content.', '2013-05-08 19:01:07', '2013-05-08 19:01:07');
```

Open MySQL

Excecute



S Options Windows Help

Databases Databases

Database Database

blog on 192.168.56.101 |

General General

- Execute
- Execute under Cursor
- Explain query
- SQL Editor options
- Results on Edit tab
- Disable all code features

Queries Queries

- Add new query
- Rename current query
- Delete current query
- Delete all queries
- Add to Favorite Queries

Edit Edit

- Find text
- Load from file
- Save to file
- Save to file as
- Save all

1

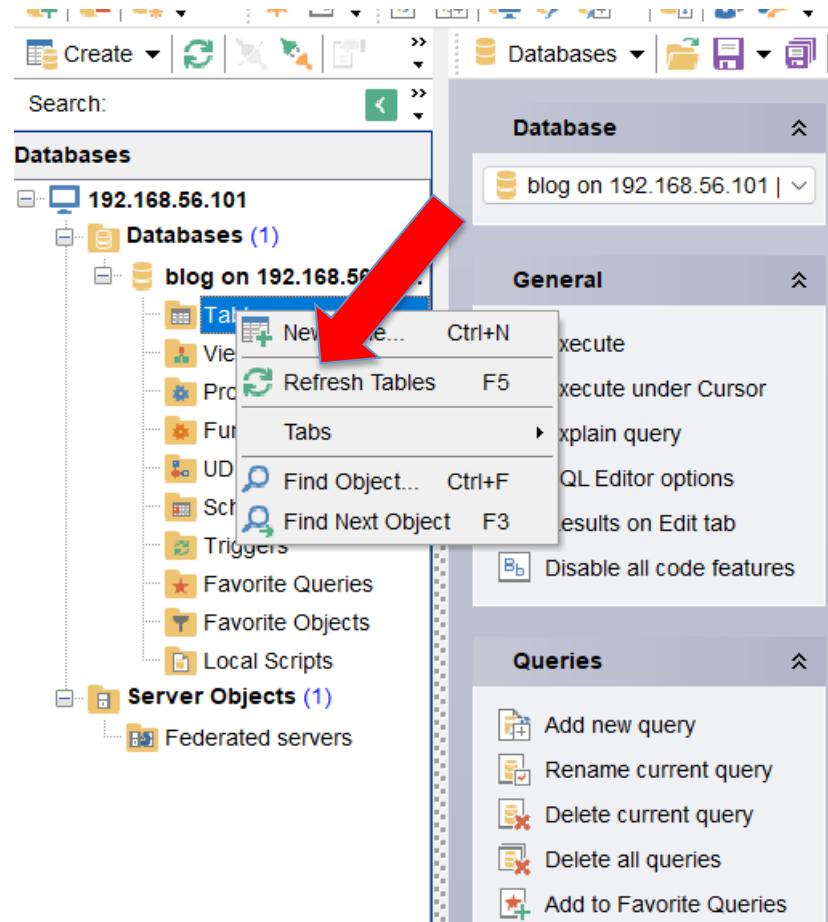
--
-- Table structure for table `posts`
--
CREATE TABLE IF NOT EXISTS `posts` (
 `id` int(11) NOT NULL AUTO_INCREMENT,
 `title` varchar(255) NOT NULL,
 `content` text NOT NULL,
 `created_at` timestamp NOT NULL DEFAULT '0000-00-00 00:00:00',
 `updated_at` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP,
 PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=5 ;

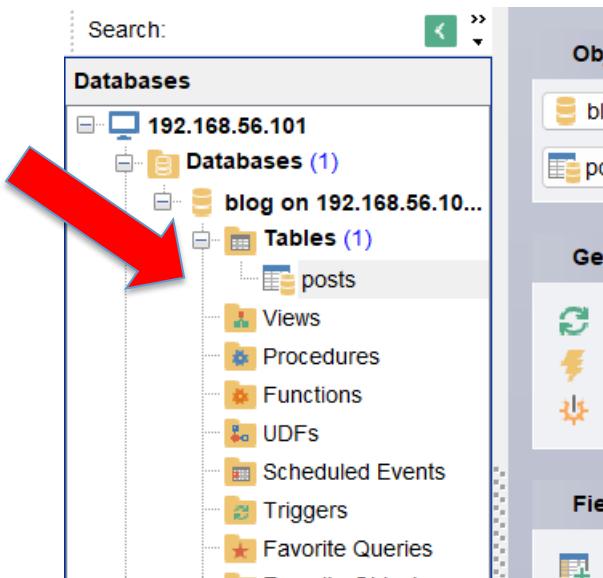
--
-- Dumping data for table `posts`
--
INSERT INTO `posts` (`id`, `title`, `content`, `created_at`, `updated_at`) VALUES
 (1, 'Luctus Metus Libero', 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus hendrerit. Pellentesque aliquet nib',
 (2, 'Consectetuer Adipiscing', 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec odio. Quisque volutpat mattis eros.',
 (4, 'New Post', 'This is some content.', '2013-05-08 19:01:07', '2013-05-08 19:01:07');

1

Query OK, 0 rows affected (31 ms)

Query OK, 3 rows affected (31 ms)





➤ Double click on posts

The screenshot shows the MySQL Workbench interface. On the left, the database tree is visible, with a red arrow pointing to the 'posts' table under the 'Tables (1)' section of the 'blog' database. The main window displays the 'posts' table structure. The 'Fields' tab of the properties grid is selected, showing the following columns:

Field Name	Field Type	Size / ...	Scale	Not Null	Unsigned	Zerofill	Autonc	Default	Generated	Description
id	INTEGER	11	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>			
title	VARCHAR	255	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
content	TEXT	0	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
created_at	TIMESTAMP	0	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0000-00-00 00:00:00		
updated_at	TIMESTAMP	0	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	current_timestamp()		

A screenshot of the MySQL Workbench interface. On the left, the navigation pane shows a connection to '192.168.56.101' with 'Databases (1)' containing 'blog' and 'Tables (1)' containing 'posts'. The main workspace displays the 'posts' table under the 'Data' tab. A red arrow points to the 'Data' tab in the top navigation bar. The table has columns 'id' and 'title', with data rows: 1 | Luctus Metus Libero, 2 | Consectetuer Adipiscing, and 4 | New Post.

		Drag a column header here to group by that column
	id	title
	1	Luctus Metus Libero
	2	Consectetuer Adipiscing
	4	New Post



Stung Eye - Index

[Home](#)[New Post](#)

New Post

May 8, 2013, 7:01 pm

This is some content.

Consectetuer Adipiscing

May 8, 2013, 6:12 pm

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec odio. Quisque volutpat mattis eros. Nullam malesuada erat ut turpis. Suspendisse urna nibh, viverra non, semper suscipit, posuere.

Luctus Metus Libero

May 8, 2013, 3:50 pm

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Phasellus hendrerit. Pellentesque aliquet nibh nec urna. In nisi neque, aliquet vel, dapibus id, mattis vel, nisi. Sed pretium, ligula sollicitudin laoreet viverra, tortor libero sodales leo, eget blandit nunc tortor eu nibh. Nullam mollis. Ut justo. Suspendisse potenti.

Sed egestas, ante et vulputate volutpat, eros pede semper est, vitae luctus metus libero eu augue. Morbi purus libero, faucibus adipiscing, commodo quis, gravida id, est. Sed lectus. Praesent elementum hendrerit tortor. Sed semper lorem at felis. Vestibulum volutpat, lacus a ultrices sagittis, mi neque euismod dui, eu pulvinar nunc sapien ornare nisl. Phasellus pede arcu, dapibus eu, fermentum et, dapibus sed, urna.



A screenshot of a web browser window displaying a blog creation form. The URL in the address bar is 192.168.56.101/blog/create.php. The page title is "Stung Eye - New Post". There are two navigation buttons: "Home" (underlined) and "New Post". The main content area is titled "New Blog Post". It has two input fields: "Title" containing "This is a test" and "Content" containing "blah blah blah". A blue rectangular box highlights the "Content" field. At the bottom left is a "Create" button. At the bottom right is a copyright notice: "Copywrong 2024 - No Rights Reserved".



Stung Eye - Index

[Home](#)[New Post](#)

This is a test

February 2, 2024, 9:19 pm

blah blah blah

New Post

May 8, 2013, 7:01 pm

This is some content.

Consectetuer Adipiscing

May 8, 2013, 6:12 pm

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec odio. Quisque volutpat mattis eros. Nullam malesuada erat ut turpis. Suspendisse urna nibh, viverra non, semper suscipit, posuere.

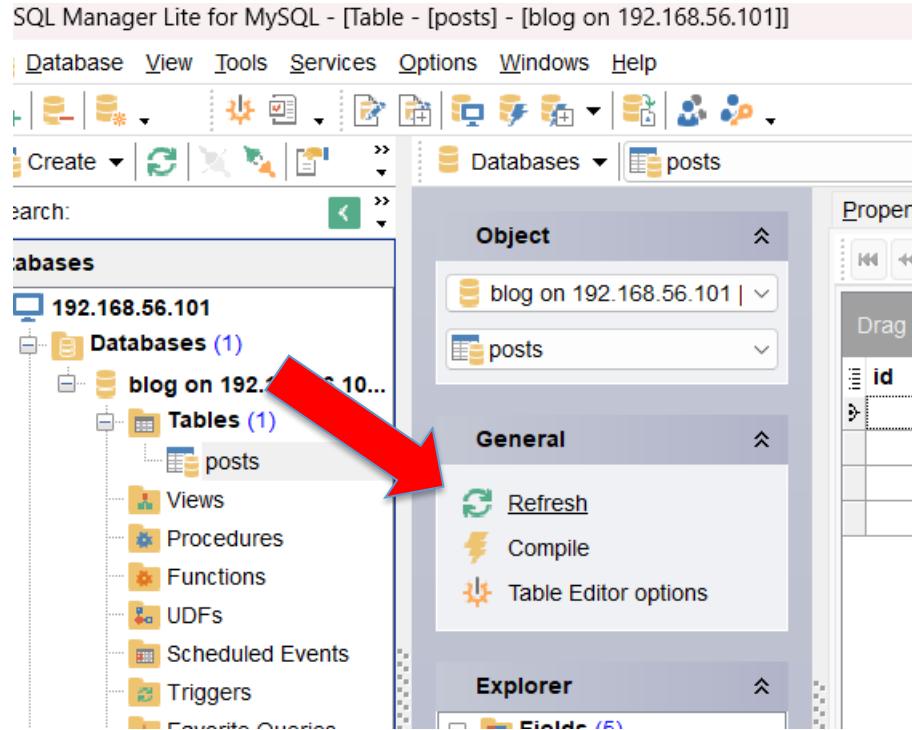
Luctus Metus Libero

May 8, 2013, 3:50 pm

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Phasellus hendrerit. Pellentesque aliquet nibh nec urna. In nisi neque, aliquet vel, dapibus id, mattis vel, nisi. Sed pretium, ligula sollicitudin laoreet viverra, tortor libero sodales leo, eget blandit nunc tortor eu nibh. Nullam mollis. Ut justo. Suspendisse potenti.

Sed egestas, ante et vulputate volutpat, eros pede semper est, vitae luctus metus libero eu augue. Morbi purus libero, faucibus adipiscing, commodo quis, gravida id, est. Sed lectus. Praesent elementum hendrerit tortor. Sed semper lorem at felis. Vestibulum volutpat, lacus a ultrices sagittis, mi neque euismod dui, eu pulvinar nunc sapien ornare nisl. Phasellus pede arcu, dapibus eu, fermentum et, dapibus sed, urna.





➤ Select record 5, hit the delete key

The screenshot shows a MySQL Workbench interface with a table named 'posts' containing five records. Record 5, titled 'This is a test', is selected. A confirmation dialog box titled 'Question' is overlaid on the interface, asking 'Delete record?' with options 'Yes' and 'No'. A large red arrow points from the bottom left towards the 'Yes' button.

	id	title
1	Luctus Metus Libero	
2	Consectetuer Adipiscing	
4	New Post	
5	This is a test	

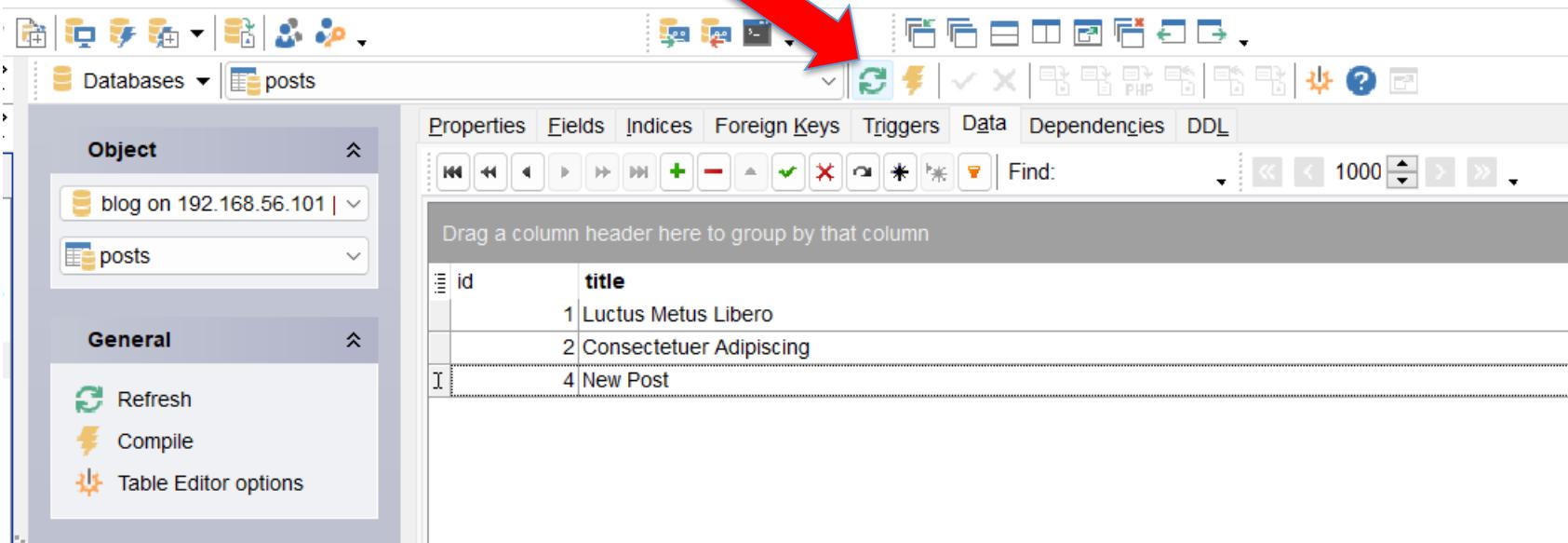
Question

Delete record?

Delete without confirmation

Yes No

➤ Refresh data: the data is gone





Stung Eye - Index

[Home](#) [New Post](#)

New Post

May 8, 2013, 7:01 pm

This is some content.

Consectetuer Adipiscing

May 8, 2013, 6:12 pm

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec odio. Quisque volutpat mattis eros. Nullam malesuada erat ut turpis. Suspendisse urna nibh, viverra non, semper suscipit, posuere.

Luctus Metus Libero

May 8, 2013, 3:50 pm

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Phasellus hendrerit. Pellentesque aliquet nibh nec urna. In nisi neque, aliquet vel, dapibus id, mattis vel, nisi. Sed pretium, ligula sollicitudin laoreet viverra, tortor libero sodales leo, eget blandit nunc tortor eu nibh. Nullam mollis. Ut justo. Suspendisse potenti.

Sed egestas, ante et vulputate volutpat, eros pede semper est, vitae luctus metus libero eu augue. Morbi purus libero, faucibus adipiscing, commodo quis, gravida id, est. Sed lectus. Praesent elementum hendrerit tortor. Sed semper lorem at felis. Vestibulum volutpat, lacus a ultrices sagittis, mi neque euismod dui, eu pulvinar nunc sapien ornare nisl. Phasellus pede arcu, dapibus eu, fermentum et, dapibus sed, urna.



Setting up the Login Script

- Course Overview 10
- Tips and Fixes 12
- Module 1 - Ethical Hacking 12
- Module 2 - VM Setup 40
- Module 3 - SQL/XSS Injection 23
- SQL Injections and Login Scripts 10
- Videos 3
- Database/XSS Security 13

- blog Zip Compressed File
- Database Security PowerPoint Presentation 
- Database Security PowerPoint Presentation 
- PHP MairaDB login script with encryption tutorial Word Document
- Database Security Zip Compressed File
- setup SQL File
- php_login Zip Compressed File

Download and put in your folder



Name	Date modified	Type	Size
checklogin	10/26/2018 1:09 AM	PHP Source File	2 KB
encrypted_check_login	10/26/2018 1:33 AM	PHP Source File	2 KB
encrypted_main_login	10/25/2018 10:38 PM	PHP Source File	1 KB
encryption_examples	10/26/2018 1:00 AM	PHP Source File	2 KB
login_success	10/25/2018 10:38 PM	PHP Source File	1 KB
logout	10/25/2018 10:38 PM	PHP Source File	1 KB
main_login	10/25/2018 10:38 PM	PHP Source File	1 KB
process_register	10/26/2018 1:25 AM	PHP Source File	2 KB
register	10/25/2018 10:38 PM	PHP Source File	1 KB
setup	10/25/2018 10:36 PM	SQL File	1 KB

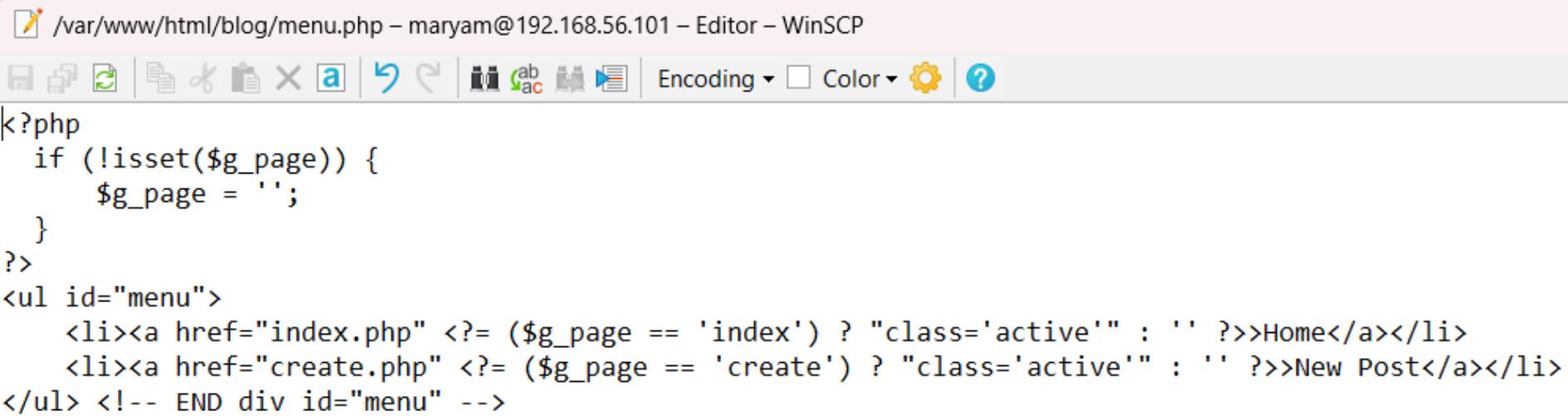
WinSCP

The screenshot shows the WinSCP interface with two panes. The left pane is titled 'C:\Users\mghanbari\OneDrive - Red River College Polytech\Documents\' and the right pane is titled '/var/www/html/blog/'. A red arrow points from the left pane to the right pane, indicating a transfer operation.

Name	Size	Type	Changed	Rights
..		Parent directory	2/1/2024 9:55:51 PM	
Arduino		File folder	10/28/2023 1:59:02 PM	rw-rw-r--
Custom Office Templa...		File folder	9/11/2023 11:05:30 AM	rw-rw-r--
SQL Manager for MyS...		File folder	2/1/2024 9:55:51 PM	rw-rw-r--
VPPProjects		File folder	1/26/2024 4:47:49 PM	rw-rw-r--

Name	Size	Changed	Rights
..		2/1/2024 10:55:44 AM	rw-rwxr-x
config.php	1 KB	2/2/2024 6:21:27 PM	rw-r--r--
create.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
database.php	2 KB	5/8/2013 3:44:52 PM	rw-r--r--
footer.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
header.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
index.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
menu.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
posts.sql	2 KB	5/8/2013 3:45:42 PM	rw-r--r--
process_post.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
show.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
style.css	2 KB	5/8/2013 3:44:52 PM	rw-r--r--

menu.php



The screenshot shows a WinSCP file editor window with the following details:

- Title Bar:** /var/www/html/blog/menu.php – maryam@192.168.56.101 – Editor – WinSCP
- Toolbar:** Includes icons for New, Open, Save, Copy, Paste, Find, Replace, Undo, Redo, and various file operations.
- Menu Bar:** Encoding ▾, Color ▾, and Help icon.
- Code Area:** Displays the PHP code for the menu.

