CSE487: Cybersecurity, Law and Ethics

[Spring 2022]

Section: 3

Implementing SSL on a Website

Mini-Project Report

Submitted to:

Rashedul Amin Tuhin

Senior Lecturer,

Department of Computer Science & Engineering,

East West University

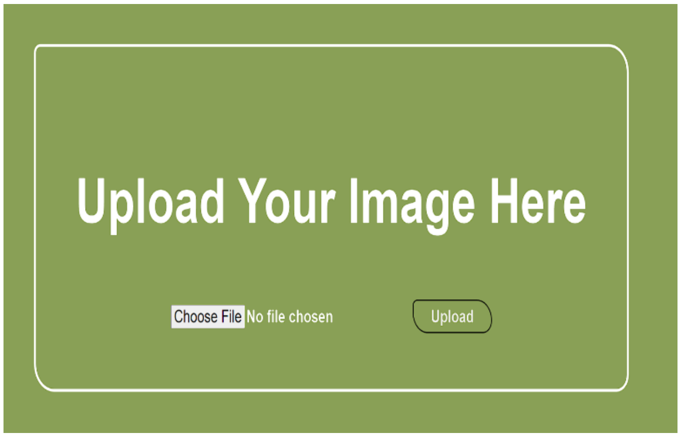
Submitted by:

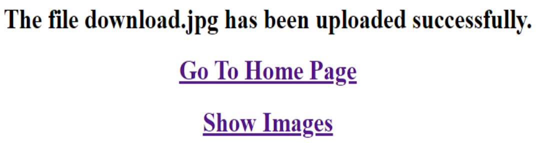
Student ID	Student Name
2019-1-60-036	Hasib Ar Rafiul Fahim
2018-3-60-088	Rashik Buksh Rafsan
2019-1-60-068	Md. Shahadat Anik Sheikh

Project Explanation:

Step-1: Creating the Website:

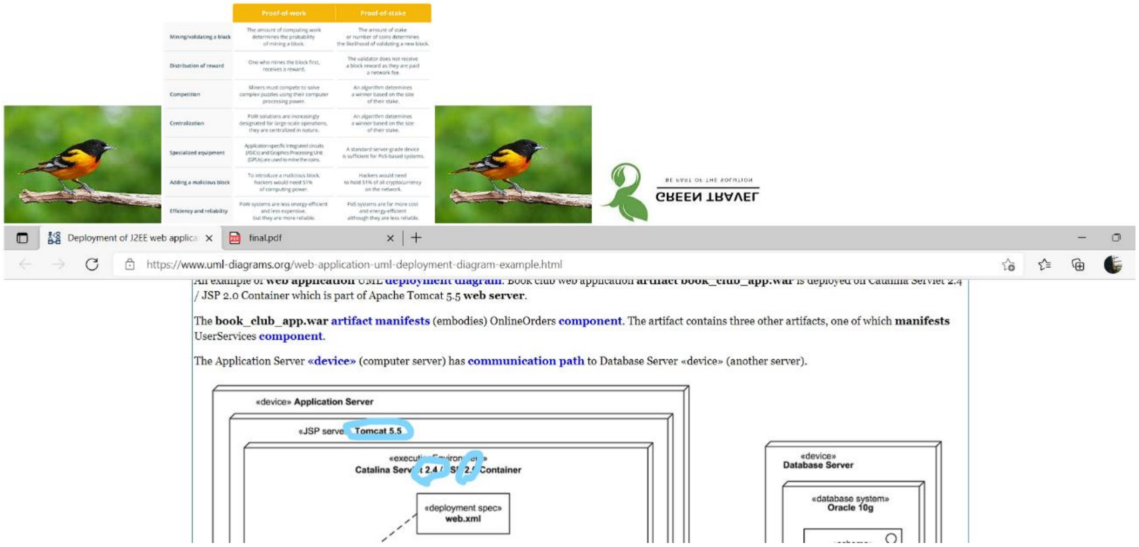
First of all, we created a simple website which uploads images to MySQL database and show them. The images are stored in our localhost.




The file download.jpg has been uploaded successfully.

