НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО”

Факультет прикладної математики
Кафедра системного програмування і спеціалізованих комп’ютерних систем

Лабораторна робота № 1

з дисципліни «Захист інформації в комп’ютерних системах»

Виконав: Стецюренко І. С,
Студент групи КВ-03
Перевірив(ла):_____

Київ 2022

Частина 1
«ТЕХНОЛОГІЯ УСТАНОВКИ ТА ПЕРШОЧЕРГОВОГО НАЛАШТУВАННЯ APACHE + PHP+ MYSQL»

Метою лабораторної роботи є оволодіння практичними навичками налаштування базових параметрів захисту веб-сторінок за допомогою стандартних засобів веб-серверу Apache.

Теоретичні відомості. Перед виконанням лабораторної роботи слід ознайомитись із розділами навчального посібника, що присвячені засобам налаштування базових параметрів захисту веб-серверу Apache.

Завдання:

1. Інсталювати веб-сервер Apache та вивчити особливості його налаштування.
2. Інсталювати інтерпретатор PHP5.
3. Інсталювати СУБД MySQL 5.
4. Перевірити працездатність Apache, PHP, MySQL в цілому.

Налаштування

1. Встановлюємо Apache, MariaDB(форк MySQL) та PHP на Arch Linux:
   $ sudo pacman -Suy --noconfirm apache mysql php php-apache php-pgsql nano
2. Вимикаємо Apache та MariaDB для подальшого налаштування:
   $ sudo systemctl stop httpd.service mysql.service
3. Перевіряємо наявність налаштованого localhost у системі:
   $ cat /etc/hosts
   файл: «/etc/hosts»:
   1. # Static table lookup for hostnames.
   2. # See hosts(5) for details.
   3. 127.0.0.1 localhost
   4. ::1 localhost
4. Створимо кореневу теку з даними веб-серверу:
   $ sudo mkdir -p /srv/int
   В теці «/srv/int» будуть зберігатись файли веб-сайту
5. Налаштовуємо конфігураційний файл Apache:
   $ sudo nano /etc/httpd/conf/httpd.conf
   Додаємо рядок «LoadModule php_module modules/libphp.so» після рядку «LoadModule dir_module modules/mod_dir.so».
   Розміщаємо рядок «Include conf/extra/php_module.conf» у кінці списку «Include».
   Рядок «LoadModule mpm_event_module modules/mod_mpm_event.so» заміняємо на
   «LoadModule mpm_prefork_module modules/mod_mpm_prefork.so».
6. Створюємо тестові файли:
   $ sudo usermod -a -G http $(users)

   $ sudo chown http:http -R /srv/int

   $ sudo chmod -R 771 /srv/int

   $ echo "<html><head><title>Hello</title></head><body>Hello</body></html>" > /srv/int/index.html

   $ echo "<?php phpinfo(); ?>" > /srv/int/1.php

$ echo '<?php print "Current PHP version: ". phpversion() .""; ini_set("display_errors", 1); ini_set("display_startup_errors", 1); error_reporting(E_ALL); $link = mysqli_connect("localhost", "root","") or die("Could not connect"); if(!$link) die(mysqli_error()); $db_list = mysqli_query($link, "SHOW DATABASES");/* mysqli_list_dbs($link); */ while ($row = mysqli_fetch_object($db_list)) { echo "<h3>Database \"".$row->Database."\"</h3>\n"; $result = mysqli_query($link, "SHOW TABLES FROM $row->Database"); /* mysqli_list_tables($row->Database); */ if(!$result) die("DB Error, could not list tables\n MySQL Error: ".mysqli_error()); else { while ($row = mysqli_fetch_row($result)) print "Table: $row[0]
"; mysqli_free_result($result); } }?>' > /srv/int/2.php