```
<?php
if (!isset($g_page)) {
    $g_page = '';
}
?>
<ul id="menu">
    <li><a href="index.php" <?= ($g_page == 'index') ? "class='active'" : '' ?>>Home</a></li>
    <li><a href="create.php" <?= ($g_page == 'create') ? "class='active'" : '' ?>>New Post</a></li>
</ul> <!-- END div id="menu" -->
```

Edit menu.php

```
<?php
if (!isset($g_page)) {
    $g_page = '';
}
?>
<ul id="menu">
    <li><a href="index.php" <?= ($g_page == 'index') ? "class='active'" : '' ?>>Home</a></li>
    <li><a href="create.php" <?= ($g_page == 'create') ? "class='active'" : '' ?>>New Post</a></li>
    <li><a href="login.php" <?= ($g_page == 'login') ? "class='active'" : '' ?>>Login</a></li>
</ul>-- END div id="menu" -->
```

Browser - > http://192.168.56.101/blog/index.php

Stung Eye - Index

192.168.56.101/blog/

90%

[Home](#) [New Post](#) [Login](#)

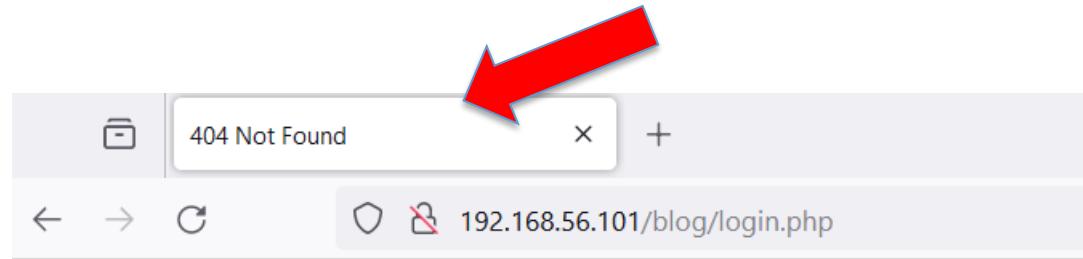
New Post
May 8, 2013, 7:01 pm
This is some content.

Consectetuer Adipiscing
May 8, 2013, 6:12 pm
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec odio. Quisque volutpat mattis eros. Nullam malesuada erat ut turpis. Suspendisse urna nibh, viverra non, semper suscipit, posuere.

Luctus Metus Libero
May 8, 2013, 3:50 pm
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Phasellus hendrerit. Pellentesque aliquet nibh nec urna. In nisi neque, aliquet vel, dapibus id, mattis vel, nisi. Sed pretium, ligula sollicitudin laoreet viverra, tortor libero sodales leo, eget blandit nunc tortor eu nibh. Nullam mollis. Ut justo. Suspendisse potenti.
Sed egestas, ante et vulputate volutpat, eros pede semper est, vitae luctus metus libero eu augue. Morbi purus libero, faucibus adipiscing, commodo quis, gravida id, est. Sed lectus. Praesent elementum hendrerit tortor. Sed semper lorem at felis. Vestibulum volutpat, lacus a ultrices sagittis, mi neque euismod dui, eu pulvinar nunc sapien ornare nisl. Phasellus pede arcu, dapibus eu, fermentum et, dapibus sed, urna.

Copywrong 2024 - No Rights Reserved

Click on Login menu

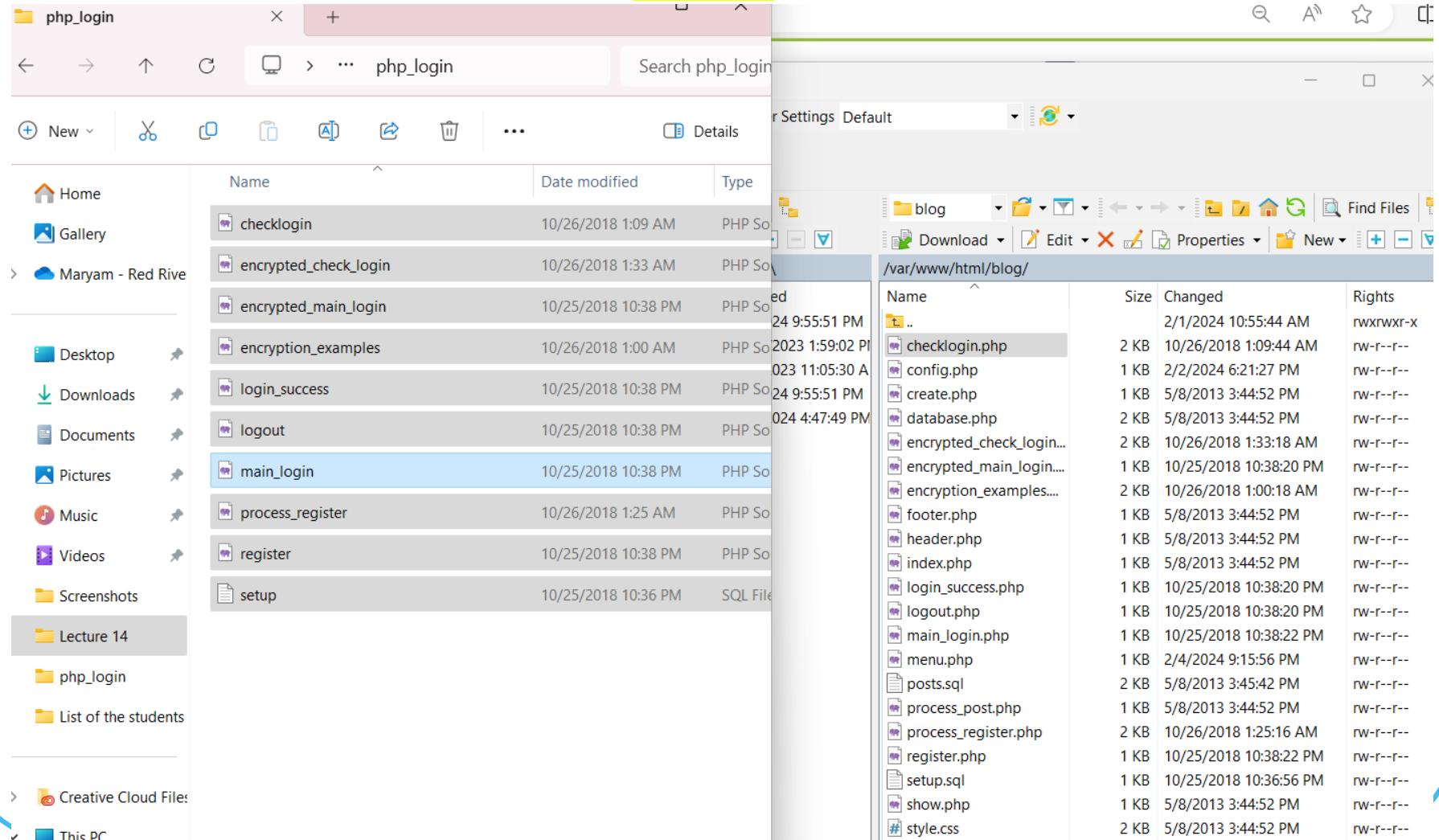


Not Found

The requested URL was not found on this server.

Apache/2.4.57 (Debian) Server at 192.168.56.101 Port 80

Drag the files from the “**php_login**” folder to the website in the “**blog**” directory



Create our Table “members”

➤ from

STEP 2: Create table "members"

Test your above and log into your database with the account created above. Use the SQL below for testing this code. It will create a table called members in your blog database.

Database		
Table "members"		
id	username	password
1	john	1234