Go To Home Page

Show Images



	Proof-of-work	Proof-of-stake
Mining/validating a block	The amount of computing work determines the probability of mining a block.	The amount of stake or number of coins determines the likelihood of validating a new block.
Distribution of reward	One who mines the block first, receives a reward.	The validator does not receive a block reward as they are paid a network fee.
Competition	Miners must compete to solve complex puzzles using their computer processing power.	An algorithm determines a winner based on the size of their stake.
Centralization	PoW solutions are increasingly designated for large-scale operations, they are centralized in nature.	An algorithm determines a winner based on the size of their stake.
Specialized equipment	Application-specific integrated circuits (ASICs) and Graphics Processing Unit (GPUs) are used to mine the coins.	A standard server-grade device is sufficient for PoS-based systems.
Adding a malicious block	To introduce a malicious block, hackers would need 51% of computing power.	Hackers would need to hold 51% of all cryptocurrency on the network.
Efficiency and reliability	PoW systems are less energy-efficient and less expensive, but they are more reliable.	PoS systems are far more cost and energy-efficient although they are less reliable.

BE PART OF THE SOLUTION
GREEN TRAVEL
Deployment of J2EE web applica
final.pdf
https://www.uml-diagrams.org/web-application-uml-deployment-diagram-example.html

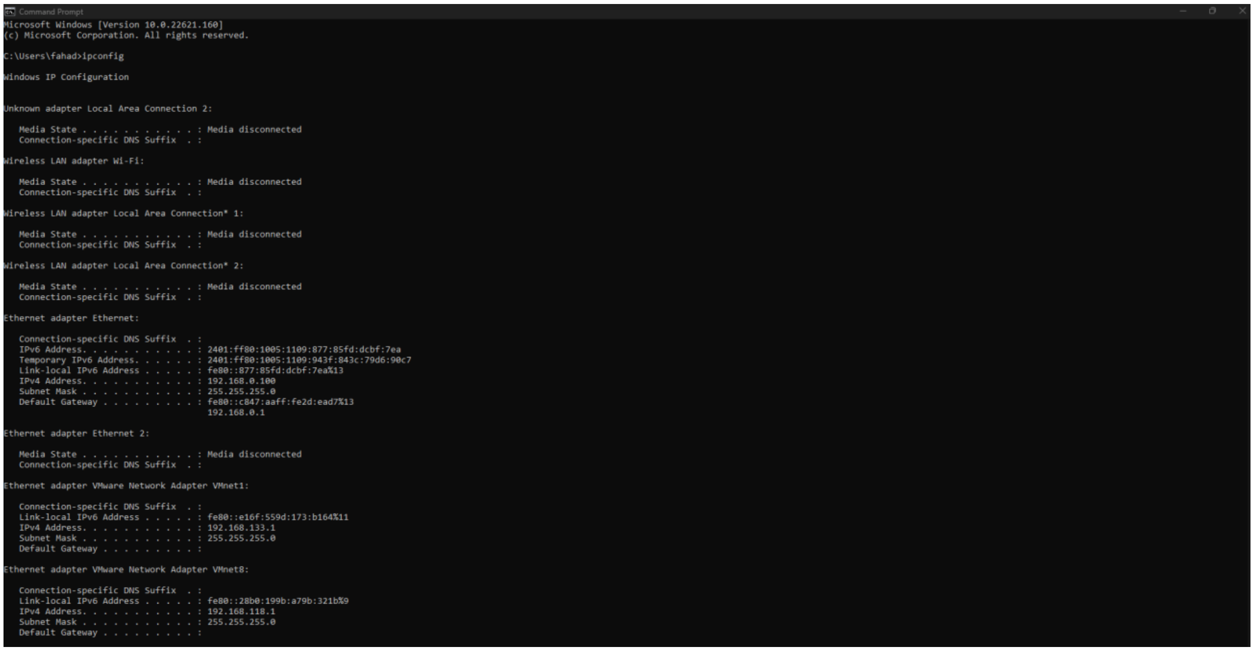
An example of **web application** UML **deployment diagram**. Book club web application **artifact book_club_app.war** is deployed on Catalina Servlet 2.4 / JSP 2.0 Container which is part of Apache Tomcat 5.5 **web server**.

