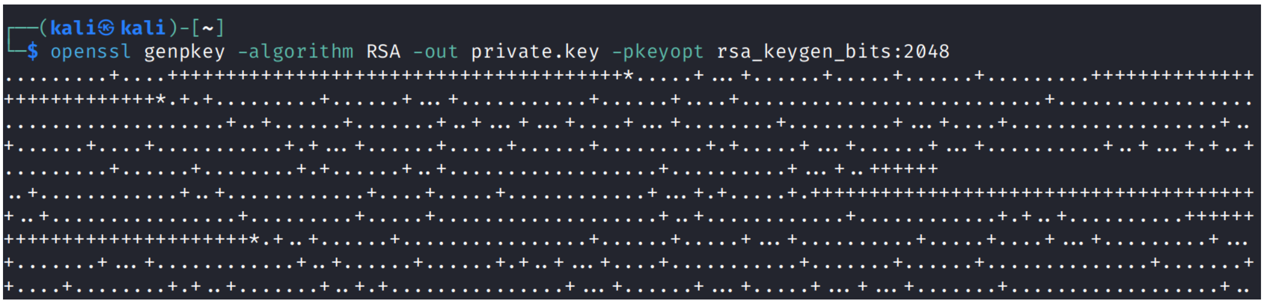
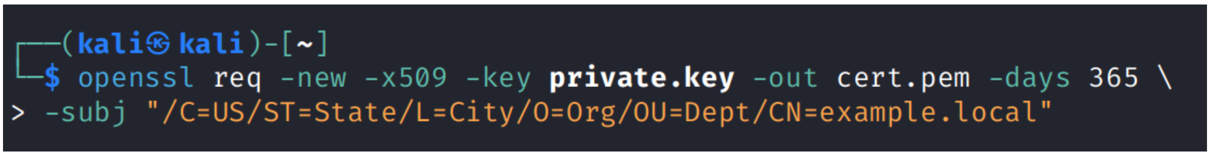
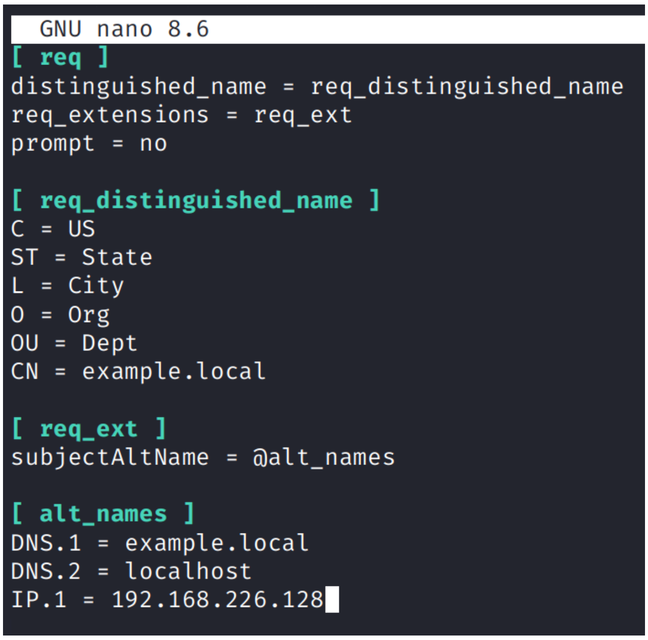