```
CREATE TABLE `members` (
`id` int(4) NOT NULL auto_increment,
`username` varchar(255) NOT NULL default '',
`password` varchar(255) NOT NULL default '',
PRIMARY KEY (`id`)
) AUTO_INCREMENT=2 ;
-- 
-- Dumping data for table `members`
-- 
INSERT INTO `members` VALUES (1, 'john', '1234');
```

Create our Table “members”

➤ or

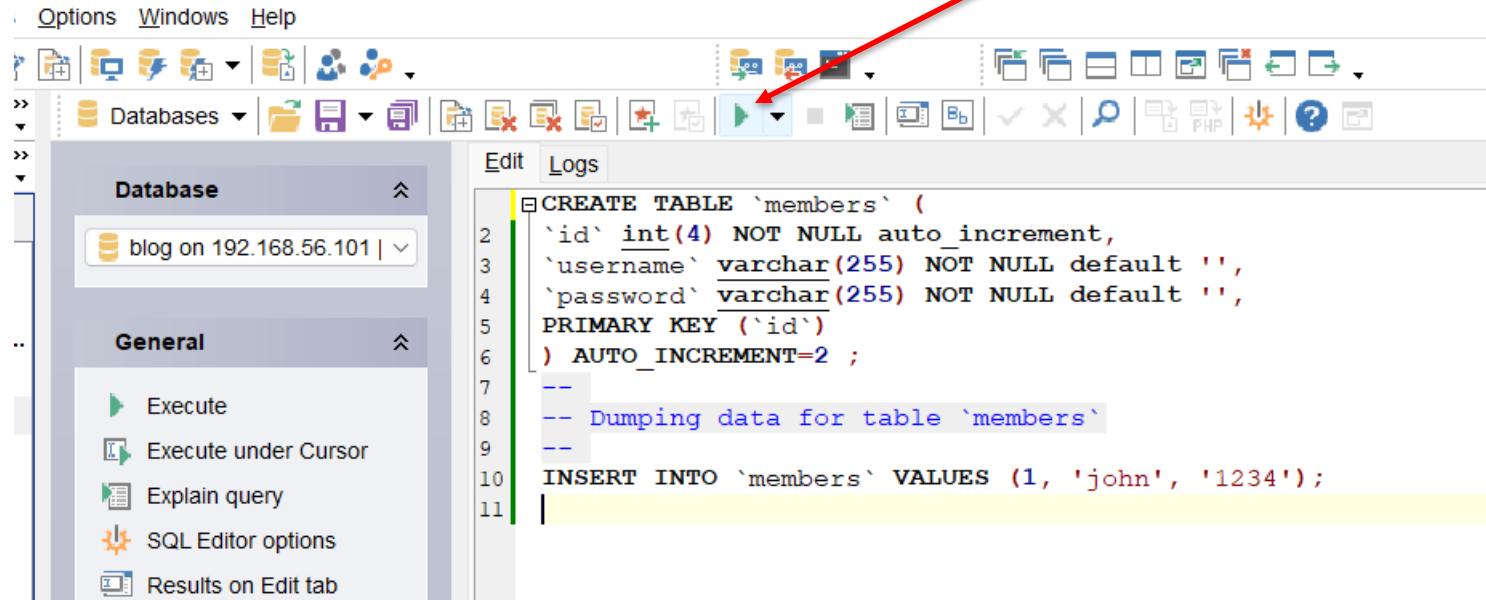
```
setup × +  
File Edit View  
  
CREATE TABLE `members` (  
    `id` int(4) NOT NULL auto_increment,  
    `username` varchar(200) NOT NULL default '',  
    `password` varchar(200) NOT NULL default '',  
    PRIMARY KEY (`id`)  
) AUTO_INCREMENT=2 ;  
--  
-- Dumping data for table `members`  
--  
INSERT INTO `members` VALUES (1, 'john', '1234');  
  
-- Set Permissions  
-- Create user login_user, and allow him to select only on username and password:  
CREATE USER 'login_user'@'localhost' IDENTIFIED BY '1234';  
GRANT SELECT ON `blog`.`members` TO 'login_user'@'localhost';  
  
-- Create user register_user and let him insert records into database:  
CREATE USER 'register_user'@'localhost' IDENTIFIED BY '1234';  
GRANT INSERT ON `blog`.`members` TO 'register_user'@'localhost';  
  
-- Create a 3rd user that will have normal access to the system:  
CREATE USER 'normal_user'@'localhost' IDENTIFIED BY '1234';  
  
GRANT SELECT , INSERT , UPDATE , DELETE , REFERENCES ON `blog`.* TO 'normal_user'@'%';  
  
-- Update privileges in database. RUN AGAINST LOCALHOST, NOT ON DATABASE blog.  
FLUSH PRIVILEGES
```

SQL editor

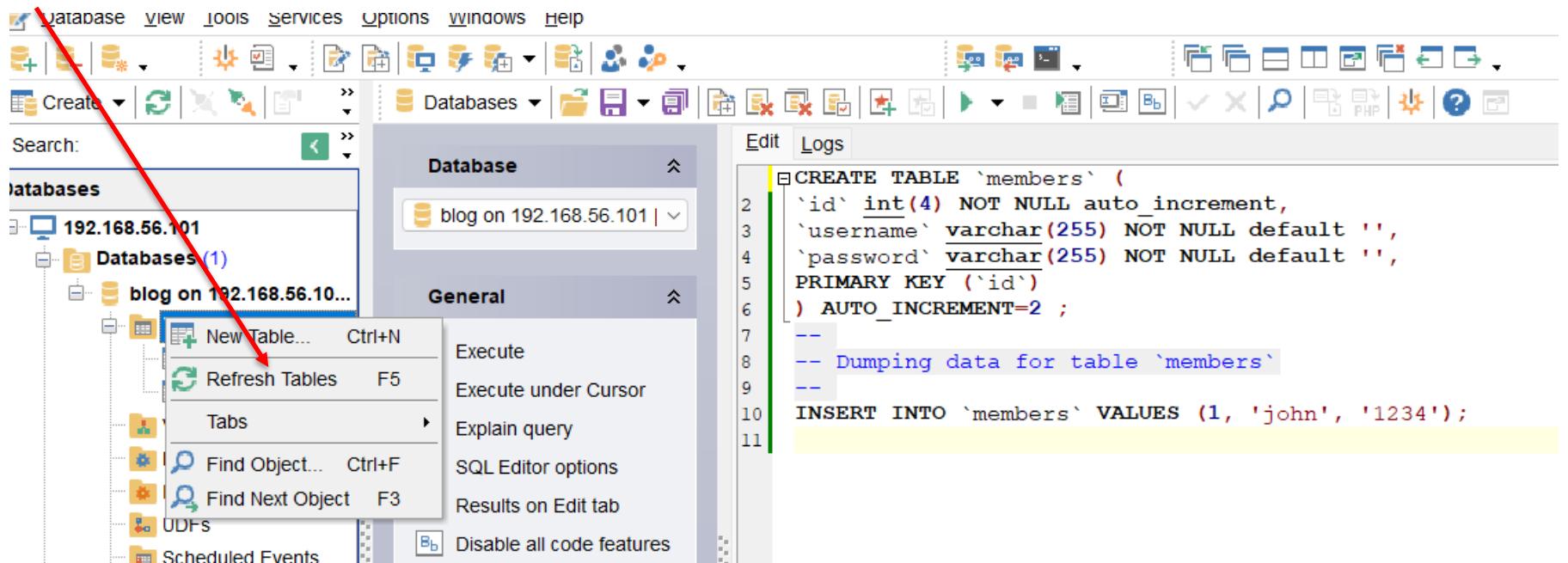
A screenshot of the MySQL Workbench application. On the left, there's a sidebar with a tree view of database objects. A red arrow points from the title 'SQL editor' at the top to the 'SQL Editor' tab in the sidebar. The main area shows the SQL Editor with the following code:

```
1 -- Table structure for table `posts`
2 --
3 --
4 
5 CREATE TABLE IF NOT EXISTS `posts` (
6     `id` int(11) NOT NULL AUTO_INCREMENT,
7     `title` varchar(255) NOT NULL,
8     `content` text NOT NULL,
9     `created_at` timestamp NOT NULL DEFAULT '0000-00-00 00:00:00',
10    `updated_at` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP,
11    PRIMARY KEY (`id`)
12 ) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=5 ;
13 
14 --
15 -- Dumping data for table `posts`
16 --
17 
18 INSERT INTO `posts` (`id`, `title`, `content`, `created_at`, `updated_at`) VALUES
19     (1, 'Luctus Metus Libero', 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus hendrerit. Pellentesque aliquet nib',
20      (2, 'Consectetuer Adipiscing', 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec odio. Quisque volutpat mattis eros.
21      (4, 'New Post', 'This is some content.', '2013-05-08 19:01:07', '2013-05-08 19:01:07');
```

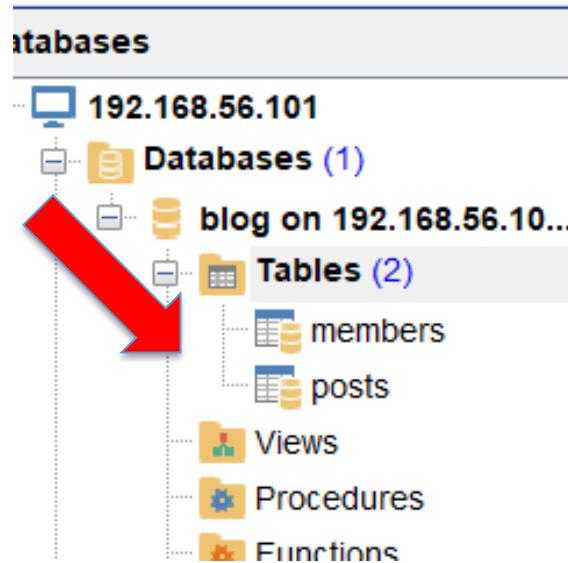
Run Query



Refresh Tables



Two Tables

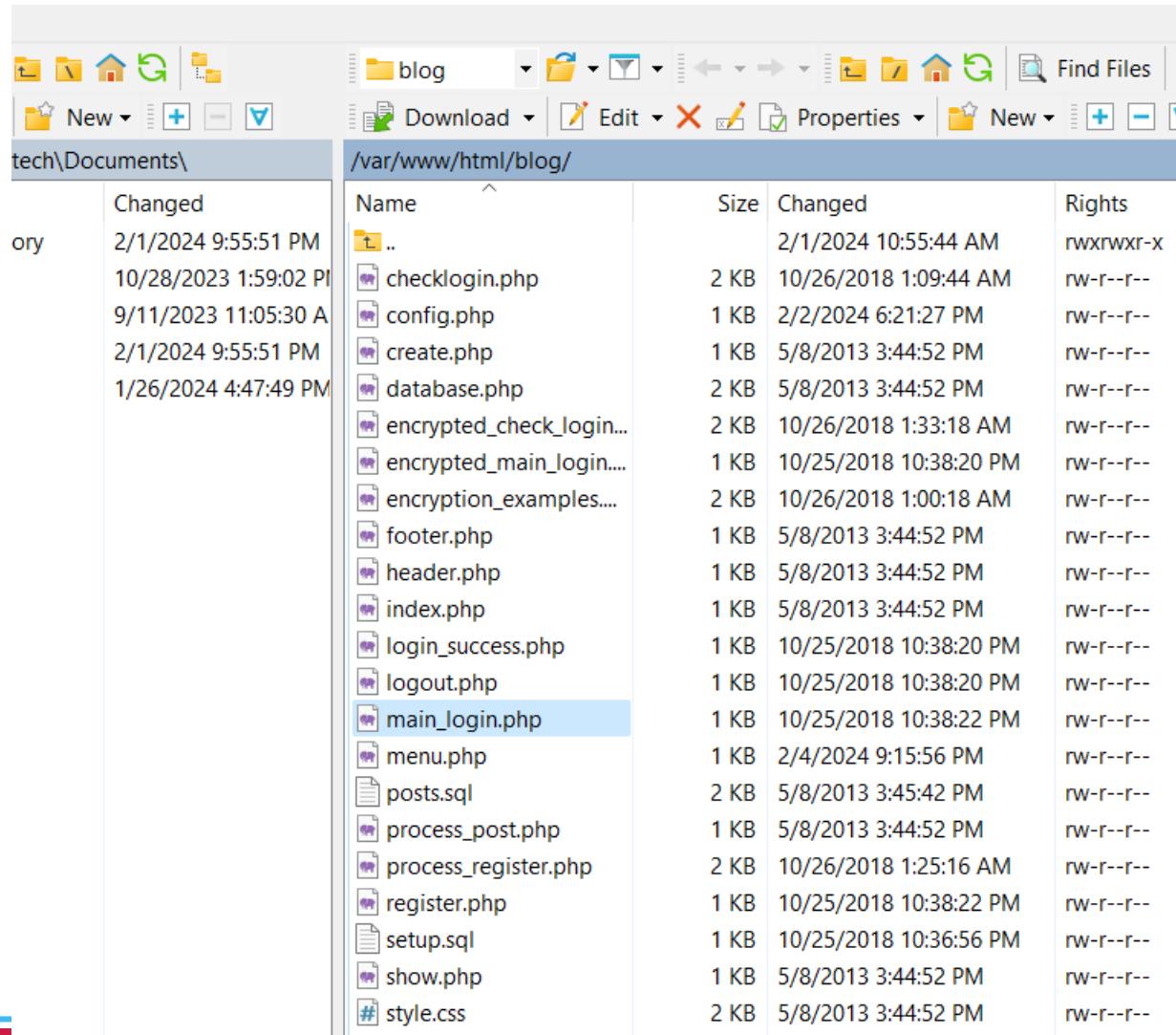


members Table



Properties			Fields	Indices	Foreign Keys	Triggers	Data	Dependencies	DDL
Drag a column header here to group by that column									
ini	id	username							password
	1	john							1234

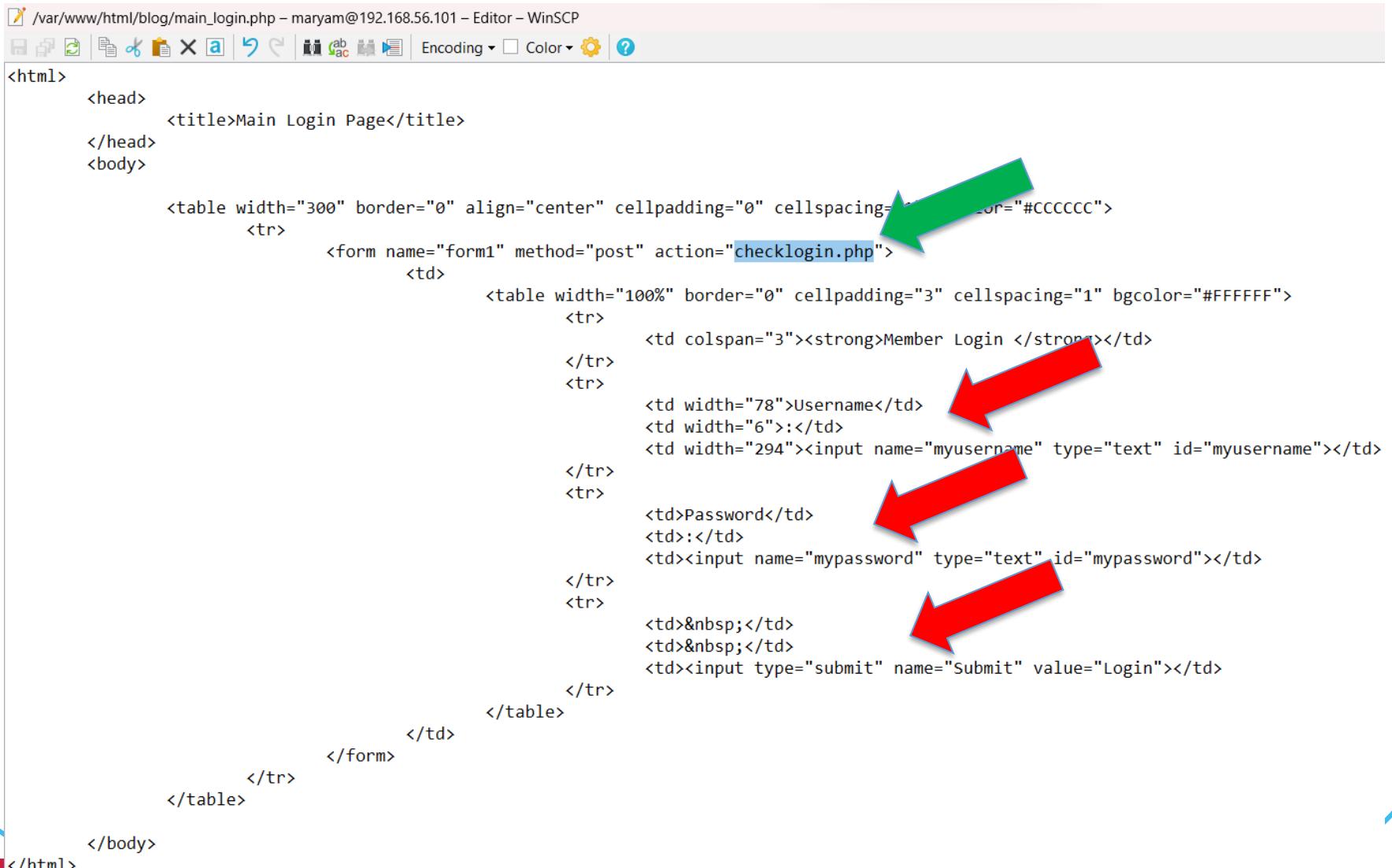
Look at the “main_login.php”



Name	Size	Changed	Rights
..		2/1/2024 10:55:44 AM	rwxrwxr-x
checklogin.php	2 KB	10/26/2018 1:09:44 AM	rw-r--r--
config.php	1 KB	2/2/2024 6:21:27 PM	rw-r--r--
create.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
database.php	2 KB	5/8/2013 3:44:52 PM	rw-r--r--
encrypted_check_login...	2 KB	10/26/2018 1:33:18 AM	rw-r--r--
encrypted_main_login....	1 KB	10/25/2018 10:38:20 PM	rw-r--r--
encryption_examples....	2 KB	10/26/2018 1:00:18 AM	rw-r--r--
footer.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
header.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
index.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
login_success.php	1 KB	10/25/2018 10:38:20 PM	rw-r--r--
logout.php	1 KB	10/25/2018 10:38:20 PM	rw-r--r--
main_login.php	1 KB	10/25/2018 10:38:22 PM	rw-r--r--
menu.php	1 KB	2/4/2024 9:15:56 PM	rw-r--r--
posts.sql	2 KB	5/8/2013 3:45:42 PM	rw-r--r--
process_post.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
process_register.php	2 KB	10/26/2018 1:25:16 AM	rw-r--r--
register.php	1 KB	10/25/2018 10:38:22 PM	rw-r--r--
setup.sql	1 KB	10/25/2018 10:36:56 PM	rw-r--r--
show.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--
# style.css	2 KB	5/8/2013 3:44:52 PM	rw-r--r--

main_login.php

