# Node.js Application SSL Lab

In this lab, let us develop a node.js server-side application running to serve requests using the protocol **https!**

1. Open a command window, create a directory for this lab and cd to the directory.

   **mkdir nodejs-labs**

   **cd nodejs-labs**

```
C:\WINDOWS\system32\cmd.exe

C:\>mkdir nodejs-labs

C:\>cd nodejs-labs

C:\nodejs-labs>
```

2. Run the following command to initialize a new npm project

   **npm init --y**

```
C:\WINDOWS\system32\cmd.exe

C:\nodejs-labs>npm init --y
Wrote to C:\nodejs-labs\package.json:

{
  "name": "nodejs-labs",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "keywords": [],
  "author": "",
  "license": "ISC"
}


C:\nodejs-labs>
```

3. Install express dependency. Type the following command

   **npm install --save express**

```
C:\WINDOWS\system32\cmd.exe

C:\nodejs-labs>npm install --save express
npm [redacted] created a lockfile as package-lock.json. You should commit this file.
npm WARN nodejs-labs@1.0.0 No description
npm WARN nodejs-labs@1.0.0 No repository field.

+ express@4.19.2
added 64 packages from 41 contributors and audited 64 packages in 4.29s

12 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities


C:\nodejs-labs>
```

3. Review the package.json document.

```
package.json
{
  "name": "nodejs-labs",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "keywords": [],
  "author": "",
  "license": "ISC",
  "dependencies": {
    "express": "^4.19.2"
  }
}
```

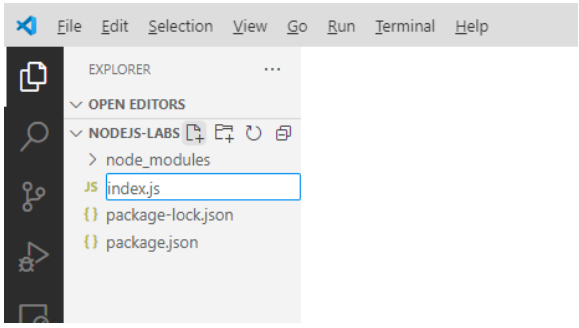
4. Add the following line to **scripts** block in package.json.

   **"start": "node index.js",**

and **save** it.

```
package.json
{
  "name": "nodejs-labs",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "start": "node index.js",
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "keywords": [],
  "author": "",
  "license": "ISC",
  "dependencies": {
    "express": "^4.19.2"
  }
}
```

5. We must create this file **index.js** in our project environment.
   Add a file called **index.js** to your application.



6. Add the following code in **index.js** and save it.

---

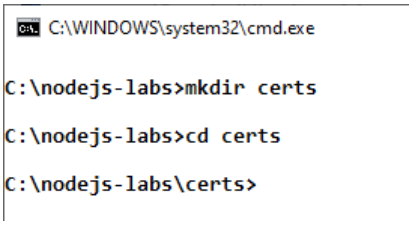
```
const express= require('express')
const https=require('https')
const fs=require('fs')
const path=require('path')
const app=express();
app.use('/',(req,res,next)=>{
res.send('hello, This response is from SSL  node Server !')
})
const options={
key: '',
cert: ''
}
const sslServer=https.createServer(options,app);
sslServer.listen(8443,()=>{
console.log('Secure server is listening on port 8443')
})
```

---

9. We must create ssl key and ssl certificate and configure the code to use them. Create a directory to store ssl certificates Type the following commands in the command window

**mkdir certs**

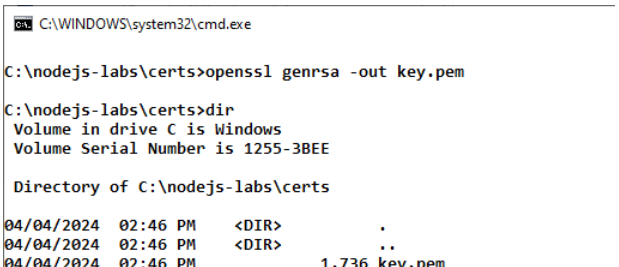
**cd certs**

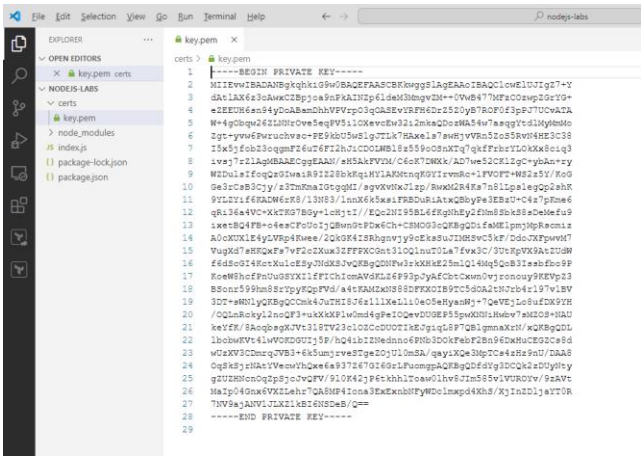



10. Let us generate a private key using openssl. Use the following command

**openssl genrsa -out key.pem**

This command will generate the private key and save it in **key.pem** file inside certs directory.



