

TASK 1: How to setup Apache Server and alert using logfile

Step 1: Update your local package index

Command:

```
$ sudo apt update
```

Install the apache2 package:

Command:

```
$ sudo apt install apache2
```

Step 2: Configure Your Firewall

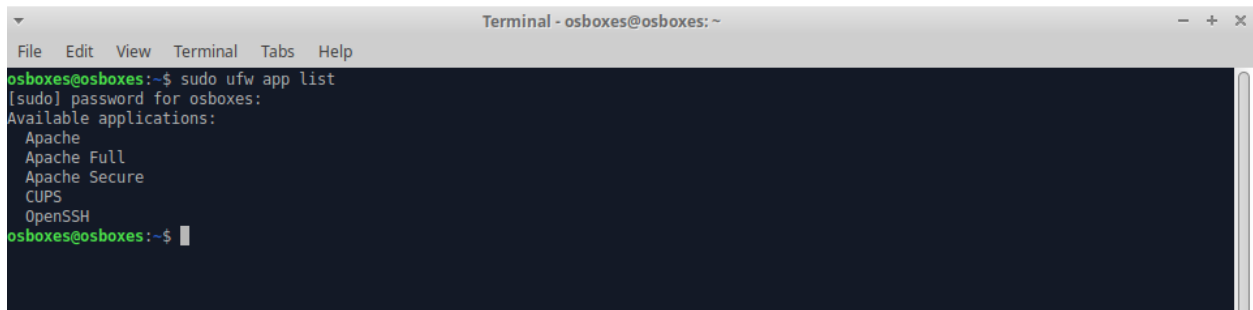
Although the Apache installation process is complete, there is one more additional step. Configure the default UFW firewall to allow traffic on port 80.

Start by displaying available app profiles on UFW:

Command:

```
$ sudo ufw app list
```

The terminal should respond by listing all available application profiles, as seen in the example below.

A terminal window titled "Terminal - osboxes@osboxes: ~" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the command "sudo ufw app list" being executed. The output is: "[sudo] password for osboxes:", "Available applications:", and a list of applications: Apache, Apache Full, Apache Secure, CUPS, and OpenSSH. The prompt "osboxes@osboxes:~\$" is visible at the bottom.

```
Terminal - osboxes@osboxes: ~
File Edit View Terminal Tabs Help
osboxes@osboxes:~$ sudo ufw app list
[sudo] password for osboxes:
Available applications:
Apache
Apache Full
Apache Secure
CUPS
OpenSSH
osboxes@osboxes:~$
```

Let's enable the most restrictive profile that will still allow the traffic you've configured, permitting traffic on port 80 (regular, unencrypted web traffic):

Command:

```
$ sudo ufw allow 'Apache'
```

Verify the change:

```
$ sudo ufw status
```

In case your firewall's status is inactive, you can use the command “sudo ufw enable” to activate.

```
osboxes@osboxes:~$ sudo ufw enable
Firewall is active and enabled on system startup
osboxes@osboxes:~$ sudo ufw status
Status: active

To Action From
--
Apache ALLOW Anywhere
Apache (v6) ALLOW Anywhere (v6)

osboxes@osboxes:~$
```

Step 3: Checking your Web Server

Check with the systemd init system to make sure the service is running by typing:

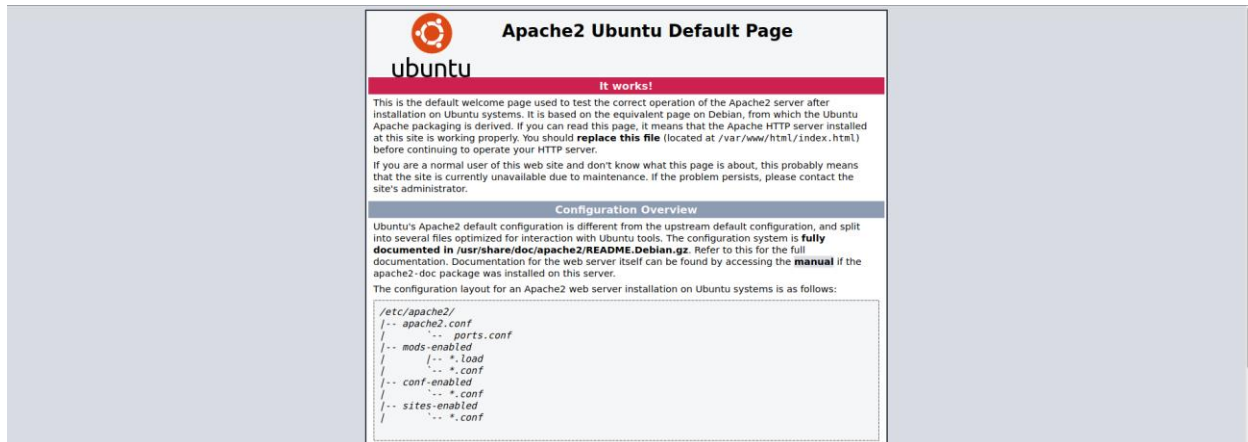
Command:

```
$ sudo systemctl status apache2
```

```
osboxes@osboxes:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-10-12 16:16:23 +07; 52min ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 614 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 662 (apache2)
    Tasks: 55 (limit: 4656)
   Memory: 9.0M
    CGroup: /system.slice/apache2.service
            └─662 /usr/sbin/apache2 -k start
              └─663 /usr/sbin/apache2 -k start
                └─664 /usr/sbin/apache2 -k start

Oct 12 16:16:23 osboxes systemd[1]: Starting The Apache HTTP Server...
Oct 12 16:16:23 osboxes apachectl[635]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using
Oct 12 16:16:23 osboxes systemd[1]: Started The Apache HTTP Server.
lines 1-16/16 (END)
```

Access the default Apache landing page to confirm that the software is running correctly through your IP address: http://your_server_ip



Step 4: Set up password Authentication

* Installing the Apache Utilities Package

Command:

```
$ sudo apt-get update
$ sudo apt-get install apache2-utils
```

— Creating the Password File

We now have access to the `htpasswd` command. We can use this to create a password file that Apache can use to authenticate users. We will create a hidden file for this purpose called `.htpasswd` within our `/etc/apache2` configuration directory. The first time we use this utility, we need to add the `-c` option to create the specified file. We specify a username (jupyter in this example) at the end of the command to create a new entry within the file:

```
osboxes@osboxes:~$ sudo htpasswd -c /etc/apache2/.htpasswd jupyter
New password:
Re-type new password:
Adding password for user jupyter
osboxes@osboxes:~$
```

Leave out the `-c` argument for any additional users you wish to add:

```
osboxes@osboxes:~$ sudo htpasswd /etc/apache2/.htpasswd group1
New password:
Re-type new password:
Adding password for user group1
osboxes@osboxes:~$
```

If we view the contents of the file, we can see the username and the encrypted password for each record:

```
osboxes@osboxes:~$ cat /etc/apache2/.htpasswd
jupyter:$apr1$ZcLjXov3$b.L58CdCSvF4i959Mr/0w1
group1:$apr1$S3g8bm33$zvB4905tJyClcc5SCGm8v1
osboxes@osboxes:~$
```

STEP 5: — Configuring Apache Password Authentication

Configuring Access Control within the Virtual Host Definition

Begin by opening up the virtual host file that you wish to add a restriction to. For our example, we'll be using the 000-default.conf file that holds the default virtual host installed through Ubuntu's apache package:

```
$ sudo nano /etc/apache2/sites-enabled/000-default.conf
```

Authentication is done on a per-directory basis. To set up authentication, you will need to target the directory you wish to restrict with a <Directory ____> block. In our example, we'll restrict the entire document root, but you can modify this listing to only target a specific directory within the webspace.

Within this directory block, specify that we wish to set up Basic authentication. For the AuthName, choose a realm name displayed to the user when prompting for credentials. Use the AuthUserFile directive to point Apache to the password file we created. Finally, we will require a valid-user to access this resource, which means anyone who can verify their identity with a password will be allowed in:

```

<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
    <Directory "/var/www/html">
        AuthType Basic
        AuthName "Restricted Content"
        AuthUserFile /etc/apache2/.htpasswd
        Require valid-user
    </Directory>
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

```

Save and close the file when you are finished.