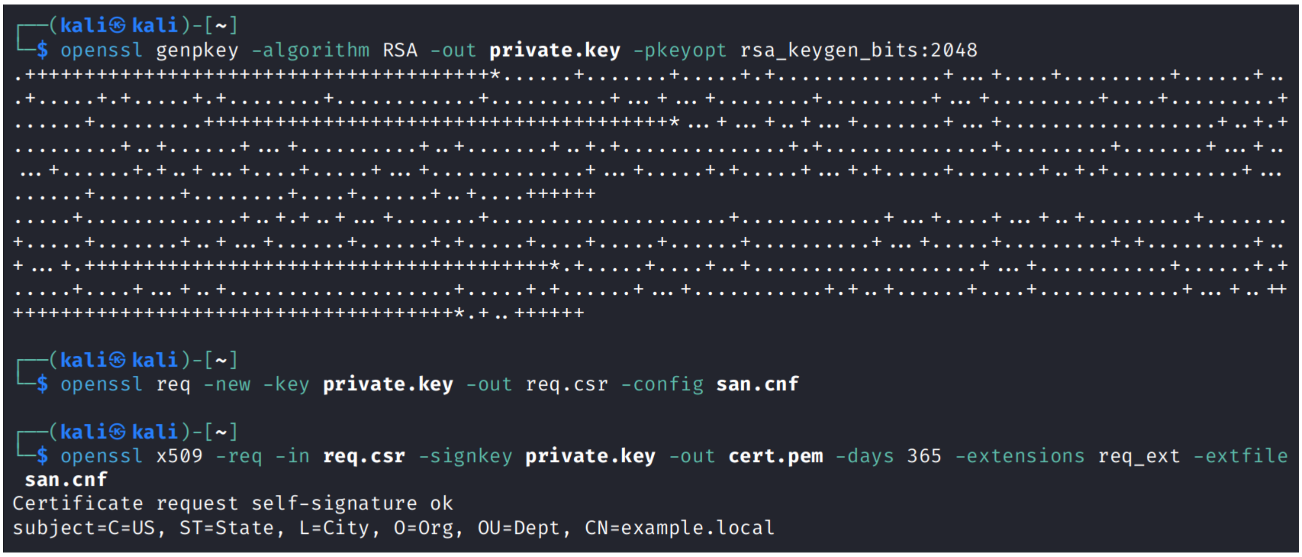
```
┌──(kali㉿kali)-[~]
└─$ openssl genpkey -algorithm RSA -out private.key -pkeyopt rsa_keygen_bits:2048
........+....+++++++++++++++++++++++++++++++++++++++*.....+...+......+.....+......+.........+++++++++++++
+++++++++++++*.+.+.........+......+...+...........+......+....+...........................+...............
...................+..+......+.......+..+...+...+....+...+........+.........+...+....+..................+..
+......+....+...........+.+...+......+.....+......+.........+.+.....+...+......+...+..........+..+...+.+..+
.........+......+........+.+......+..+..................+..........+...+..++++++
..+............+..+............+....+.....+............+...+.+.....+.++++++++++++++++++++++++++++++++++++
+..+................+.........+.....+..................+..+............+............+.+..+..........++++++
+++++++++++++++++++++*.+..+......+.................+......+.....+...+...........+.....+....+...+.........+...
+.......+...+............+..+......+......+.+..+...+....+...........+.......+......+...............+.......+
+....+........+.+..+.......+..+.+...............+...+......+...+.....+...+...+.......+..................+..
```



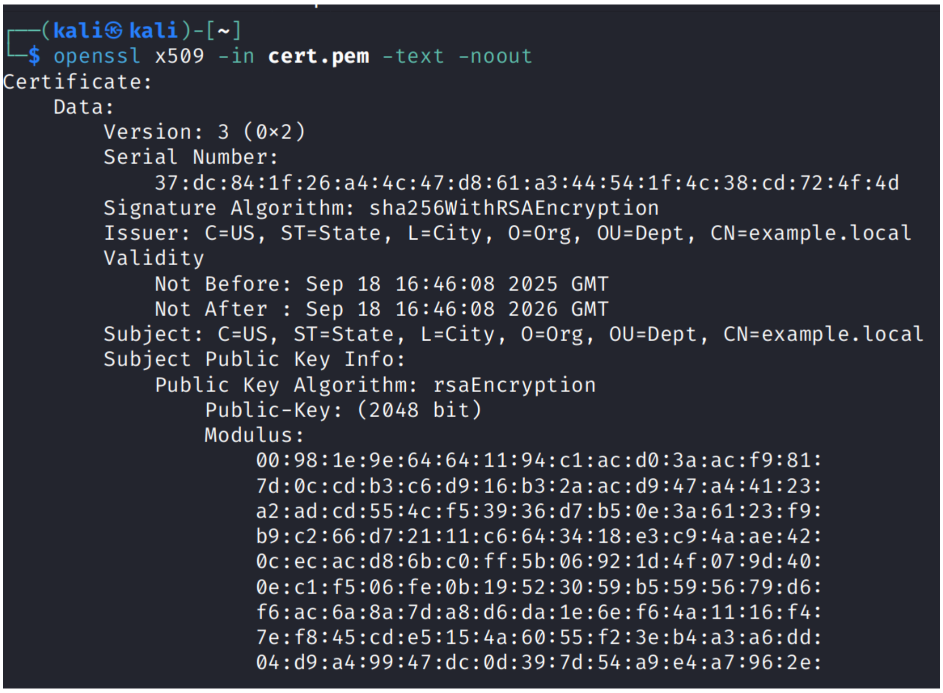
```
┌──(kali㉿kali)-[~]
└─$ openssl req -new -x509 -key private.key -out cert.pem -days 365 \
> -subj "/C=US/ST=State/L=City/O=Org/OU=Dept/CN=example.local"
```



