**2019831074 – Mehrajul Islam**

**LAB 6 REPORT**

**Objective**

The objective of this lab is to extend the functionalities of a previously secured web server by incorporating authentication mechanisms to control access to the server. We aim to achieve the following:

* Redirect HTTP traffic to HTTPS.
* Implement basic authentication using .htpasswd.
* Implement authentication using MySQL database.

**Checkpoint 1: Redirect HTTP to HTTPS**

1. Used the command sudo a2enmod rewrite to enable the mod\_rewrite module.
2. Edited the configuration file for port 80 located in /etc/apache2/sites-enabled/ directory.
3. Used sudo apache2ctl configtest to test the Apache configuration
4. Restarted the server and Accessed http://example.com in the browser to confirm it redirects to <https://example.com>.

**Observations:**

* Successfully redirected HTTP traffic to HTTPS, ensuring secure communication by default.

**Checkpoint 2: Basic Authentication using .htpasswd**

1. Added users to the Apache server using the htpaswd
2. Added another user in same way
3. Verified the users
4. Configured the example.com and added a code snippet at example.conf file to enable htpsswd authentication
5. Accessed https://example.com and provided the credentials when prompted.

**Observations:**

* Successfully implemented basic authentication using .htpasswd. Only authenticated users could access the website.

**Checkpoint 3: Authentication using MySQL Database**

1. Installed mysql
2. Configured mysql using mysql\_secure\_installation
3. Created Apache database and users table and added the users and hashed passwords
4. Then I enabled some Apache Modules
5. Then removed the configuration before and added new config for mysql
6. Accessed https://example.com and logged in with the MySQL credentials.

**Observations:**

* Successfully implemented database-backed authentication. The website could be accessed only by users authenticated through MySQL.

Here are some screenshots of my work:

