

Module 7 Activity 1: Generating SSL Certificate and Configuring HTTPS Server in

Node.js on Windows

Brandon Trinkle

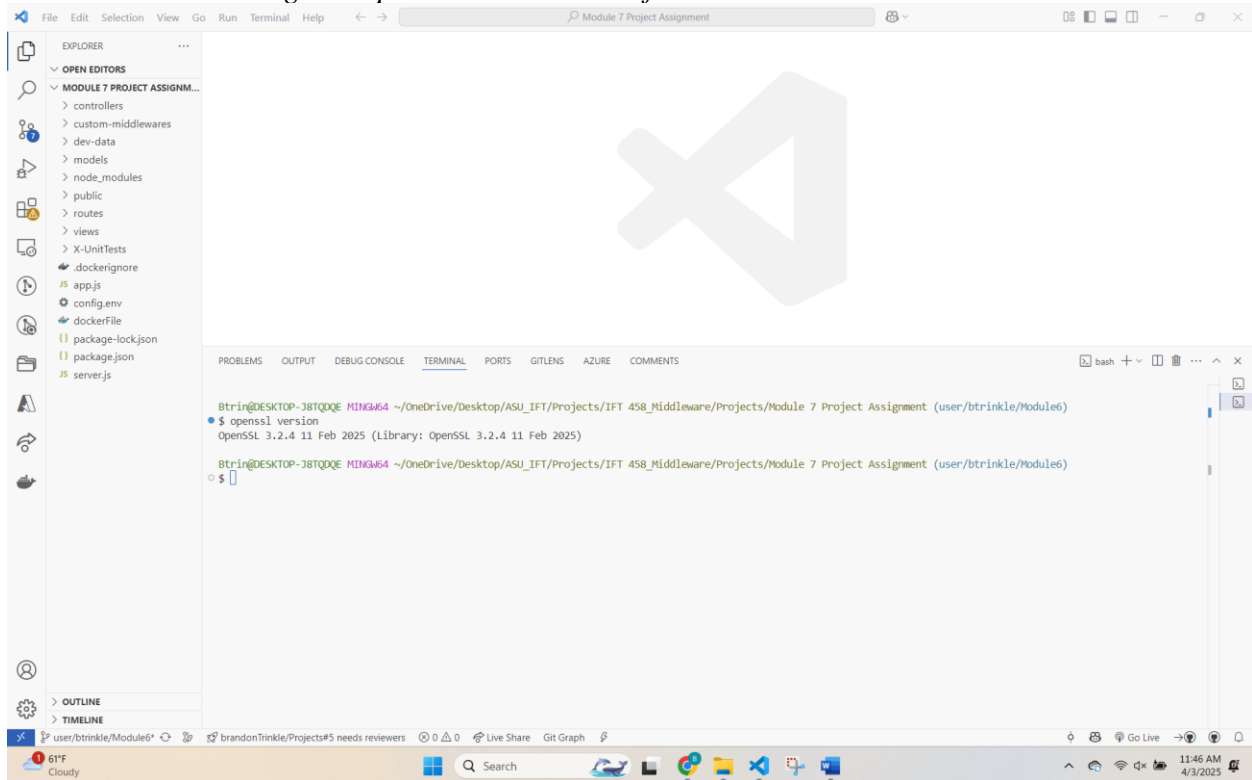
IFT 458: Middleware Programming

Professor Dinesh Sthapit

April 3, 2025

Module 7 Activity 1: Generating SSL Certificate and Configuring HTTPS Server in Node.js on Windows

Screenshot 1: Showing the OpenSSL installed confirmation.



Screenshot 2: Showing Command Prompt after generating server.key.

This screenshot shows the Visual Studio Code interface with a terminal window open. The Explorer panel on the left shows the file structure of the 'Module 7 Project Assignment' project, with 'server.key' highlighted. The terminal window displays the following commands and output:

```

Btr@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user/btrinkle/Module6)
$ openssl version
OpenSSL 3.2.4 11 Feb 2025 (Library: OpenSSL 3.2.4 11 Feb 2025)

Btr@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user/btrinkle/Module6)
$ openssl genrsa -out server.key 2048

Btr@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user/btrinkle/Module6)
$

```

The status bar at the bottom indicates the current file is 'server.key' and the user is 'btrinkle/Module6'.

Screenshot 3: Showing execution of command to generate server.cert.