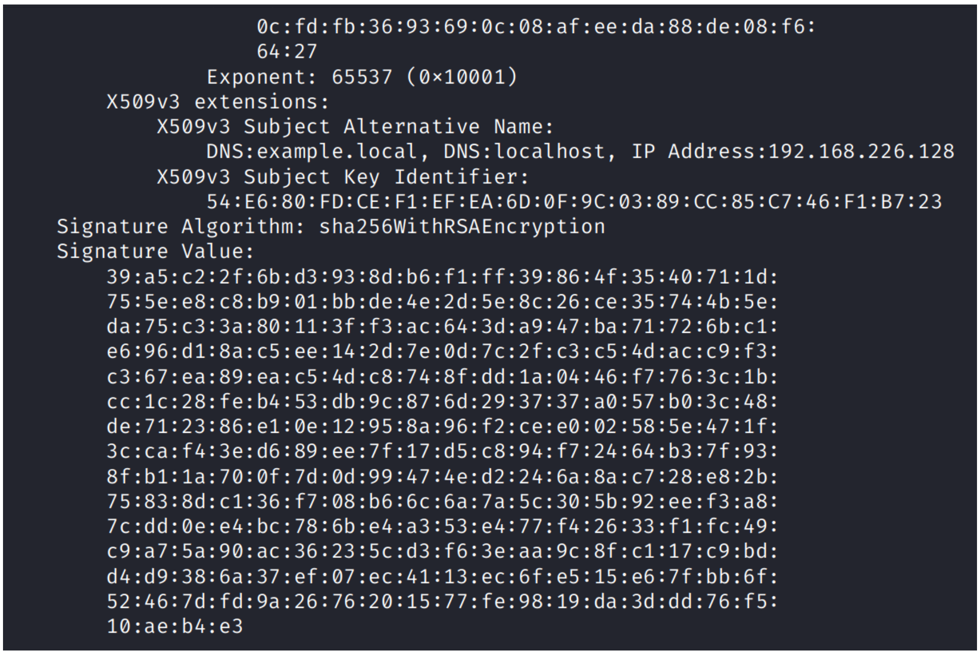
```
  GNU nano 8.6
[ req ]
distinguished_name = req_distinguished_name
req_extensions = req_ext
prompt = no

[ req_distinguished_name ]
C = US
ST = State
L = City
O = Org
OU = Dept
CN = example.local

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = example.local
DNS.2 = localhost
IP.1 = 192.168.226.128
```



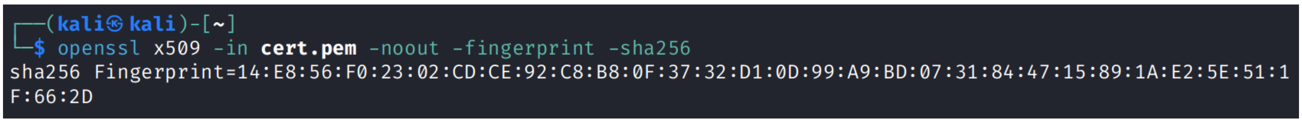
```
┌──(kali㉿kali)-[~]
└─$ openssl genpkey -algorithm RSA -out private.key -pkeyopt rsa_keygen_bits:2048
.+++++++++++++++++++++++++++++++++++++++*......+.......+.....+.+..............+...+....+.........+......+..
.+.....+.+.....+.+........+...........+..........+...+...+........+.........+...+.........+....+.........+
......+.........+++++++++++++++++++++++++++++++++++++++*...+...+..+...+.......+...+.................+..+.+
.........+..+......+...+..........+..+.......+..+.+..............+.+..............+.........+.......+...+..
...+......+.+..+...+....+.....+...+.............+...+.....+.+.....+...+.+.....+.......+..+.+............+...
......+.......+........+....+......+..+....++++++
.....+.............+..+.+..+...+.......+....................+...........+...+....+...+..+.........+.......
+.....+.......+..+...+......+......+.+.....+....+.....+......+..........+...+.....+..........+.+.........+..
+...+.+++++++++++++++++++++++++++++++++++++++*.+.....+....+..+....................+...+...........+......+.+
.....+....+...+..+...................+.....+.+......+...+...........+.+..+......+....+...........+...+..++
+++++++++++++++++++++++++++++++++++++*.+..++++++

┌──(kali㉿kali)-[~]
└─$ openssl req -new -key private.key -out req.csr -config san.cnf

┌──(kali㉿kali)-[~]
└─$ openssl x509 -req -in req.csr -signkey private.key -out cert.pem -days 365 -extensions req_ext -extfile
 san.cnf
Certificate request self-signature ok
subject=C=US, ST=State, L=City, O=Org, OU=Dept, CN=example.local
```