11. Create a CSR (Certificate Signing Request). Use the following command

**openssl req -new -key key.pem -out csr.pem**

This command will prompt a dialog to get input and run. Provide meaningful input.

```
C:\WINDOWS\system32\cmd.exe

C:\nodejs-labs\certs>openssl req -new -key key.pem -out csr.pem
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]:Michigan
Locality Name (eg, city) []:Farmington Hills
Organization Name (eg, company) [Internet Widgits Pty Ltd]:WebAge Solutions
Organizational Unit Name (eg, section) []:Training
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\nodejs-labs\certs>_
```

Check the directory. You will see the **csr.pem** file.

```
C:\WINDOWS\system32\cmd.exe

C:\nodejs-labs\certs>dir
 Volume in drive C is Windows
 Volume Serial Number is 1255-3BEE

 Directory of C:\nodejs-labs\certs

04/04/2024  02:50 PM    <DIR>          .
04/04/2024  02:50 PM    <DIR>          ..
04/04/2024  02:50 PM             1,022 csr.pem
04/04/2024  02:46 PM             1,736 key.pem
               2 File(s)          2,758 bytes
               2 Dir(s)  27,419,635,712 bytes free

C:\nodejs-labs\certs>_
```

12. Let us use the **key.pem** and **csr.pem** files to generate your ssl certificate.

Type the following command using openssl

**openssl x509 -req -days 365 -in csr.pem -signkey key.pem -out cert.pem**

```
C:\WINDOWS\system32\cmd.exe

C:\nodejs-labs\certs>openssl x509 -req -days 365 -in csr.pem -signkey key.pem -out cert.pem
Certificate request self-signature ok
subject=C=US, ST=Michigan, L=Farmington Hills, O=WebAge Solutions, OU=Training
```