The **book_club_app.war artifact manifests** (embodies) OnlineOrders **component**. The artifact contains three other artifacts, one of which **manifests** UserServices **component**.

The Application Server **«device»** (computer server) has **communication path** to Database Server «device» (another server).

Step-2: Securing a public IP:

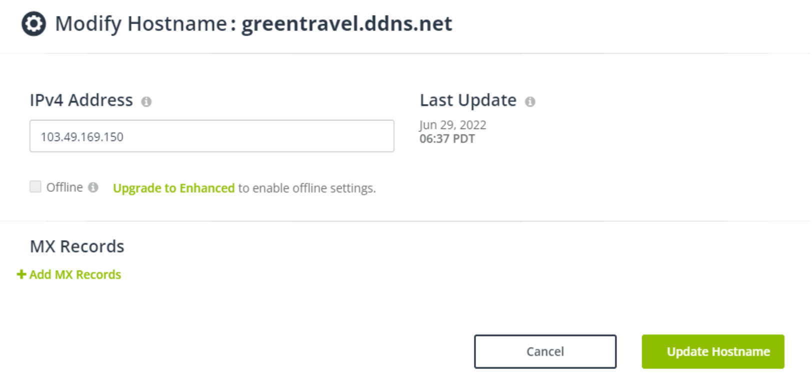
We secured a static IP Address from an ISP. As a result, we have a public IP address through which our localhost can be accessible.



```
Microsoft Windows [Version 10.0.22621.160]
(c) Microsoft Corporation. All rights reserved.

C:\Users\fahad>ipconfig

Windows IP Configuration


Unknown adapter Local Area Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:ff80:1005:1109:877:85fd:dcbf:7ea
   Temporary IPv6 Address. . . . . . : 2401:ff80:1005:1109:943f:843c:79d6:90c7
   Link-local IPv6 Address . . . . . : fe80::877:85fd:dcbf:7ea%13
   IPv4 Address. . . . . . . . . . . : 192.168.0.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::c847:aaff:fe2d:ead7%13
                                       192.168.0.1

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e16f:559d:173:b164%11
   IPv4 Address. . . . . . . . . . . : 192.168.133.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::28b0:199b:a79b:321b%9
