

Lab 6: Securing Apache Web Server - 2

Task-1 (5 Marks):

In lab 5 you have created an HTTPS profile for your web server that you can access via <https://example.com>. However, the HTTP profile still remains there, meaning anyone can access your site using HTTP (<http://example.com>) as well. Try it to test it. If you want to fully secure your website, you must ensure that nobody can access it via HTTP. For this, we will use a specific module of Apache called mod_rewrite.

The mod_rewrite (https://httpd.apache.org/docs/current/mod/mod_rewrite.html) module can be utilised to redirect a user from one URL to another URL or one port to another port. In this task, you will need to redirect the user from the default port (80) of HTTP to the default port of HTTPS which is 443. In this way, even when a user tries to access <http://example.com>, the user will be redirected to <https://example.com> by the Apache web server!

Step 1: You can use the a2enmod command to enable a module and the a2dismod command to disable a module. Enable the mod_rewrite module using a2enmod command.

sudo a2enmod rewrite

Adding Authentication to Apache:

Step 2: Look at the /etc/apache2/sites-enabled directory to find the configuration file for port 80 for example.com. If unsure, look at the lab 4 manual once again to find this. Add the following lines in the virtual host for the 80 port within your respective configuration file.

Step 3: Test your Apache configuration using the following command:

```
RewriteEngine On  
RewriteCond %{HTTPS} !=on  
RewriteRule ^/?(.*)  
https:// %{SERVER_NAME}/$1 [R,L]
```

sudo apache2ctl configtest

Step 4: Restart the Apache server.

sudo systemctl restart apache2

The screenshot shows a terminal window with three tabs open, all titled "ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled". The terminal background is dark purple.

The first tab contains configuration prompts for an SSL certificate:

```
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:BD  
State or Province Name (full name) [Some-State]:Dhaka  
Locality Name (eg, city) []:Dhaka  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SUST  
Organizational Unit Name (eg, section) []:SWE  
Common Name (e.g. server FQDN or YOUR name) []:example.com  
Email Address []:
```

The second tab shows the command to change file permissions:

```
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ sudo chmod 600 /etc/ssl/private/apache-selfsigned.key
```

The third tab shows the command to change file permissions and then runs the Apache configuration test:

```
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ sudo chmod 644 /etc/ssl/certs/apache-selfsigned.crt  
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ sudo apache2ctl configtest
```

An error message is displayed:

```
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
```

The terminal then shows the command to start the Apache service:

```
Syntax OK  
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ sudo systemctl start apache2
```

It asks for a password for the user "ridwan-siam":

```
[sudo] password for ridwan-siam:
```

The command to enable the rewrite module is run:

```
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ sudo a2enmod rewrite
```

It asks for a password again:

```
[sudo] password for ridwan-siam:
```

The module is enabled:

```
Enabling module rewrite.
```

The command to activate the new configuration is run:

```
To activate the new configuration, you need to run:  
    systemctl restart apache2
```

The command to restart the Apache service is run:

```
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ systemctl restart apache2
```

The command to change the Apache configuration file is run:

```
ridwan-siam@ridwan-siam-VirtualBox:/etc/apache2/sites-enabled$ sudo nano example.com.conf
```

The command to restart the Apache service is run again:

```
ridwan-siam@ridwan-siam-VirtualBox:/etc/apache2/sites-enabled$ sudo systemctl restart apache2
```

The command to change the Apache configuration file is run again:

```
ridwan-siam@ridwan-siam-VirtualBox:/etc/apache2/sites-enabled$ sudo nano example.com.conf
```

The command to exit the terminal is run:

```
ridwan-siam@ridwan-siam-VirtualBox:/etc/apache2/sites-enabled$
```

Step 5: Test example.com on your browser. It should be redirected automatically to https://example.com. If this happens, show it to your teacher and tick off the first checkpoint.

Task-2 (7 Marks):

In this task, we will utilise a rudimentary authentication mechanism of Apache. The premise is that not all users can access your site. It can be accessed only by properly authenticated users. There are a couple of ways to do this. However, we will be using a method that uses an authentication file (called `.htpasswd`) containing the names and hashed passwords of allowed users.