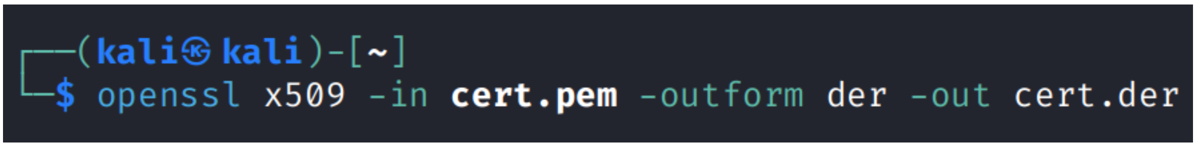
```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number:
            37:dc:84:1f:26:a4:4c:47:d8:61:a3:44:54:1f:4c:38:cd:72:4f:4d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=State, L=City, O=Org, OU=Dept, CN=example.local
        Validity
            Not Before: Sep 18 16:46:08 2025 GMT
            Not After : Sep 18 16:46:08 2026 GMT
        Subject: C=US, ST=State, L=City, O=Org, OU=Dept, CN=example.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:98:1e:9e:64:64:11:94:c1:ac:d0:3a:ac:f9:81:
                    7d:0c:cd:b3:c6:d9:16:b3:2a:ac:d9:47:a4:41:23:
                    a2:ad:cd:55:4c:f5:39:36:d7:b5:0e:3a:61:23:f9:
                    b9:c2:66:d7:21:11:c6:64:34:18:e3:c9:4a:ae:42:
                    0c:ec:ac:d8:6b:c0:ff:5b:06:92:1d:4f:07:9d:40:
                    0e:c1:f5:06:fe:0b:19:52:30:59:b5:59:56:79:d6:
                    f6:ac:6a:8a:7d:a8:d6:da:1e:6e:f6:4a:11:16:f4:
                    7e:f8:45:cd:e5:15:4a:60:55:f2:3e:b4:a3:a6:dd:
                    04:d9:a4:99:47:dc:0d:39:7d:54:a9:e4:a7:96:2e:
```



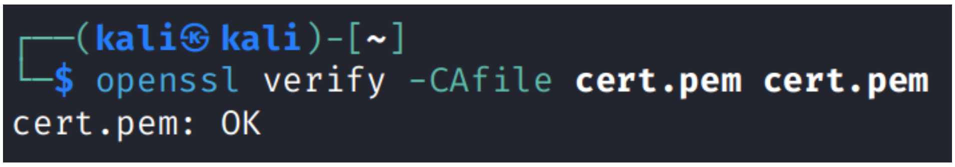
```
                    0c:fd:fb:36:93:69:0c:08:af:ee:da:88:de:08:f6:
                    64:27
                Exponent: 65537 (0×10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:example.local, DNS:localhost, IP Address:192.168.226.128
            X509v3 Subject Key Identifier:
                54:E6:80:FD:CE:F1:EF:EA:6D:0F:9C:03:89:CC:85:C7:46:F1:B7:23
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        39:a5:c2:2f:6b:d3:93:8d:b6:f1:ff:39:86:4f:35:40:71:1d:
        75:5e:e8:c8:b9:01:bb:de:4e:2d:5e:8c:26:ce:35:74:4b:5e:
        da:75:c3:3a:80:11:3f:f3:ac:64:3d:a9:47:ba:71:72:6b:c1:
        e6:96:d1:8a:c5:ee:14:2d:7e:0d:7c:2f:c3:c5:4d:ac:c9:f3:
        c3:67:ea:89:ea:c5:4d:c8:74:8f:dd:1a:04:46:f7:76:3c:1b:
        cc:1c:28:fe:b4:53:db:9c:87:6d:29:37:37:a0:57:b0:3c:48:
        de:71:23:86:e1:0e:12:95:8a:96:f2:ce:e0:02:58:5e:47:1f:
        3c:ca:f4:3e:d6:89:ee:7f:17:d5:c8:94:f7:24:64:b3:7f:93:
        8f:b1:1a:70:0f:7d:0d:99:47:4e:d2:24:6a:8a:c7:28:e8:2b:
        75:83:8d:c1:36:f7:08:b6:6c:6a:7a:5c:30:5b:92:ee:f3:a8:
        7c:dd:0e:e4:bc:78:6b:e4:a3:53:e4:77:f4:26:33:f1:fc:49:
        c9:a7:5a:90:ac:36:23:5c:d3:f6:3e:aa:9c:8f:c1:17:c9:bd:
        d4:d9:38:6a:37:ef:07:ec:41:13:ec:6f:e5:15:e6:7f:bb:6f:
        52:46:7d:fd:9a:26:76:20:15:77:fe:98:19:da:3d:dd:76:f5:
        10:ae:b4:e3
```