13. Check your **certs** directory. Can you see the following files?

**cert.pem**

**csr.pem**

**key.pem**

14. Run the following command in the command window, to view the details of your certificate.

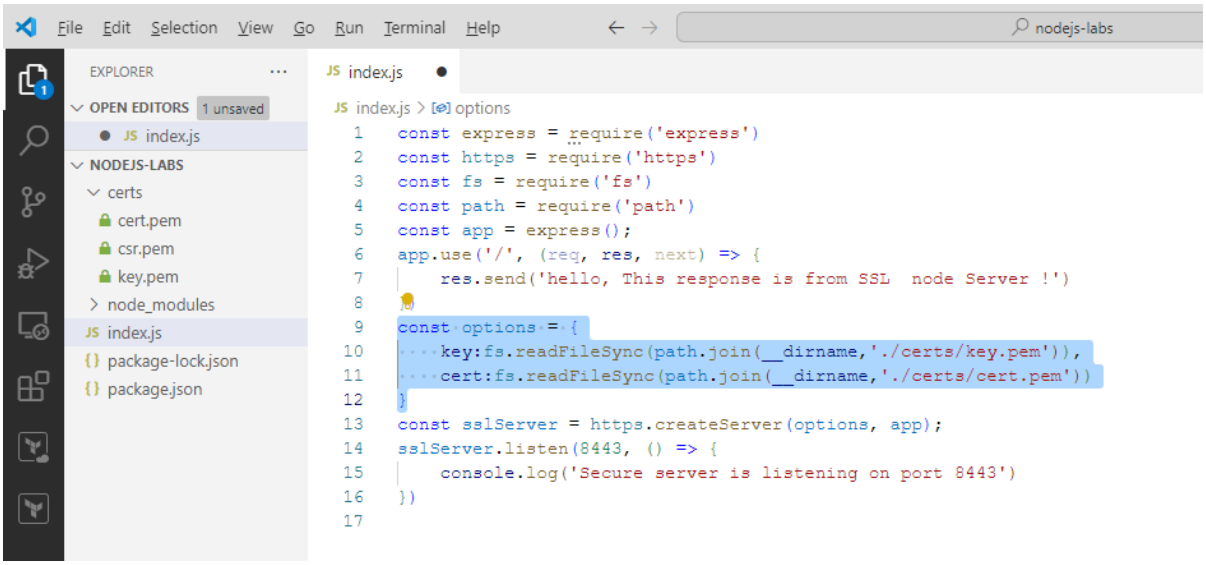
**openssl x509 -in cert.pem -noout -text**

```
C:\WINDOWS\system32\cmd.exe
C:\nodejs-labs\certs>openssl x509 -in cert.pem -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            67:f3:91:6f:34:a6:94:46:83:9b:96:b0:f3:7b:4d:5b:9c:ad:a8:ee
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Michigan, L=Farmington Hills, O=WebAge Solutions, OU=Training
        Validity
            Not Before: Apr  4 18:52:49 2024 GMT
            Not After : Apr  4 18:52:49 2025 GMT
        Subject: C=US, ST=Michigan, L=Farmington Hills, O=WebAge Solutions, OU=Training
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b5:73:01:25:50:92:20:67:bf:98:74:0b:65:01:
                    7e:b3:de:80:30:c4:26:41:a6:3a:1a:f6:73:e4:00:
                    83:59:a7:a9:5d:78:cd:cc:9a:0b:d9:33:ef:b4:57:
                    00:78:ef:b3:05:cc:23:b3:c2:96:46:ad:81:be:79:
                    91:04:50:7e:ac:9f:de:32:0e:80:01:6a:60:e1:85:
                    53:d5:ae:93:b7:a8:e0:12:12:f6:11:14:7e:83:ad:
                    9e:59:d3:20:7b:44:e1:74:7f:7a:4f:27:b5:02:bc:
                    04:c0:5b:ee:20:39:ba:b0:db:a6:4b:34:da:ce:bd:
                    ee:5e:a8:f5:79:8b:53:97:7a:f7:04:c3:7d:a2:da:
                    69:1a:40:3a:33:58:0e:78:c3:b6:ac:aa:06:2d:76:
                    53:32:32:63:28:66:0b:7e:ca:fc:3a:3f:0a:ee:72:
                    1b:ec:73:e3:c4:f6:46:d4:e7:04:b5:80:94:cb:93:
                    b1:c0:c5:e9:6c:ee:cc:07:8e:f5:51:9f:96:68:4b:
                    94:6f:37:81:c4:dc:2d:fc:23:9c:79:8d:fa:1b:67:
                    7a:2a:82:61:59:ea:e4:fa:14:8d:a1:26:20:83:38:
                    b5:81:97:cc:f9:e7:da:0e:4a:75:d3:ab:ba:a4:7c:
                    5a:db:ad:82:ce:91:7c:7c:72:2a:b7:8a:fb:23:ee:
                    b6:65
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                9D:FF:65:68:4C:7D:4D:57:FD:43:4E:0C:4C:30:9A:A8:CC:2D:1C:2B
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        28:2f:8c:2d:2b:f1:a5:9b:b8:85:b3:6f:c3:e8:96:4d:df:c8:
        25:4d:16:49:5e:e7:a7:51:9d:27:cb:3a:f0:5d:be:91:14:ea:
        69:2e:e3:fe:30:47:4f:1c:de:50:1c:8c:50:3c:cd:27:fc:76:
        df:3d:f4:f8:9a:47:21:8a:0e:f3:f0:7a:00:e1:43:84:50:1b:
        ae:d2:39:c2:80:25:40:77:6f:60:fd:15:4c:ce:cf:2f:59:a9:
        73:12:9f:61:cc:c9:bc:7b:9f:92:77:80:d5:96:20:47:ab:00:
        8d:29:f8:03:57:6b:bc:2e:f7:e5:54:48:b5:c8:7f:15:11:7b:
        4a:4f:6d:0f:32:b3:08:a3:c5:0a:d5:02:e2:45:c2:68:8a:00:
        be:d2:a6:68:99:a2:e6:ce:8a:ca:75:ef:ca:93:3b:2d:4a:18:
        75:70:d9:cf:56:b3:88:b5:76:3a:2a:c1:cd:51:10:25:8b:b2:
        34:d2:cf:6a:4c:43:a6:96:42:15:f0:53:26:3b:72:3f:72:85:
        2d:b5:8d:47:6d:74:ae:f0:60:7e:38:e1:07:7f:de:f5:17:f5:
```

15. **How to integrate your certificate and key to express code**?

Add the following code in index.js and save it.

```
const options = {
    key:fs.readFileSync(path.join(__dirname,'./certs/key.pem')),
    cert:fs.readFileSync(path.join(__dirname,'./certs/cert.pem'))
}
```




16. In the command window, cd to C:\nodejs-labs

**cd C:\nodejs-labs**

Run the node server using the command in the command window.

**npm start**

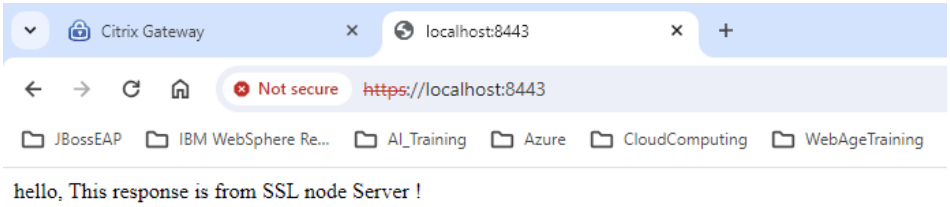
```
npm

C:\nodejs-labs>npm start

> nodejs-labs@1.0.0 start C:\nodejs-labs
> node index.js

Secure server is listening on port 8443
```

17. Open a browser, go to https://localhost:8443




Notice the Not Secure https **warning ! How can you fix this?**