```
/var/www/html/blog/main_login.php - maryam@192.168.56.101 - Editor - WinSCP  
Encoding ▾ Color ▾ ?  
<html>  
    <head>  
        <title>Main Login Page</title>  
    </head>  
    <body>  
  
        <table width="300" border="0" align="center" cellpadding="0" cellspacing="0" bordercolor="#CCCCCC">  
            <tr>  
                <td>  
                    <form name="form1" method="post" action="checklogin.php">  
                        <td>  
                            <table width="100%" border="0" cellpadding="3" cellspacing="1" bgcolor="#FFFFFF">  
                                <tr>  
                                    <td colspan="3"><strong>Member Login </strong></td>  
                                </tr>  
                                <tr>  
                                    <td width="78">Username</td>  
                                    <td width="6">:</td>  
                                    <td width="294"><input name="myusername" type="text" id="myusername"></td>  
                                </tr>  
                                <tr>  
                                    <td>Password</td>  
                                    <td>:</td>  
                                    <td><input name="mypassword" type="text" id="mypassword"></td>  
                                </tr>  
                                <tr>  
                                    <td>&nbsp;</td>  
                                    <td>&nbsp;</td>  
                                    <td><input type="submit" name="Submit" value="Login"></td>  
                                </tr>  
                            </table>  
                        </td>  
                    </form>  
                </td>  
            </tr>  
        </table>  
    </body>  
</html>
```



checklogin.php

➤ We will check it in the next competency.



The screenshot shows a WinSCP file editor window with the following details:

- Path: /var/www/html/blog/checklogin.php
- User: maryam@192.168.56.101
- Editor: WinSCP

The code in the editor is a PHP script for a login page. It includes database connection setup, user input validation, SQL query execution, and password comparison logic.

```
<html>
    <head>
        <title>Main Login Page</title>
    </head>
    <body>

    <?php

    ob_start();
    $host="localhost"; // Host name
    $username="bloguser"; // Mysql username
    $password="bloguser"; // Mysql password
    $db_name="blog"; // Database name
    $tbl_name="members"; // Table name
    $mysqli = new mysqli($host, $username, $password, $db_name);

    /* check connection */
    if ($mysqli->connect_errno) {
        printf("Connect failed: %s\n", $mysqli->connect_error);
        exit();
    }

    $myusername=$_POST['myusername'];
    $mypassword=$_POST['mypassword'];
    // To protect MySQL injection
    $myusername = stripslashes($myusername);
    $mypassword = stripslashes($mypassword);

    $cleanusername = $mysqli->real_escape_string($myusername);
    $cleanpassword = $mysqli->real_escape_string($mypassword);

    $sql="SELECT password FROM $tbl_name WHERE username='".$cleanusername' \n limit
    // $result=mysql_query($sql);
    $result = $mysqli->query($sql);

    while ($row = $result->fetch_assoc()) {
        $returnedpassword=$row['password'];
    }
    // If returned password matches entered password, valid login

    if($mypassword==$returnedpassword && $mypassword<>''){
        // Register $myusername and redirect to file "login success.php"
    }
}
```

encrypted_check_login.php

```
</head>
<body>

<?php

ob_start();
$host="localhost"; // Host name
$username="bloguser"; // Mysql username
$password="bloguser"; // Mysql password
$db_name="blog"; // Database name
$tbl_name="members"; // Table name

$mysqli = new mysqli($host, $username, $password, $db_name);

/* check connection */
if ($mysqli->connect_errno) {
    printf("Connect failed: %s\n", $mysqli->connect_error);
    exit();
}

$myusername=$_POST['myusername'];
$mypassword=$_POST['mypassword'];
// To protect MySQL injection
$myusername = stripslashes($myusername);
$mypassword = stripslashes($mypassword);

$cleanusername = $mysqli->real_escape_string($myusername);
$cleanpassword = $mysqli->real_escape_string($mypassword);

$sql="SELECT password,salt FROM $tbl_name WHERE username='$cleanusername' \n limit 1";
// $result=mysql_query($sql);
$result = $mysqli->query($sql);
while ($row = $result->fetch_assoc()) {
    $returnedpassword=$row['password'];
    $returnedsalt=$row['salt'];
}

// take clean password, salt and encrypt it as we did in the register page
$salted_password=$returnedsalt.$cleanpassword;
$checkpassword = hash("sha512", $salted_password);

// If returned password matches entered password, valid login
```

SQL Manager -> Data Tab

The screenshot shows the SQL Manager interface with the 'Data' tab selected. On the left, the Object browser displays a connection to 'blog on 192.168.56.101' with one database ('members') and two tables ('members', 'posts'). The 'members' table is currently selected. The main area shows the table data in a grid format:

	id	username	password
	1	john	1234

Below the grid, there is a message: "Drag a column header here to group by that column". The top right corner of the interface shows a page navigation bar with a 'Find:' field and a page number '1000'.

SQL Manager -> Fields Tab

A screenshot of the SQL Manager interface. On the left, there's a tree view with a node labeled 'members'. The main area shows a table structure for the 'members' table. At the top, there are tabs: Properties, Fields (which is highlighted with a red arrow), Indices, Foreign Keys, Triggers, Data, Dependencies, and DDL. Below the tabs is a toolbar with various icons. The table has columns for Field Name, Field Type, Size / ... (Scale), Not Null, Unsigned, Zerofill, Autoinc, Default, Generated, and Description. There are three rows in the table: 'id' (type INTEGER, size 4, scale 0, unsigned checked, zerofill checked, autoinc checked), 'username' (type VARCHAR, size 255, scale 0, unsigned checked), and 'password' (type VARCHAR, size 255, scale 0, unsigned checked).

Field Name	Field Type	Size / ... Scale	Not Null	Unsigned	Zerofill	Autoinc	Default	Generated	Description
id	INTEGER	4 0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
username	VARCHAR	255 0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
password	VARCHAR	255 0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			

SQL Manager -> New Field

Field Name	Field Type	Size / ...	Scale	Not Null	Unsigned	Zerofill	Autonc	Default
id	INTEGER	4	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
username	VARCHAR	255	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
password	VARCHAR	255	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

- [New Field...](#)
- [Edit Field id...](#)
- [Insert Field...](#)
- [Drop Field id](#)
-
- [Duplicate Field...](#)
- [Reorder Fields...](#)
-
- [Copy List of Fields Names to Clipboard](#)
- [Create foreign key for this field](#)

SQL Manager -> Add “salt”

Properties Fields Indices Foreign Keys Triggers Data Dependencies DDL

Field Name	Field Type	Size / ...	Scale	Not Null	Unsigned	Zerofill	Autolnc
id	INTEGER	11	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
username	VARCHAR	200	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
password	VARCHAR	200	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add new field

Field name: salt

Description:

Type: VARCHAR

Size / precision: 200

Scale: 0

Character set: Default

Collation: Default

Generated Type: NONE

Not null:

Use size:

Primary key:

Unique:

Unsigned:

Zerofill:

Autoincrement:

Expression:

Values:

Default value:

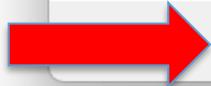
Empty string

Insert Mode:

Insert first Insert last Insert after field

Insert after:

OK Cancel Help



- 74 of 125 -

SQL Manager

Changing Metadata

Compile SQL

```
1 ALTER TABLE `members` ADD COLUMN `salt` VARCHAR(200) DEF
```

Don't show this window on success



SQL Manager - > the New Column Is Added

The screenshot shows the SQL Manager interface for managing a database named 'members'. The left sidebar displays the 'Object' dropdown set to 'blog on 192.168.56.101' and the 'members' table selected. The main panel shows the 'Fields' tab of the 'members' table properties. A new column, 'salt', has been added to the table structure. The table structure is as follows:

Field Name	Field Type	Size / ...	Scale	Not Null	Unsigned	Zerofill	Autoninc	Default	Generated
id	INTEGER	4	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
username	VARCHAR	255	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
password	VARCHAR	255	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
salt	VARCHAR	200	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Null	

“process_register.php” File -> Store Information about the user

```
<html>
    <head>
        <title>Main Register Page</title>
    </head>
    <body>

        <?php

        ob_start();
        $host="localhost"; // Host name
        $username="bloguser"; // Mysql username
        $password="bloguser"; // Mysql password
        $db_name="blog"; // Database name
        $tbl_name="members"; // Table name

        $mysqli = new mysqli($host, $username, $password, $db_name);

        /* check connection */
        if ($mysqli->connect_errno) {
            printf("Connect failed: %s\n", $mysqli->connect_error);
            exit();
        }
        $myusername=$_POST['myusername'];
        $mypassword=$_POST['mypassword'];

        // To protect MySQL injection (more detail about MySQL injection)
        $cleanusername = $myusername;
        $cleanpassword = $mypassword;

        // salting adds uniqueness to each entry.
        $salt=uniqid() ;
        $salted_password=$salt.$cleanpassword;
        $encrypted_password = hash("sha512", $salted_password);

        $sql="insert into $tbl_name (username,password,salt) values ('$cleanusername','$encrypted_password','$salt')";
        if (!$mysqli->query($sql)) {
            echo "INSERT failed: (" . $mysqli->errno . ") " . $mysqli->error;
        }
        else
        {
            echo "Registered";
        }

    </body>
</html>
```



“process_register.php” File -> salt

```
// salting adds uniqueness to each entry.  
$salt=uniqid() ;  
$salted_password=$salt.$cleanpassword;  
$encrypted_password = hash("sha512", $salted_password);  
  