This screenshot shows the Visual Studio Code interface with a terminal window open. The Explorer panel on the left shows the file structure of the 'Module 7 Project Assignment' project, with 'server.cert' highlighted. The terminal window displays the following commands and output:

```

Btr@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user/btrinkle/Module6)
$ openssl version
OpenSSL 3.2.4 11 Feb 2025 (Library: OpenSSL 3.2.4 11 Feb 2025)

Btr@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user/btrinkle/Module6)
$ openssl genrsa -out server.key 2048

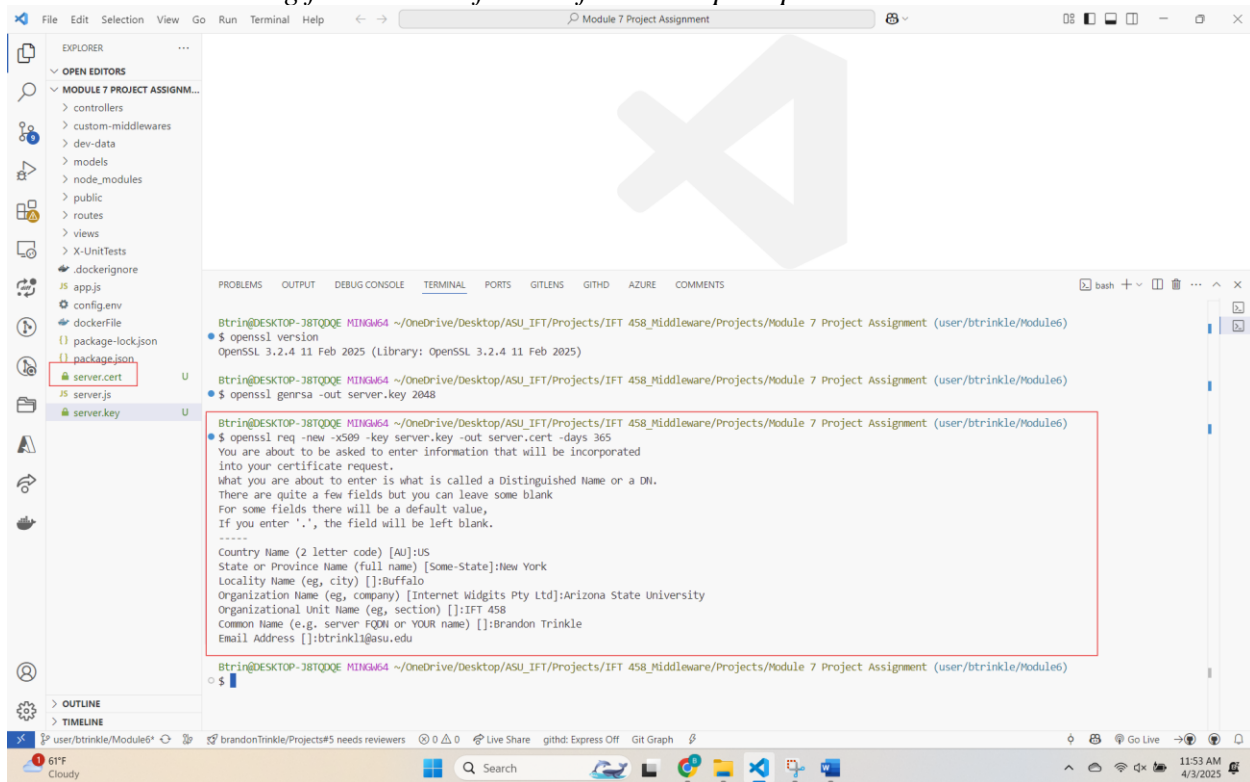
Btr@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user/btrinkle/Module6)
$ openssl req -new -x509 -key server.key -out server.cert -days 365
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:Buffalo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Arizona State University
Organizational Unit Name (eg, section) []:IFT 458
Common Name (e.g. server FQDN or YOUR name) []:Brandon Trinkle
Email Address []:btrinkle1@asu.edu

Btr@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user/btrinkle/Module6)
$

```

The status bar at the bottom indicates the current file is 'server.cert' and the user is 'btrinkle/Module6'.

Screenshot 4: Showing filled-in certificate information prompts.