   IPv4 Address. . . . . . . . . . . : 192.168.118.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Step-3: Configuring DDNS:

We configured DDNS (Dynamic Display Name Server) for our public IP. We used NOIP to assign a particular DDNS for our corresponding public IP. This DDNS accesses our public IP addresses and communicates with our localhost via a default port which is 80. So, we had to port forward our localhost through port 80.

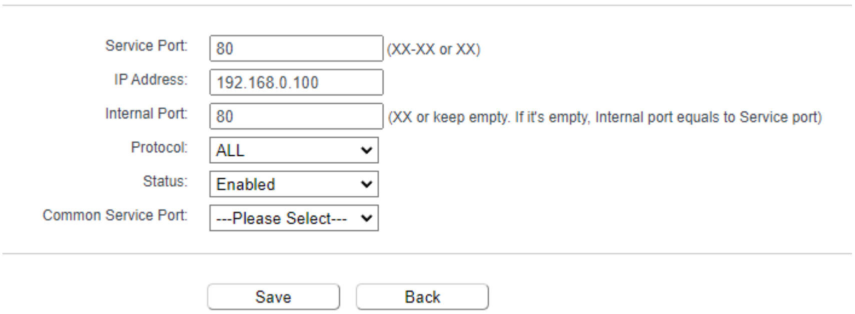


Modify Hostname : **greentravel.ddns.net**

IPv4 Address: 103.49.169.150

Last Update: Jun 29, 2022 06:37 PDT

□ Offline



Service Port: 80 (XX-XX or XX)
IP Address: 192.168.0.100
Internal Port: 80 (XX or keep empty. If it's empty, Internal port equals to Service port)
Protocol: ALL
Status: Enabled
Common Service Port: ---Please Select---

Step-4: Generating Signed Certificate:

Now, our website is up and running but it is not secured because there is no SSL certificate. In this part, we will create a signed certificate for our server. We used OpenSSL tool to generate private key and certificate request for our server. We used our DDNS as the name for signing the certificate. Then, we used OpenSSL to generate a signed certificate for our corresponding DDNS. The certificate request CSR (Certificate Signing Request) must be created with a key length of 2048 and SHA256 as the hash algorithm. It checks if DDNS is owned by us or not. After successful check, it gives us the signed certificate.

