

# LAB 5 REPORT

**Checkpoint 1:** Access <https://localhost:4433> and describe observations.

**Steps I have followed:**

1. Here in this portion I have created an apache server
2. Then by default it was hosted on localhost (127.0.0.1)
3. It was not secure and used protocol <http://>
4. Then I added example.com in the  
`/var/www/example.com/html/index.html`
5. Then I added index.html in the file and it will be hosted in example.com
6. Then I virtually configured at http protocol port 80 and hosted the site at example.com in <http://> which is not secure

**Checkpoint 2:** Repeat the setup for webserverlab.com and show the results.

**Steps I have followed:**

1. Then I followed the same way and served the  
`/var/www/html/index.html`
2. Configured the default-ssl.conf and added the webserverlab.com to the localhost
3. Then webserverlab.com and example.com were hosted on [http](http://)

**Checkpoint 3:** Demonstrate accessing <https://example.com> via HTTPS.

**Steps I have followed:**

1. Then I first became a CA by copying openssl.cnf in demoCA. I generated RSA key pair and then followed the instruction to make the certificate
2. Then I configured 443 (HTTPS) for the example.com and there I added the configuration blocks and added the route of the `var/www/example.com/html/index.html`
3. Then I configured SSLCertificateFile & SSLCertificateKeyFile which was generated before
4. Then I forcefully make the exception to trust my local CA by the mozilla browser that is how I was able to access <https://example.com> properly. Though I used external sources to fix some certificate issues.

1. **Checkpoint 4:** Set up and access <https://webserverlab.com> via HTTPS.

**Steps I have followed:**

1. I followed the same steps to host <https://webserverlab.com> using https

Here are some of the screenshots of my process:



```

</html>
(base) taohid@me0r:/var/www/example.com/html$ cd ..
(base) taohid@me0r:/var/www/example.com$ cd ..
(base) taohid@me0r:/var/www$ ls
example.com  html
(base) taohid@me0r:/var/www$ cd html/
(base) taohid@me0r:/var/www/html$ ls
index.html
(base) taohid@me0r:/var/www/html$ cat index.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2022-03-22
    See: https://launchpad.net/bugs/1966004
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
      * {
        margin: 0px 0px 0px 0px;
        padding: 0px 0px 0px 0px;
      }

      body, html {
        padding: 3px 3px 3px 3px;

        background-color: #D8DBE2;

```

```

GNU nano 6.2 default-ssl.conf
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin admin@webserverlab.com
    ServerName webserverlab.com

    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

    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

    # Server Certificate Chain:
    # Point SSLCertificateChainFile at a file containing the
    # concatenation of PEM encoded CA certificates which form the

```

```

(base) taohid@me0r:/etc/apache2/sites-available$ ls
000-default.conf default-ssl.conf default-ssl.conf.bak example.com.conf
(base) taohid@me0r:/etc/apache2/sites-available$ █

```

```
GNU nano 6.2                                000-default.conf
<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
</VirtualHost>

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

```
GNU nano 6.2                                example.com.conf *
S<VirtualHost _default_:443>
    ServerAdmin admin@example.com
    ServerName example.com

    DocumentRoot /var/www/example.com/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

    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

    # Server Certificate Chain:
    # Point SSLCertificateChainFile at a file containing the
    # concatenation of PEM encoded CA certificates which form the
    # certificate chain for the server certificate. Alternatively
```



```
GNU nano 6.2 default-ssl.conf
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    ServerAdmin admin@webserverlab.com
    ServerName webserverlab.com

    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

    #
    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    #
    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

    #
    # Server Certificate Chain:
    # Point SSLCertificateChainFile at a file containing the
    # concatenation of PEM encoded CA certificates which form the
```




## LAB 5 TASK by MEHRAJ

Apache2 Ubuntu Default Page

THIS IS LAB 5 TASK

https://example.com



Ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2` and is managed using `systemd`, so to start/stop the service use `systemctl start apache2` and `systemctl stop apache2`, and use `systemctl status apache2` and `journalctl -u apache2` to check status. `systemd` and `apache2ctl` can also be used for service management if desired. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

Apache2 Ubuntu Default Po...THIS IS LAB 5 TASKCertificate for example.com

Firefoxabout:certificate?cert=MIIDTCCAp2GawIBAgIUtB3QYtqYw6tBwzobiEUwy%2FVZowDQYJKoZIhvcNAQELBQAwajELMAKGA1UEBhMCQkQxQzA2JgNVBAGwMakJEMQswCQYDVQQHDA...

Validity

Not BeforeSat, 06 Jul 2024 23:02:30 GMT

Not AfterSun, 06 Jul 2025 23:02:30 GMT

Public Key Info

AlgorithmRSA

Key Size2048

Exponent65537

ModulusBE-44:1CD1:63:D4:BA:01:01:6A:43:4D:8A:96:67:A4:8F:DF:E2:FEE7:DE:63:2...

Miscellaneous

Serial Number4E:D0:77:41:8B:6A:5F:25:BA:B5:B5:B3:A1:B8:84:53:0C:BF:55:9D

Signature AlgorithmSHA-256 with RSA Encryption

Version3

Download[PEM \(cert\)](#) [PEM \(chain\)](#)

Fingerprints

SHA-2565C:C5:FF:A7:7B:B3:E7:39:A1:EA:D6:7A:ED:6D:17:89:9D:A6:C7:83:24:D5:C7:7...

SHA-176:13:EA:9F:A5:50:0D:50:A1:96:73:3C:8F:7F:8C:E6:4D:59:B3:C9

Basic Constraints

Certificate AuthorityYes

Subject Key ID

Key IDA1:0E:21:48:19:E5:BF:3D:4B:A4:81:F5:1C:1C:1E:BB:35:7E:BC:94

Authority Key ID

Key IDA1:0E:21:48:19:E5:BF:3D:4B:A4:81:F5:1C:1C:1E:BB:35:7E:BC:94

Apache2 Ubuntu Default Po...THIS IS LAB 5 TASKCertificate for example.com

Firefoxabout:certificate?cert=MIIDTCCAp2GawIBAgIUtB3QYtqYw6tBwzobiEUwy%2FVZowDQYJKoZIhvcNAQELBQAwajELMAKGA1UEBhMCQkQxQzA2JgNVBAGwMakJEMQswCQYDVQQHDA...

example.com

Subject Name

CountryBD

State/ProvinceBD

LocalityBD

OrganizationBD

Organizational UnitBD

Common Nameexample.com

Email AddressBD

Issuer Name

CountryBD

State/ProvinceBD

LocalityBD

OrganizationBD

Organizational UnitBD

Common Nameexample.com

Email AddressBD

Validity

Not BeforeSat, 06 Jul 2024 23:02:30 GMT

Not AfterSun, 06 Jul 2025 23:02:30 GMT

Public Key Info

AlgorithmRSA

Key Size2048

Exponent65537

ModulusBE-44:1CD1:63:D4:BA:01:01:6A:43:4D:8A:96:67:A4:8F:DF:E2:FEE7:DE:63:2...

Miscellaneous

Serial Number4E:D0:77:41:8B:6A:5F:25:BA:B5:B5:B3:A1:B8:84:53:0C:BF:55:9D

Signature AlgorithmSHA-256 with RSA Encryption

Version3