$sql="insert into $tbl_name (username,password,salt) values ('$cleanusername','$encrypted_password','$salt')";  
if (!$mysqli->query($sql)) {  
    echo "INSERT failed: (" . $mysqli->errno . ") " . $mysqli->error;  
}  
else  
{  
    echo "Registered";  
}
```

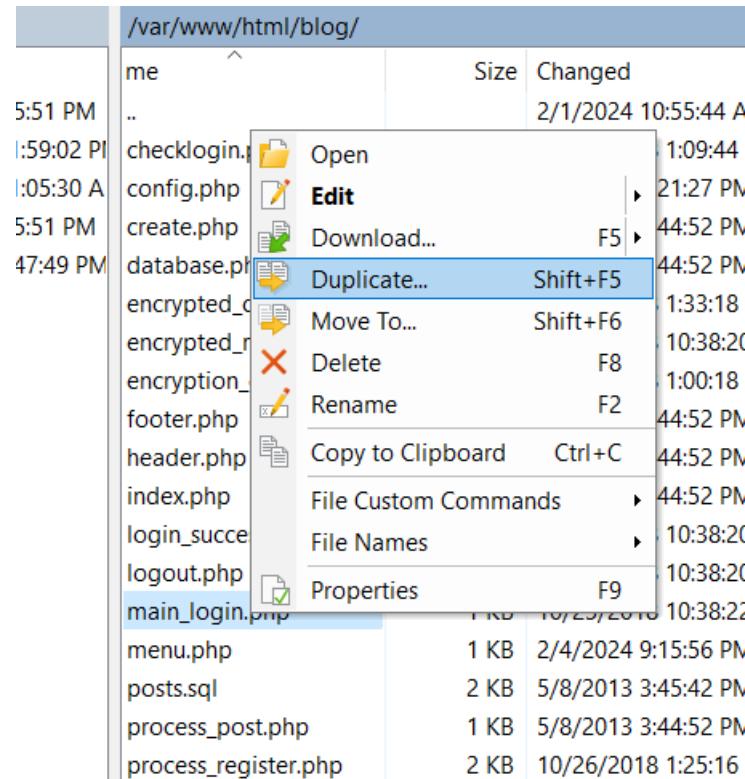


Hashing process

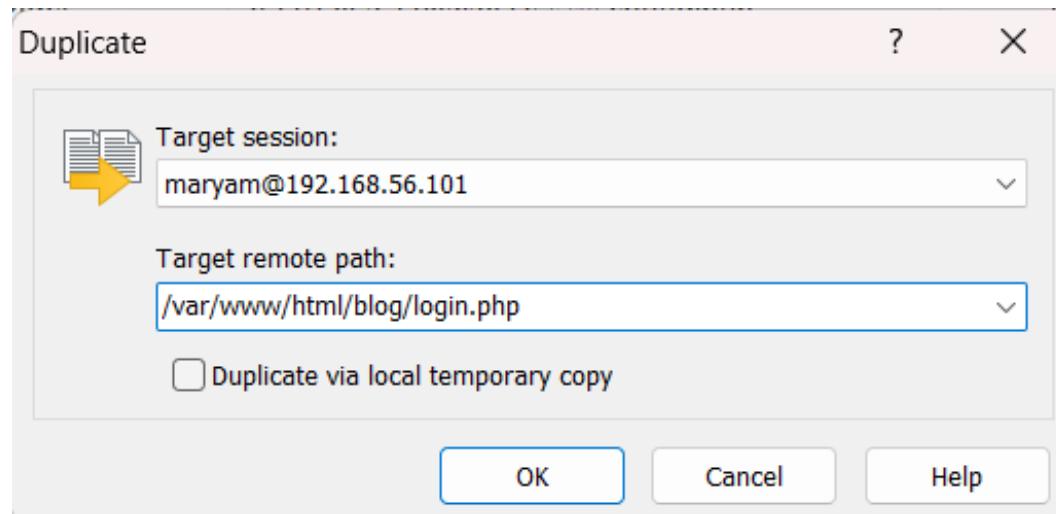
“main_login.php” File

/var/www/html/blog/			
	Name	Size	Changed
1	..		2/1/2024 10:5
4 9:55:51 PM	checklogin.php	2 KB	10/26/2018 1
023 1:59:02 PM	config.php	1 KB	2/2/2024 6:21
23 11:05:30 AM	create.php	1 KB	5/8/2013 3:44
4 9:55:51 PM	database.php	2 KB	5/8/2013 3:44
24 4:47:49 PM	encrypted_check_login...	2 KB	10/26/2018 1
	encrypted_main_login....	1 KB	10/25/2018 1
	encryption_examples....	2 KB	10/26/2018 1
	footer.php	1 KB	5/8/2013 3:44
	header.php	1 KB	5/8/2013 3:44
	index.php	1 KB	5/8/2013 3:44
	login_success.php	1 KB	10/25/2018 1
	logout.php	1 KB	10/25/2018 1
	main_login.php	1 KB	10/25/2018 1
	menu.php	1 KB	2/4/2024 9:15
	posts.sql	2 KB	5/8/2013 3:44
	process_post.php	1 KB	5/8/2013 3:44
	process_register.php	2 KB	10/26/2018 1
	register.php	1 KB	10/25/2018 1
	setup.sql	1 KB	10/25/2018 1
	show.php	1 KB	5/8/2013 3:44
	# style.css	2 KB	5/8/2013 3:44

Duplicate “main_login.php” File



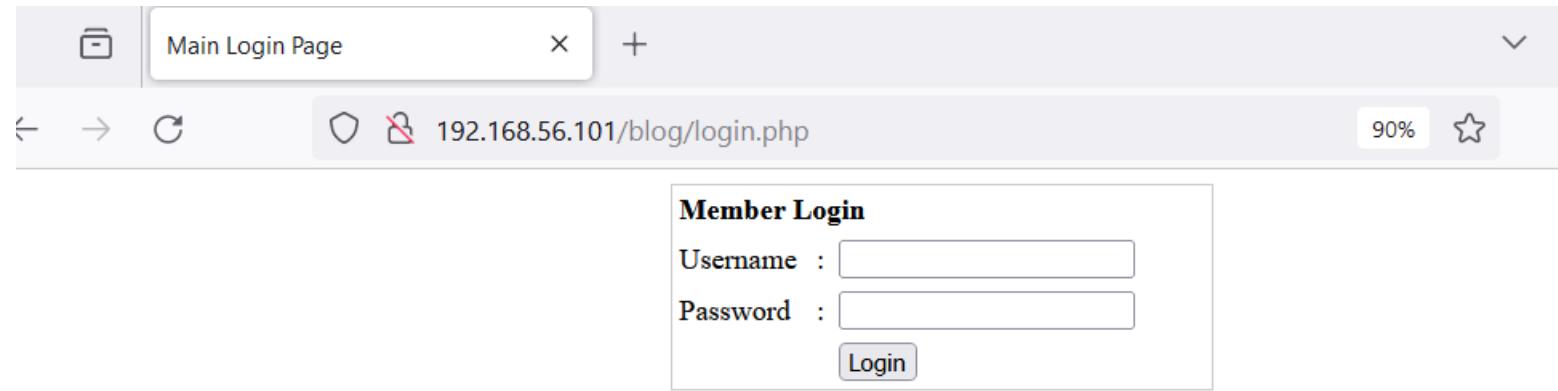
SQL Manager



SQL Manager

Name	Size
checklogin.php	2 KB
config.php	1 KB
create.php	1 KB
database.php	2 KB
encrypted_check_login...	2 KB
encrypted_main_login....	1 KB
encryption_examples....	2 KB
footer.php	1 KB
header.php	1 KB
index.php	1 KB
login.php	1 KB
login_success.php	1 KB
logout.php	1 KB
main_login.php	1 KB
menu.php	1 KB
posts.sql	2 KB
process_post.php	1 KB
process_register.php	2 KB
register.php	1 KB
setup.sql	1 KB
show.php	1 KB
style.css	2 KB

Browser -> login page



➤ We have to improve the web page.

index.php -> copy

The screenshot shows a WinSCP Editor window and a file browser window side-by-side.

WinSCP Editor Content:

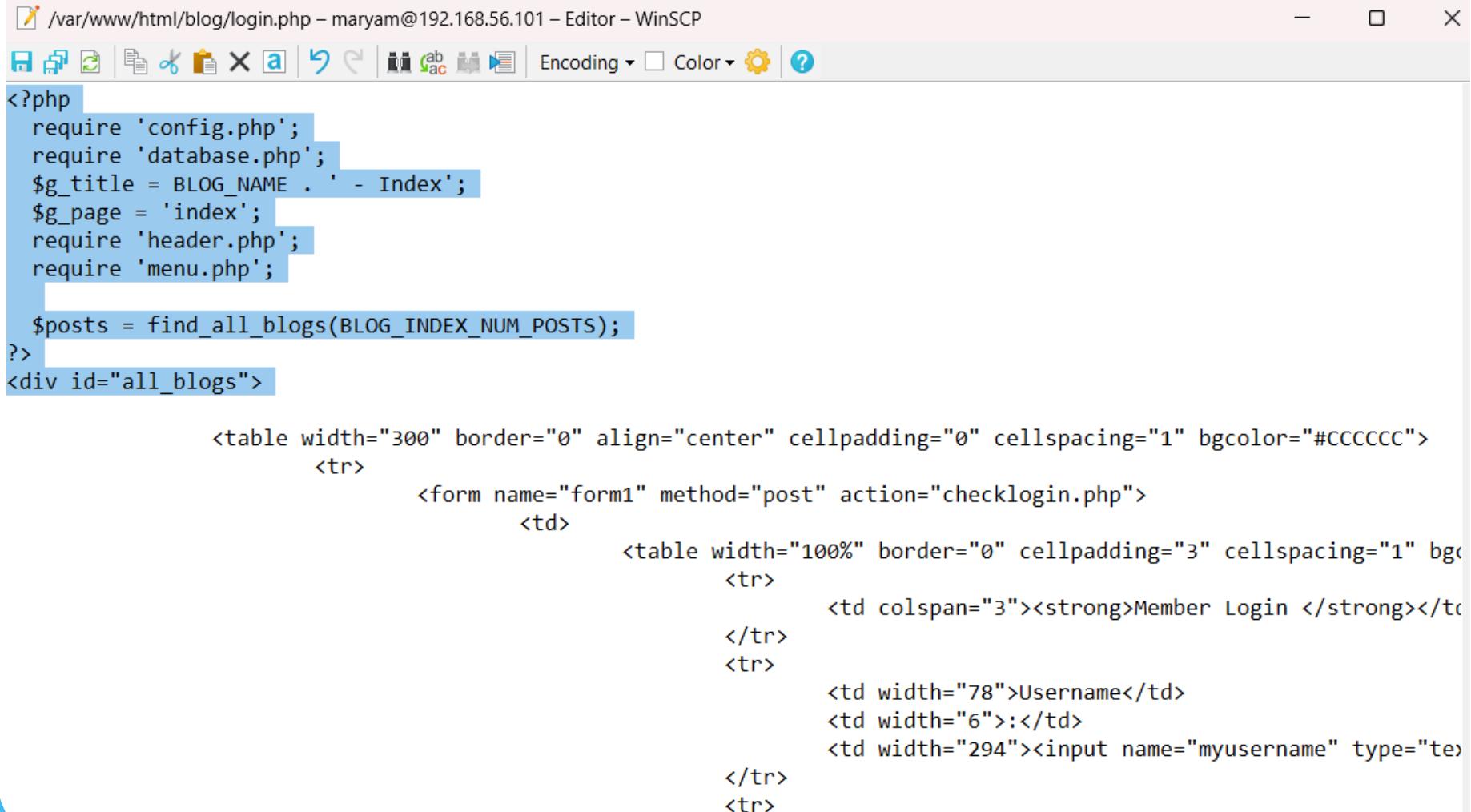
```
<?php
    require 'config.php';
    require 'database.php';
    $g_title = BLOG_NAME . ' - Index';
    $g_page = 'index';
    require 'header.php';
    require 'menu.php';

    $posts = find_all_blogs(BLOG_INDEX_NUM_POSTS);
?>
<div id="all_blogs">
    <?php foreach($posts as $post): ?>
        <div class="blog_post">
            <h2><a href="show.php?id=<?=$post['id']?>"><?= htmlspecialchars($post['title']) ?></a></h2>
            <p>
                <small>
                    <?= $post['created_at'] ?>
                </small>
            </p>
            <div class='blog_content'>
                <?= nl2br(htmlspecialchars($post['content'])) ?>
            </div>
        </div>
    <?php endforeach; ?>
</div>
<?php
    require 'footer.php';
?>
```

File Browser Content:

Name	Size	Changed
..		2/1/2024 1
checklogin.php	2 KB	10/26/2018
config.php	1 KB	2/2/2024 6
create.php	1 KB	5/8/2013 3
database.php	2 KB	5/8/2013 3
encrypted_check_login...	2 KB	10/26/2018
encrypted_main_login...	1 KB	10/25/2018
encryption_examples....	2 KB	10/26/2018
footer.php	1 KB	5/8/2013 3
header.php	1 KB	5/8/2013 3
index.php	1 KB	5/8/2013 3
login.php	1 KB	2/4/2024 1
login_success.php	1 KB	10/25/2018
logout.php	1 KB	10/25/2018
main_login.php	1 KB	10/25/2018
menu.php	1 KB	2/4/2024 9
posts.sql	2 KB	5/8/2013 3

login page -> paste (1/2)



The screenshot shows a WinSCP Editor window displaying PHP code for a login page. The code includes file requirements, session variables, and a form for user input.

```
<?php
require 'config.php';
require 'database.php';
$g_title = BLOG_NAME . ' - Index';
$g_page = 'index';
require 'header.php';
require 'menu.php';

$posts = find_all_blogs(BLOG_INDEX_NUM_POSTS);
?>
<div id="all_blogs">

    <table width="300" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCCC">
        <tr>
            <form name="form1" method="post" action="checklogin.php">
                <td>
                    <table width="100%" border="0" cellpadding="3" cellspacing="1" bgcolor="#CCCCCC">
                        <tr>
                            <td colspan="3"><strong>Member Login </strong></td>
                        </tr>
                        <tr>
                            <td width="78">Username</td>
                            <td width="6">:</td>
                            <td width="294"><input name="myusername" type="text">
                        </tr>
                        <tr>
                            <td width="78">Password</td>
                            <td width="6">:</td>
                            <td width="294"><input name="mypassword" type="password">
                        </tr>
                        <tr>
                            <td colspan="3"><input type="submit" value="Login" /></td>
                        </tr>
                    </table>
                </td>
            </form>
        </tr>
    </table>
</div>
```

index.php -> copy

```
<tr>
    <td><input name="myusername" type="text" id="myusername" value="User Name">
    </td>
</tr>
<tr>
    <td>&ampnbsp</td>
    <td>&ampnbsp</td>
    <td><input type="submit" name="Submit" value="Log In">
    </td>
</tr>
</table>
</td>
</form>
</tr>
</table>

</div>
<?php
    require 'footer.php';
?>
```

login page -> paste (2/2)

```
<tr>
    <td><input name="myusername" type="text" id="myusername" value="admin" />
    <td><input name="mypassword" type="text" id="mypassword" value="password" />
</tr>
<tr>
    <td>&nbsp;</td>
    <td>&nbsp;</td>
    <td><input type="submit" name="Submit" value="Log In" />
</tr>
</table>
</td>
</form>
</tr>
</table>

</div>
<?php
    require 'footer.php';
?>
```

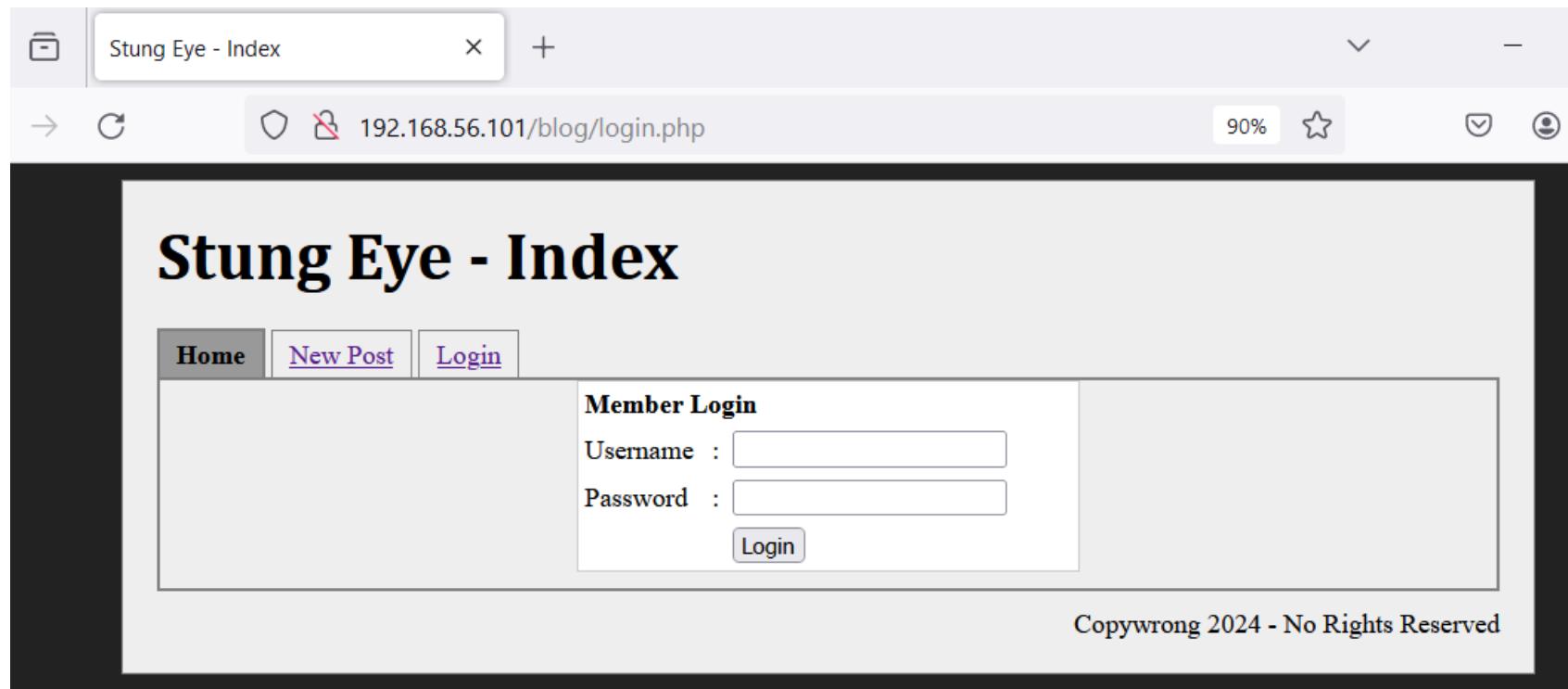
If you want, you can add the <HTML> and </HTML>