- First of all, we need to install OPENSSL in our Windows. For that, we need to run cmd as administrator. Then we used the following command,
  choco install openssl
- To generate a pair of private key and public Certificate Signing Request (CSR) for a web server, “server”, use the following command:
  openssl req -new -nodes -keyout myserver.key -out server.csr
  This creates two files. The file myserver.key contains a private key. The private key is used as input in the command to generate a Certificate Signing Request (CSR). We will now be asked to enter details to be entered into the CSR. What we are about to enter is what is called a Distinguished Name or a DN.

  Country Name (2 letter code) [AU]: BD
  State or Province Name (full name) [Some-State]: Dhaka
  Locality Name (eg, city) []: Dhaka
  Organization Name (eg, company) [Internet Widgits Pty Ltd]:
  Organizational Unit Name (eg, section) []: IT
  Common Name (eg, YOUR name) []: greentravel.ddns.net
  Email Address []:

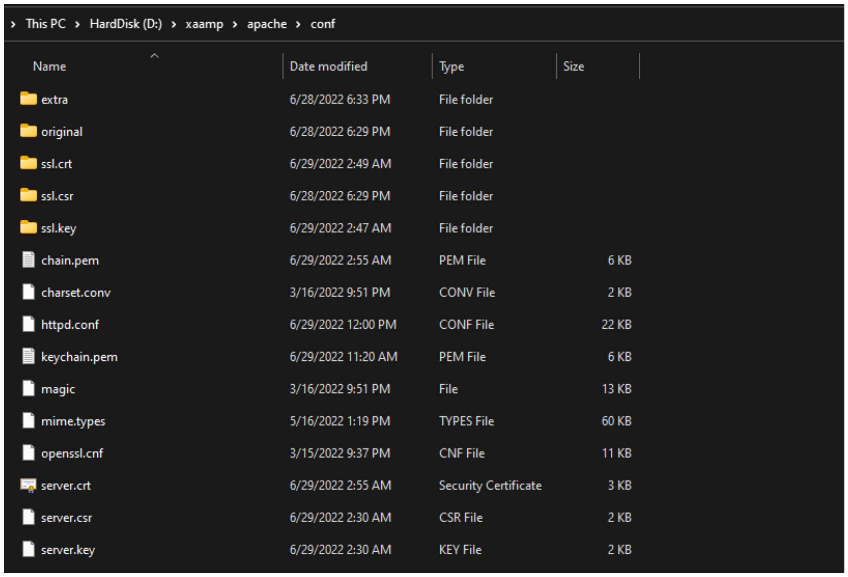
  Please enter the following ‘extra’ attributes to be sent with your certificate request.

A challenge password []: (leave this blank)
