
PROJECT PART I

420-635-AB-Network Installation and Administration I

OBJECTIVES

In this 1st part of the project, you will **install and configure an Apache web server and** create your first website by applying the necessary security rules.

GUIDELINES

The **Project Part 1** is graded out of **100** and accounts for **11%** of the final score.

You must provide a **detailed report** documenting the **commands executed in each section, the results obtained, and any relevant remarks. (Include clear and prominent screenshots.)**

You must also submit a **compressed file** containing of the **/etc/httpd/conf/httpd.conf** file and containing of **/var/www/html_project1** and **/var/www/htdocs** directories.

The report must be submitted upon completion and before the deadline. Submission must be done via **Moodle**. The report file must be named: **FirstName_LastName_Report_P1.pdf**.

PONDERATION

Task	Graded on
Task 1 – Creating a website	10%
Task 2 – Authentication	25%
Task 3 – Accessibility	25%
Task 4 – Authorization	25%
Report quality	15%
Total	100%

TASK 1 – CREATING A WEBSITE (10 POINTS)

1. Install and configure the Apache server to read web pages from the directory **"/var/www/html_project1"**.
 - You must copy the **httpd.conf** file to **httpd.conf.original**.
 - Configure the server to be accessible via the IP address **192.168.50.10**.
 - Ensure the **httpd** service is started and enabled to run at boot.
2. Create a new homepage named **index.html** in the **/var/www/html_project1** directory.
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.

TASK 2 – AUTHENTICATION (25 POINTS)

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


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

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

TASK 3 – ACCESSIBILITY (25 POINTS)

1. In the **/var/www/html_project1** directory add the following subdirectories:
 - **Project1**
 - **Project2**
 - **Project3**
 - **Project4**
2. In each of these directories, create a web page named after the directory itself. For example, **Project1/project1.html**, **Project2/project2.html**, etc.
3. **Do not place an index.html file** in these directories. Instead, configure Apache to display a **directory listing** when accessed.
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.
 - **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.
 - **Project2**: Not accessible only from the **10.35.16.0/24** subnet. All files must be accessible to others.
 - **Project3**: Accessible only from the **192.168.100.0/24** subnet. All ***.gif** files must not be accessible.
 - **Project4**: Accessible only from **10.35.16.0/24** and **192.168.100.0/24**. All **test.html** files must not be accessible.
5. For all directories, ***.txt** files must not be accessible. Place the corresponding **directive outside** of any **<Directory>** blocks.

TASK 4 – 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.
 3. Websites must be placed in the `/var/www/htdocs/<group_name>` directory. For example: `/var/www/htdocs/vendors`, `/var/www/htdocs/accountants`, etc.
 4. You must use **aliases** to make these websites accessible. For example, to access the vendors' website, use: **`http://10.50.1.1/vendors`**
 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.
-  **Note:** Make sure to demonstrate the enforcement of each access control rule through appropriate tests and screenshots or logs as evidence.

Example - index.html

Project Part 1

Task 2 - Secure directories:

[secure1 \(user01 - accessible\)](#)

[secure2 \(user01 and 192.168.50.0/24 - accessible\)](#)

[secure2 \(user01 and 10.35.16.1/24- Not accessible\)](#)

[secure3 \(user01 or 192.168.50.0/24 - accessible\)](#)

[secure3 \(user01 or 192.168.50.0/24 - accessible\)](#)

[secure4 \(user02 - accessible\)](#)

[secure5 \(user01 with .htaccess - accessible\)](#)

[secure6 \(user01 and 192.168.50 with .htaccess - Accessible\)\)](#)

[secure6 \(user01 and 10.35.16.1/24 with .htaccess - Not accessible\)\)](#)

[secure7 \(user01 or 192.168.50 with .htaccess - Accessible\)](#)

[secure7 \(user01 or 192.168.50 with .htaccess- Accessible\)](#)

Task 3 - Project 1:

[Project1 \(192.168.50.10 - All is accessible\)](#)

[Project1 \(10.35.16.1 accessible except files secret.* and *.txt\)](#)

[Project1 \(10.35.17.1 accessible except files secret.* and *.txt\)](#)

[Project1 \(192.168.100.1 Not accessible\)](#)

Task 3 - Project 2:

[Project2 \(192.168.50.10 - All is accessible\)](#)

[Project2 \(10.35.16.1 Not accessible\)](#)

[Project2 \(10.35.17.1 accessible except files *.txt\)](#)

[Project2 \(192.168.100.1 accessible except files *.txt\)](#)

Task 3 - Project 3:

[Project3 \(192.168.50.10 - All is accessible\)](#)

[Project3 \(10.35.16.1 Not accessible\)](#)

[Project3 \(10.35.17.1 Not accessible\)](#)

[Project3 \(192.168.100.1 accessible except files *.gif and *.txt\)](#)

Task 3 - Project 4:

[Project4 \(192.168.50.10 - All is accessible\)](#)

[Project4 \(10.35.16.1 accessible except files test.html\)](#)

[Project4 \(10.35.17.1 Not accessible\)](#)

[Project4 \(192.168.100.1 accessible except files test.html\)](#)

Task 4 - Vendors website:

[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 to Programmers \(10.53.1.0/24\) but not *.gif and *.jpg files](#)

Task 4 - Accountants website:

[Not accessible to Vendors \(10.50.1.0/24\) but not *.html files](#)

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

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

[Accessible to Programmers \(10.53.1.0/24\) but not *.gif and *.jpg files](#)

Task 4 - Programmers website:

[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 to Programmers \(10.53.1.0/24\)](#)

Task 4 - Administrators website:

[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 to Programmers \(10.53.1.0/24\) but not *.gif and *.jpg files](#)