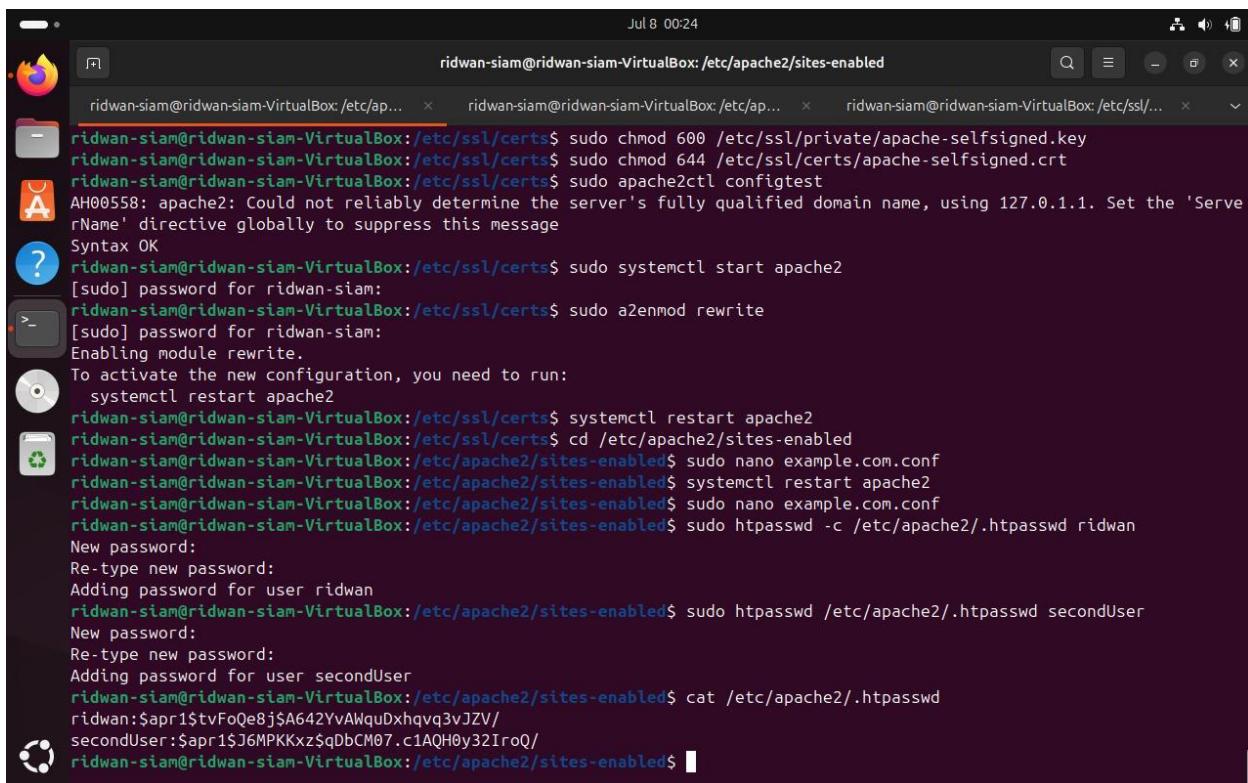
Step 1: Add users to your Apache web server using the following command:

sudo htpasswd -c /etc/apache2/.htpasswd username (change `username` with the username that you want for your first user). The `-c` option is used to create the first user. To add other users, you will need to skip that option.

- Add a second user to your Apache server using the `htpasswd` command.

Step 2: Use the following command to cat the contents of `.htpasswd` file:

cat /etc/apache2/.htpasswd



The screenshot shows a terminal window titled "ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled". The session starts with changing permissions for SSL certificates. It then runs `apache2ctl configtest`, which outputs an error about the server's FQDN. This is followed by starting Apache with `sudo systemctl start apache2` and enabling the rewrite module with `sudo a2enmod rewrite`. A note says to restart Apache after configuration changes. The user then creates a new user "ridwan" with `sudo htpasswd -c /etc/apache2/.htpasswd ridwan`. They are prompted for a password twice. Finally, they check the contents of the `.htpasswd` file with `cat /etc/apache2/.htpasswd`.