The screenshot shows the Visual Studio Code interface with a terminal window open. The terminal displays the following commands and prompts:

```

btrink@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user:btrinkle/Module6)
$ openssl version
OpenSSL 3.2.4 11 Feb 2025 (Library: OpenSSL 3.2.4 11 Feb 2025)

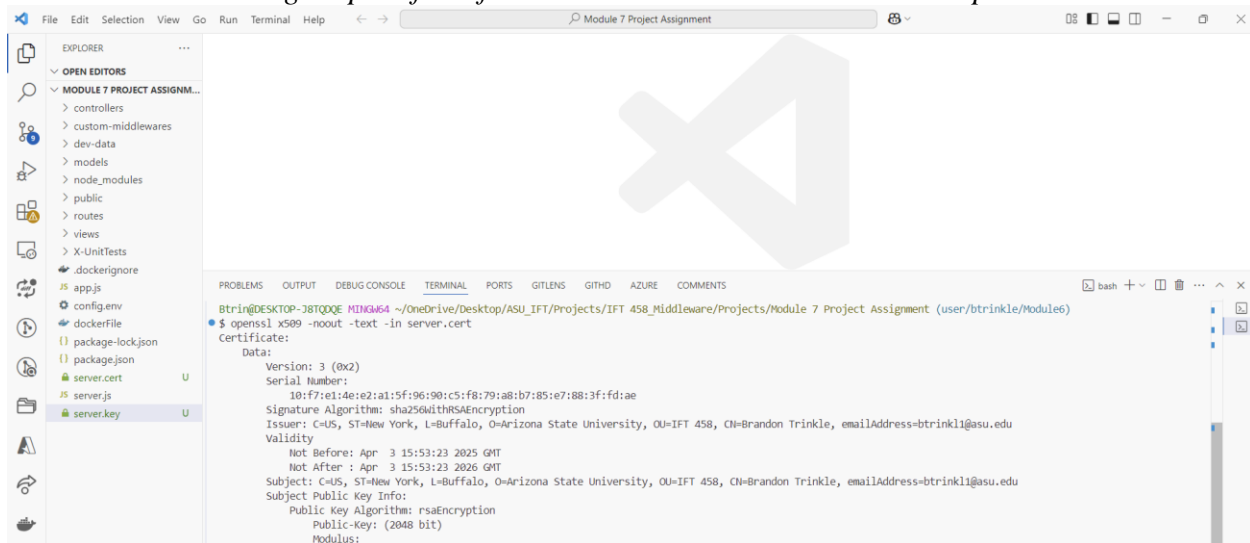
btrink@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user:btrinkle/Module6)
$ openssl genrsa -out server.key 2048

btrink@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user:btrinkle/Module6)
$ openssl req -new -x509 -key server.key -out server.cert -days 365
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) [:]:Buffalo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Arizona State University
Organizational Unit Name (eg, section) [:]:IFT 458
Common Name (e.g. server FQDN or YOUR name) [:]:Brandon Trinkle
Email Address [:]:btrinkl1@asu.edu

btrink@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user:btrinkle/Module6)
$
  
```

The Explorer sidebar on the left shows the file structure of the project, with files like `package.json`, `server.cert`, `server.js`, and `server.key` visible.

Screenshot 5: Showing output of verification commands in Command Prompt.