Our CSR will now have been created.

- We used trustcor standard DV to issue a signed standard SSL certificate. It issued us a certificate using our CSR and gave us the certificate in .pem format.

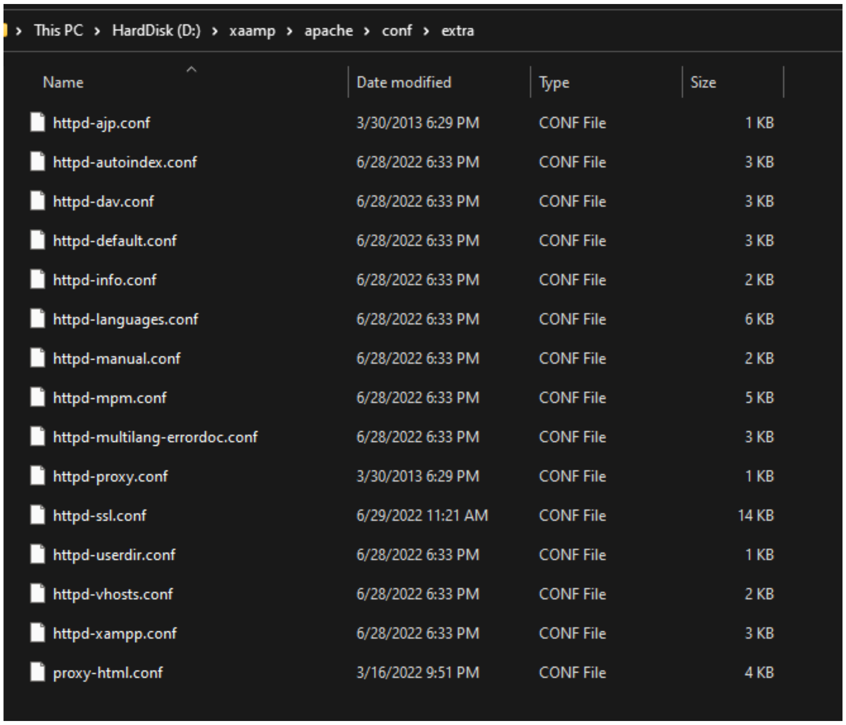
Step-5: Installing Certificate:

We opened apache server /apache/conf and we replaced our signed certificates there. We edited httpd.conf to point our certificates to be used by the server and included our DDNS. We opened /apache/conf/extra/httpd-ssl.conf and put our ssl configuration. Then we restarted the server.



› This PC › HardDisk (D:) › xaamp › apache › conf

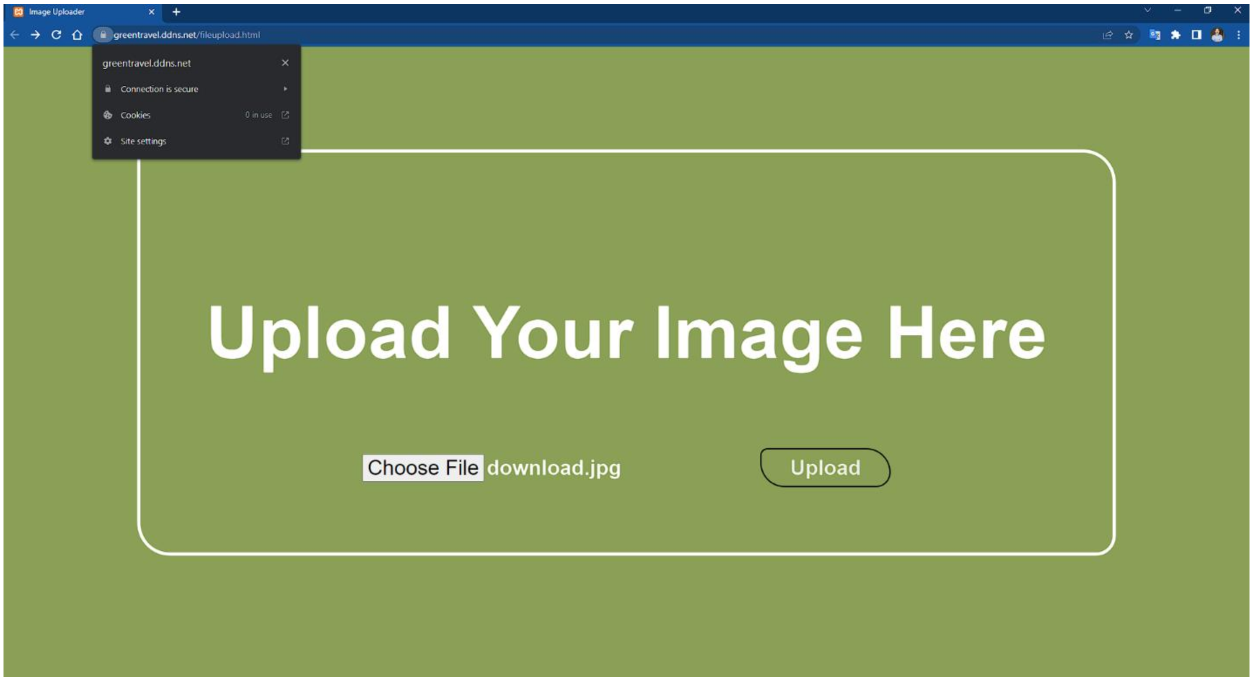
Name	Date modified	Type	Size
extra	6/28/2022 6:33 PM	File folder	
original	6/28/2022 6:29 PM	File folder	
ssl.crt	6/29/2022 2:49 AM	File folder	
ssl.csr	6/28/2022 6:29 PM	File folder	
ssl.key	6/29/2022 2:47 AM	File folder	
chain.pem	6/29/2022 2:55 AM	PEM File	6 KB
charset.conv	3/16/2022 9:51 PM	CONV File	2 KB
httpd.conf	6/29/2022 12:00 PM	CONF File	22 KB
keychain.pem	6/29/2022 11:20 AM	PEM File	6 KB
magic	3/16/2022 9:51 PM	File	13 KB
mime.types	5/16/2022 1:19 PM	TYPES File	60 KB
openssl.cnf	3/15/2022 9:37 PM	CNF File	11 KB
server.crt	6/29/2022 2:55 AM	Security Certificate	3 KB
server.csr	6/29/2022 2:30 AM	CSR File	2 KB
server.key	6/29/2022 2:30 AM	KEY File	2 KB