$ sudo chmod -R g+xr-w /srv/int

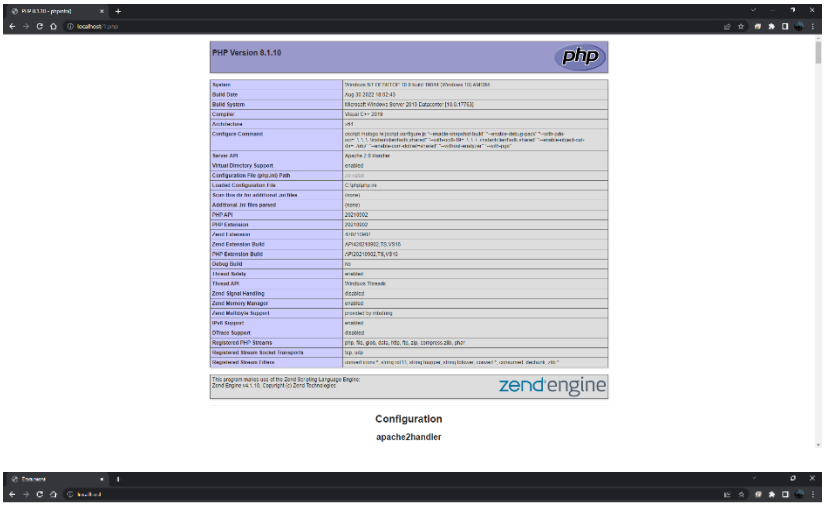
7. Налаштовуємо MariaDB:
   $ sudo mariadb-install-db --user=mysql --basedir=/usr --datadir=/var/lib/mysql

   $ sudo systemctl restart mysql.service

   Встановлюємо пустий пароль для користувача «root»
   $ sudo mariadb-admin password
8. Вмикаємо підтримку модуля «mysqli» для PHP:
   У файлі «/etc/php/php.ini» знайти та розкомментувати рядок «extension=mysqli».
9. Запустимо Apache та MariaDB:
   $ sudo systemctl restart mysql.service httpd.service

Результати

Завантажимо сторінку http://localhost:80/, щоб побачити результати.



Частина 2
«КОНФІГУРАЦІЯ ПАРАМЕТРІВ ЗАХИСТУ ВЕБ-СЕРВЕРУ»

Завдання на частину 2:

1. Заборонити перегляд структури всіх веб-документів.
2. Заборонити доступ до всіх ресурсів за межами теки з вебдокументами.
3. Заборонити перехід веб-сервера по символьним посиланням.
4. Обмежити параметр Timeout величиною 45 секунд.
5. Мінімізувати службову інформацію, що передається від веб-серверу.
6. Обмежити обсяг файлів, які можливо завантажити на веб-сервер величиною 1 МБ.
7. Встановити, що час очікування наступного запиту перед розривом з'єднання дорівнює 15 секунд.
8. Встановити, що максимальна кількість одночасно підтримуваних запитів на одне з'єднання дорівнює 200.
9. Заборонити запуск програм в теці з веб-документами.
10. Заборонити підтримку директив в файлах .htaccess.
11. Заборонити доступ до кореневої теки веб-документів з доменного імені www.rrr.ua та IP-адрес 172.16.16.0 і 172.16.16.8.
12. Дозволити доступ до теки AAA з IP-адреси 127.0.01 тільки користувачеві useraaa. Пароль – 1111. Використати базовий тип перевірки парольних даних.
13. Дозволити доступ до теки BBB з IP-адреси 127.0.01 тільки користувачеві userbbb. Пароль – 2222. Використати цифровий тип перевірки парольних даних.
14. Зняти всі обмеження доступу до теки CCC.
15. Встановити файл q.html в якості головного файлу директорії CCC.
16. Заборонити доступ до файлу CCC методом POST.
17. Заборонити доступ всіх користувачів веб-серверу до файлу myf.html, розміщеному в теці AAA.
18. Заборонити доступ всіх користувачів веб-серверу до теки DDD.
19. Дозволити доступ всіх користувачів до файлу rrr.htm, розміщеному в теці DDD.
20. Визначити файл y.html в якості відповіді веб-серверу при виникненні помилки (зверненні до неіснуючого файлу).
21. Використовуючи метод підбору паролю по словнику спробувати підібрати пароль до теки AAA. Визначити термін підбору.
22. Використовуючи метод підбору паролю по словнику спробувати підібрати пароль до теки BBB. Визначити термін підбору.
23. Використовуючи метод повного перебору підібрати пароль до теки AAA. Використати парольний алфавіт, що відповідає обмеженням парольних даних для веб-сторінки. Визначити термін підбору для кількості потоків 1, 5, 20, 50.
24. Використовуючи метод повного перебору підібрати пароль до теки BBB. Використати парольний алфавіт, що відповідає обмеженням парольних даних для веб-сторінки. Визначити термін підбору для кількості потоків 1, 5, 20, 50

