



INSTALLATION AND CONFIGURATION OF AN APACHE WEB SERVER

Creating a website and applying the necessary
security rules.

Brunet-Desgent, Patrick

Contents

CREATING A WEBSITE (10 POINTS)	3
1. Install and configure the Apache server to read web pages from the directory	3
2. Create a new homepage named index.html in the /var/www/html_project1 directory.	4
3. The page must include all of the following HTML tags (each used at least once): <html>, <head>, <title>, <body>, <p>, <hr>, <a href>, , , , <i>, and <u>.	5
AUTHENTICATION (25 POINTS)	6
Initial Setup	6
1. Create a secure1 directory and configure Apache using the <Directory> directive so that only the user user01 with the password “secret” can access it from any subnet. No other users should have access.	8
2. Create a secure2 directory and configure Apache so that only user01 can access it when connecting from the subnet 192.168.50.0/24.	9
3. Create a secure3 directory and configure Apache so that either user01 or any user from the 192.168.50.0/24 subnet can access it.	10
4. Create a secure4 directory and configure it similarly to secure1 but grant access only to the user user02 (password “secret”).	11
5. Create a secure5 directory and place an .htaccess file inside it to restrict access to only user01 from any subnet.	12
6. Create a secure6 directory and use an .htaccess file to restrict access to user01, but only when connecting from the 192.168.50.0/24 subnet.	12
7. Create a secure7 directory and use an .htaccess file to allow access to either the user01 or any user from the 192.168.50.0/24 subnet.....	13
ACCESSIBILITY (25 POINTS)	14
1. In the /var/www/html_project1 directory add the following subdirectories and initial setup (adding IP addresses):	14
2. In each of these directories, create a web page named after the directory itself. For example, Project1/project1.html, Project2/project2.html, etc.	16
4. Add <Directory> and <Files> directives to implement the following access controls:	17
➤ Project1: Accessible only from the 10.35.16.0/24 and 10.35.17.0/24 subnets. Any files named secret.* must not be accessible.	18
➤ Project2: Not accessible only from the 10.35.16.0/24 subnet. All files must be accessible to others.	20
➤ Project3: Accessible only from the 192.168.100.0/24 subnet. All *.gif files must not be accessible.....	21

➤ Project4: Accessible only from 10.35.16.0/24 and 192.168.100.0/24. All test.html files must not be accessible.	23
5. For all directories, *.txt files must not be accessible. Place the corresponding directive outside of any <Directory> blocks.	25
AUTHORIZATION (25 POINTS)	26
1. Identify the network subnet of each department:	26
2. Each department has its own dedicated web directory on the server.	26
4. You must use aliases to make these websites accessible. For example, to access the vendors' website, use: http://10.50.1.1/vendors	27
5. Configure the Apache server with the following access rules:	27
Now test each links in ubuntu:	29

CREATING A WEBSITE (10 POINTS)

1. Install and configure the Apache server to read web pages from the directory

"/var/www/html_project1".

```
[root@server15 ~]# dnf install httpd -y
```

```
Installed:
  almalinux-logos-httpd-90.5.1-1.1.el9.noarch
  apr-util-bdb-1.6.1-23.el9.x86_64
  httpd-2.4.62-1.el9_5.2.x86_64
noarch  httpd-tools-2.4.62-1.el9_5.2.x86_64
  mod_lua-2.4.62-1.el9_5.2.x86_64

Complete!
```

Open the configuration file by typing `vim /etc/httpd/conf/httpd.conf` and look for the DocumentRoot variable in order to change the directory of the website

```
DocumentRoot "/var/www/html_project1"

#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html_project1">
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

Exit and save

➤ You must copy the httpd.conf file to httpd.conf.original.

```
[root@server15 ~]# cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.original
[root@server15 ~]# cd /etc/httpd/conf
[root@server15 conf]# ls -l
total 40
-rw-r--r--. 1 root root 12013 Apr 15 20:04 httpd.conf
-rw-r--r--. 1 root root 12013 Apr 15 20:05 httpd.original
-rw-r--r--. 1 root root 13430 Jan 21 16:24 magic
[root@server15 conf]#
```

➤ Configure the server to be accessible via the IP address 192.168.50.10.

```
ServerRoot "/etc/httpd"

Listen 192.168.50.10:80

Include conf.modules.d/*.conf
User apache
Group apache
ServerAdmin root@localhost
#ServerName www.example.com:80
```

➤ Ensure the httpd service is started and enabled to run at boot.

```
[root@server15 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2025-04-18 19:49:46 EDT; 10s ago
     Docs: man:httpd.service(8)
   Main PID: 51210 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests served 0/0"
   Tasks: 177 (limit: 22829)
```

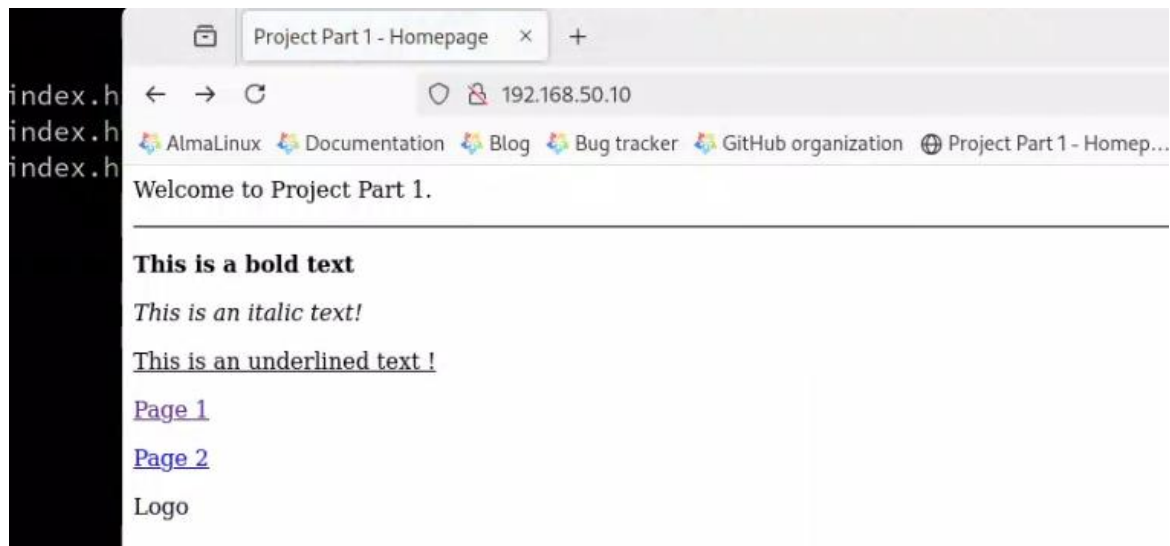
2. Create a new homepage named index.html in the /var/www/html_project1 directory.