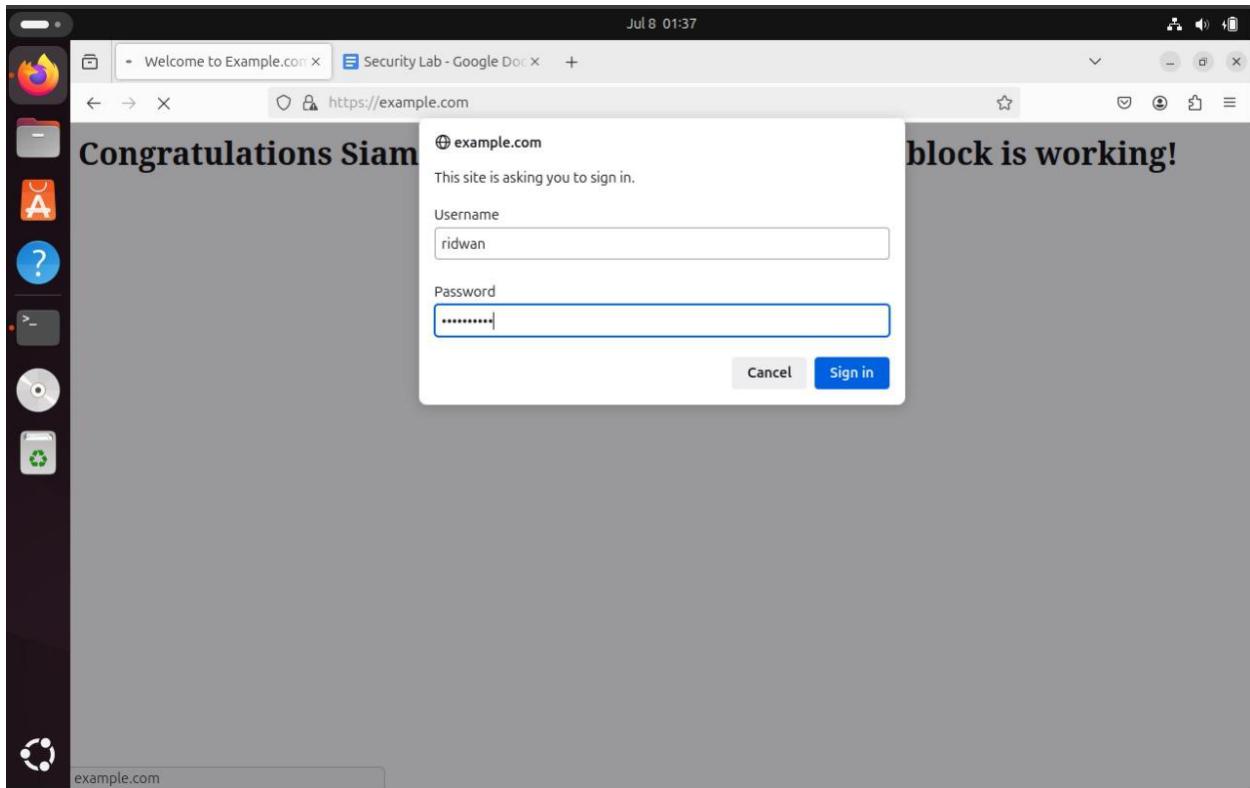
```
ridwan-siam@ridwan-siam-VirtualBox: /etc/ssl/certs$ sudo chmod 600 /etc/ssl/private/apache-selfsigned.key
ridwan-siam@ridwan-siam-VirtualBox: /etc/ssl/certs$ sudo chmod 644 /etc/ssl/certs/apache-selfsigned.crt
ridwan-siam@ridwan-siam-VirtualBox: /etc/ssl/certs$ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
ridwan-siam@ridwan-siam-VirtualBox: /etc/ssl/certs$ sudo systemctl start apache2
[sudo] password for ridwan-siam:
ridwan-siam@ridwan-siam-VirtualBox: /etc/ssl/certs$ sudo a2enmod rewrite
[sudo] password for ridwan-siam:
Enabling module rewrite.
To activate the new configuration, you need to run:
    systemctl restart apache2
ridwan-siam@ridwan-siam-VirtualBox: /etc/ssl/certs$ systemctl restart apache2
ridwan-siam@ridwan-siam-VirtualBox: /etc/ssl/certs$ cd /etc/apache2/sites-enabled
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ sudo nano example.com.conf
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ systemctl restart apache2
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ sudo nano example.com.conf
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ sudo htpasswd -c /etc/apache2/.htpasswd ridwan
New password:
Re-type new password:
Adding password for user ridwan
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ sudo htpasswd /etc/apache2/.htpasswd secondUser
New password:
Re-type new password:
Adding password for user secondUser
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ cat /etc/apache2/.htpasswd
ridwan:$apr1$tvFoQe8j$A642YvAkquDxhqvq3vJZV/
secondUser:$apr1$J6MPKKxz$QDbCM07.c1AQH0y32IroQ/
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$
```

You will something like the following, containing the usernames and their corresponding hashed passwords:

Step 3: Next, add the following into your https configuration file for `example.com`.

Step 4: Restart the apache server.

Step 5: Try to access `https://example.com` from your browser. When prompted for username and password, provide the ones that you created earlier. If you can access the site, show it to your teacher to tick off the second checkpoint.