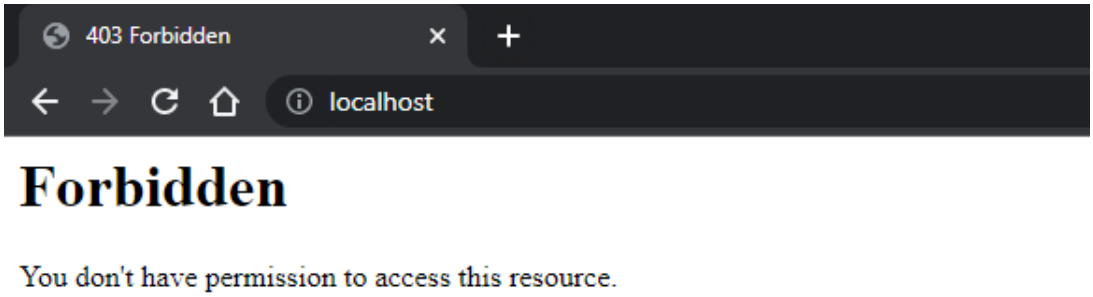
Налаштування

1. Створюємо теки AAA, BBB, CCC, DDD та файли q.html, rrr.html та y.html.
   $ sudo chmod -R 771 /srv/int
   $ mkdir -p /srv/int/AAA /srv/int/BBB /srv/int/CCC /srv/int/DDD
   $ echo "index.html AAA" > /srv/int/AAA/index.html
   $ echo "index.html BBB" > /srv/int/BBB/index.html
   $ echo "index.html CCC" > /srv/int/CCC/index.html
   $ echo "index.html DDD" > /srv/int/DDD/index.html
   $ echo "myf.html AAA" > /srv/int/AAA/myf.html
   $ echo "rrr.html DDD" > /srv/int/DDD/rrr.html
   $ echo "q.html CCC" > /srv/int/CCC/q.html
   $ echo "Поганий запит" > /srv/int/y.html
   $ sudo chown http:http -R /srv/int
   $ sudo chmod -R g+xr-w /srv/int

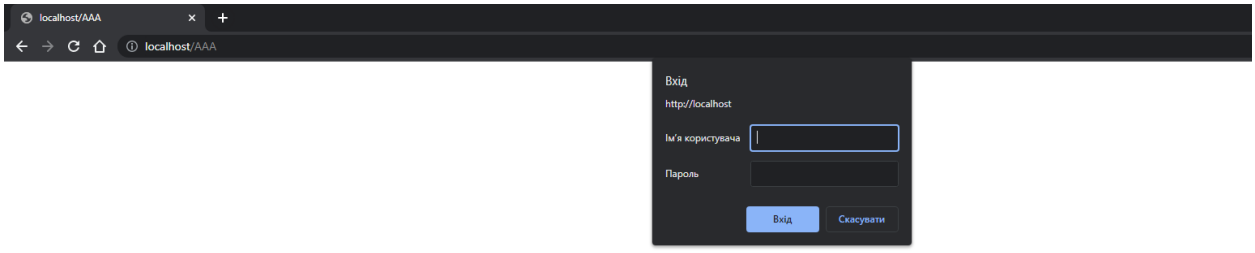
2. Реєструємо користувачів useraaa та userbbb:
   $ sudo htpasswd -c /etc/httpd/conf/passwords useraaa
   $ sudo htdigest -c /etc/httpd/conf/.hhh bbb userbbb
3. Налаштовуємо конфігураційний файл Apache згідно з завданням:
   $ sudo nano /etc/httpd/conf/httpd.conf

Результати

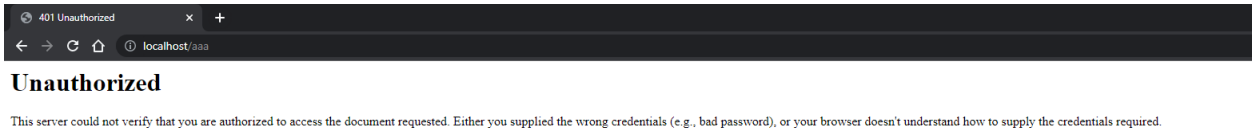
При доступу до структури всіх веб-документів з’явиться повідомлення



При спробі доступу до http://localhost:80/AAA з’яввиться відповідне вікно вводу парольних даних



При невдалій спробі ідентифікації виводиться інформація про помилку



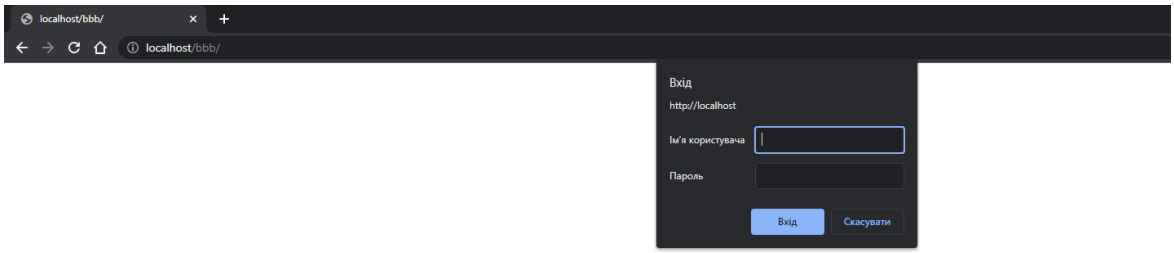
Unauthorized

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.