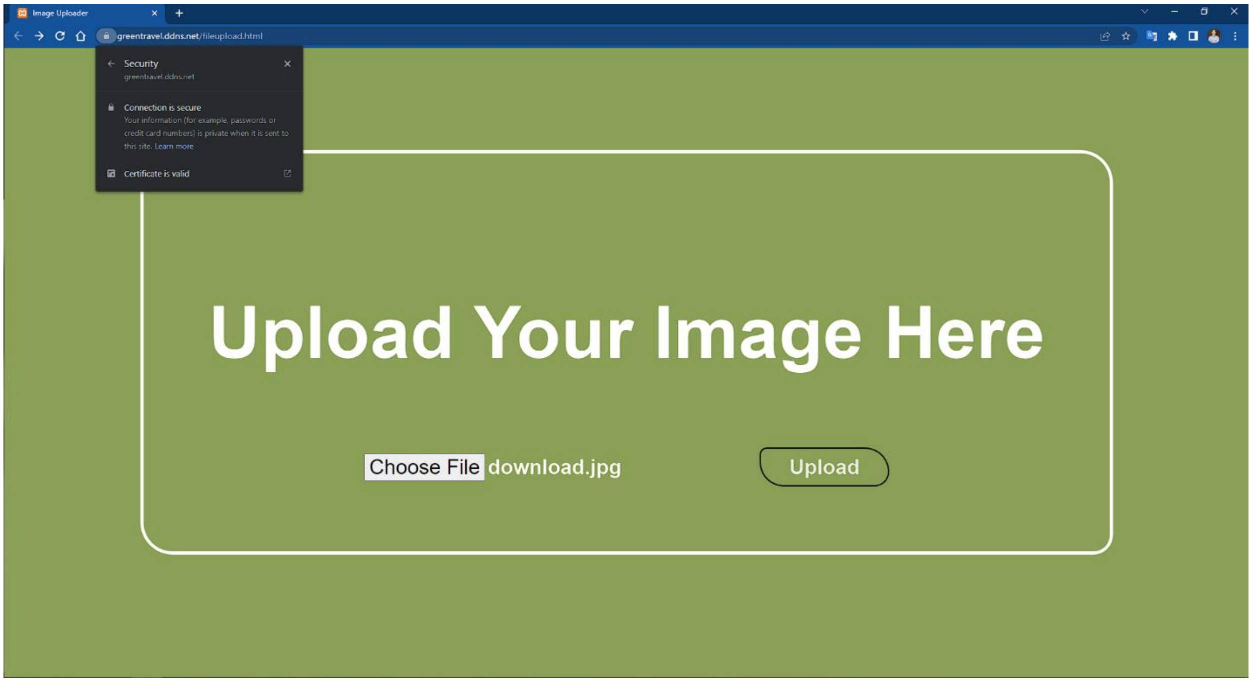
› This PC › HardDisk (D:) › xaamp › apache › conf › extra

Name	Date modified	Type	Size
httpd-ajp.conf	3/30/2013 6:29 PM	CONF File	1 KB
httpd-autoindex.conf	6/28/2022 6:33 PM	CONF File	3 KB
httpd-dav.conf	6/28/2022 6:33 PM	CONF File	3 KB
httpd-default.conf	6/28/2022 6:33 PM	CONF File	3 KB
httpd-info.conf	6/28/2022 6:33 PM	CONF File	2 KB
httpd-languages.conf	6/28/2022 6:33 PM	CONF File	6 KB
httpd-manual.conf	6/28/2022 6:33 PM	CONF File	2 KB
httpd-mpm.conf	6/28/2022 6:33 PM	CONF File	5 KB
httpd-multilang-errordoc.conf	6/28/2022 6:33 PM	CONF File	3 KB
httpd-proxy.conf	3/30/2013 6:29 PM	CONF File	1 KB
httpd-ssl.conf	6/29/2022 11:21 AM	CONF File	14 KB
httpd-userdir.conf	6/28/2022 6:33 PM	CONF File	1 KB
httpd-vhosts.conf	6/28/2022 6:33 PM	CONF File	2 KB
httpd-xampp.conf	6/28/2022 6:33 PM	CONF File	3 KB
proxy-html.conf	3/16/2022 9:51 PM	CONF File	4 KB

Finally, our website is running with SSL Certificate. We have also showed our certification path.



Upload Your Image Here

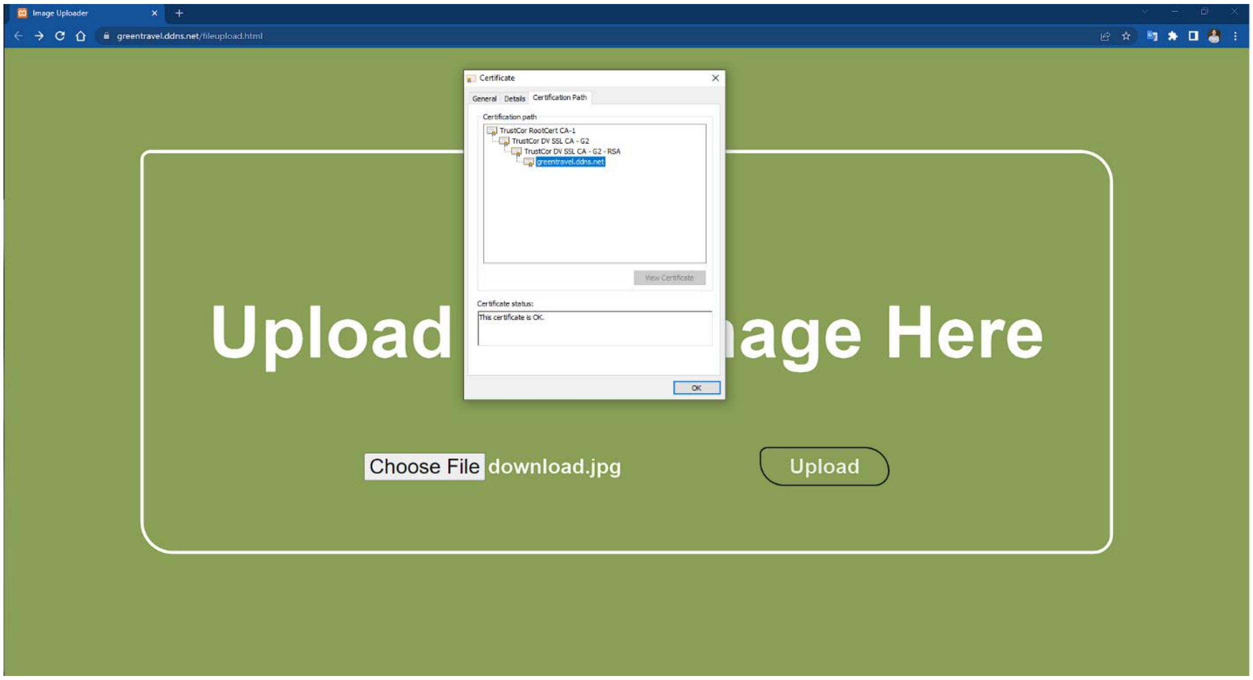


Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid

Upload Your Image Here



Certification path

TrustCor RootCert CA-1
TrustCor DV SSL CA - G2
TrustCor DV SSL CA - G2 - RSA
greentravel.ddns.net

Certificate status:

This certificate is OK.