Before restarting the webserver, you can check the configuration with the following command:

Command:

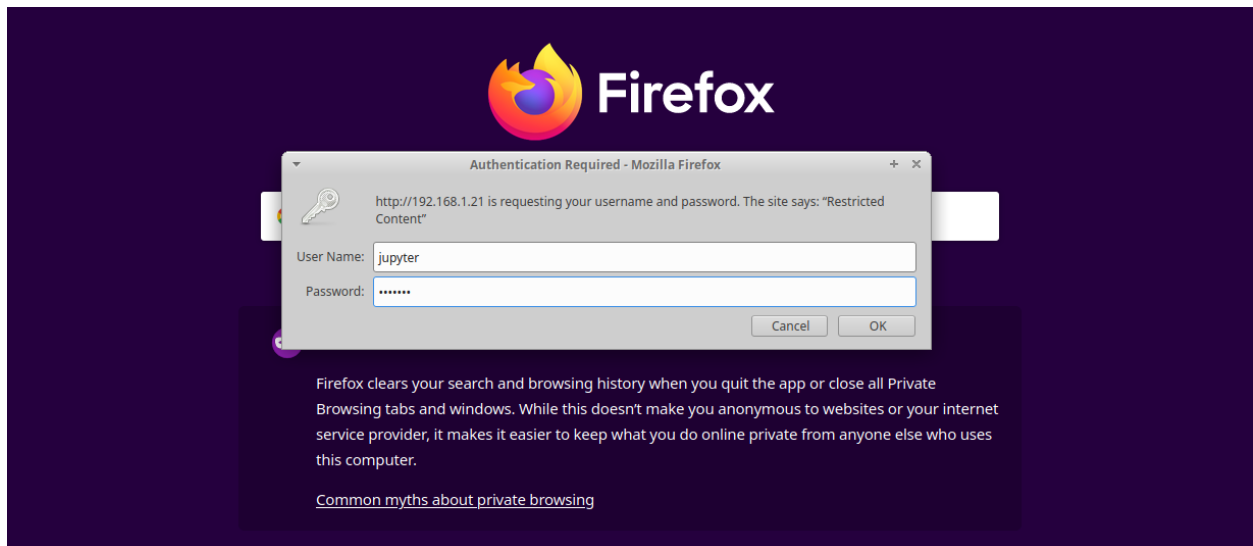
```
$ sudo apache2ctl configtest
```

```

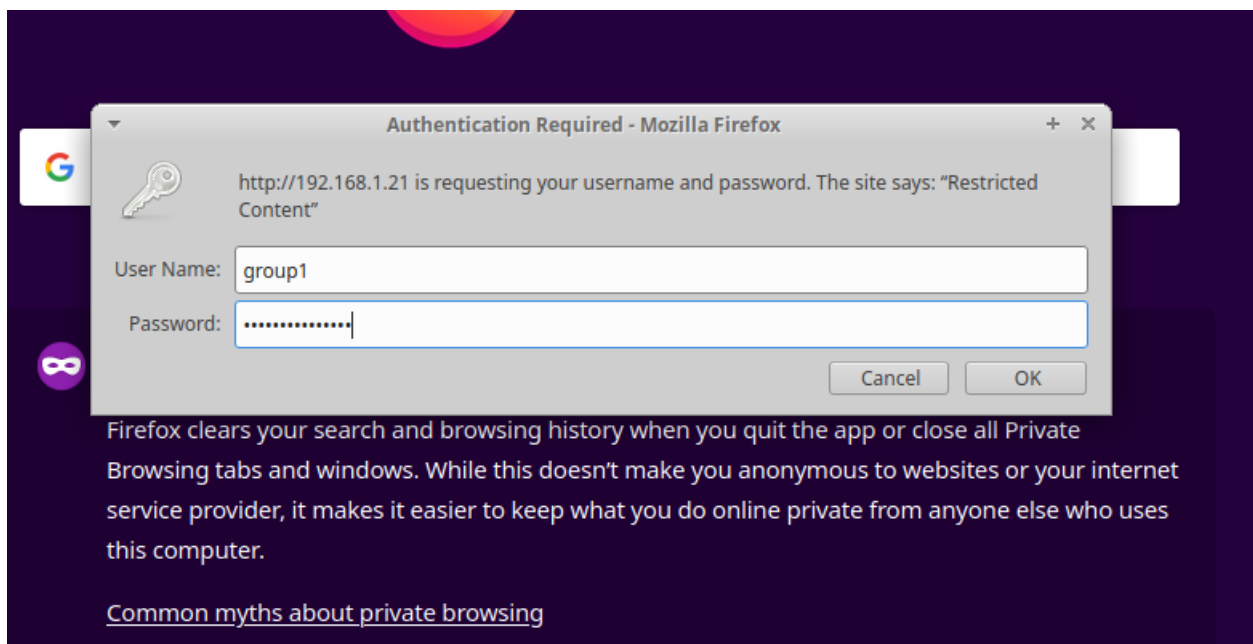
osboxes@osboxes:~$ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
osboxes@osboxes:~$

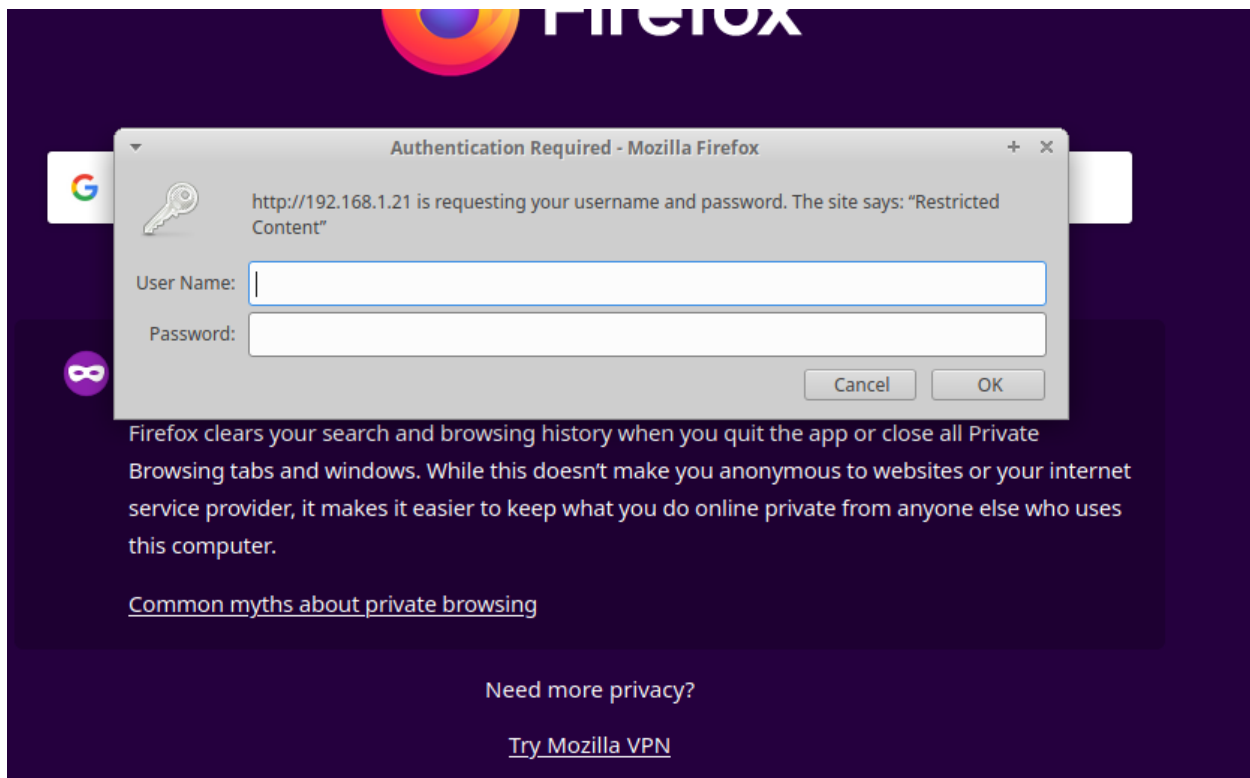
```

— Confirming Password Authentication



In case I type the wrong password, I can not access the webserver:





Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

[Common myths about private browsing](#)

Need more privacy?

[Try Mozilla VPN](#)

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/2.4.41 (Ubuntu) Server at 192.168.1.21 Port 80

In case you want to see all the log files, this is the path: `/var/log/apache2/`. It contains all the processes and action from the user with the webserver.

```
File Edit Search View Document Help
/var/log/apache2/error.log - Mousepad

[Mon Oct 12 10:12:45.798249 2020] [mpm_event:notice] [pid 2644:tid 140474283056192] AH00489: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
[Mon Oct 12 10:12:45.798538 2020] [core:notice] [pid 2644:tid 140474283056192] AH00894: Command Line: '/usr/sbin/apache2'
[Mon Oct 12 11:17:42.536667 2020] [mpm_event:notice] [pid 2644:tid 140474283056192] AH00491: caught SIGTERM, shutting down
[Mon Oct 12 11:17:42.626662 2020] [mpm_event:notice] [pid 8523:tid 139717994101824] AH00489: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
[Mon Oct 12 11:17:42.626799 2020] [core:notice] [pid 8523:tid 139717994101824] AH00894: Command Line: '/usr/sbin/apache2'
[Mon Oct 12 11:23:27.578622 2020] [mpm_event:notice] [pid 8523:tid 139717994101824] AH00491: caught SIGTERM, shutting down
[Mon Oct 12 11:27:42.691714 2020] [mpm_event:notice] [pid 9105:tid 140093053516864] AH00489: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
[Mon Oct 12 11:27:42.691853 2020] [core:notice] [pid 9105:tid 140093053516864] AH00894: Command Line: '/usr/sbin/apache2'
[Mon Oct 12 11:28:10.892751 2020] [mpm_event:notice] [pid 9105:tid 140093053516864] AH00491: caught SIGTERM, shutting down
[Mon Oct 12 11:30:09.583997 2020] [mpm_event:notice] [pid 674:tid 139696175438912] AH00489: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
[Mon Oct 12 11:30:09.586058 2020] [core:notice] [pid 674:tid 139696175438912] AH00894: Command Line: '/usr/sbin/apache2'
[Mon Oct 12 11:31:53.787084 2020] [auth_basic:error] [pid 675:tid 139696067823360] [client 192.168.1.21:36780] AH01617: user jupyter: authentication failure for "/": Password Mismatch
[Mon Oct 12 16:16:23.966488 2020] [mpm_event:notice] [pid 662:tid 140082410748992] AH00489: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
[Mon Oct 12 16:16:23.966488 2020] [core:notice] [pid 662:tid 140082410748992] AH00894: Command Line: '/usr/sbin/apache2'
[Mon Oct 12 17:31:58.166749 2020] [auth_basic:error] [pid 663:tid 140082262550272] [client 192.168.1.21:39930] AH01617: user group: authentication failure for "/": Password Mismatch
[Mon Oct 12 17:32:54.261389 2020] [auth_basic:error] [pid 664:tid 140082228979456] [client 192.168.1.21:39932] AH01618: user not found: /
[Mon Oct 12 17:34:34.698072 2020] [auth_basic:error] [pid 664:tid 140082212194040] [client 192.168.1.21:39952] AH01617: user group: authentication failure for "/": Password Mismatch
[Mon Oct 12 17:34:36.364254 2020] [auth_basic:error] [pid 664:tid 140082245764864] [client 192.168.1.21:39952] AH01618: user not found: /
[Mon Oct 12 17:34:37.389531 2020] [auth_basic:error] [pid 664:tid 140082136659712] [client 192.168.1.21:39952] AH01618: user not found: /
```

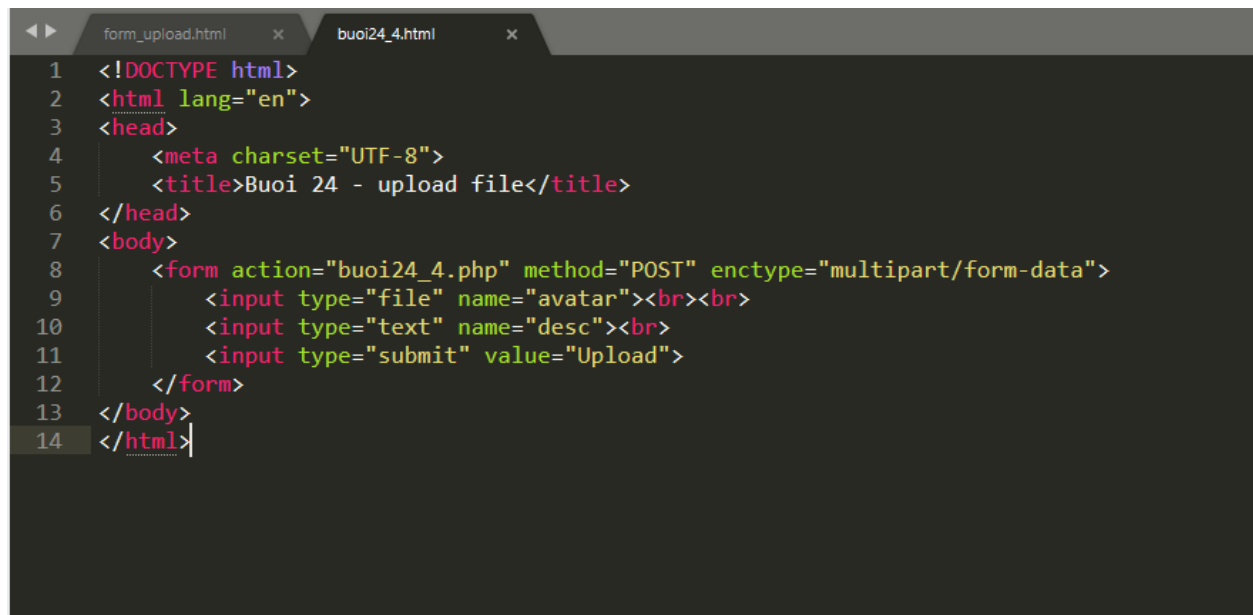
Event: Unauthorized

```
127.0.0.1 - - [25/Oct/2020:14:27:05 +0700] "GET / HTTP/1.1" 401 728 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0"
127.0.0.1 - group1 [25/Oct/2020:14:27:09 +0700] "GET / HTTP/1.1" 401 727 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0"
127.0.0.1 - asdsadasd [25/Oct/2020:14:27:12 +0700] "GET / HTTP/1.1" 401 727 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0"
127.0.0.1 - asdsadasdad [25/Oct/2020:14:27:14 +0700] "GET / HTTP/1.1" 401 727 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0"
127.0.0.1 - asdsadasdad [25/Oct/2020:14:27:16 +0700] "GET / HTTP/1.1" 401 727 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0"
127.0.0.1 - asdsadasdasdsadasd [25/Oct/2020:14:27:19 +0700] "GET / HTTP/1.1" 401 727 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0"
```

In an unauthorized event, consecutive login with failed password, the status code printed in the access.log file will be 401.

Event: File too large

I write a simple HTML code in the webserver.

A screenshot of a code editor with two tabs: 'form_upload.html' and 'buoi24_4.html'. The 'buoi24_4.html' tab is active, showing the following HTML code:

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4     <meta charset="UTF-8">
5     <title>Buoi 24 - upload file</title>
6 </head>
7 <body>
8     <form action="buoi24_4.php" method="POST" enctype="multipart/form-data">
9         <input type="file" name="avatar"><br><br>
10        <input type="text" name="desc"><br>
11        <input type="submit" value="Upload">
12    </form>
13 </body>
14 </html>
```

Source code:

```
<!DOCTYPE html>
```

```
<html lang="en">
```

```
<head>
```

```
    <meta charset="UTF-8">
```

```
    <title>Buoi 24 - upload file</title>
```

```
</head>
```


<body>

<form action="buoi24_4.php" method="POST" enctype="multipart/form-data">

<input type="file" name="avatar">

<input type="text" name="desc">

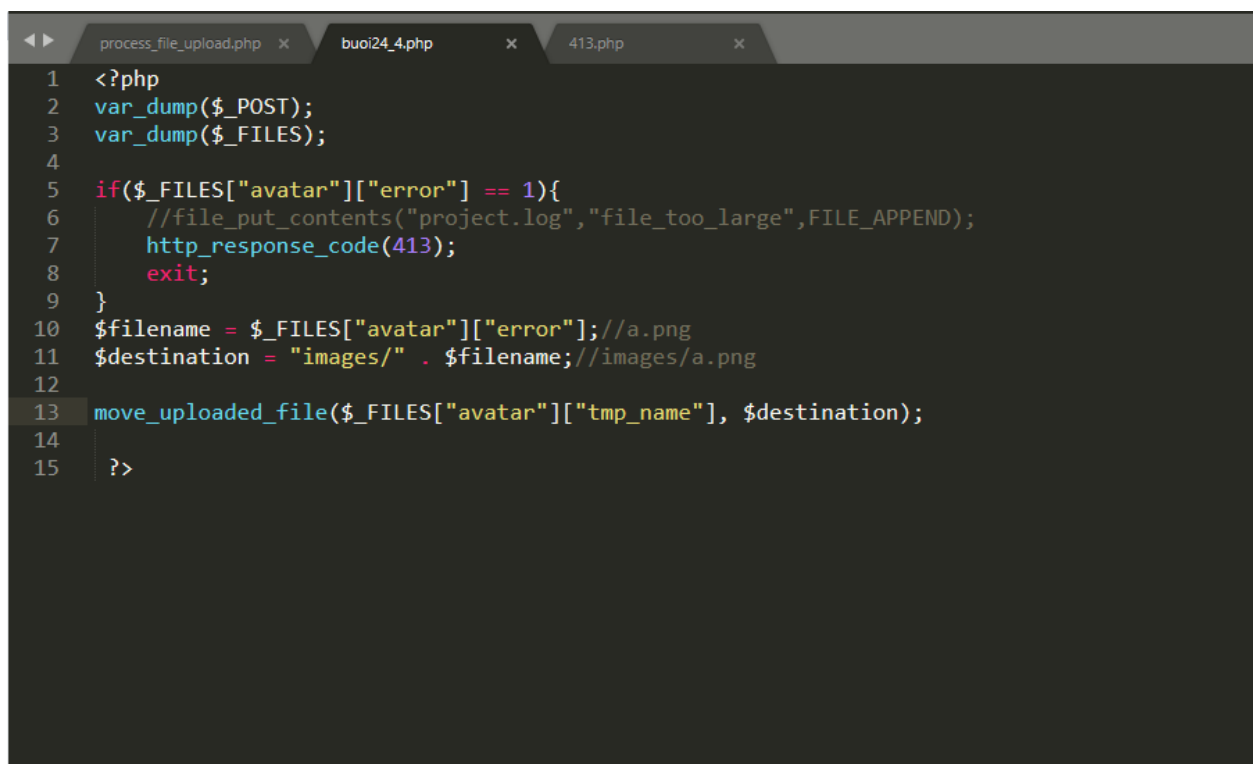
<input type="submit" value="Upload">

</form>

</body>

</html>

And php code:

A screenshot of a code editor with a dark background. The editor has three tabs at the top: 'process_file_upload.php', 'buoi24_4.php', and '413.php'. The 'buoi24_4.php' tab is active. The code is written in PHP and is as follows:

```
1 <?php
2 var_dump($_POST);
3 var_dump($_FILES);
4
5 if($_FILES["avatar"]["error"] == 1){
6     //file_put_contents("project.log", "file_too_large", FILE_APPEND);
7     http_response_code(413);
8     exit;
9 }
10 $filename = $_FILES["avatar"]["error");//a.png
11 $destination = "images/" . $filename;//images/a.png
12
13 move_uploaded_file($_FILES["avatar"]["tmp_name"], $destination);
14
15 ?>
```

Source code:

<?php

var_dump(\$_POST);

var_dump(\$_FILES);

```

if($_FILES["avatar"]["error"] == 1){

    //file_put_contents("project.log","file_too_large",FILE_APPEND);

    http_response_code(413);

    exit;

}

$filename = $_FILES["avatar"]["error");//a.png

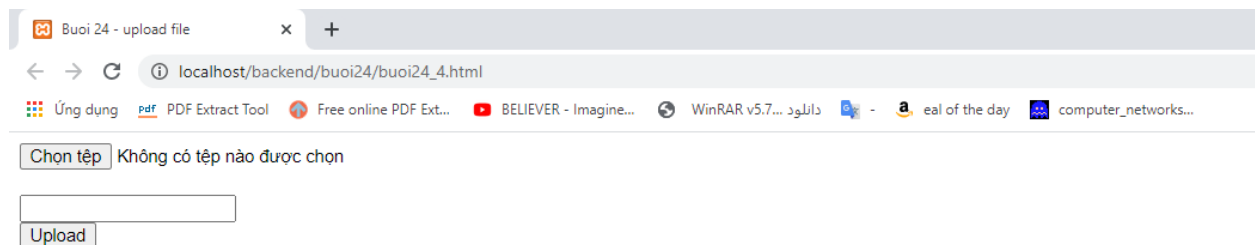
$destination = "images/" . $filename;//images/a.png

move_uploaded_file($_FILES["avatar"]["tmp_name"], $destination);

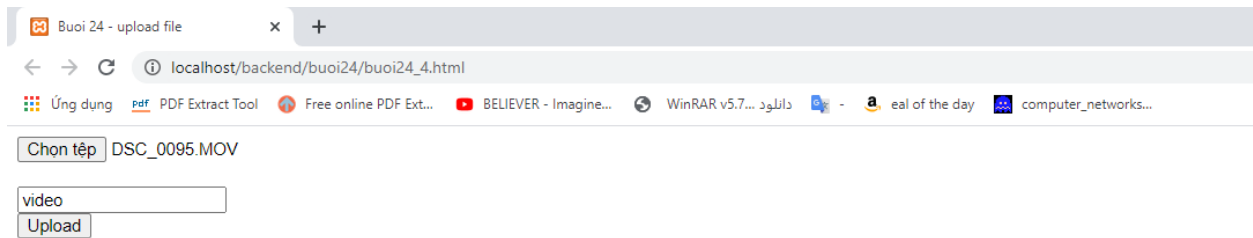
?>

```

After that, I'm running the code on the server.



Then, uploading the file larger than 8M.



```
C:\xampp\htdocs\backend\buoi24\buoi24_4.php:2:
array (size=1)
  'desc' => string 'video' (length=5)

C:\xampp\htdocs\backend\buoi24\buoi24_4.php:3:
array (size=1)
  'avatar' =>
    array (size=5)
      'name' => string 'DSC_0095.MOV' (length=12)
      'type' => string '' (length=0)
      'tmp_name' => string '' (length=0)
      'error' => int 1
      'size' => int 0
```

Now I check the access.log file:

```
1 - - [23/Oct/2020:08:52:37 +0700] "GET /backend/buoi24/413.php HTTP/1.1" 413 156 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36"
1 - - [23/Oct/2020:08:54:00 +0700] "POST /backend/buoi24/buoi24_4.php HTTP/1.1" 413 1045 "http://localhost/backend/buoi24/buoi24_4.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86"
1 - - [23/Oct/2020:13:07:44 +0700] "POST /backend/buoi24/buoi24_4.php HTTP/1.1" 413 1045 "http://localhost/backend/buoi24/buoi24_4.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86"
1 - - [23/Oct/2020:13:07:44 +0700] "GET /favicon.ico HTTP/1.1" 200 30894 "http://localhost/backend/buoi24/buoi24_4.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/5"
1 - - [23/Oct/2020:13:11:53 +0700] "POST /backend/buoi24/buoi24_4.php HTTP/1.1" 413 1045 "http://localhost/backend/buoi24/buoi24_4.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86"
1 - - [23/Oct/2020:13:16:53 +0700] "-" 408 - "-" "-"
1 - - [25/Oct/2020:16:23:50 +0700] "POST /backend/buoi24/buoi24_4.php HTTP/1.1" 413 1049 "http://localhost/backend/buoi24/buoi24_4.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86"
```

The status code '413' means that the file uploaded to the server is too large.

REFERENCES:

1. <https://phoenixnap.com/kb/how-to-install-apache-web-server-on-ubuntu-18-04>
2. <https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-18-04-quickstart>
3. <https://www.digitalocean.com/community/tutorials/how-to-set-up-password-authentication-with-apache-on-ubuntu-16-04>