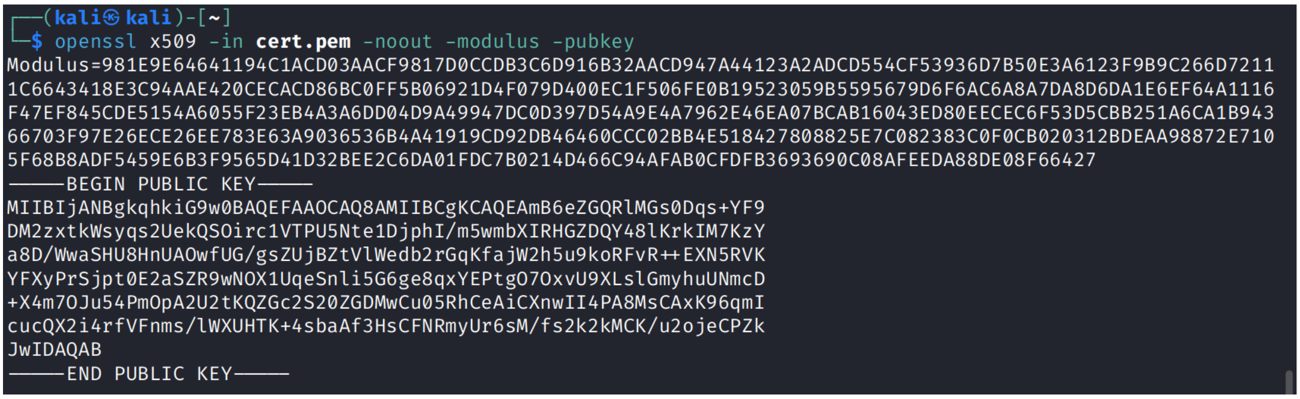
```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in cert.pem -noout -fingerprint -sha256
sha256 Fingerprint=14:E8:56:F0:23:02:CD:CE:92:C8:B8:0F:37:32:D1:0D:99:A9:BD:07:31:84:47:15:89:1A:E2:5E:51:1
F:66:2D
```



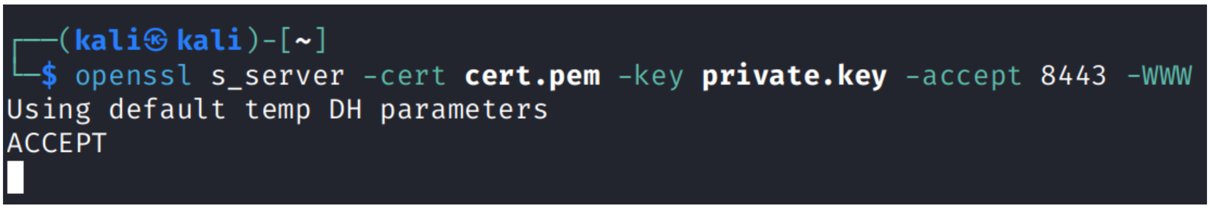
```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in cert.pem -outform der -out cert.der
```



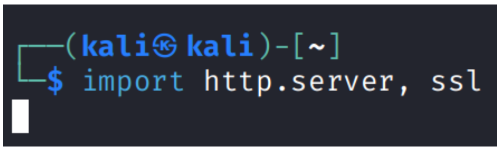
```
┌──(kali㉿kali)-[~]
└─$ openssl verify -CAfile cert.pem cert.pem
cert.pem: OK
```



