IT 324 Web Systems and Technologies
Midterms Activity: [Group] Apache HTTP Server Installation and Configuration

**Activity Requirements:**

- For each group member, create a virtual host mapped to the domain name **www.*idnumber*.org**, where ***idnumber*** is the member's ID number (e.g., **www.2151234.org**). Use the contents of the member's personal profile website for each virtual host's content.
- Check that each virtual host is accessible from a browser in the host machine (after adding the appropriate local DNS entry to the **hosts** file on the host machine).
- Configure each virtual host to enable serving up compressed content to clients that are able to handle the compressed encoding, as specified in the HTTP **Accept-Encoding** header. Limit the compression to HTML and CSS files only.
- Configure the virtual host to enable clients to cache PNG, JPG, and GIF files for up to 24 hours from the time they are accessed.

- Create a virtual host mapped to the domain name **webtek.negotiate.org**. Create two dummy files, named **content.html** and **content.txt**, in the document root of the virtual host, and configure the virtual host to enable clients to negotiate with the server, using the HTTP **Accept** header, which of the two files is served when clients access the URL **http://webtek.negotiate.org/content**.
- Create two other dummy files, named **language.html.en** and **language.html.fil**, in the document root of the virtual host, and configure the virtual host to enable clients to negotiate with the server, using the HTTP **Accept-Language** header, which of the two files is served when clients access the URL **http://webtek.negotiate.org/language.html**.

- Create a virtual host mapped to the domain name **webtek.access.org**, with a dummy **index.html** file in the virtual host's document root. Configure access to the virtual host such that:
  - only requests from host with ***.edu** or ***.org** domains will be allowed
  - only **GET**, **HEAD**, and **POST** requests will be allowed
  - **POST** requests will be allowed only for valid users authenticated via basic authentication, using the ID numbers of the group's members as user credentials (i.e., usernames and passwords)

- Create a virtual host mapped to the domain name **webtek.ssi.org**. Enable server-side includes on the virtual host, and create dummy contents illustrating two different ways (i.e., using either the filename extension-based approach, or using the **XBitHack** directive) of serving HTML pages with server-side included content.

- Create a virtual host mapped to the domain name **webtek.secure.org**, with a dummy index.html file in the virtual host's document root. Configure the virtual host such that its contents are only accessible via **https**, with **http** requests automatically redirected as **https** requests. Use **openssl** to generate a self-signed **X.509** certificate with **RSA-2048** encryption for the virtual host, with the certificate details provided below:

  Country Name: **PH**
  State or Province Name: **Benguet**
  Locality Name: **Baguio City**
  Organization Name: **SLU-SCIS**
  Organizational Unit Name: **WebTek Group #** (e.g., **WebTek Group 1**)
  Common Name: **webtek.secure.org**
  Email Address: ***any email address***

**Online Resources:**

- Apache HTTP Server Documentation
  - http://httpd.apache.org/docs/
- OpenSSL Manual
  - https://www.openssl.org/docs/manmaster/man1/req.html