

Password protecting your Labs directory for CSCI311

Overview

This document describes how to password protect the contents of your Labs directory for CSCI 311. We will use `.htaccess` file to achieve this. This will prevent other class members from viewing your solutions to the Labs.

How `.htaccess` works

We password protect a directory (and all of its contents) by:

- placing a `.htaccess` file in that directory
- specifying in the `.htaccess` file
 - where to redirect on failure to authenticate
 - where to look for the passwords
 - how to authenticate
 - what users have access to that directory
- setting up appropriate error html pages

This document will walk you through this process. Once done, you will have the following directory structure in your home directory:

```
passwords/
passwords/.htpasswd
public_html/
public_html/.htaccess
public_html/error404.html
public_html/index.html
public_html/csci311/
public_html/csci311/.htaccess
public_html/csci311/error404.html
public_html/csci311/index.html
public_html/csci311/labs/
public_html/csci311/labs/.htaccess
public_html/csci311/labs/index.html
```

passwords directory

We create a `passwords` directory that contains the username-password pairs for individuals or groups that are permitted to access files or directories. These passwords are encrypted. This directory must:

- be outside the `public_html` directory (so that it is not world searchable)
- have appropriate permissions set: `751` or `drwxr-x--x`
- contain a `.htpasswd` file that includes passwords for me and you (at minimum)

How to set up your `.htpasswd` file

I will send you a `.htpasswd` file which you need to place in the `passwords` directory. It must have the permissions set to `644`, using the following command:

- `chmod 644 .htpasswd`

Add a line for yourself with the following format:

- `username:hashedPassword`

You can generate a hashed password here:

- <http://www.joeswebtools.com/security/htpasswd-generator/>

NOTE: Do not use a password that is used anywhere else. This is, of course, good advice in general, but more important than usual as something as simple as incorrectly setting permissions could reveal it (by brute force attacking the hashes), and thereby reveal a password used elsewhere.

Set up .htaccess and error files in all other directories

Using the file list above as a guide, create .htaccess files and error404.html files for all of the following directories:

- public_html
- public_html/csc311
- public_html/csc311/labs

.htaccess files

the htaccess file in each directory is what controls access to this directory, and its contents. You will create a separate .htaccess file for each of the following directories, as described below:

- public_html
- public_html/csc311
- public_html/csc311/labs

public_html

The .htaccess file for public_html directory should contain the following:

```
ErrorDocument 404 /~username/error404.html
```

(where username is your csci username)

public_html/csci311

The .htaccess file for public_html/csci311 should contain the following:

```
ErrorDocument 404 /~username/csci311/error404.html
```

(where username is your csci username)

public_html/csci311/labs

The .htaccess file for public_html/csci311/labs should contain the following:

```
ErrorDocument 404 /~username/csci311/error404.html
AuthUserFile "/home/student/username/passwords/.htpasswd"
AuthName "Please Enter Password"
AuthType Basic
Require valid-user
```

(where username is your csci username)

error404.html file contents

This is the file that will be shown on failure to authenticate. You can download the error404.html file from the course page found under the Lab1 resources. Place a copy of it in:

- public_html
- public_html/csci311

Once set up, test your setup with a lab mate. See if they can access your labs directory.