Task-3 (8 Marks):

In this task, you will add a bit more advanced authentication mechanism. Even though you can use the basic authentication mechanism using the steps of Task-2, it is not very convenient. Modern web servers often rely on a database to authenticate a user. In this task, you will need an authentication mechanism that relies on MySQL database. For this at first, you will need to add a user with his/her corresponding password into the database and then configure the Apache server to initiate authentication using MySQL.

Step 1: Install MySQL server on your ubuntu using the following commands:

sudo apt-get update

sudo apt-get install mysql-server.

```
Jul 8 05:36
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled
File Edit View Search Terminal Tabs Help
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ systemctl restart apache2
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ sudo nano example.com.conf
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ systemctl restart apache2
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ sudo nano example.com.conf
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ systemctl restart apache2
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ sudo apt-get update
[sudo] password for ridwan-siam:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://bd.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://bd.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://bd.archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 126 kB in 4s (33.1 kB/s)
Reading package lists... Done
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ sudo apt-get install mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
 libaio1t64 libcgifast-perl libcgipm-perl libevent-pthreads-2.1-7t64 libfcgi-bin
 libfcgi-perl libfcgi0t64 libhtml-template-perl libmecab2 libprotobuf-lite32t64 mecab-ipadic mecab-ipadic-utf8
 mecab-utils mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server-8.0 mysql-server-core-8.0
Suggested packages:
 libipc-sharedcache-perl mailx tinyca
The following NEW packages will be installed:
 libaio1t64 libcgifast-perl libcgipm-perl libevent-pthreads-2.1-7t64 libfcgi-bin