```
[root@server15 ~]# cd /var/www/html_project1
[root@server15 html_project1]# ls
[root@server15 html_project1]# ll
total 0
[root@server15 html_project1]# vim index.html
```

3. The page must include all of the following HTML tags (each used at least once): <html>, <head>, <title>, <body>, <p>, <hr>, <a href>, ,
, , <i>, and <u>.

- The page title must be Project Part I - Homepage
- You must add a link to each web page of this project inside the index.html page.
- Add a hyperlink to each web page created for this project inside the index.html page. Each link should open the corresponding web page of each question, allowing you to test its functionality. See the example provided on the last page of this document.

```
<html>
  <head>
    <title>Project Part 1 - Homepage</title>
  </head>
  <body>
    <p>Welcome to Project Part 1.</p>
    <hr>
    <p><b>This is a bold text</b></p>
    <p><i> This is an italic text!</i></p>
    <p><u>This is an underlined text !</u></p>
    <p><a href="page1.html">Page 1</a></p>
    <p><a href="page2.html">Page 2</a></p>
    
    <br>
  </body>
</html>
```



This page is only for demonstration and testing purposes; it will evolve as we do the exercises.

AUTHENTICATION (25 POINTS)

All files for this section should be created within the `/var/www/html_project1` directory.

Initial Setup

Change back to Listen 80, this allows us to have the server listen to all our future Ips.

```
ServerRoot "/etc/httpd"

Listen 80
Include conf.modules.d/*.conf
User apache
Group apache
ServerAdmin root@localhost
#ServerName www.example.com:80
```

Create directories

```
[root@server15 html_project1]# mkdir secure1
```

```
[root@server15 html_project1]# mkdir secure2
[root@server15 html_project1]# mkdir secure3
[root@server15 html_project1]# mkdir secure4
[root@server15 html_project1]# mkdir secure5
[root@server15 html_project1]# mkdir secure6
[root@server15 html_project1]# mkdir secure7
```

Put indexes in each one and have basic code

```
<!doctype html>
<html>
  <head>
    <title> Project Part 1 </title>
  </head>
  <body>
    <p><b><u>Secure1</b></u></p>
  </body>
</html>
```

```
[root@server15 html_project1]# tree secure*
secure1
├── index.html
secure2
├── index.html
secure3
├── index.html
secure4
├── index.html
secure5
├── index.html
secure6
├── index.html
secure7
├── index.html
```

Add these lines into the index.html file to test everything after setting up the secure folders.

```
<p><a href="http://192.168.50.10/secure1">Secure 1, user01 - accessible</a></p>

<p><a href="http://192.168.50.10/secure2">Secure 2, user01 AND 192.168.50.0/24 accessible </a></p>
<p><a href="http://10.35.16.1/secure2">Secure 2, user01 AND 10.35.16.1/24 Not accessible</a></p>

<p><a href="http://192.168.50.10/secure3">Secure 3, user01 or 192.168.50.0/24 accessible </a></p>
<p><a href="http://10.35.16.1/secure3">Secure 3, user01 or 192.168.50.0/24 accessible </a></p>

<p><a href="http://192.168.50.10/secure4">Secure 4, user02 - any IP accessible</a></p>

<p><a href="http://192.168.50.10/secure5">Secure 5, user01 with .htaccess - accessible</a></p>

<p><a href="http://192.168.50.10/secure6">Secure 6, user01 and 192.168.50.0/24 with .htaccess - accessible</a></p>
<p><a href="http://10.35.16.1/secure6">Secure 6, user01 - 10.35.16.1/24 with .htaccess - no access </a></p>

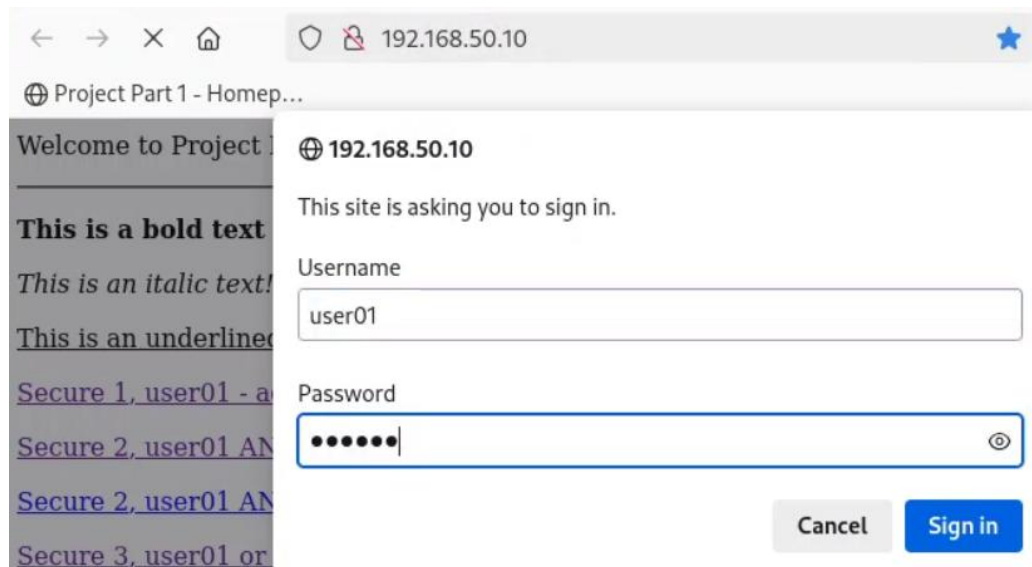
<p><a href="http://192.168.50.10/secure7">Secure 7, user01 or on 192.168.50 with .htaccess - accessible</a></p>
<p><a href="http://10.35.16.1/secure7">Secure 7, user01 or 192.168.50 with .htaccess - accessible </a></p>
```


1. Create a secure1 directory and configure Apache using the <Directory> directive so that only the user user01 with the password “secret” can access it from any subnet. No other users should have access.

```
[root@server15 httpd]# htpasswd -bc /var/www/.htpasswd user01 secret
Adding password for user user01
[root@server15 httpd]#
```