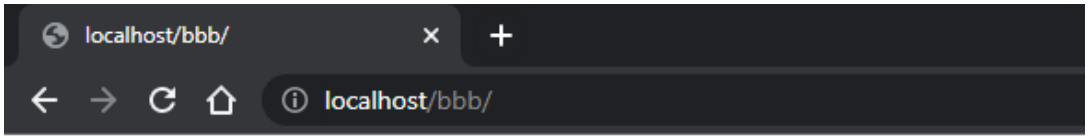
Після вводу правильної комбінації логіну та паролю маємо доступ до теки

index.html AAA

При спробі доступу до http://localhost:80/BBB з'яввиться відповідне вікно вводу парольних даних

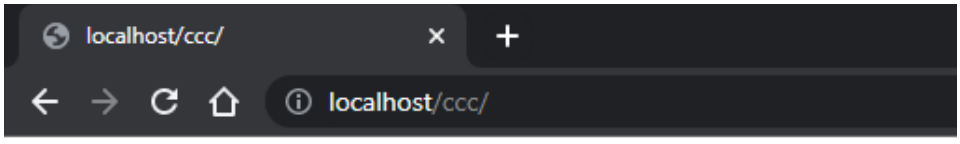


Після вводу потрібних данних маємо, інакше буде помилка 401



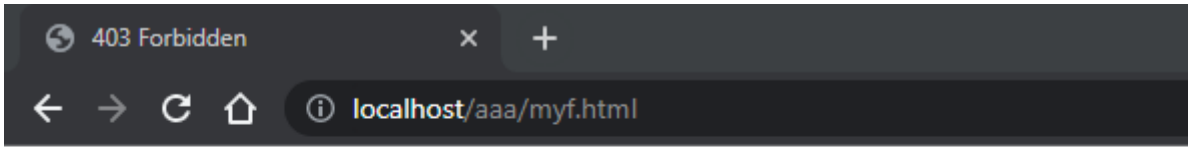
index.html BBB

Пересвідчимось, що при доступі до теки CCC відкривається файл q.html замість index.html



q.html CCC

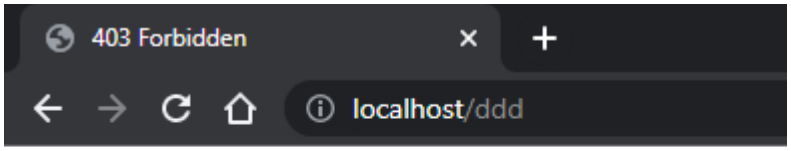
При спробі відкрити вміст файлу myf.html в теці AAA:



Forbidden

You don't have permission to access this resource.

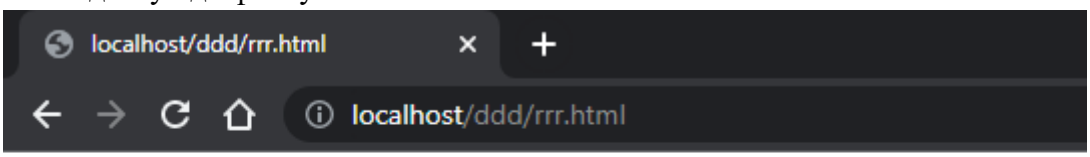
Для папки DDD маємо заборону на всі файли:



Forbidden

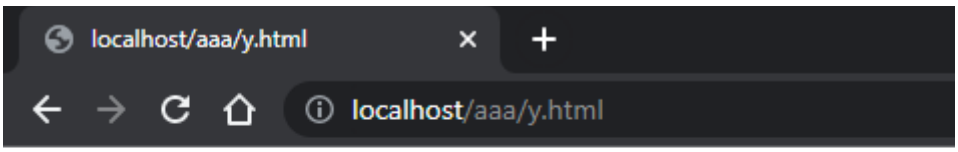
You don't have permission to access this resource.

Але наявний доступ до файлу rrr.html:



rrr.html DDD

При спробі звернутись до неіснуючого файлу, а саме http:/localhost/CCC/1.html маємо:



Bad request