 libfcgi-perl libfcgi0t64 libhtml-template-perl libmecab2 libprotobuf-lite32t64 mecab-ipadic mecab-ipadic-utf8
 mecab-utils mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server mysql-server-8.0 mysql-server-core-8.0
0 upgraded, 20 newly installed, 0 to remove and 62 not upgraded.
Need to get 29.3 MB of archives.
After this operation, 242 MB of additional disk space will be used.
```

You might be required to submit a password for root. Use cse for this.

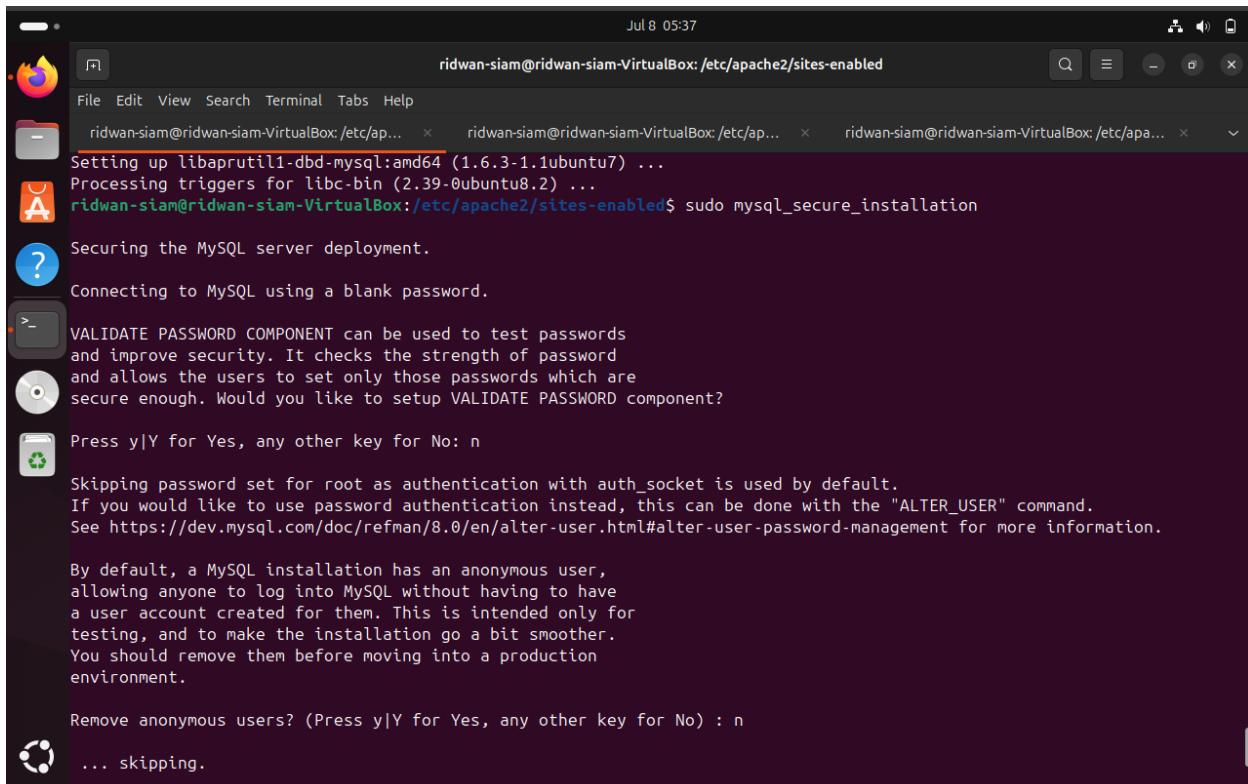
sudo apt-get install libaprutil1-dbd-mysql

```
Jul 8 05:37
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled
File Edit View Search Terminal Tabs Help
mysqld will log errors to /var/log/mysql/error.log
mysqld is running as pid 17613
Created symlink /etc/systemd/system/multi-user.target.wants/mysql.service → /usr/lib/systemd/system/mysql.service.
Setting up mysql-server (8.0.37-0ubuntu0.24.04.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.2) ...
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ sudo apt-get install libaprutil1-dbd-mysql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
 libmysqlclient21
The following NEW packages will be installed:
 libaprutil1-dbd-mysql libmysqlclient21
0 upgraded, 2 newly installed, 0 to remove and 62 not upgraded.
Need to get 1,267 kB of archives.
After this operation, 6,899 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://bd.archive.ubuntu.com/ubuntu noble-updates/main amd64 libmysqlclient21 amd64 8.0.37-0ubuntu0.24.04.1 [1,254 kB]
Get:2 http://bd.archive.ubuntu.com/ubuntu noble/universe amd64 libaprutil1-dbd-mysql amd64 1.6.3-1.1ubuntu7 [13.4 kB]
Fetched 1,267 kB in 3s (366 kB/s)
Selecting previously unselected package libmysqlclient21:amd64.
(Reading database ... 148956 files and directories currently installed.)
Preparing to unpack .../libmysqlclient21_8.0.37-0ubuntu0.24.04.1_amd64.deb ...
Unpacking libmysqlclient21:amd64 (8.0.37-0ubuntu0.24.04.1) ...
Selecting previously unselected package libaprutil1-dbd-mysql:amd64.
Preparing to unpack .../libaprutil1-dbd-mysql_1.6.3-1.1ubuntu7_amd64.deb ...
Unpacking libaprutil1-dbd-mysql:amd64 (1.6.3-1.1ubuntu7) ...
Setting up libmysqlclient21:amd64 (8.0.37-0ubuntu0.24.04.1) ...
```

Step 2: Configuring MySQL using the following command:

mysql_secure_installation

Select no for every option except the last when you are prompted to reload the privilege table. Remember, in production environment you most probably will need to choose more sensible options as per your organization's policy. So don't choose all nos in a production environment.



The screenshot shows a terminal window titled "ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled". The terminal is displaying the output of the "mysql_secure_installation" command. It starts with some system setup messages, then asks if the user wants to secure the MySQL server deployment. The user responds with "n". It then asks if the user wants to connect to MySQL using a blank password, and again the user responds with "n". It then asks if the user wants to validate password components, and the user responds with "n". Finally, it asks if the user wants to remove anonymous users, and the user responds with "n". The terminal window has a dark background with light-colored text and icons.

Step 3: After this, check the status of the mysql service:

systemctl status mysql.service

If you see the service is running, then proceed to the next step.

Step 4: Login to the MySQL using the following command:

mysql -u root -p

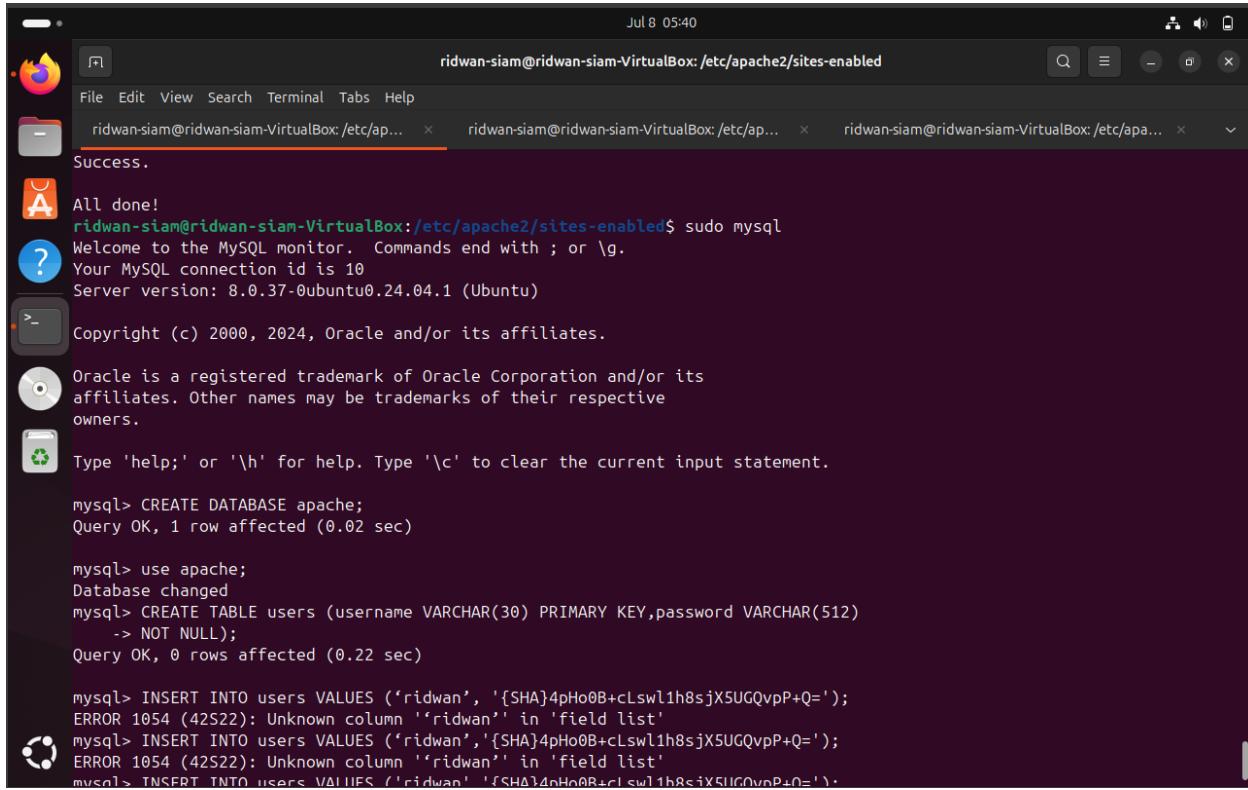
Step 5: Create a database called apache using the following command in the MySQL console:

CREATE DATABASE apache;

Step 6: Use the following command to use the apache database in the MySQL console: **use apache;**

Step 7: Create a table called users using the following command with the supplied attributes in the MySQL console:

CREATE TABLE users (username VARCHAR(30) PRIMARY KEY,password VARCHAR(512) NOT NULL);



```
Jul 8 05:40
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled
File Edit View Search Terminal Tabs Help
ridwan-siam@ridwan-siam-VirtualBox: /etc/ap... x ridwan-siam@ridwan-siam-VirtualBox: /etc/ap... x ridwan-siam@ridwan-siam-VirtualBox: /etc/ap...
Success.

All done!
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled$ sudo mysql
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.37-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE apache;
Query OK, 1 row affected (0.02 sec)

mysql> use apache;
Database changed
mysql> CREATE TABLE users (username VARCHAR(30) PRIMARY KEY,password VARCHAR(512)
-> NOT NULL);
Query OK, 0 rows affected (0.22 sec)

mysql> INSERT INTO users VALUES ('ridwan', '{SHA}4pHo0B+cLswl1h8sjX5UGQvpP+Q=');
ERROR 1054 (42S22): Unknown column 'ridwan' in 'field list'
mysql> INSERT INTO users VALUES ('ridwan', '{SHA}4pHo0B+cLswl1h8sjX5UGQvpP+Q=');
ERROR 1054 (42S22): Unknown column 'ridwan' in 'field list'
mysql> INSERT INTO users VALUES ('ridwan', '{SHA}4pHo0B+cLswl1h8sjX5UGQvpP+Q=');

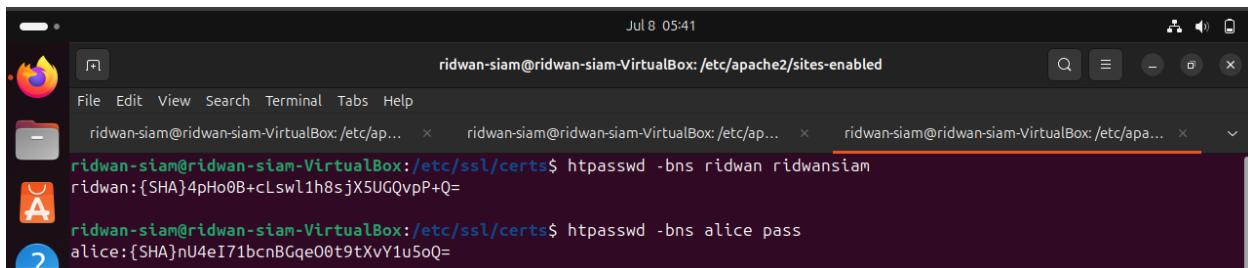