```
<Directory "/var/www/html_project1/secure1">
    AuthType Basic
    AuthName "Secure1 folder"
    AuthUserFile "/var/www/.htpasswd"
    Require user user01
</Directory>
```

Test:



← → × 🏠 🔒 192.168.50.10 ★

🌐 Project Part 1 - Homep...

Welcome to Project 1

This is a bold text

This is an italic text!

This is an underlined

[Secure 1, user01 - a](#)

[Secure 2, user01 AN](#)

[Secure 2, user01 AN](#)

[Secure 3, user01 or](#)

🌐 192.168.50.10

This site is asking you to sign in.

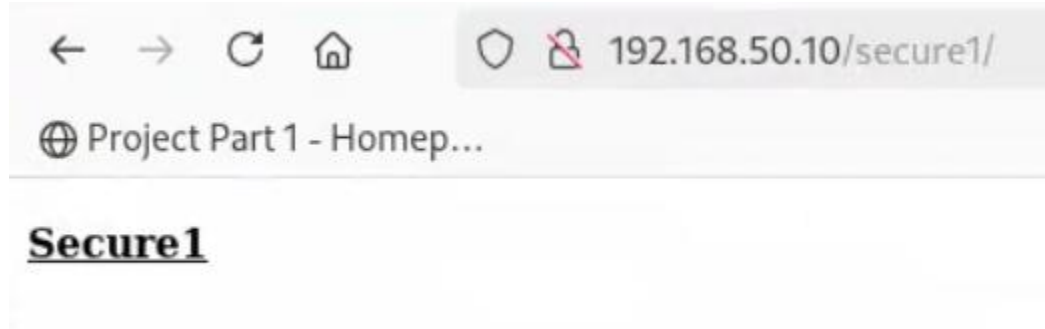
Username

user01

Password

•••••

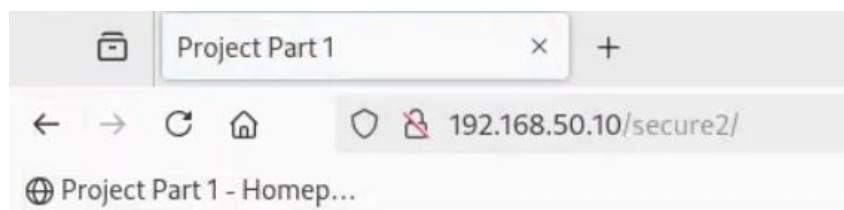
Cancel Sign in



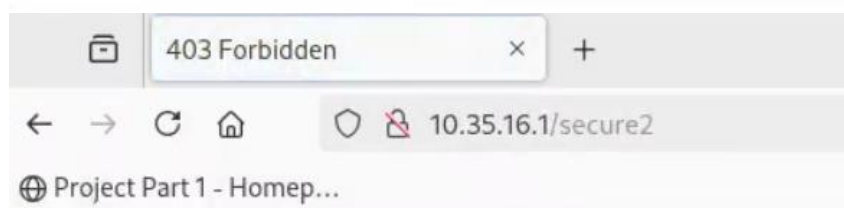
2. Create a secure2 directory and configure Apache so that only user01 can access it when connecting from the subnet 192.168.50.0/24.

```
<Directory "/var/www/html_project1/secure2">
  <RequireAll>
    AuthType Basic
    AuthName "Secure2 folder"
    AuthUserFile "/var/www/.htpasswd"
    Require user user01
    Require ip 192.168.50.0/24
  </RequireAll>
</Directory>
```

Test (still logged as user01):



Secure2



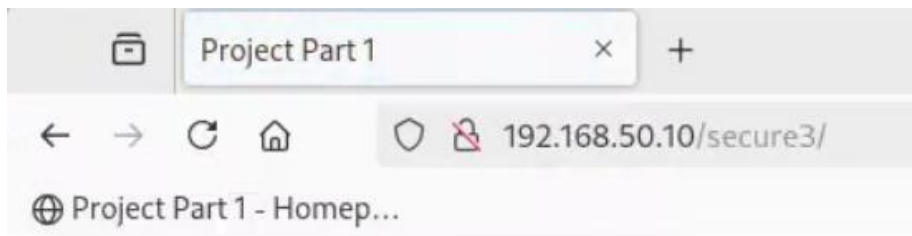
Forbidden

You don't have permission to access this resource.

This is normal since we're not logged in 192.168.50

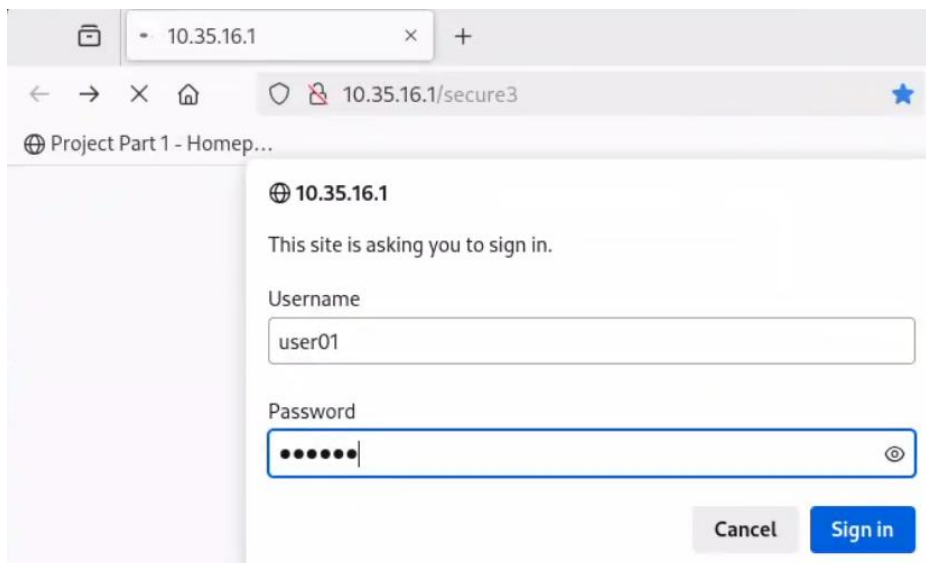
3. Create a secure3 directory and configure Apache so that either user01 or any user from the 192.168.50.0/24 subnet can access it.

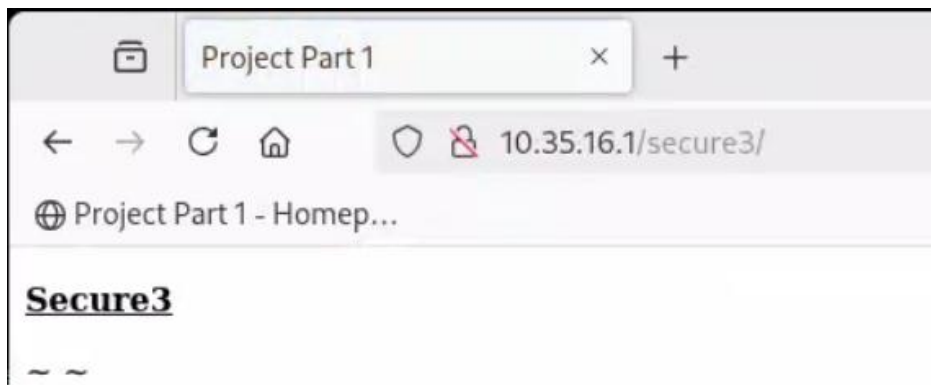
```
<Directory "/var/www/html_project1/secure3">
  <RequireAny>
    AuthType Basic
    AuthName "secure3 folder"
    AuthUserFile "/var/www/.htpasswd"
    Require user user01
    Require ip 192.168.50
  </RequireAny>
</Directory>
```



Secure3

~ ~





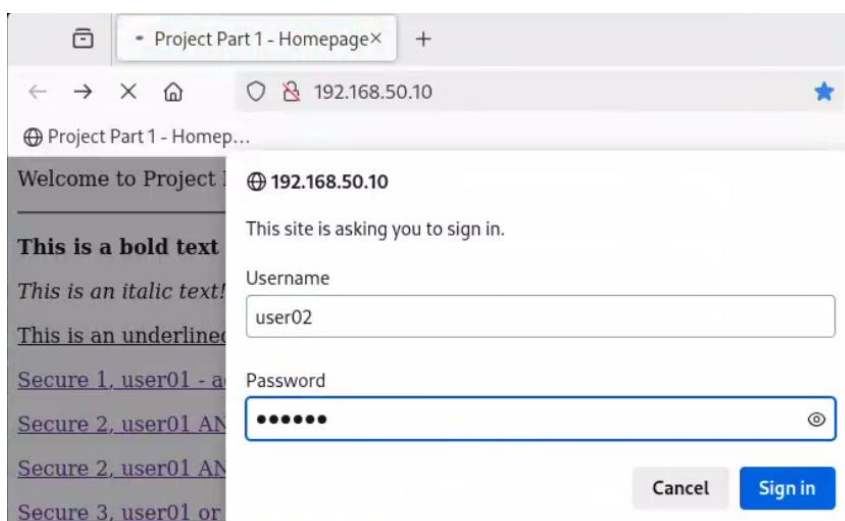
Now this is because we changed our ip, but logging as user01 makes it work as intended

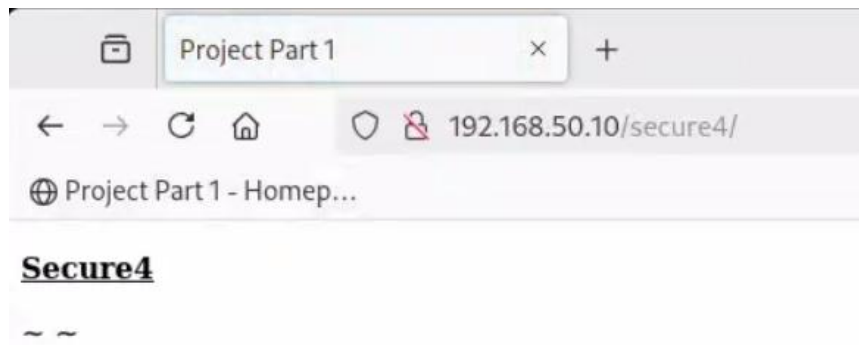
4. Create a secure4 directory and configure it similarly to secure1 but grant access only to the user user02 (password “secret”).

```
[root@server15 www]# htpasswd -b /var/www/.htpasswd user02 secret
Adding password for user user02
[root@server15 www]#
```

```
<Directory "/var/www/html_project1/secure4">
    AuthType Basic
    AuthName "Secure4 folder"
    AuthUserFile "/var/www/.htpasswd"
    Require user user02
</Directory>
```

Test:





Logging as user02 makes it accessible

5. Create a secure5 directory and place an .htaccess file inside it to restrict access to only user01 from any subnet.

```
[root@server15 ~]# vim /var/www/html_project1/secure5/.htaccess
[root@server15 ~]#
```

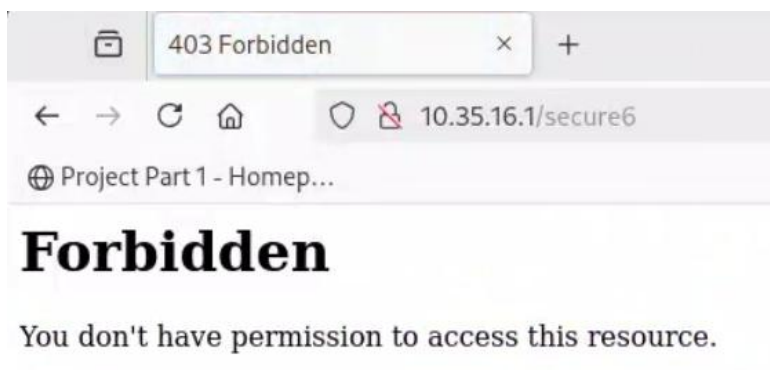
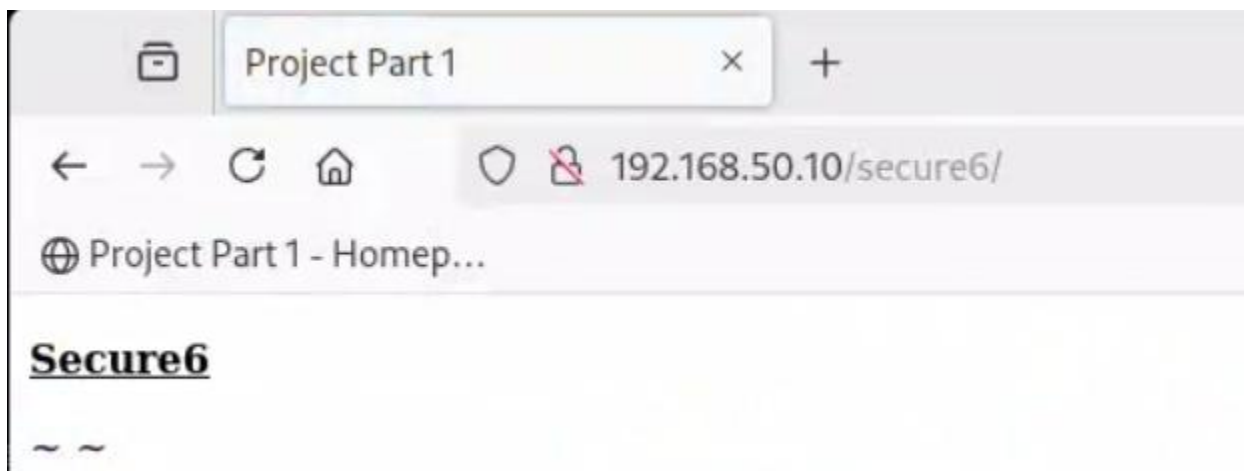
```
AuthType Basic
Authname "Restricted Area"
AuthUserFile /var/www/.htpasswd
Require user user01
```

6. Create a secure6 directory and use an .htaccess file to restrict access to user01, but only when connecting from the 192.168.50.0/24 subnet.

```
[root@server15 secure5]# vim /var/www/html_project1/secure6/.htaccess
```

```
Activities Terminator
AuthType Basic
AuthName "Restricted Area"
AuthUserFile /var/www/.htpasswd
<RequireAll>
  Require user user01
  Require ip 192.168.50.0/24
</RequireAll>
```

Test

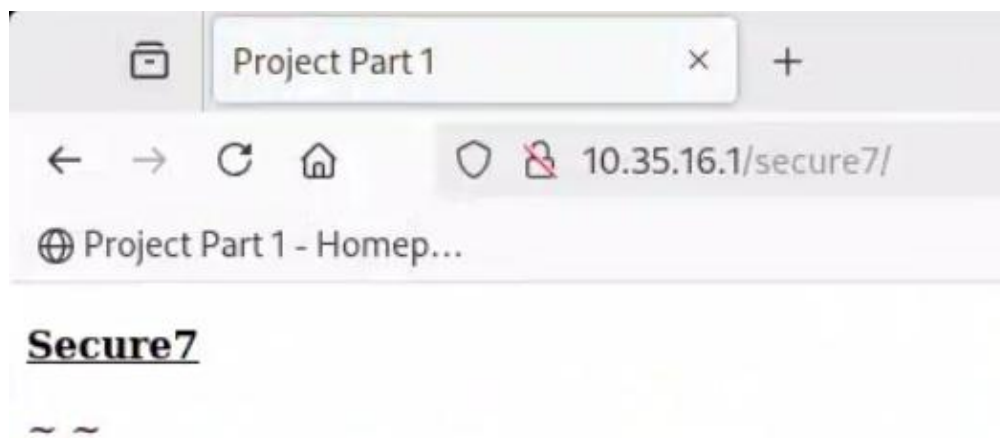
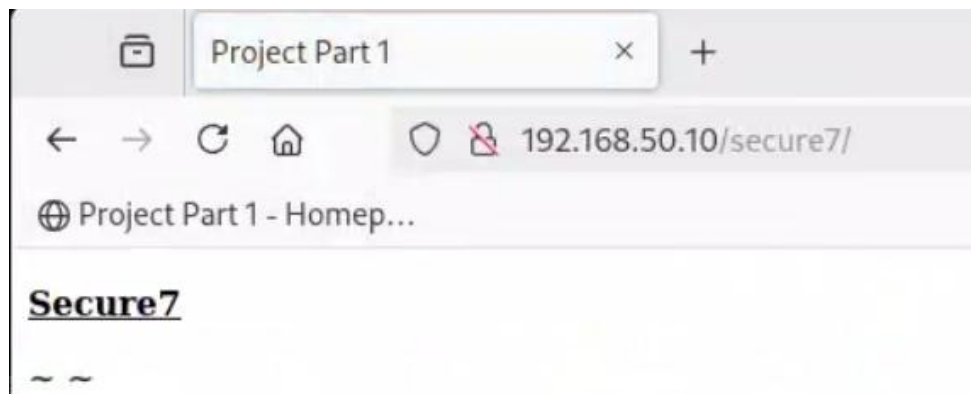


7. Create a secure7 directory and use an .htaccess file to allow access to either the user01 or any user from the 192.168.50.0/24 subnet

```
[root@server15 secure5]# vim /var/www/html_project1/secure7/.htaccess
[root@server15 secure5]#
```

```
AuthType Basic
AuthName "Restricted Area"
AuthUserFile /var/www/.htpasswd
<RequireAny>
  Require user user01
  Require ip 192.168.50.0/24
</RequireAny>
```

Test



As user01 in this subnet

ACCESSIBILITY (25 POINTS)

1. In the /var/www/html_project1 directory add the following subdirectories and initial setup (adding IP addresses):

➤ Project1

➤ Project2

➤ Project3

➤ Project4

Adding all IP addresses (from task 4 and task 3) right now so we can test our settings ASAP.

```
[root@server15 ~]# nmcli con mod LAN1 +ipv4.addresses 10.50.1.1/24 +ipv4.addresses 10.51.1.1/24 +ipv4.addresses 10.52.1.1/24 +ipv4.addresses 10.53.1.1/24 +ipv4.addresses 10.35.16.1/24 +ipv4.addresses 10.35.17.1/24 +ipv4.addresses 192.168.100.1/24
```

Now add them on ubuntu as well, switching the “1” for a “2” in the last octet of each IP:

```
root@client15:~# nmcli con mod LAN1 +ipv4.addresses 10.50.1.2/24 +ipv4.addresses 10.51.1.2/24 +ipv4.addresses 10.52.1.2/24 +ipv4.addresses 10.53.1.2/24 +ipv4.addresses 10.35.16.2/24 +ipv4.addresses 10.35.17.2/24 +ipv4.addresses 192.168.100.2/24
```

```
root@client15:~# nmcli con d LAN1 ; nmcli con u LAN1
Connection 'LAN1' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/16)
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/17)
root@client15:~#
```

```
[root@server15 ~]# nmcli con d LAN1 ; nmcli con u LAN1
Connection 'LAN1' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/4)
[root@server15 ~]#
```

Now create the directories

```
[root@server15 html_project1]# ls
index.html  secure1  secure2  secure3  secure4  secure5  secure6  secure7
[root@server15 html_project1]# mkdir Project1
[root@server15 html_project1]# mkdir Project2
[root@server15 html_project1]# mkdir Project3
[root@server15 html_project1]# mkdir Project4
[root@server15 html_project1]# ls
index.html  Project1  Project2  Project3  Project4  secure1  secure2  secure3  secure4  secure5  secure6  secure7
[root@server15 html_project1]#
```


2. In each of these directories, create a web page named after the directory itself. For example, Project1/project1.html, Project2/project2.html, etc.

```
[root@server15 html_project1]# cd Project1
[root@server15 Project1]# ls
project1.html
[root@server15 Project1]# cd ..
[root@server15 html_project1]# cd Project2
[root@server15 Project2]# ls
project2.html
[root@server15 Project2]# cd ..
[root@server15 html_project1]# cd Project3
[root@server15 Project3]# ls
project3.html
[root@server15 Project3]# cd ..
[root@server15 html_project1]# cd Project4
[root@server15 Project4]# ls
project4.html
```

We also include files like photo.gif, doc.txt and secret.doc in every folder for future testing purposes

```
[root@server15 Project1]# ll
total 0
-rw-r--r--. 1 root root 0 Apr 20 22:03 doc.txt
-rw-r--r--. 1 root root 0 Apr 19 21:18 project1.html
-rw-r--r--. 1 root root 0 Apr 20 22:03 secret.doc
[root@server15 Project1]#
```

3. Do not place an index.html file in these directories. Instead, configure Apache to display a directory listing when accessed.

```
[root@server15 html_project1]# tree Project*
Project1
├── doc.txt
├── project1.html
└── secret.doc
Project2
├── doc.txt
├── photo.gif
├── project2.html
└── secret.doc
Project3
├── doc.txt
├── photo.gif
├── photto.jpg
└── project3.html
Project4
├── doc.txt
├── photo.gif
├── project4.html
└── secret.doc
```

Setup the index.html:

```
<p>Project 1</p>
<p><a href="http://192.168.50.10/Project1">Project 1 (192.168.50.10 - All is accessible)</a></p>
<p><a href="http://10.35.16.1/Project1">Project 1 (10.35.16.1 - accessible except files secret.*)</a></p>
<p><a href="http://10.35.17.1/Project1">Project 1 (10.35.17.1 - accessible except files secret.*)</a></p>
<p><a href="http://192.168.100.1/Project1">Project 1 (192.168.100.1 - Not accessible )</a></p>

<p>Project 2</p>
<p><a href="http://192.168.50.10/Project2">Project 2 (192.168.50.10 - accessible)</a></p>
<p><a href="http://10.35.16.1/Project2">Project 2 (10.35.16.1 - Not accessible)</a></p>
<p><a href="http://10.35.17.1/Project2">Project 2 (10.35.17.1 - accessible)</a></p>
<p><a href="http://192.168.100.1/Project2">Project 2 (192.168.100.1 - accessible )</a></p>

<p>Project 3</p>
<p><a href="http://192.168.50.10/Project3">Project 3 (192.168.50.10 - All accessible) </a></p>
<p><a href="http://10.35.16.1/Project3">Project 3 (10.35.16.1 - Not accessible )</a></p>
<p><a href="http://10.35.17.1/Project3">Project 3 (10.35.17.1 - Not accessible )</a></p>
<p><a href="http://192.168.100.1/Project3">Project 3 (192.168.100.1 - accessible except *.gif files)</a></p>

<p>Project 4</p>
<p><a href="http://192.168.50.10/Project4">Project 4 (192.168.50.1 - All accessible) </a></p>
<p><a href="http://10.35.16.1/Project4">Project 4 (10.35.16.1 - All accessible excpet files test.html) </a></p>
<p><a href="http://10.35.17.1/Project4">Project 4 (10.35.17.1 - Not accessible) </a></p>
<p><a href="http://192.168.100.1/Project4">Project 4 (192.168.100.1 - All accessible except files test.html)</a></p>
```

4. Add <Directory> and <Files> directives to implement the following access controls:

- All directories and their contents must be accessible from the 192.168.50.0/24 subnet.

```

<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

<Directory "/var/www/html_project1">
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

```

View STEP 5 before testing*

➤ Project1: Accessible only from the 10.35.16.0/24 and 10.35.17.0/24 subnets. Any files named secret.* must not be accessible.

```

<Directory "/var/www/html_project1/Project1">
<RequireAny>
Require ip 10.35.16
Require ip 192.168.50
Require ip 10.35.17
</RequireAny>
    <Files "secret.*">
        Require ip 192.168.50
    </Files>
</Directory>

```

Going into ubuntu, we test each links :

Project 1

[Project 1 \(192.168.50.10 - All is accessible\)](#)




[Project 1 \(10.35.16.1 - accessible except files secret.*\)](#)

[Project 1 \(10.35.17.1 - accessible except files secret.*\)](#)

[Project 1 \(192.168.100.1 - Not accessible \)](#)



← → 🔄 ⚠ Not secure 192.168.50.10/Project1/

Index of /Project1

	<a>Name	<a>Last modified	<a>Size	<a>Description
	<a>Parent Directory		-	
	<a>doc.txt	2025-04-20 22:03	0	
	<a>project1.html	2025-04-19 21:18	0	
	<a>secret.doc	2025-04-20 22:03	0	



← → 🔄 ⚠ Not secure 10.35.16.1/Project1/

Index of /Project1

	<a>Name	<a>Last modified	<a>Size	<a>Description
	<a>Parent Directory		-	
	<a>project1.html	2025-04-19 21:18	0	

← → 🔄 ⚠ Not secure 10.35.17.1/Project1/

Index of /Project1

	<a>Name	<a>Last modified	<a>Size	<a>Description
	<a>Parent Directory		-	
	<a>project1.html	2025-04-19 21:18	0	

← → 🔄 ⚠ Not secure 192.168.100.1/Project1

Forbidden

You don't have permission to access this resource.

➤ Project2: Not accessible only from the 10.35.16.0/24 subnet. All files must be accessible to others.

```
<Directory "/var/www/html_project1/Project2">
  <RequireAll>
    Require all granted
    Require not ip 10.35.16
  </RequireAll>
</Directory>
```

Going into ubuntu, we test each links :

Project 2

[Project 2 \(192.168.50.10 - accessible\)](#)

[Project 2 \(10.35.16.1 - Not accessible\)](#)

[Project 2 \(10.35.17.1 - accessible\)](#)

[Project 2 \(192.168.100.1 - accessible\)](#)

← → ↻ ⚠ Not secure 192.168.50.10/Project2/

Index of /Project2

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 doc.txt	2025-04-20 22:03	0	
 photo.gif	2025-04-20 22:03	0	
 project2.html	2025-04-19 21:17	0	
 secret.doc	2025-04-20 22:03	0	

← → ↻ ⚠ Not secure 10.35.16.1/Project2

Forbidden

You don't have permission to access this resource.

← → ↻ ⚠ Not secure 10.35.17.1/Project2/

Index of /Project2

Name	Last modified	Size	Description
 Parent Directory		-	
 photo.gif	2025-04-20 22:03	0	
 project2.html	2025-04-19 21:17	0	
 secret.doc	2025-04-20 22:03	0	

← → ↻ ⚠ Not secure 192.168.100.1/Project2/

Index of /Project2

Name	Last modified	Size	Description
 Parent Directory		-	
 photo.gif	2025-04-20 22:03	0	
 project2.html	2025-04-19 21:17	0	
 secret.doc	2025-04-20 22:03	0	

➤ Project3: Accessible only from the 192.168.100.0/24 subnet. All *.gif files must not be accessible.

```
<Directory "/var/www/html_project1/Project3">
  Options +Indexes
  AllowOverride None
  <RequireAny>
    Require ip 192.168.50
    Require ip 192.168.100
  </RequireAny>

  <Files "*.gif">
    Require ip 192.168.50
  </Files>
</Directory>
```


Going into ubuntu, we test each links :

Project 3

[Project 3 \(192.168.50.10 - All accessible\)](#)

[Project 3 \(10.35.16.1 - Not accessible \)](#)

[Project 3 \(10.35.17.1 - Not accessible \)](#)

[Project 3 \(192.168.100.1 - accessible except *.gif files\)](#)

← → ↻ ⚠ Not secure 192.168.50.10/Project3/

Index of /Project3

	Name	Last modified	Size	Description
	Parent Directory		-	
	doc.txt	2025-04-20 22:03	0	
	photo.gif	2025-04-20 22:03	0	
	photto.jpg	2025-04-20 22:11	0	
	project3.html	2025-04-19 21:17	0	

← → ↻ ⚠ Not secure 10.35.16.1/Project3

Forbidden

You don't have permission to access this resource.

← → ↻ ⚠ Not secure 10.35.17.1/Project3

Forbidden

You don't have permission to access this resource.

← → ↻ ⚠ Not secure 192.168.100.1/Project3/

Index of /Project3

	Name	Last modified	Size	Description
	Parent Directory		-	
	photto.jpg	2025-04-20 22:11	0	
	project3.html	2025-04-19 21:17	0	

➤ Project4: Accessible only from 10.35.16.0/24 and 192.168.100.0/24.
All test.html files must not be accessible.

```
<Directory "/var/www/html_project1/Project4">
  Options +Indexes
  AllowOverride None

  <RequireAny>
    Require ip 192.168.100
    Require ip 192.168.50
    Require ip 10.35.16
  </RequireAny>

  <Files "test.html">
    Require ip 192.168.50
    Require all denied
  </Files>
</Directory>
```


Going into ubuntu, we test each links :

Project 4

[Project 4 \(192.168.50.1 - All accessible\)](#)

[Project 4 \(10.35.16.1 - All accessible except files test.html\)](#)

[Project 4 \(10.35.17.1 - Not accessible\)](#)

[Project 4 \(192.168.100.1 - All accessible except files test.html\)](#)

← → ↻ ⚠ Not secure 192.168.50.10/Project4/

Index of /Project4

	Name	Last modified	Size	Description
🔙	Parent Directory		-	
📄	doc.txt	2025-04-20 22:04	0	
🖼	photo.gif	2025-04-20 22:04	0	
📄	project4.html	2025-04-19 21:17	0	
🔍	secret.doc	2025-04-20 22:04	0	

← → ↻ ⚠ Not secure 10.35.16.1/Project4/

Index of /Project4

	Name	Last modified	Size	Description
🔙	Parent Directory		-	
🖼	photo.gif	2025-04-20 22:04	0	
📄	project4.html	2025-04-19 21:17	0	
🔍	secret.doc	2025-04-20 22:04	0	



5. For all directories, *.txt files must not be accessible. Place the corresponding directive outside of any <Directory> blocks. (This was added prior to testing)

```
<Files "*.txt">
  <RequireAny>
    Require ip 192.168.50
    Require all denied
  </RequireAny>
</Files>
```

AUTHORIZATION (25 POINTS)

1. Identify the network subnet of each department:

- Vendors use the subnet 10.50.1.0/24
- Accountants use the subnet 10.51.1.0/24
- Administrators use the subnet 10.52.1.0/24
- Programmers use the subnet 10.53.1.0/24

2. Each department has its own dedicated web directory on the server.

Websites must be placed in the /var/www/html/<group_name> directory. For

example: /var/www/html/vendors, /var/www/html/accountants, etc.

Create the htdocs file and add the folders:

```
[root@server15 www]# pwd
/var/www
[root@server15 www]# ll
total 4
drwxr-xr-x. 2 root root  6 Jan 21 16:23 cgi-bin
drwxr-xr-x. 2 root root  6 Apr 20 19:03 htdocs
drwxr-xr-x. 2 root root  6 Jan 21 16:23 html
drwxr-xr-x. 13 root root 4096 Apr 20 19:02 html_project1
[root@server15 www]#
```

```
[root@server15 www]# cd htdocs
[root@server15 htdocs]# mkdir vendors
[root@server15 htdocs]# mkdir accountants
[root@server15 htdocs]# mkdir administrators
[root@server15 htdocs]# mkdir programmers
[root@server15 htdocs]# ll
total 0
drwxr-xr-x. 2 root root 6 Apr 20 19:04 accountants
drwxr-xr-x. 2 root root 6 Apr 20 19:04 administrators
drwxr-xr-x. 2 root root 6 Apr 20 19:04 programmers
drwxr-xr-x. 2 root root 6 Apr 20 19:04 vendors
[root@server15 htdocs]#
```

4. You must use aliases to make these websites accessible. For example, to access the

vendors' website, use: <http://10.50.1.1/vendors>

At the end of the httpd.conf file, I added these lines to fit with the index file href"/vendors".. etc

```
Alias /vendors "/var/www/htdocs/vendors"  
Alias /accountants "/var/www/htdocs/accountants"  
Alias /administrators "/var/www/htdocs/administrators"  
Alias /programmers "/var/www/htdocs/programmers"
```

5. Configure the Apache server with the following access rules:

- Vendors can access only their own website.
- Accountants can access only the accountants' website and must not be able to view any *.html files.
- Administrators must be able to view all department websites.
- Programmers must be able to access their own website and to view all department websites except their *.gif or *.jpg files.

```
[root@server15 htdocs]# tree  
.  
├── accountants  
│   ├── accountants.html  
│   ├── Photo1.gif  
│   └── Photo1.jpg  
├── administrators  
│   ├── admin.html  
│   ├── Photo1.gif  
│   └── Photo1.jpg  
├── programmers  
│   ├── Photo1.gif  
│   ├── Photo1.jpg  
│   └── programmers.html  
└── vendors  
    ├── doc.txt  
    ├── Photo1.gif  
    ├── Photo1.jpg  
    └── vendors.html
```

Under the Aliases, add these lines to follow expected behaviors:

```
<Directory "/var/www/htdocs/">
    Options Indexes
    AllowOverride None
    Require all granted
</Directory>

<Directory "/var/www/htdocs/vendors">
<RequireAny>
    Require ip 10.50.1
    Require ip 10.52.1
    Require ip 10.53.1
</RequireAny>
<FilesMatch "\.(gif|jpg)$">
<RequireAny>
    Require ip 10.50.1
    Require ip 10.52.1
</RequireAny>
</FilesMatch>
</Directory>
```

```
<Directory "/var/www/htdocs/accountants">
<RequireAny>
    Require ip 10.51.1
    Require ip 10.52.1
    Require ip 10.53.1
</RequireAny>
<FilesMatch "\.(gif|jpg)$">
<RequireAny>
    Require ip 10.51.1
    Require ip 10.52.1
</RequireAny>
</FilesMatch>
</Directory>
```

```
<Directory "/var/www/htdocs/administrators">
<RequireAny>
    Require ip 10.52.1
    Require ip 10.53.1
</RequireAny>
    <FilesMatch "\.(gif|jpg)$">
    <RequireAny>
        Require ip 10.52.1
    </RequireAny>
    </FilesMatch>
</Directory>

<Directory "/var/www/htdocs/programmers">
<RequireAny>
    Require ip 10.52.1
    Require ip 10.53.1
</RequireAny>
</Directory>
```

Now test each links in ubuntu:

Vendors

Task 4 - Vendors website (10.50.1.0/24)

Accessible to Vendors(10.50.1.0/24)

Not Accessible to Accountants(10.51.1.0/24)

Accessible to Administrators(10.52.1.0/24)





Accessible from Programmers (10.53.1.0/24) (no *gif and *jpg files)

[←](#)[→](#)[↻](#)[🏠](#)

🔒 [10.50.1.1/vendors/](#)

🌐 Project Part 1 - Homep...

Index of /vendors

Name	Last modified	Size	Description
 Parent Directory		-	
 Photo1.gif	2025-04-20 23:23	0	
 Photo1.jpg	2025-04-20 23:23	0	
 vendors.html	2025-04-20 23:23	0	

[←](#)[→](#)[↻](#)[🏠](#)

🔒 [10.51.1.1/vendors](#)

🌐 Project Part 1 - Homep...

Forbidden





You don't have permission to access this resource.

[←](#)[→](#)[↻](#)[🏠](#)

🔒 [10.52.1.1/vendors/](#)

🌐 Project Part 1 - Homep...

Index of /vendors

Name	Last modified	Size	Description
 Parent Directory		-	
 Photo1.gif	2025-04-20 23:23	0	
 Photo1.jpg	2025-04-20 23:23	0	
 vendors.html	2025-04-20 23:23	0	

<div> <div> <div>←</div> <div>→</div> <div>↻</div> <div>🏠</div> </div> <div> <div>🛡️</div> <div>🔒</div> <div>10.53.1.1/vendors/</div> </div> </div> <div>🌐 Project Part 1 - Homep...</div>				
Index of /vendors				
	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔙	Parent Directory		-	
📄	vendors.html	2025-04-20 23:23	0	

Accountants

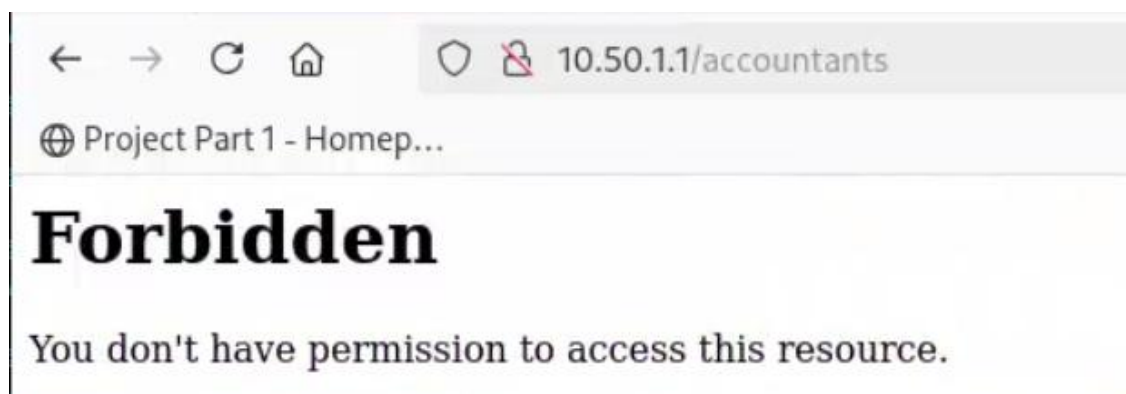
[Task 4 - Accountants Website \(10.51.1.0/24\)](#)

[Not Accessible to Vendors\(10.50.1.0/24\)](#)

[Accessible to Accountants\(10.51.1.0/24\)](#)

[Accessible to Administrators\(10.52.1.0/24\)](#)

[Accessible from Programmers \(10.53.1.0/24\).\(no *.gif and *.jpg files\)](#)



[←](#)[→](#)[↻](#)[🏠](#)

🔒 [10.51.1.1/accountsants/](#)

🌐 Project Part 1 - Homep...

Index of /accountsants

Name	Last modified	Size	Description
 Parent Directory		-	
 Photo1.gif	2025-04-20 23:21	0	
 Photo1.jpg	2025-04-20 23:21	0	
 accountants.html	2025-04-20 23:21	0	

[←](#)[→](#)[↻](#)[🏠](#)

🔒 [10.52.1.1/accountsants/](#)

🌐 Project Part 1 - Homep...

Index of /accountsants



Name	Last modified	Size	Description
 Parent Directory		-	
 Photo1.gif	2025-04-20 23:21	0	
 Photo1.jpg	2025-04-20 23:21	0	
 accountants.html	2025-04-20 23:21	0	

[←](#)[→](#)[↻](#)[🏠](#)

🔒 [10.53.1.1/accountsants/](#)

🌐 Project Part 1 - Homep...

Index of /accountsants

Name	Last modified	Size	Description
 Parent Directory		-	
 accountants.html	2025-04-20 23:21	0	

Administrators

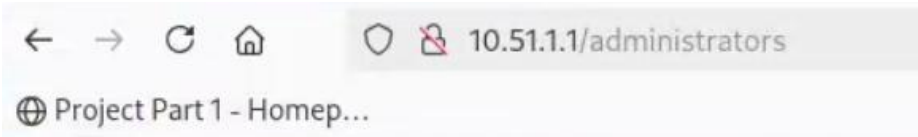
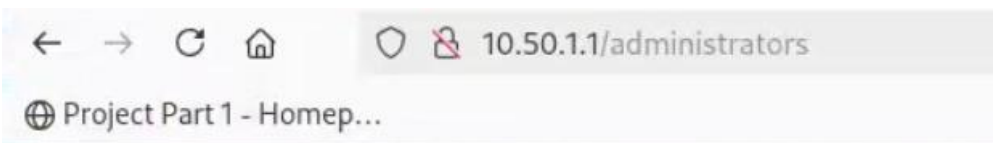
[Task 4 - Administrators website \(10.52.0.1/24\)](#)

[Not Accessible to Vendors\(10.50.1.0/24\)](#)

[Not Accessible to Accountants\(10.51.1.0/24\)](#)

[Accessible to Administrators\(10.52.1.0/24\)](#)

[Accessible from Programmers \(10.53.1.0/24\) \(no *.gif and *.jpg files\)](#)



← → ↻ 🏠 10.52.1.1/administrators/

🌐 Project Part 1 - Homep...

Index of /administrators

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔙 Parent Directory		-	
🖼️ Photo1.gif	2025-04-20 23:22	0	
🖼️ Photo1.jpg	2025-04-20 23:22	0	
📄 admin.html	2025-04-20 23:22	0	

← → ↻ 🏠 10.53.1.1/administrators/

🌐 Project Part 1 - Homep...

Index of /administrators

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔙 Parent Directory		-	
📄 admin.html	2025-04-20 23:22	0	

Programmers

[Task 4 - Programmers website \(10.53.0.1/24\)](#)

[Not Accessible to Vendors\(10.50.1.0/24\)](#)

[Not Accessible to Accountants\(10.51.1.0/24\)](#)

[Accessible to Administrators\(10.52.1.0/24\)](#)

[Accessible from Programmers \(10.53.1.0/24\)](#)

←

→

↻

🏠

🛡️

🔒

10.50.1.1/programmers

🌐 Project Part 1 - Homep...

Forbidden

You don't have permission to access this resource.

←

→

↻

🏠

🛡️

🔒

10.51.1.1/programmers

🌐 Project Part 1 - Homep...

Forbidden

You don't have permission to access this resource.

←

→

↻

🏠

🛡️

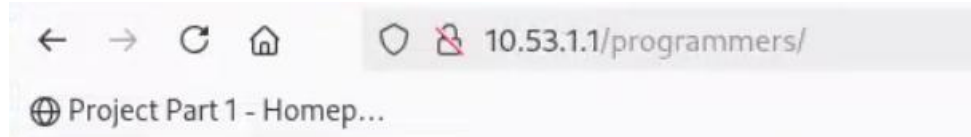
🔒

10.52.1.1/programmers/

🌐 Project Part 1 - Homep...

Index of /programmers

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔙 Parent Directory		-	
🖼️ Photo1.gif	2025-04-20 23:23	0	
🖼️ Photo1.jpg	2025-04-20 23:22	0	
📄 programmers.html	2025-04-20 23:22	0	



Index of /programmers

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 Photo1.gif	2025-04-20 23:23	0	
 Photo1.jpg	2025-04-20 23:22	0	
 programmers.html	2025-04-20 23:22	0	

All work as intended according to the rules set up.