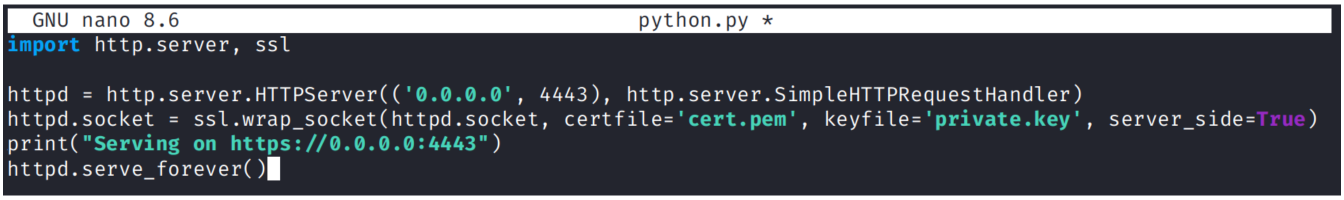
```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in cert.pem -noout -modulus -pubkey
Modulus=981E9E64641194C1ACD03AACF9817D0CCDB3C6D916B32AACD947A44123A2ADCD554CF53936D7B50E3A6123F9B9C266D7211
1C6643418E3C94AAE420CECACD86BC0FF5B06921D4F079D400EC1F506FE0B19523059B5595679D6F6AC6A8A7DA8D6DA1E6EF64A1116
F47EF845CDE5154A6055F23EB4A3A6DD04D9A49947DC0D397D54A9E4A7962E46EA07BCAB16043ED80EECEC6F53D5CBB251A6CA1B943
66703F97E26ECE26EE783E63A9036536B4A41919CD92DB46460CCC02BB4E518427808825E7C082383C0F0CB020312BDEAA98872E710
5F68B8ADF5459E6B3F9565D41D32BEE2C6DA01FDC7B0214D466C94AFAB0CFDFB3693690C08AFEEDA88DE08F66427
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmB6eZGQRlMGs0Dqs+YF9
DM2zxtkWsyqs2UekQSOirc1VTPU5Nte1DjphI/m5wmbXIRHGZDQY48lKrkIM7KzY
a8D/WwaSHU8HnUAOwfUG/gsZUjBZtVlWedb2rGqKfajW2h5u9koRFvR++EXN5RVK
YFXyPrSjpt0E2aSZR9wNOX1UqeSnli5G6ge8qxYEPtgO7OxvU9XLslGmyhuUNmcD
+X4m7OJu54PmOpA2U2tKQZGc2S20ZGDMwCu05RhCeAiCXnwII4PA8MsCAxK96qmI
cucQX2i4rfVFnms/lWXUHTK+4sbaAf3HsCFNRmyUr6sM/fs2k2kMCK/u2ojeCPZk
JwIDAQAB
-----END PUBLIC KEY-----
```



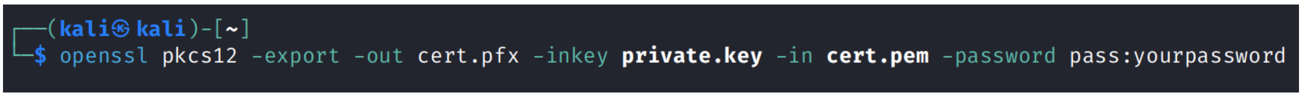
```
┌──(kali㉿kali)-[~]
└─$ openssl s_server -cert cert.pem -key private.key -accept 8443 -WWW
Using default temp DH parameters
ACCEPT
```



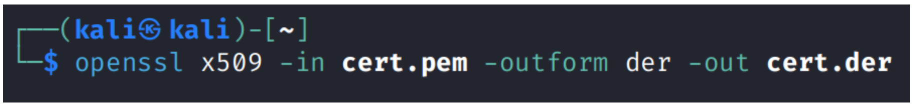
```
┌──(kali㉿kali)-[~]
└─$ import http.server, ssl
```



```
  GNU nano 8.6                                    python.py *
import http.server, ssl

httpd = http.server.HTTPServer(('0.0.0.0', 4443), http.server.SimpleHTTPRequestHandler)
httpd.socket = ssl.wrap_socket(httpd.socket, certfile='cert.pem', keyfile='private.key', server_side=True)
print("Serving on https://0.0.0.0:4443")
httpd.serve_forever()
```



```
┌──(kali㉿kali)-[~]
└─$ openssl pkcs12 -export -out cert.pfx -inkey private.key -in cert.pem -password pass:yourpassword
```



```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in cert.pem -outform der -out cert.der
```