

Şifreleme Ödev 4

Mehmet Afif Arsay
18120205036

Soru: ssl sertifikası oluşturma ve sunucuya yükleme

Çözüm:

1. Sertifika oluşturma

-Öncelikler <https://formulae.brew.sh/formula/openssl@1.1> bu adresten openssl bilgisayarımıza kuruyoruz.

-Daha sonra sertifikaları kuracağımız klasörü belirleyip terminal ile o path gidiyoruz.

- a. `openssl genrsa -out CA.key -des3 2048`
- b. `openssl req -x509 -sha256 -new -nodes -days 3650 -key CA.key -out CA.pem`
- c. `mkdir localhost`
- d. `cd localhost`
- e. `touch localhost.ext`
- f. `openssl genrsa -out localhost.key -des3 2048`
- g. `openssl req -new -key localhost.key -out localhost.csr`
- h. `openssl x509 -req -in localhost.csr -CA ../CA.pem -CAkey ../CA.key -CAcreateserial -days`
- i. `3650 -sha256 -extfile localhost.ext -out localhost.crt`
- j. `openssl rsa -in localhost.key -out localhost.decrypted.key`

2. Live Stream kurulumu

Live stream yazılan bir html kodunu tarayıcıda localde yayına almamızı sağlar. Kurulumu yapıldıktan sonra .vscode klasörünün altına settings.json oluşturulur. Ve içine aşağıdaki kod yapıştırılır.

```
{
  "liveServer.settings.https": {
    "enable": true, //set it true to enable the feature.
    "cert":
"/Users/mehmetarsay/Desktop/encryption_ssl/localhost/certificate/localhost.crt",
//full path of the certificate
    "key":
"/Users/mehmetarsay/Desktop/encryption_ssl/localhost/certificate/localhost.key",
//full path of the private key
    "passphrase": "123456"
  }
}
```

Burada sertifika path ve şifresi girilerek yayına alınır.