```

Step 8: Now, we will add users to our table. But before that we need to create a hashed password which will be stored in the database. Remember, never store plain password in your database. Use the following command to create hashed password for a user called sammy in a separate console:

htpasswd -bnS sammy sammys_password (change this to whatever you want)

You will see an output like the following in your console:

sammy:{SHA}tk7HEH6Wo7SKT6+3FHCgiGnJ6dA=



```
Jul 8 05:41
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled
File Edit View Search Terminal Tabs Help
ridwan-siam@ridwan-siam-VirtualBox: /etc/ap... x ridwan-siam@ridwan-siam-VirtualBox: /etc/ap... x ridwan-siam@ridwan-siam-VirtualBox: /etc/ap...
ridwan-siam@ridwan-siam-VirtualBox: /etc/ssl/certs$ htpasswd -bnS ridwan ridwansiam
ridwan:{SHA}4pHo0B+cLswl1h8sjX5UGQvpP+Q=
ridwan-siam@ridwan-siam-VirtualBox: /etc/ssl/certs$ htpasswd -bnS alice pass
alice:{SHA}nU4eI71bcnB0qe00t9tXvY1u5oQ=
```

Copy everything after ':' (that starts with {SHA}) and save it somewhere. In MySQL console, use the following command to add a user called Sammy:

INSERT INTO users VALUES ('sammy', '{SHA}+9C5w2dyQYmbrXe+Sdy7aUcafU=');

Change '{SHA}+9C5w2dyQYmbrXe+Sdy7aUcafU=' with the content that you copied earlier. Repeat the same steps to add another user called alice.

```
Jul 8 05:42
ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled
File Edit View Search Terminal Tabs Help
ridwan-siam@ridwan-siam-VirtualBox: /etc/ap... x ridwan-siam@ridwan-siam-VirtualBox: /etc/ap... x ridwan-siam@ridwan-siam-VirtualBox: /etc/ap...
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> CREATE DATABASE apache;
Query OK, 1 row affected (0.02 sec)

mysql> use apache;
Database changed
mysql> CREATE TABLE users (username VARCHAR(30) PRIMARY KEY,password VARCHAR(512)
-> NOT NULL);
Query OK, 0 rows affected (0.22 sec)

mysql> INSERT INTO users VALUES ('ridwan', '{SHA}4pHo0B+cLswl1h8sjX5UGQvpP+Q=');
ERROR 1054 (42S22): Unknown column ''ridwan'' in 'field list'
mysql> INSERT INTO users VALUES ('ridwan', '{SHA}4pHo0B+cLswl1h8sjX5UGQvpP+Q=');
ERROR 1054 (42S22): Unknown column ''ridwan'' in 'field list'
mysql> INSERT INTO users VALUES ('ridwan', '{SHA}4pHo0B+cLswl1h8sjX5UGQvpP+Q=');
Query OK, 1 row affected (0.10 sec)

mysql> INSERT INTO users VALUES ('ridwan', '{SHA}nU4eI71bcnBGqe00t9tXvY1u5oQ=');
ERROR 1062 (23000): Duplicate entry 'ridwan' for key 'users.PRIMARY'
mysql> INSERT INTO users VALUES ('alice', '{SHA}nU4eI71bcnBGqe00t9tXvY1u5oQ=');
Query OK, 1 row affected (0.03 sec)
mysql>
```