```
<html>
    <head>
        <title>Main Login Page</title>
    </head>
    <body>
        <?php
            require 'config.php';
            require 'database.php';
            $g_title = BLOG_NAME . ' - Index';
            $g_page = 'index';
            require 'header.php';
            require 'menu.php';

            $posts = find_all_blogs(BLOG_INDEX_NUM_POSTS);
        ?>
        <div id="all_blogs">
            <table width="300" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCCC">
                <tr>
                    <form name="form1" method="post" action="checklogin.php">
                        <td>
                            <table width="100%" border="0" cellpadding="3" cellspacing="1" bgcolor="#
```

Browser -> login page



Improve the web page

```
BLOG_INDEX_NUM_POSTS);
```

```
th="300" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCCC">
r>
<form name="form1" method="post" action="checklogin.php">
  <td>
    <table width="100%" border="0" cellpadding="3" cellspacing="1" bgcolor="#FFFFFF">
      <tr>
        <td colspan="3"><strong>Member Login </strong></td>
      </tr>
      <tr>
        <td width="78">Username</td>
        <td width="6">:</td>
        <td width="294"><input name="myusername" type="text" id="myusername"></td>
      </tr>
      <tr>
        <td>Password</td>
        <td>:</td>
        <td><input name="mypassword" type="text" id="mypassword"></td>
      </tr>
      <tr>
        <td>&ampnbsp</td>
        <td>&ampnbsp</td>
        <td><input type="submit" name="Submit" value="Login"></td>
      </tr>
    </table>
  </td>
</form>
```

Login page: Setting up StungEye Blog Software Competency



Login.php instead of checklogin.php

-> login

```
<table width="300" border="0" cellpadding="0" cellspacing="1">
    <tr>
        <form name="form1" method="post" action="login.php">
            <td>
                <table width="100%" border="0" cellpadding="3" cellspacing="1">
                    <tr>
                        <td colspan="3"><strong>Member Login </strong></td>
                    </tr>
                    <tr>
                        <td width="78">Username</td>
                        <td width="150"><input type="text" name="username" value="" /></td>
                        <td width="72"><input type="password" name="password" value="" /></td>
                    </tr>
                    <tr>
                        <td colspan="3" style="text-align: center; padding-top: 10px;"><input type="submit" value="Login" /></td>
                    </tr>
                </table>
            </td>
        </form>
    </tr>
</table>
```

\$g_page Instead of index - > login

```
<?php
    require 'config.php';
    require 'database.php';
    $g_title = BLOG_NAME . ' - Index';
    $g_page = 'login';
    require 'header.php';
    require 'menu.php';

    $posts = find_all_blogs(BLOG_INDEX_NUM_POSTS);
?>
<div id="all_blogs">

    <table width="300" border="0" cellpadding="0" cellspacing="0">
        <tr>
            <form name="form1" method="post">
```



Stung Eye - Index

[Home](#)[New Post](#)[Login](#)

New Post

May 8, 2013, 7:01 pm

This is some content.

Consectetuer Adipiscing

May 8, 2013, 6:12 pm

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec odio. Quisque volutpat mattis eros. Nullam malesuada erat ut turpis. Suspendisse urna nibh, viverra non, semper suscipit, posuere.

Luctus Metus Libero

May 8, 2013, 3:50 pm

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Phasellus hendrerit. Pellentesque aliquet nibh nec urna. In nisi neque, aliquet vel, dapibus id, mattis vel, nisi. Sed pretium, ligula sollicitudin laoreet viverra, tortor libero sodales leo, eget blandit nunc tortor eu nibh. Nullam mollis. Ut justo. Suspendisse potenti.

Sed egestas, ante et vulputate volutpat, eros pede semper est, vitae luctus metus libero eu augue. Morbi purus libero, faucibus adipiscing, commodo quis, gravida id, est. Sed lectus. Praesent elementum hendrerit tortor. Sed semper lorem at felis. Vestibulum volutpat, lacus a ultrices sagittis, mi neque euismod dui, eu pulvinar nunc sapien ornare nisl. Phasellus pede arcu, dapibus eu, fermentum et, dapibus sed, urna.



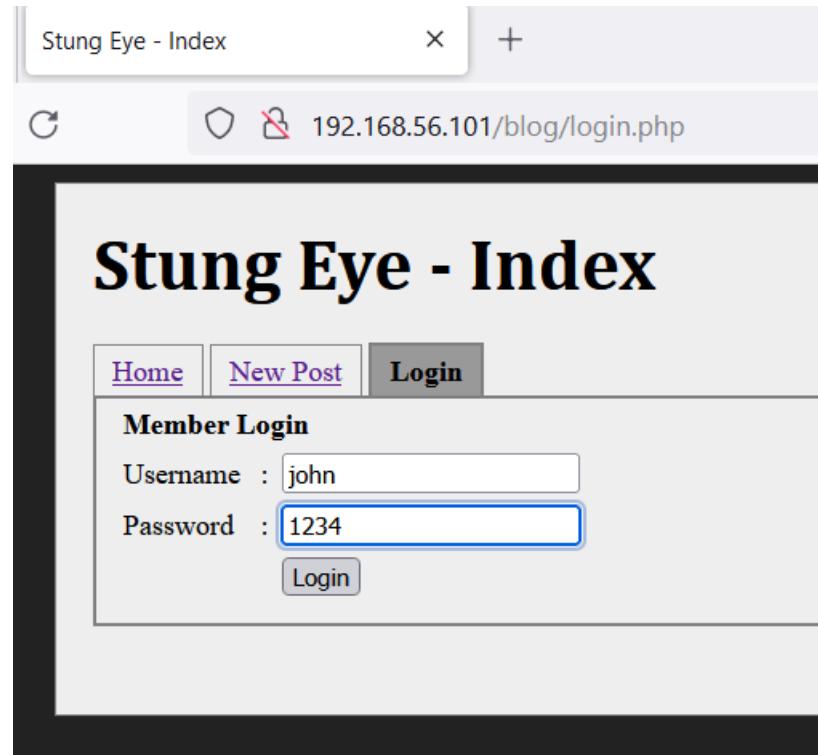
Blog website



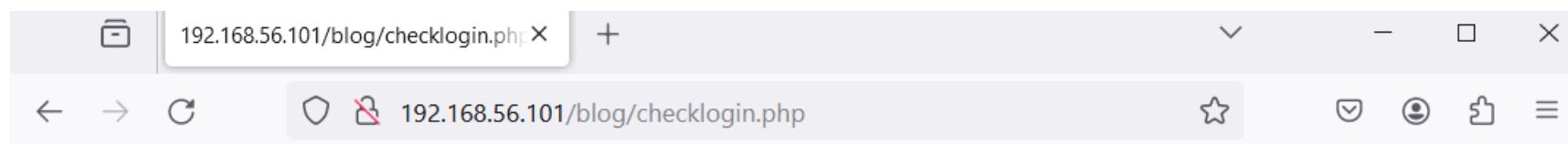
Login SQL Manager Lite for MySQL

The screenshot shows a MySQL database interface. In the left sidebar, under the 'Object' section, there is a dropdown menu set to 'blog on 192.168.56.101' and a table named 'members'. Below this, under 'General', are two buttons: 'Refresh' and 'Compile'. The main area displays a table with the following data:

	id	username	password	salt
1	john	1234	Null	



Output of Login



Show the error message in your PHP

Show the error message in your PHP

- PHP Version 7 has shown error messages.
- To fix your problem in PHP to show your error:

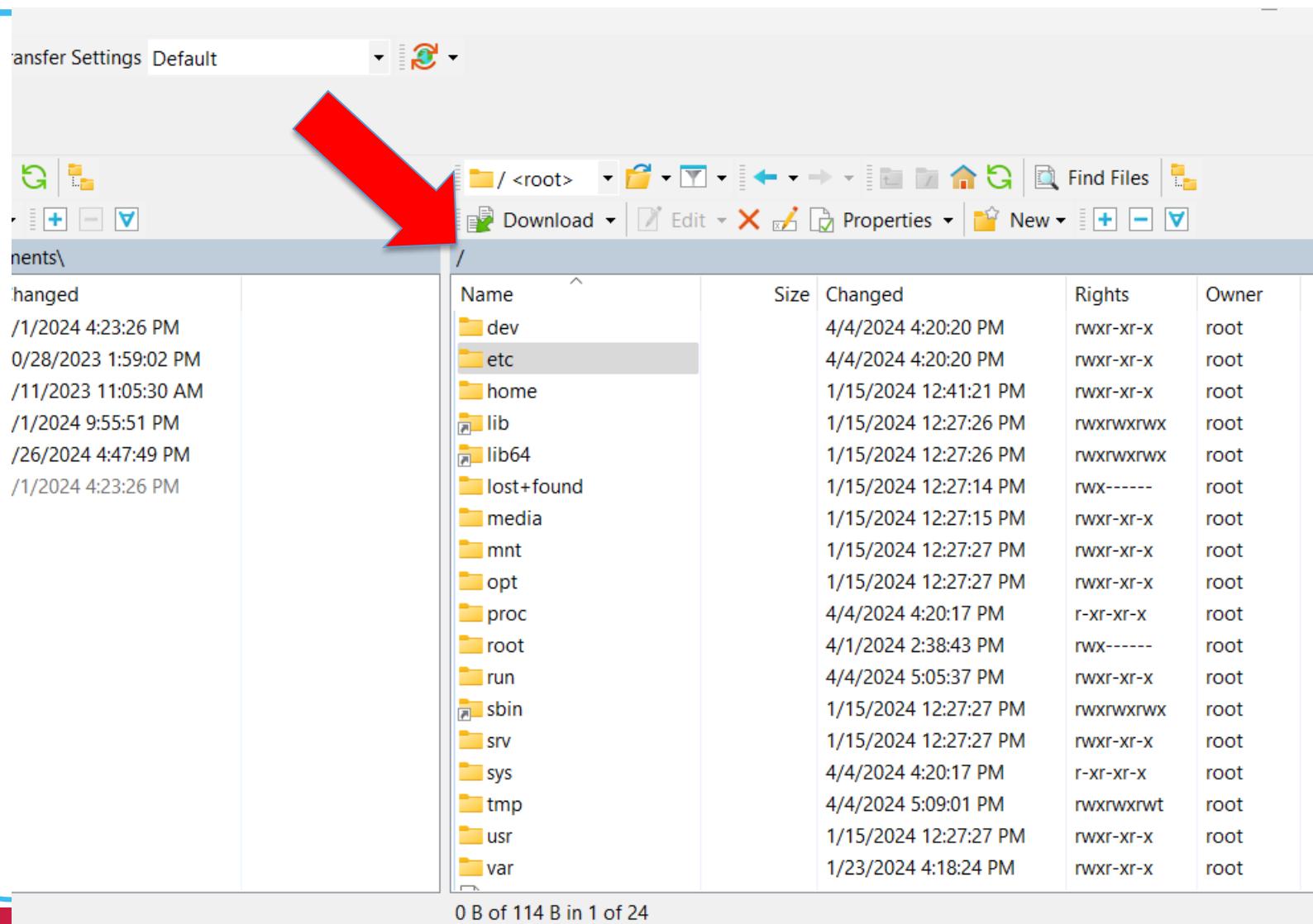
Open WinSCP

➤ You are in /var/www/html/blog

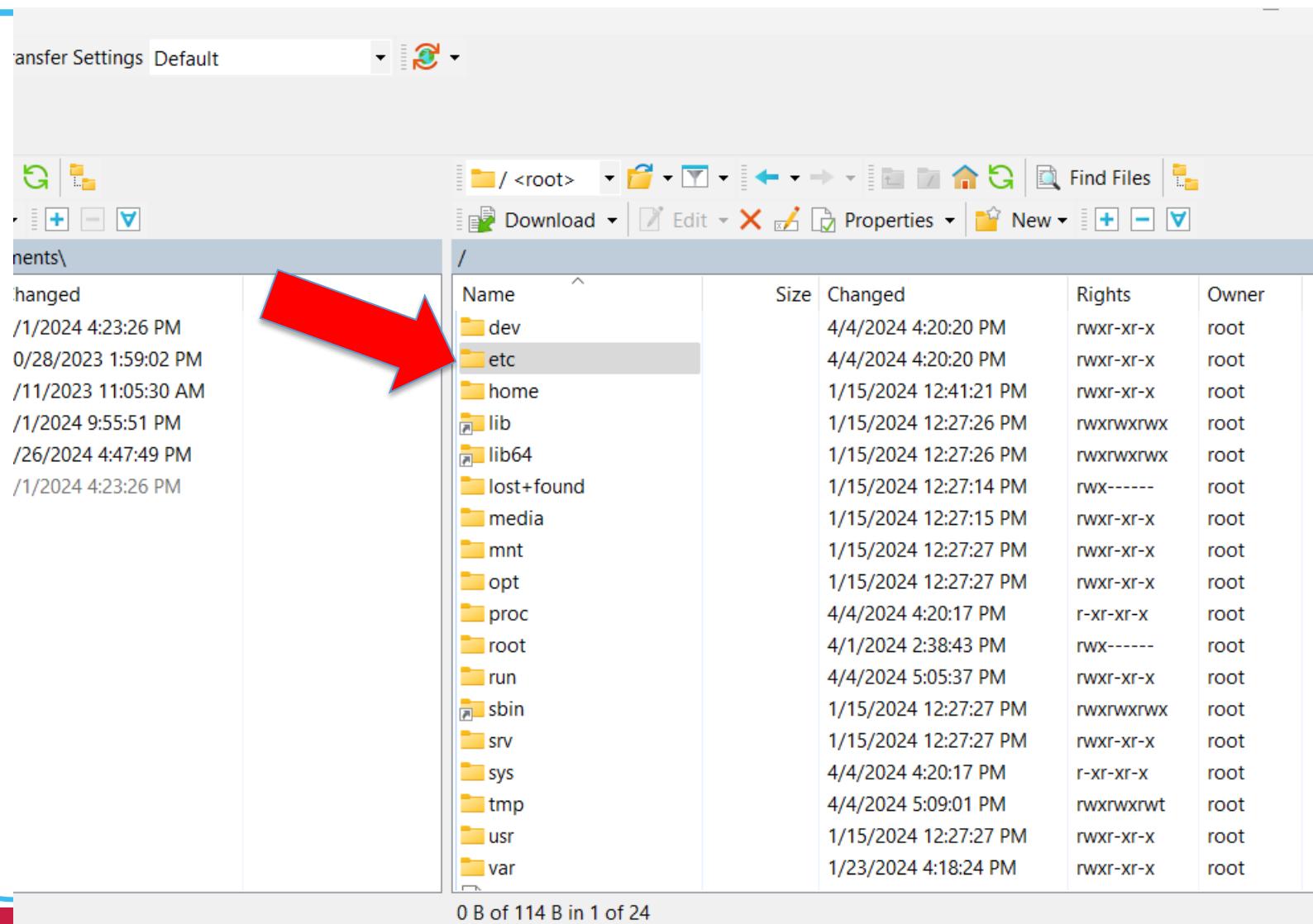
The screenshot shows the WinSCP graphical user interface. The top menu bar includes 'Queue', 'Transfer Settings' (set to 'Default'), and a connection icon. Below the menu is a toolbar with icons for Queue, Transfer Settings, Remote, Help, and various file operations. The left pane shows a local directory structure under 'Polytech\Documents\' with files like 'index.html', 'style.css', and 'script.js'. The right pane displays the contents of the '/var/www/html/blog/' directory. The directory structure includes a 'blog' folder and files such as 'checklogin.php', 'config.php', 'create.php', 'database.php', 'databaseconnection.php', 'encrypted_check_login...', 'encrypted_main_login...', 'encryption_examples....', 'footer.php', 'header.php', 'index.php', 'login.php', 'login_success.php', and 'logout.php'. The table provides details for each file, including Name, Size, Changed, Rights, and Owner.

Name	Size	Changed	Rights	Owner
index.html	2 KB	3/10/2024 5:25:31 PM	rwxrwxr-x	root
style.css	1 KB	4/4/2024 12:35:16 PM	rw-r--r--	maryam
script.js	1 KB	2/2/2024 6:21:27 PM	rw-r--r--	maryam
checklogin.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
config.php	2 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
create.php	1 KB	3/10/2024 10:06:48 PM	rw-r--r--	maryam
database.php	1 KB	10/26/2018 1:33:18 AM	rw-r--r--	maryam
databaseconnection.php	1 KB	10/25/2018 10:38:20 PM	rw-r--r--	maryam
encrypted_check_login...	2 KB	10/26/2018 1:00:18 AM	rw-r--r--	maryam
encrypted_main_login...	1 KB	10/25/2018 10:38:20 PM	rw-r--r--	maryam
encryption_examples....	2 KB	10/26/2018 1:00:18 AM	rw-r--r--	maryam
footer.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
header.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
index.php	1 KB	5/8/2013 3:44:52 PM	rw-r--r--	maryam
login.php	2 KB	4/1/2024 5:16:14 PM	rw-r--r--	maryam
login_success.php	1 KB	3/10/2024 10:02:30 PM	rw-r--r--	maryam
logout.php	1 KB	10/25/2018 10:38:20 PM	rw-r--r--	maryam

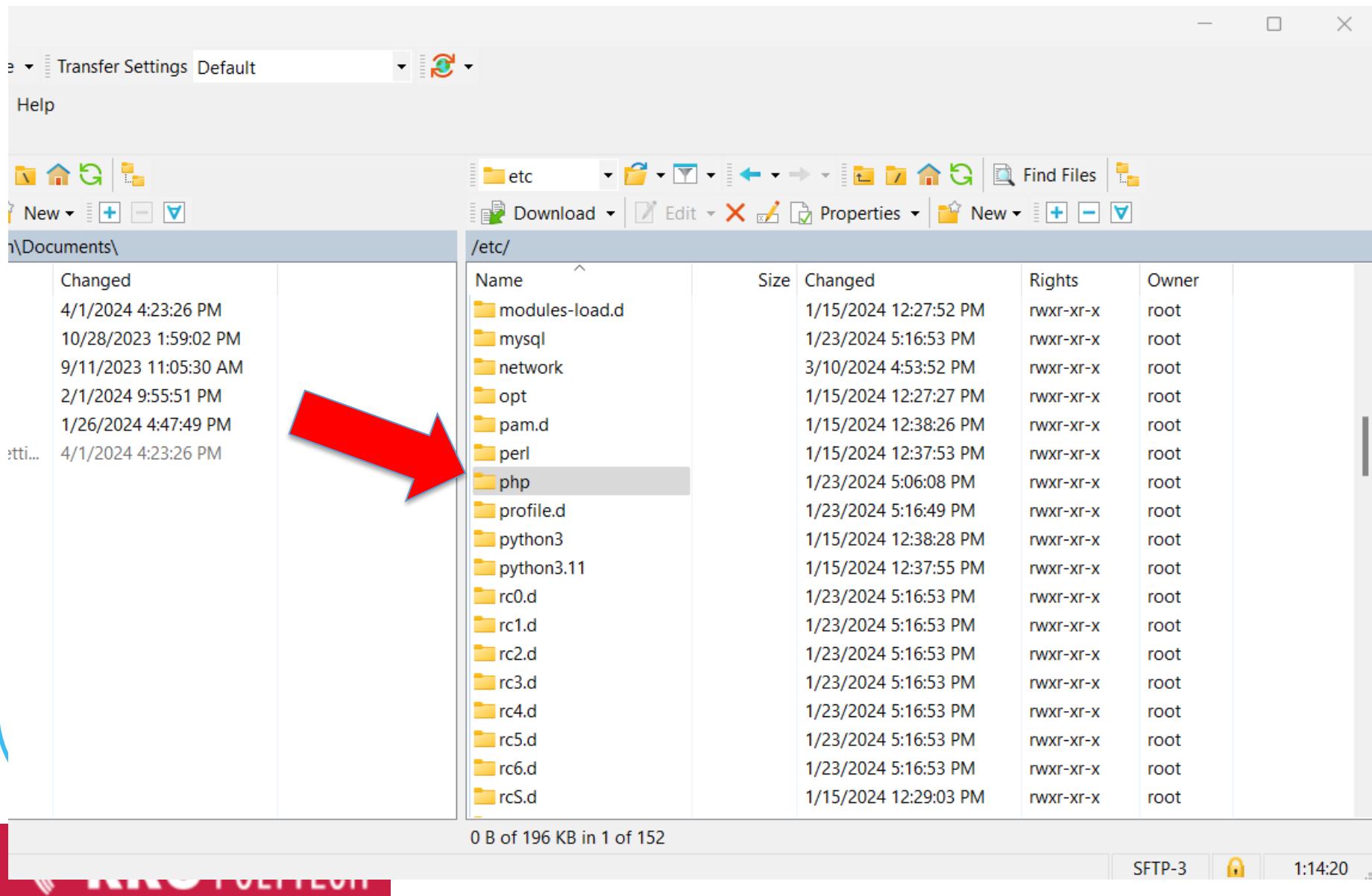
Go to the root of the system



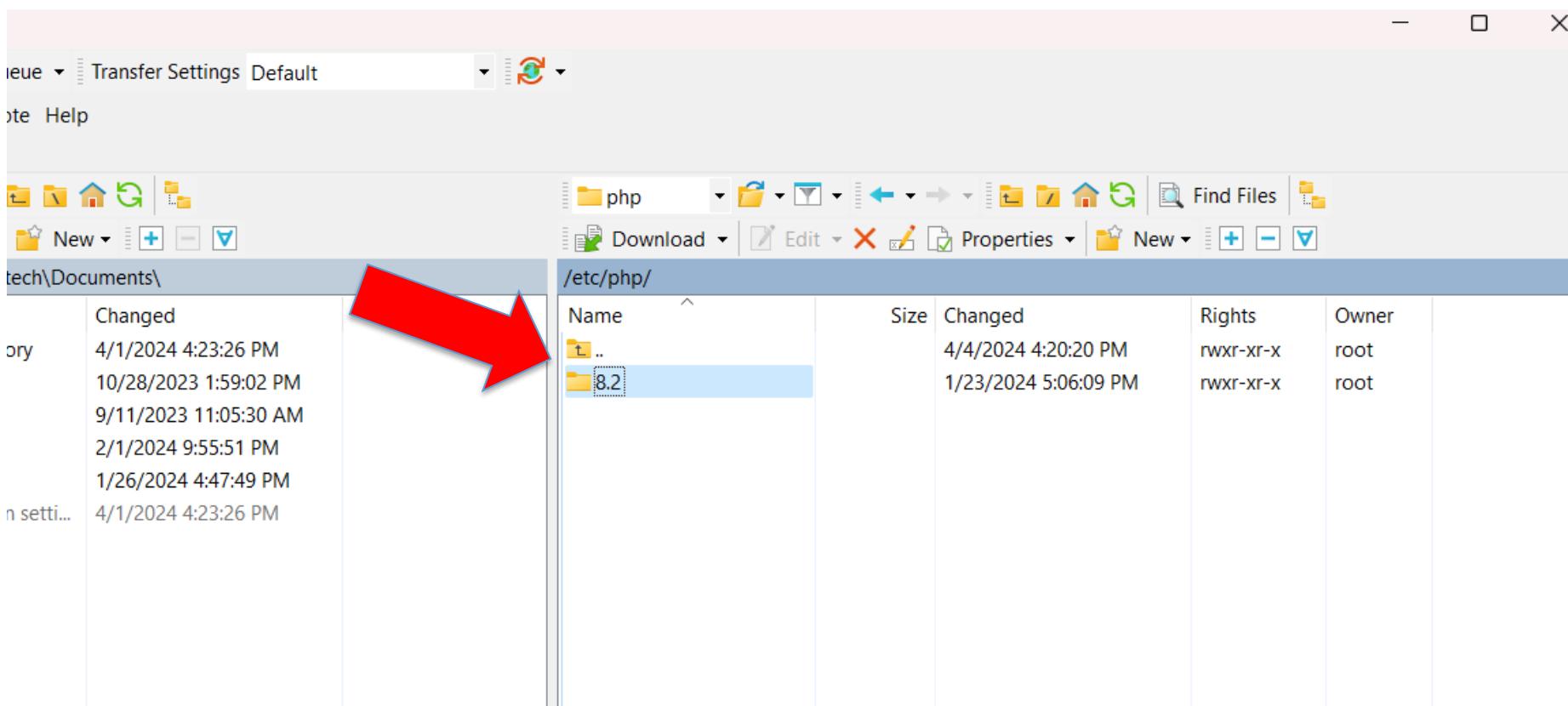
Go to the etc directory



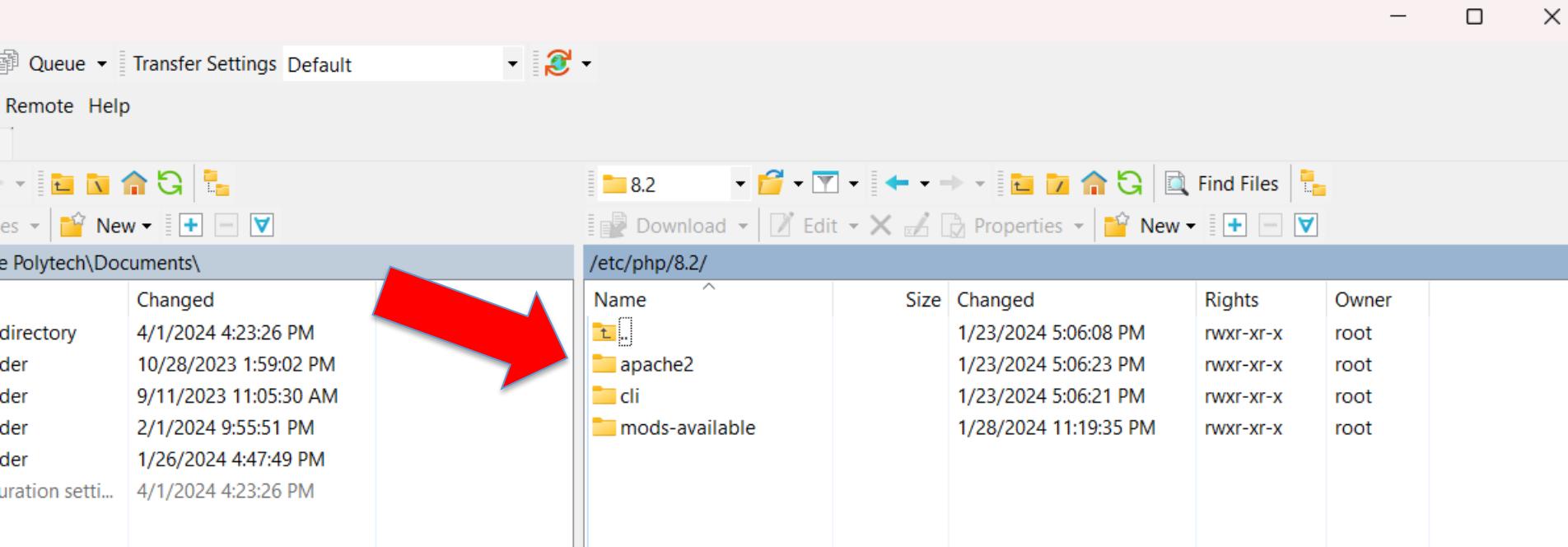
Go to the php directory



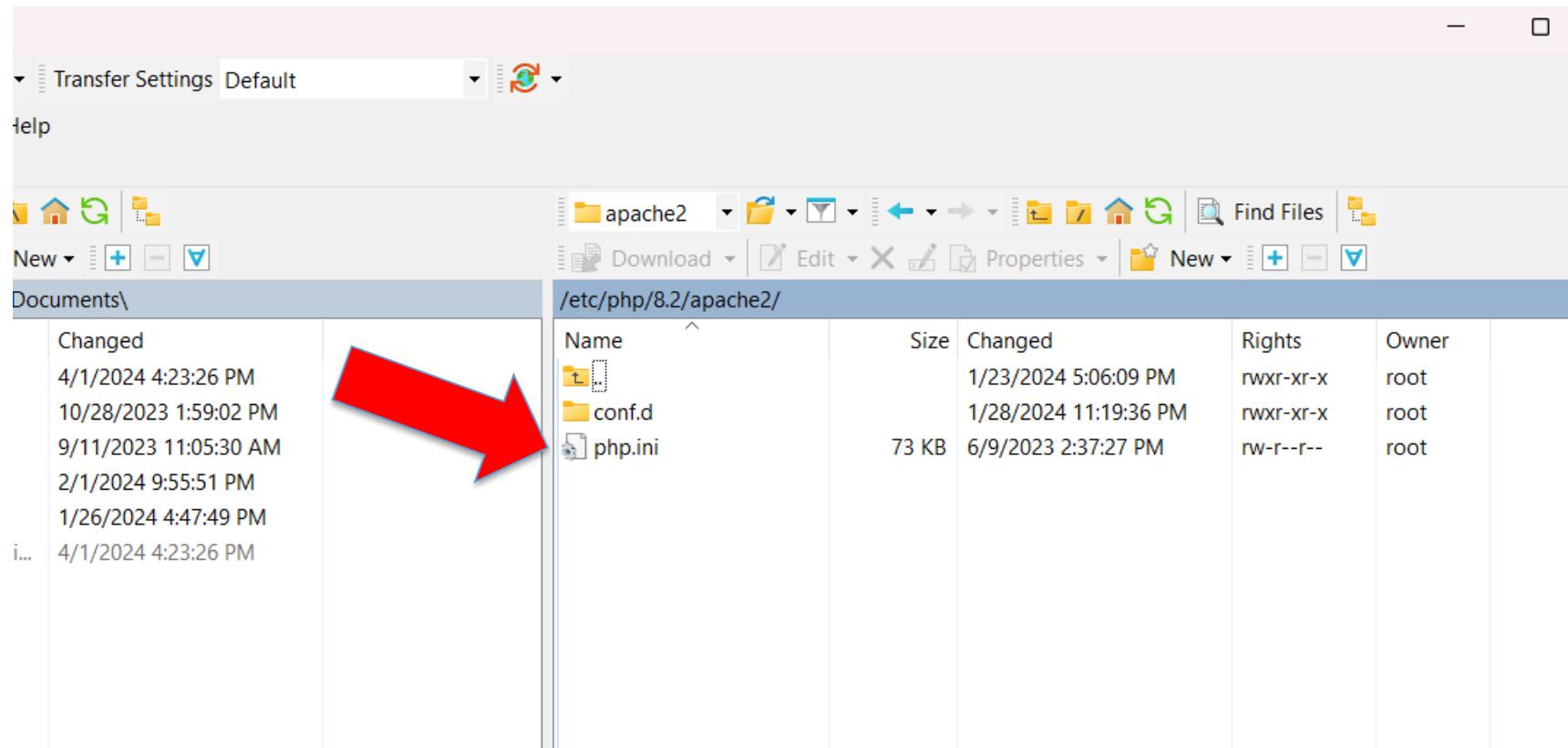
Go to the folder



Go to the apache2



There is php.ini file



Open php.ini file

C:\Users\mghanbari\AppData\Local\Temp\scp41241\etc\php\8.2\apache2\php.ini - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

php.ini