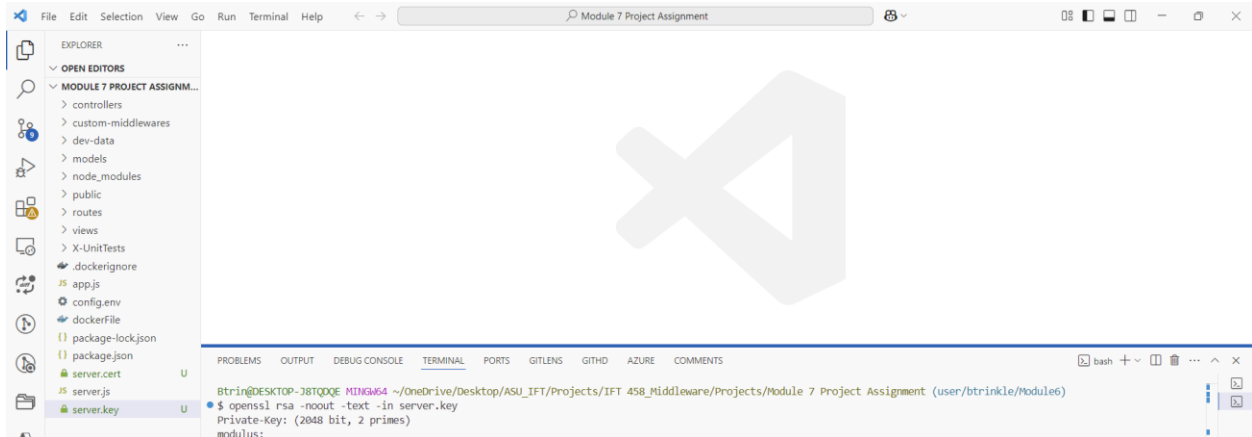


The screenshot shows the Visual Studio Code interface with a terminal window open. The terminal displays the following commands and output:

```

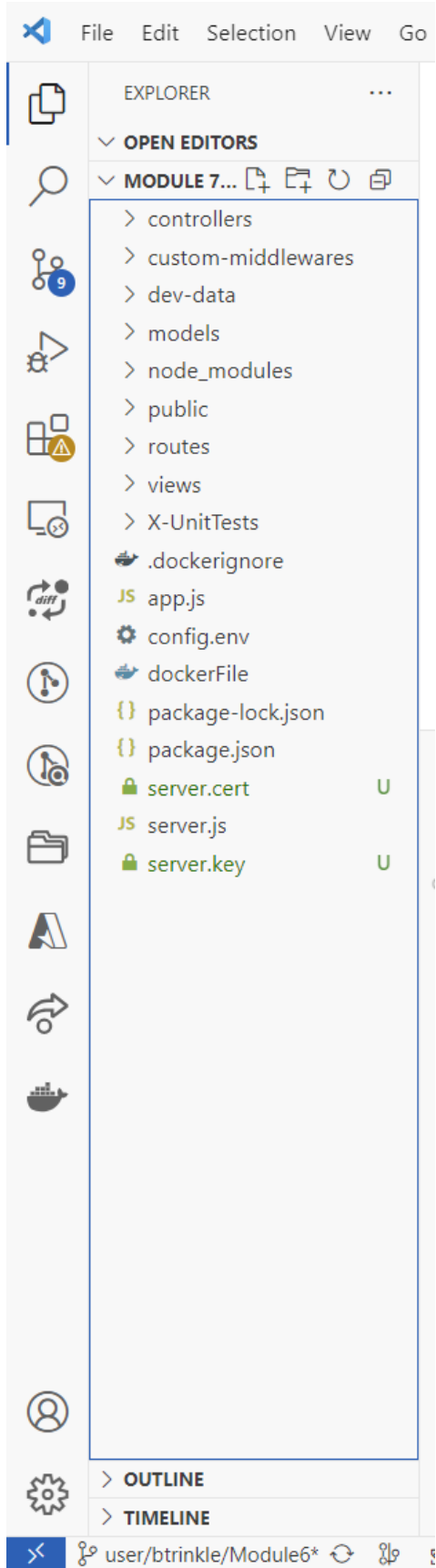
btrink@DESKTOP-38TQOQE MINGW64 ~/OneDrive/Desktop/ASU_IFT/Projects/IFT_458_Middleware/Projects/Module 7 Project Assignment (user:btrinkle/Module6)
$ openssl x509 -noout -text -in server.cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            10:f7:e1:4e:e2:a1:5f:96:90:c5:f8:79:a8:b7:85:e7:88:3f:fd:ae
        Signature Algorithm: sha256withRSAEncryption
        Issuer: C=US, ST=New York, L=Buffalo, O=Arizona State University, OU=IFT 458, CN=Brandon Trinkle, emailAddress=btrinkl1@asu.edu
        Validity
            Not Before: Apr  3 15:53:23 2025 GMT
            Not After : Apr  3 15:53:23 2026 GMT
        Subject: C=US, ST=New York, L=Buffalo, O=Arizona State University, OU=IFT 458, CN=Brandon Trinkle, emailAddress=btrinkl1@asu.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
  
```

The Explorer sidebar on the left shows the file structure of the project, with files like `package.json`, `server.cert`, `server.js`, and `server.key` visible.

