LAB TASK 6

Checkpoint-1:


```
  GNU nano 6.2
<VirtualHost *:80>
    ServerAdmin webmaster@example.com
    ServerName example.com
    ServerAlias www.example.com

    DocumentRoot /var/www/example.com/html

    # Redirect all traffic to HTTPS
    Redirect permanent / https://example.com/

    ErrorLog ${APACHE_LOG_DIR}/example.com_error.log
    CustomLog ${APACHE_LOG_DIR}/example.com_access.log combined
</VirtualHost>

<VirtualHost _default_:443>
              ServerAdmin admin@example.com
```



```
$ sudo a2enmod rewrite
Module rewrite already enabled
$ cd /etc/apache2/sites-enabled
$ ls
default-ssl.conf  example.com.conf
$ sudo nano example.com.conf
$ sudo nano example.com.conf
$
```

```
$ sudo a2enmod rewrite
Module rewrite already enabled
$ cd /etc/apache2/sites-enabled
$ ls
default-ssl.conf  example.com.conf
$ sudo nano example.com.conf
$ sudo nano example.com.conf
$
```
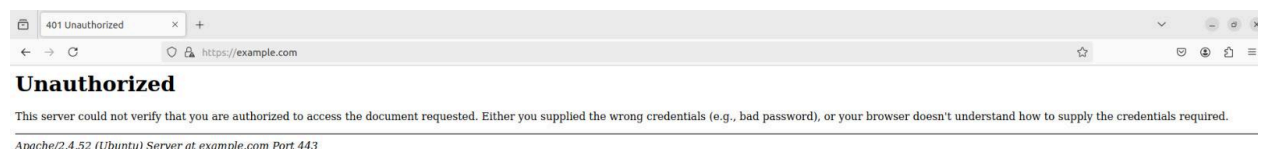
← → C   ○ 🔒 https://example.com

hello I am taohid, This is Lab task 5

Checkpoint-2:

```
$ sudo a2enmod rewrite
Module rewrite already enabled
$ cd /etc/apache2/sites-enabled
$ ls
default-ssl.conf  example.com.conf
$ sudo nano example.com.conf
$ sudo nano example.com.conf
$ sudo systemctl restart apache2
$ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualif
Syntax OK
$ sudo systemctl restart apache2
$ sudo htpasswd -c /etc/apache2/.htpasswd taohid
New password:
Re-type new password:
Adding password for user taohid
$ sudo htpasswd /etc/apache2/.htpasswd secondUser
New password:
Re-type new password:
Adding password for user secondUser
$ cat /etc/apache2/.htpasswd
taohid:$apr1$IyhcEFdn$JWCIugRxldljVf0QC/r6H/
secondUser:$apr1$VAbK1ywn$anNHvIWoM1ZS2tauBJoK5/
$
```

401 Unauthorized × +

← → C   ○ 🔒 https://example.com   ☆   ♡ ⊕ ☆ ≡

Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

Apache/2.4.52 (Ubuntu) Server at example.com Port 443

Checkpoint-3:

Save password for example.com?

Username
taohid

Password
•••••

☐ Show password

Not now ⌄   Save

hello I am taohi

```
mysql> ^C
mysql> exit
Bye
$ sudo mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: n

Skipping password set for root as authentication with auth_socket is used by default.
If you would like to use password authentication instead, this can be done with the "ALTER_USER" command.
See https://dev.mysql.com/doc/refman/8.0/en/alter-user.html#alter-user-password-management for more information.

By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : n

 ... skipping.


Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : n

 ... skipping.
By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.


Remove test database and access to it? (Press y|Y for Yes, any other key for No) : n

 ... skipping.
Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done!
$
```

```
$ htpasswd -bns taohid hello
taohid:{SHA}qvTGHdzF6KLavt4PO0gs2a6pQ00=

$ htpasswd -bns alice hello
alice:{SHA}qvTGHdzF6KLavt4PO0gs2a6pQ00=
$
```

```
$ sudo mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 16
Server version: 8.0.37-0ubuntu0.22.04.3 (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;
ERROR 1007 (HY000): Can't create database 'apache'; database exists
mysql> use apache;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> CREATE TABLE users (username VARCHAR(30) PRIMARY KEY,password VARCHAR(512)
    -> NOT NULL);
ERROR 1050 (42S01): Table 'users' already exists
mysql> INSERT INTO users VALUES (taohid, '{SHA}qvTGHdzF6KLavt4PO0gs2a6pQ00=');
ERROR 1054 (42S22): Unknown column 'taohid' in 'field list'
mysql> INSERT INTO users VALUES ('taohid', '{SHA}qvTGHdzF6KLavt4PO0gs2a6pQ00=');
Query OK, 1 row affected (0.00 sec)

mysql> INSERT INTO users VALUES ('alice', '{SHA}qvTGHdzF6KLavt4PO0gs2a6pQ00=');
ERROR 1062 (23000): Duplicate entry 'alice' for key 'users.PRIMARY'
mysql> exit
Bye
$
```

```
#    Set various options for the SSL engine.
#    o FakeBasicAuth:
#         Translate the client X.509 into a Basic Authorisation.  This means that
#         the standard Auth/DBMAuth methods can be used for access control.  The
#         user name is the `one line' version of the client's X.509 certificate.
#         Note that no password is obtained from the user. Every entry in the user
#         file needs this password: `xxj31ZMTZzkVA'.
#    o ExportCertData:
#         This exports two additional environment variables: SSL_CLIENT_CERT and
#         SSL_SERVER_CERT. These contain the PEM-encoded certificates of the
#         server (always existing) and the client (only existing when client
#         authentication is used). This can be used to import the certifica

DBDriver mysql
DBDParams "dbname=apache user=root pass=hello"
DBDMin 4
DBDKeep 8
DBDMax 20
DBDExptime 300
<Directory "/var/www/example.com/html">
AuthType Basic
AuthName "My Server"
AuthBasicProvider socache dbd
AuthnCacheProvideFor dbd
AuthnCacheContext my-server
Require valid-user
AuthDBDUserPWQuery "SELECT password FROM users WHERE username = %s"
</Directory>

<FilesMatch "\.(cgi|shtml|phtml|php)$">
              SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
```

⊕ example.com

This site is asking you to sign in.

Username

taohid

Password

••••• 👁

Cancel   **Sign in**

G   Search with Google or enter address

Next-level privacy on mobile

Firefox Focus clears your history every time while blocking
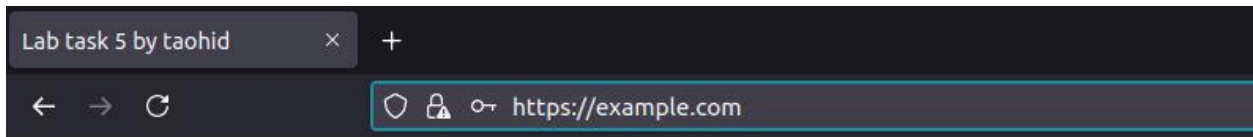
✕

401 Unauthorized × +

https://example.com

Unauthorized

This server could not verify that you are authorized to access the document requested. Either yo

Apache/2.4.52 (Ubuntu) Server at example.com Port 443

hello I am taohid, This is Lab task 5