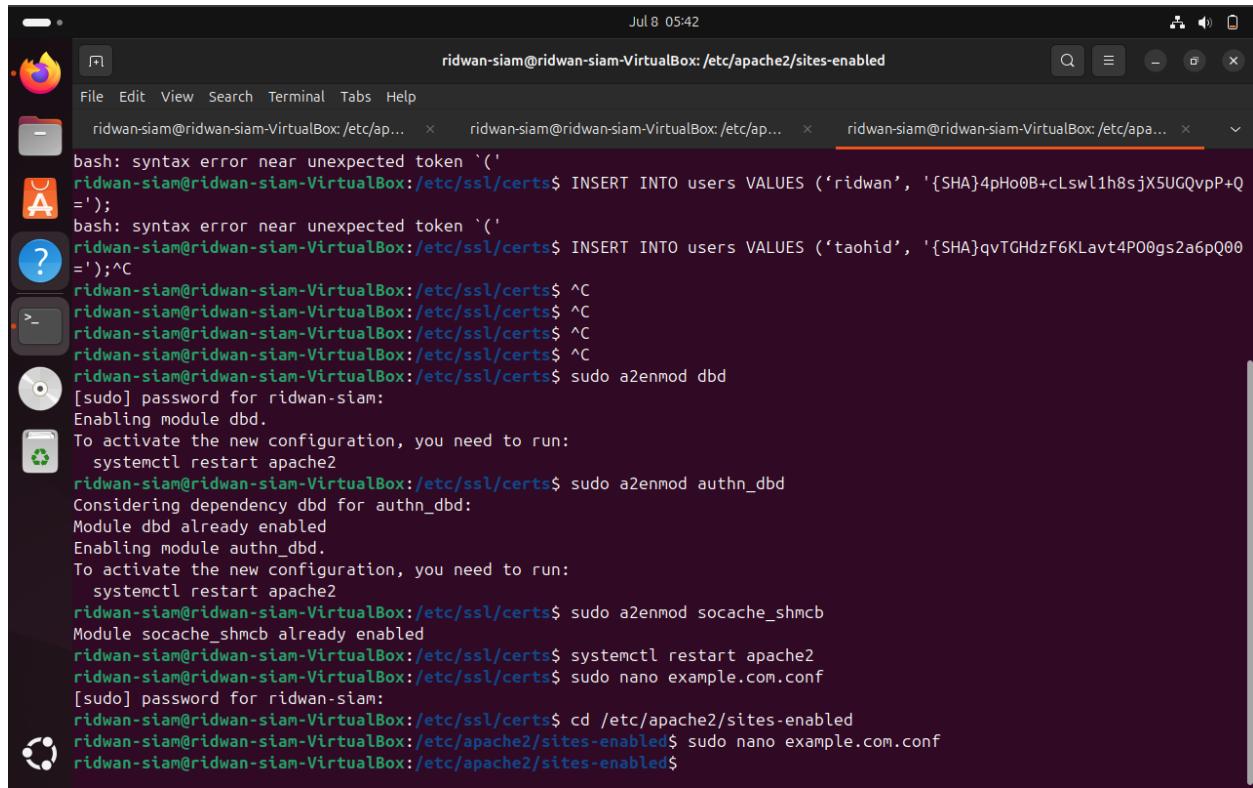
Step 9: Next, issue the following commands to enable the mod_authn_dbm module of Apache. This can be done by enabling the following modules:

sudo a2enmod dbd
sudo a2enmod authn_dbm
sudo a2enmod socache_shmcb
sudo a2enmod authn_socache

Step 10: Get rid of what you added in the Step 3 of Task 2 and replace it with the following contents:

Step 11: Restart the Apache server.

Step 12: Try to access the example.com page and when prompted for username/password, provide the one that have in your MySQL database. If everything works fine, you will be able access the page. At this stage, show it to your teacher to tick-off the final checkpoint.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "ridwan-siam@ridwan-siam-VirtualBox: /etc/apache2/sites-enabled". The terminal content shows the following steps:

```
Jul 8 05:42
File Edit View Search Terminal Tabs Help
ridwan-siam@ridwan-siam-VirtualBox:/etc/ap... x ridwan-siam@ridwan-siam-VirtualBox:/etc/ap... x ridwan-siam@ridwan-siam-VirtualBox:/etc/ap... x
bash: syntax error near unexpected token `('
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ INSERT INTO users VALUES ('ridwan', '{SHA}4pHo0B+cLswl1h8sjX5UGQvpP+Q
=');'
bash: syntax error near unexpected token `('
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ INSERT INTO users VALUES ('taohid', '{SHA}qvTGHdzF6KLavt4P00gs2a6pQ00
=');^C
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ ^C
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ ^C
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ ^C
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ sudo a2enmod dbd
[sudo] password for ridwan-siam:
Enabling module dbd.
To activate the new configuration, you need to run:
  systemctl restart apache2
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ sudo a2enmod authn_dbd
Considering dependency dbd for authn_dbd:
Module dbd already enabled
Enabling module authn_dbd.
To activate the new configuration, you need to run:
  systemctl restart apache2
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ sudo a2enmod socache_shmcb
Module socache_shmcb already enabled
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ systemctl restart apache2
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ sudo nano example.com.conf
[sudo] password for ridwan-siam:
ridwan-siam@ridwan-siam-VirtualBox:/etc/ssl/certs$ cd /etc/apache2/sites-enabled
ridwan-siam@ridwan-siam-VirtualBox:/etc/apache2/sites-enabled$ sudo nano example.com.conf
ridwan-siam@ridwan-siam-VirtualBox:/etc/apache2/sites-enabled$
```