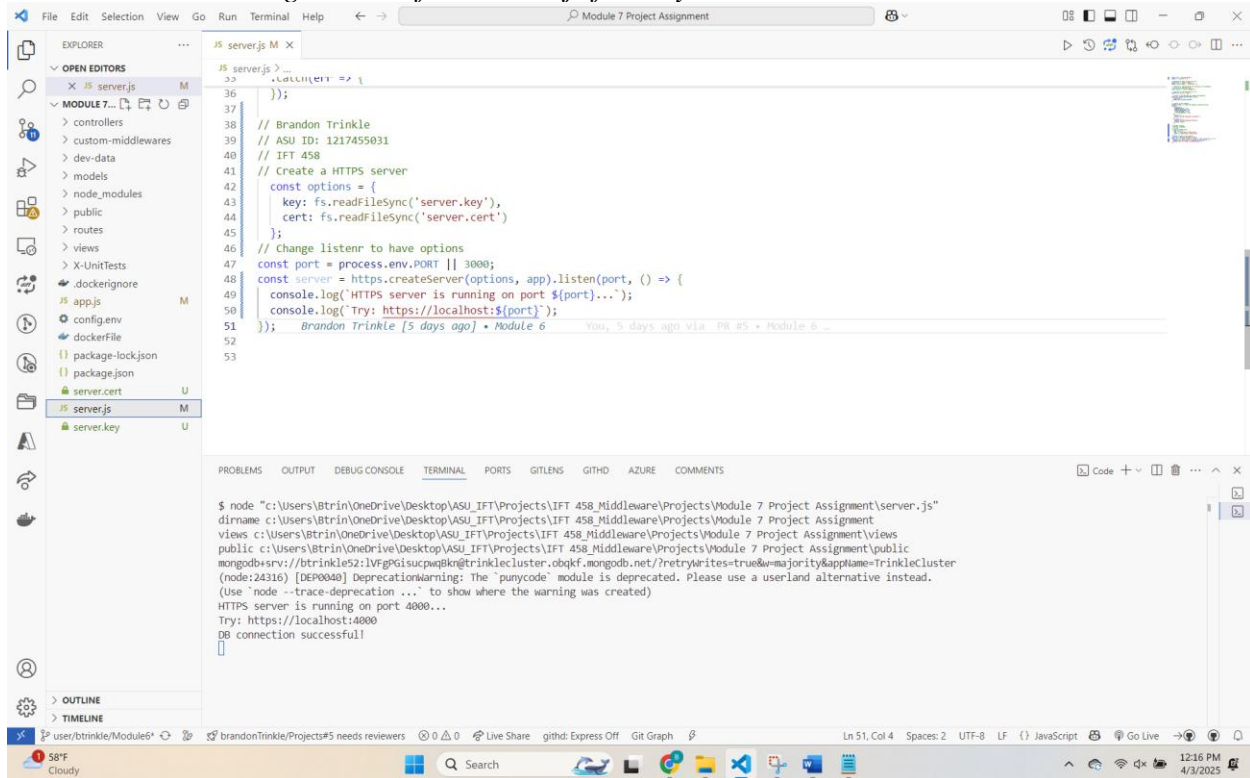


Note: Screenshot contains command line input and output, excluding key and cert information.

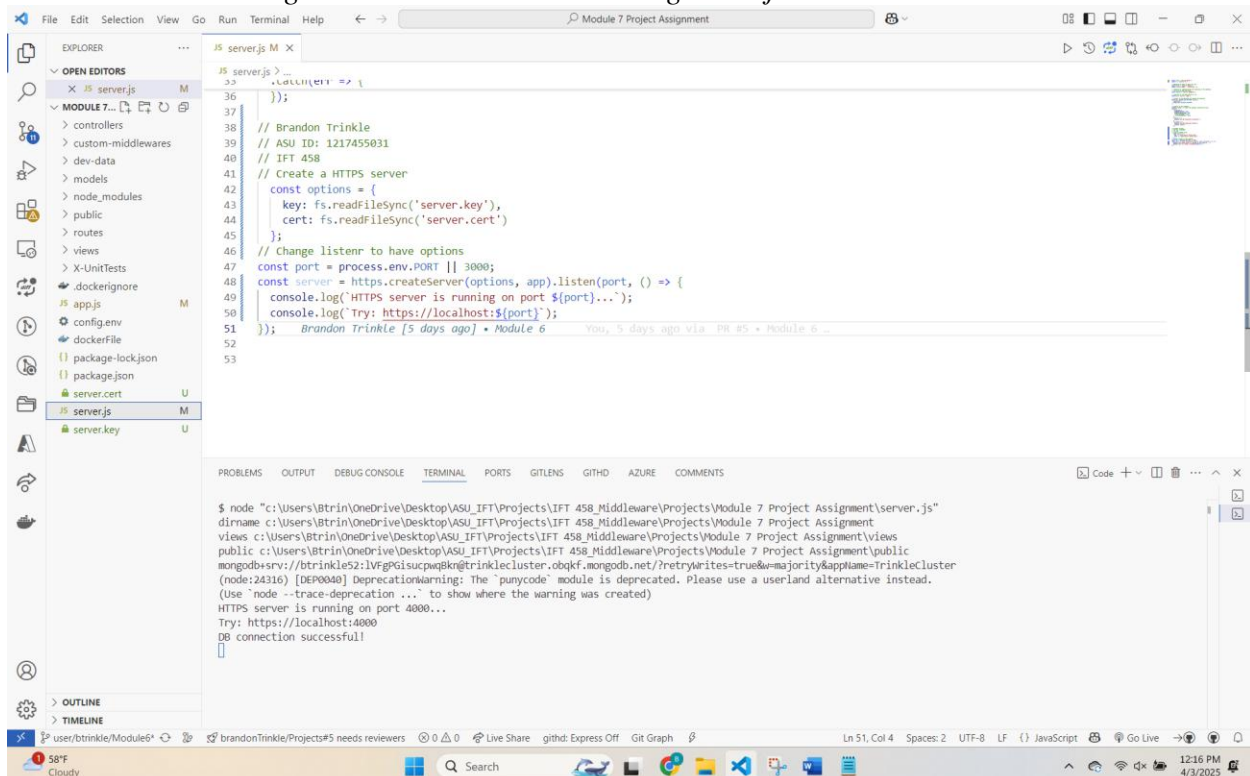
Screenshot 6: Of the project folder with server.key and server.cert files.



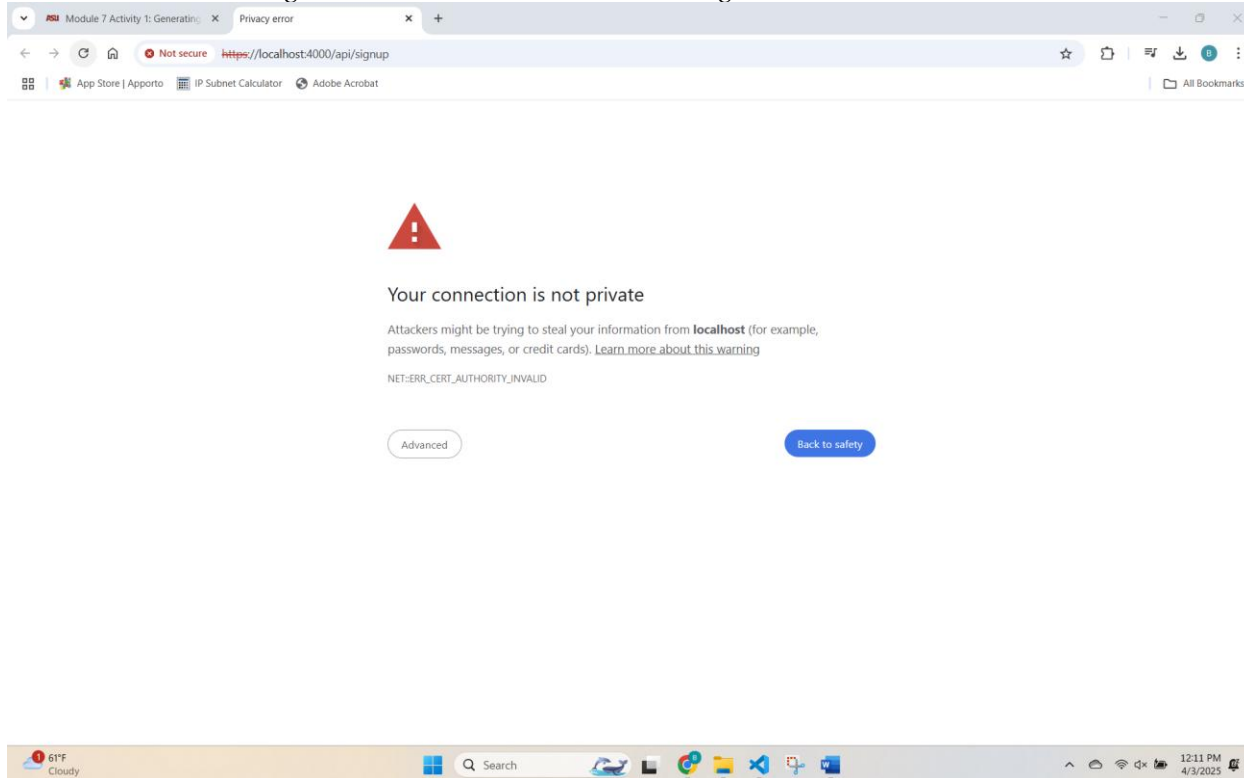
Screenshot 7: Showing the modified Server.js file in your IDE.



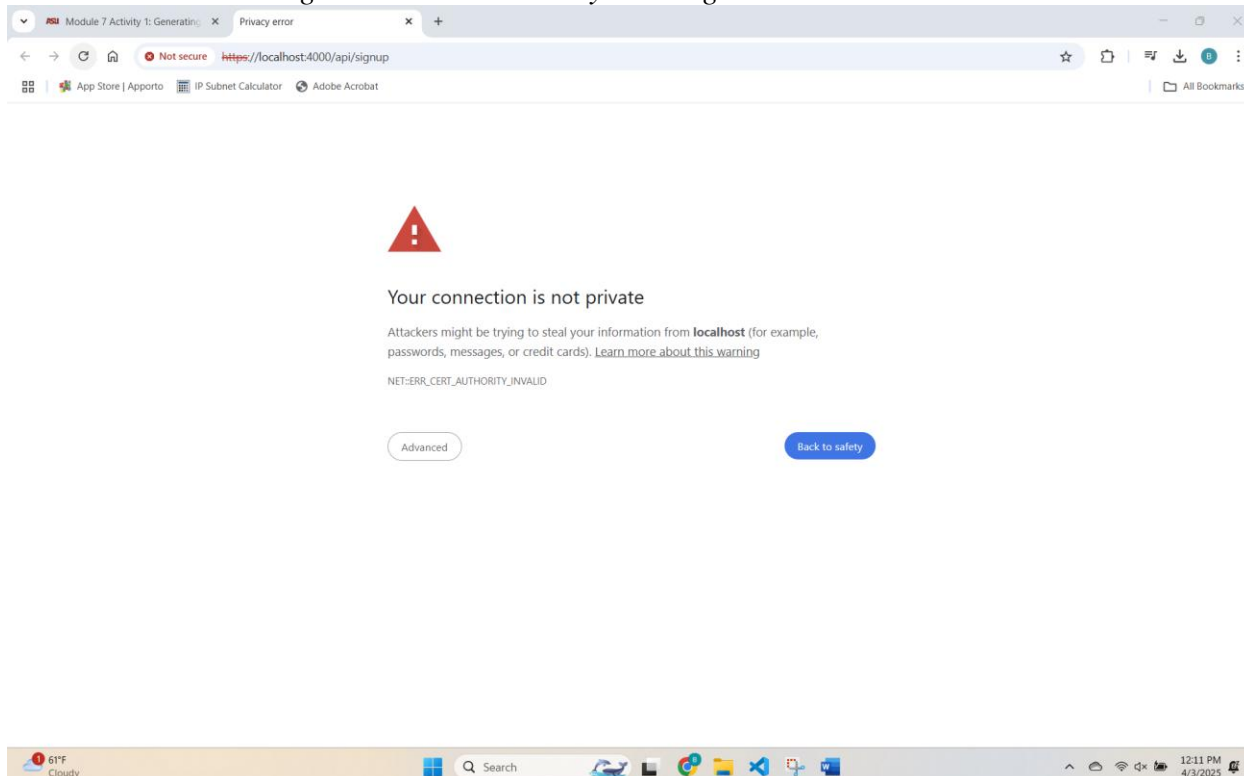
Screenshot 8: Showing the terminal with the running Node.js server.



Screenshot 9: Showing the browser view when accessing the HTTPS server.



Screenshot 10: Showing the browser's security warning.



Screenshot 11: Displaying the URL change after accepting the security warning.