```
1 [PHP]
2
3 ;;;;;;;;;;;;;;;;;;;
4 ; About php.ini ;
5 ;;;;;;;;;;;;;;;;;;;
6 ; PHP's initialization file, generally called php.ini, is
    responsible for
7 ; configuring many of the aspects of PHP's behavior.
8
9 ; PHP attempts to find and load this configuration from a
    number of locations.
10 ; The following is a summary of its search order:
11 ; 1. SAPI module specific location.
12 ; 2. The PHPRC environment variable.
13 ; 3. A number of predefined registry keys on Windows
14 ; 4. Current working directory (except CLI)
```

Modify php.ini file to give us our “error”

- Because we are regular user in WinSCP, we cannot change php.ini file
- We should become root to modify php.ini
- Find the line of “display_errors = off” in php.ini

“display_errors = off” is in line 508 in my file

C:\Users\mghanbari\AppData\Local\Temp\scp41241\etc\php\8.2\apache2\php.ini - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

php.ini

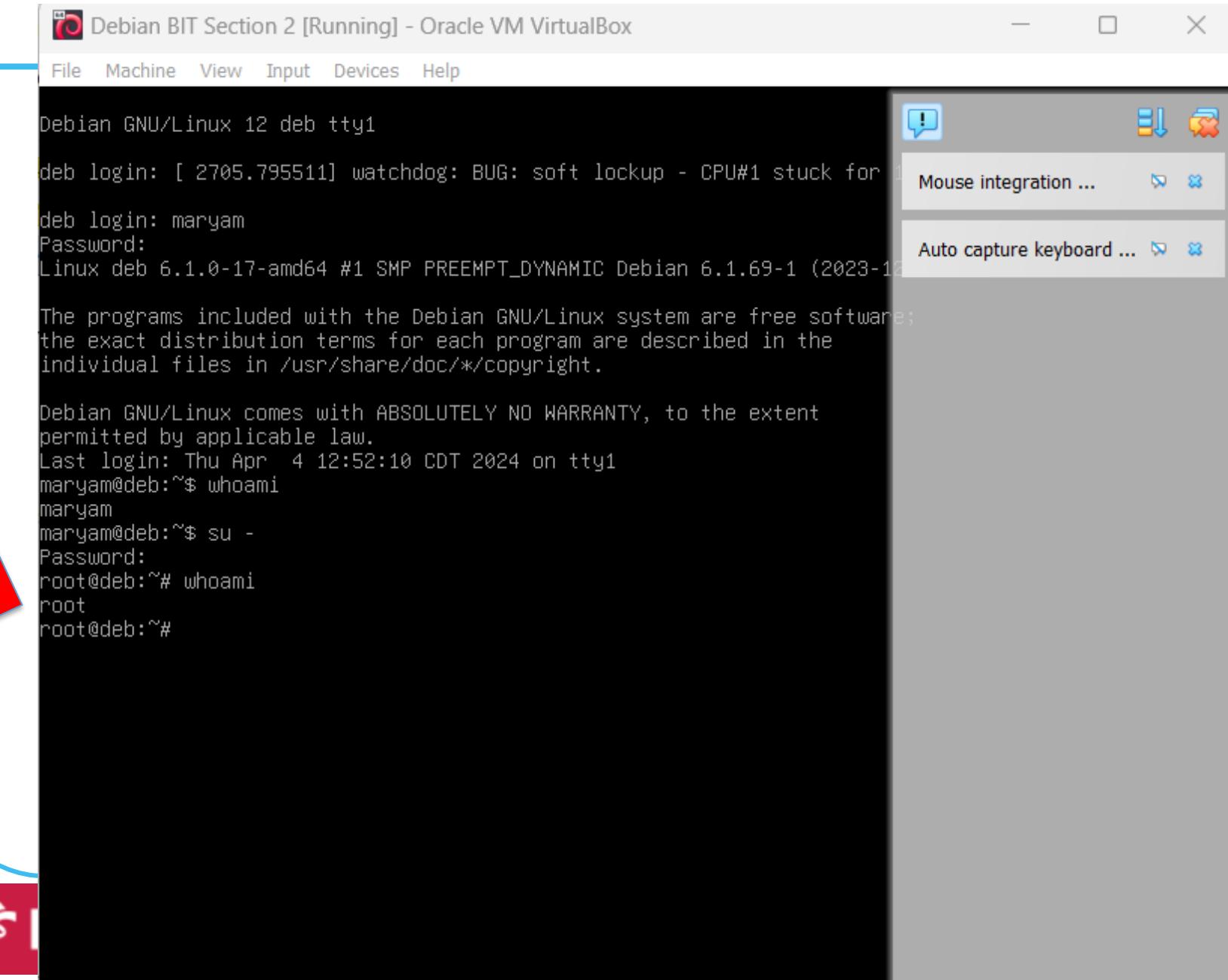
```
496 ; which is triggering the error, sensitive information could potentially leak
497 ; out of your application such as database usernames and passwords or worse.
498 ; For production environments, we recommend logging errors rather than
499 ; sending them to STDOUT.
500 ; Possible Values:
501 ; Off = Do not display any errors
502 ; stderr = Display errors to STDERR (affects only CGI/CLI binaries!)
503 ; On or stdout = Display errors to STDOUT
504 ; Default Value: On
505 ; Development Value: On
506 ; Production Value: Off
507 ; https://php.net/display-errors
508 display_errors = Off
509
510 ; The display of errors which occur during PHP's startup sequence are handled
511 ; separately from display_errors. We strongly recommend you set this to 'off'
512 ; for production servers to avoid leaking configuration details.
513 ; Default Value: On
514 ; Development Value: On
515 ; Production Value: Off
516 ; https://php.net/display-startup-errors
517 display_startup_errors = Off
518
519 ; Besides displaying errors, PHP can also log errors to locations such as a
520 ; log file, STDERR, a socket, or a file descriptor.
```

display_errors

Show Error in the Runtime

- Because “display_errors = off”, no error is shown in the runtime.
- Go to your terminal (Debian/PuTTY) and become root

Go to Your Terminal in Debian as root



Go to the etc directory

- Go to this directory and use TAB

```
root@deb:~# cd /etc/php/8.2/  
root@deb:/etc/php/8.2# _
```

Use ls to find where you should go

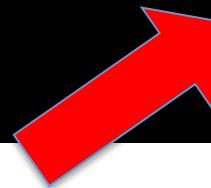
```
root@deb:/etc/php/8.2# ls  
apache2 cli mods-available  
root@deb:/etc/php/8.2# cd apache2/
```

Use ls to find where you should go

```
root@deb:/etc/php/8.2/apache2# ls
conf.d  php.ini
root@deb:/etc/php/8.2/apache2# _
```

Edit the “php.ini” File

```
root@deb:/etc/php/8.2/apache2# nano php.ini
```



Output

Debian BIT Section 2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

GNU nano 7.2 php.ini

[PHP]

```
;;;;;;;;;;;;;;;;;;;;
; About php.ini ;
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.

; PHP attempts to find and load this configuration from a number of locations.
; The following is a summary of its search order:
; 1. SAPI module specific location.
; 2. The PHPRC environment variable.
; 3. A number of predefined registry keys on Windows
; 4. Current working directory (except CLI)
; 5. The web server's directory (for SAPI modules), or directory of PHP
; (otherwise in Windows)
; 6. The directory from the --with-config-file-path compile time option, or the
; Windows directory (usually C:\windows)
; See the PHP docs for more specific information.
; https://php.net/configuration.file

; The syntax of the file is extremely simple. Whitespace and lines
; beginning with a semicolon are silently ignored (as you probably guessed).
; Section headers (e.g. [Foo]) are also silently ignored, even though
; they might mean something in the future.

; Directives following the section heading [PATH=/www/mysite] only
; apply to PHP files in the /www/mysite directory. Directives
; following the section heading [HOST=www.example.com] only apply to
; PHP files served from www.example.com. Directives set in these
; special sections cannot be overridden by user-defined INI files or
; at runtime. Currently, [PATH=] and [HOST=] sections only work under
; CGI/FastCGI.
```

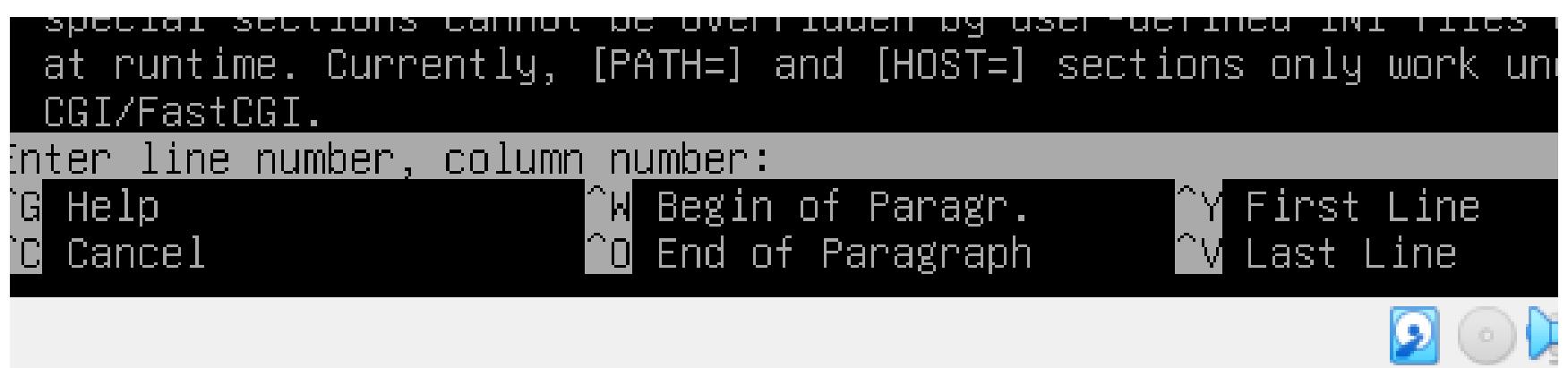
[Read 1977 lines]

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^Y Replace ^U Paste ^J Justify ^- Go To Line M-E Redo

Right Ctrl

Change the “display_errors = off” in php.ini

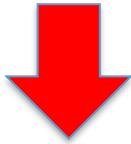
- There is a way of to go to line
- Control + underscore -> ^_



Change the “display_errors = off” in php.ini

- Go to the line number (for me it is 508)
- Hit enter
- Change the line from Off to On

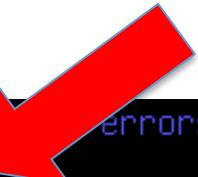
```
; https://php.net/display-errors  
display_errors = Off
```



```
; https://php.net/display-errors  
display_errors = On
```

Save the changes the “display_errors = off” in php.ini

- ^o : to save
- ^x : to exit

```
; https://php.net/display-errors
display_errors = On   
  
; The display of errors which occur during PHP's startup sequence are handled
; separately from display_errors. We strongly recommend you set this to 'off'
; for production servers to avoid leaking configuration details.
; Default Value: On
; Development Value: On
; Production Value: Off
; https://php.net/display-startup-errors
display_startup_errors = Off  
  
; Besides displaying errors, PHP can also log errors to locations such as a
; server-specific log, STDERR, or a location specified by the error_log
; directive found below. While errors should not be displayed on production
; servers they should still be monitored and logging is a great way to do that.
; Default Value: Off
; Development Value: On  
  
root@deb:/etc/php/8.2/apache2# 
```

Restart apache2

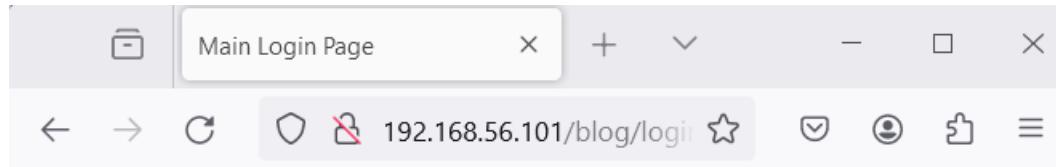
- Restart apache2 to allow you to display errors

```
root@deb:/etc/php/8.2/apache2# service apache2 restart
root@deb:/etc/php/8.2/apache2#
```

Reason of “display_errors = off” in php.ini

- This file was locked because hacker cannot compromise your server.

Output



Assignment

➤ You are ready to do Assignment 3: StungEye Blog

Thank you