SEEDLab Crypto_PKI 实验报告

原创

:风雪夜归人 于 2020-12-23 13:03:32 发布 3254 收藏 14
分类专栏： 网络安全

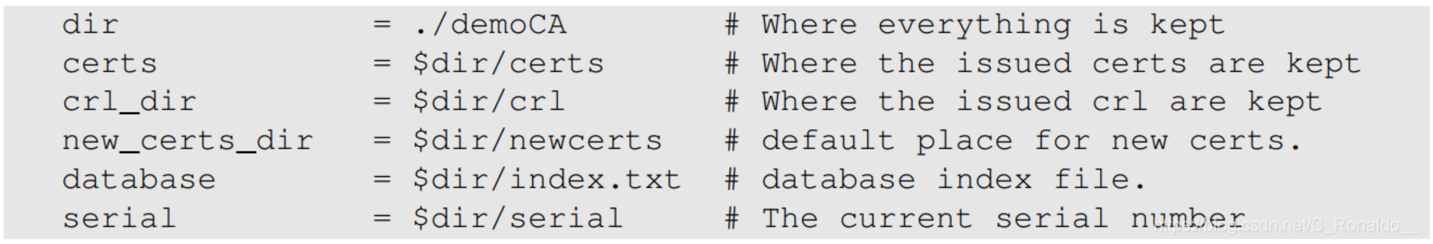
网络安全 专栏收录该内容
4 篇文章 0 订阅
订阅专栏

文章目录

实验过程

Task1 Becoming a Certificate Authority (CA)

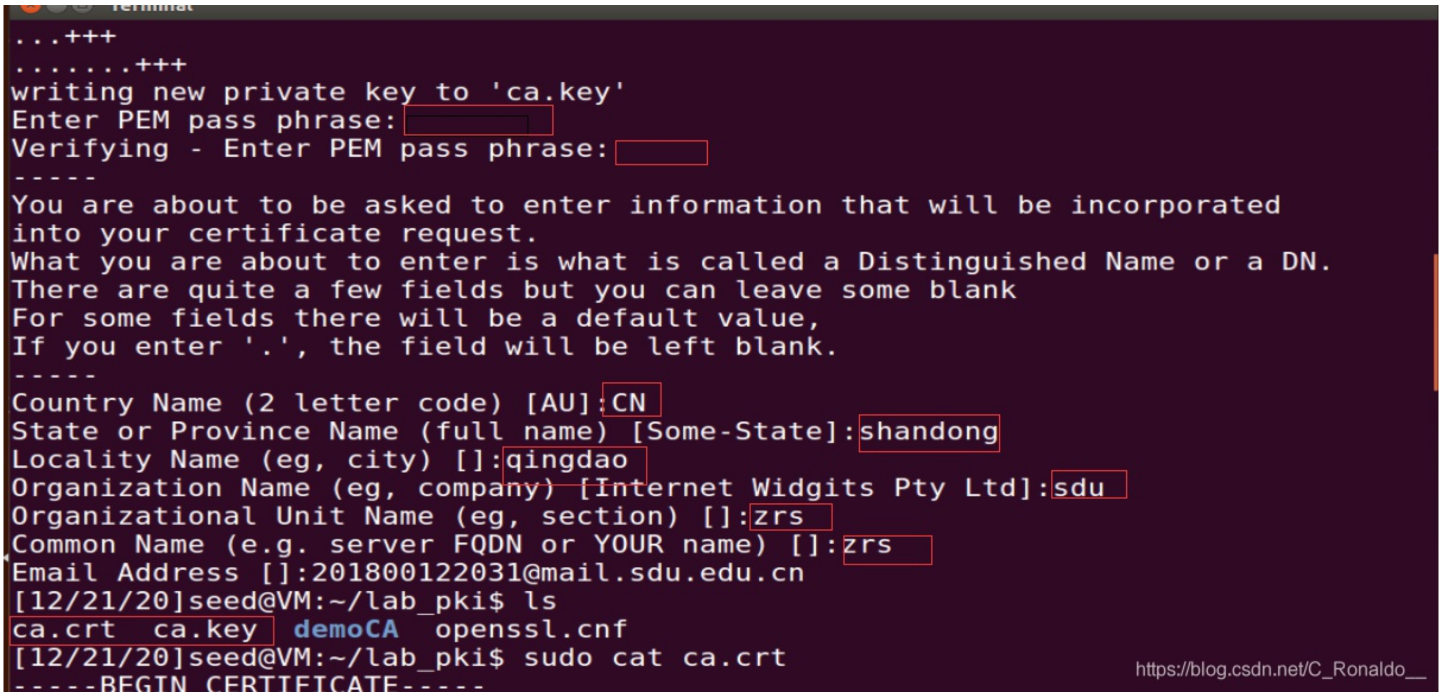
正规的CA证书需要付费购买,为了进行实验,我们可以自己搭建一个root CA,首先需要进行文件配置,openssl会使用一个默认配置文件(/usr/lib/ssl/openssl.cnf)文件,由用户生成证书请求文件(certificates signature request .csr文件),将此文件复制到实验文件夹lab_pki文件夹中,同时为根CA配置相关文件:


```
dir             = ./demoCA         # Where everything is kept
certs           = $dir/certs       # Where the issued certs are kept
crl_dir         = $dir/crl         # Where the issued crl are kept
new_certs_dir   = $dir/newcerts    # default place for new certs.
database        = $dir/index.txt   # database index file.
serial          = $dir/serial      # The current serial number
```

随后使用如下命令生成root CA证书文件.crt:

```
openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
```

需要输入相关身份信息:



```
...+++
.......+++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:CN
State or Province Name (full name) [Some-State]:shandong
Locality Name (eg, city) []:qingdao
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sdu
Organizational Unit Name (eg, section) []:zrs
Common Name (e.g. server FQDN or YOUR name) []:zrs
Email Address []:201800122031@mail.sdu.edu.cn
[12/21/20]seed@VM:~/lab_pki$ ls
ca.crt  ca.key  demoCA  openssl.cnf
[12/21/20]seed@VM:~/lab_pki$ sudo cat ca.crt
-----BEGIN CERTIFICATE-----
```

进行生成root CA的密钥文件ca.key和证书文件ca.crt

ask 2: 为SEEDPKILab2020.com创建证书

配置一个SEEDPKILab2020.com 的证书总共需要三步:

1. 生成公钥私钥对

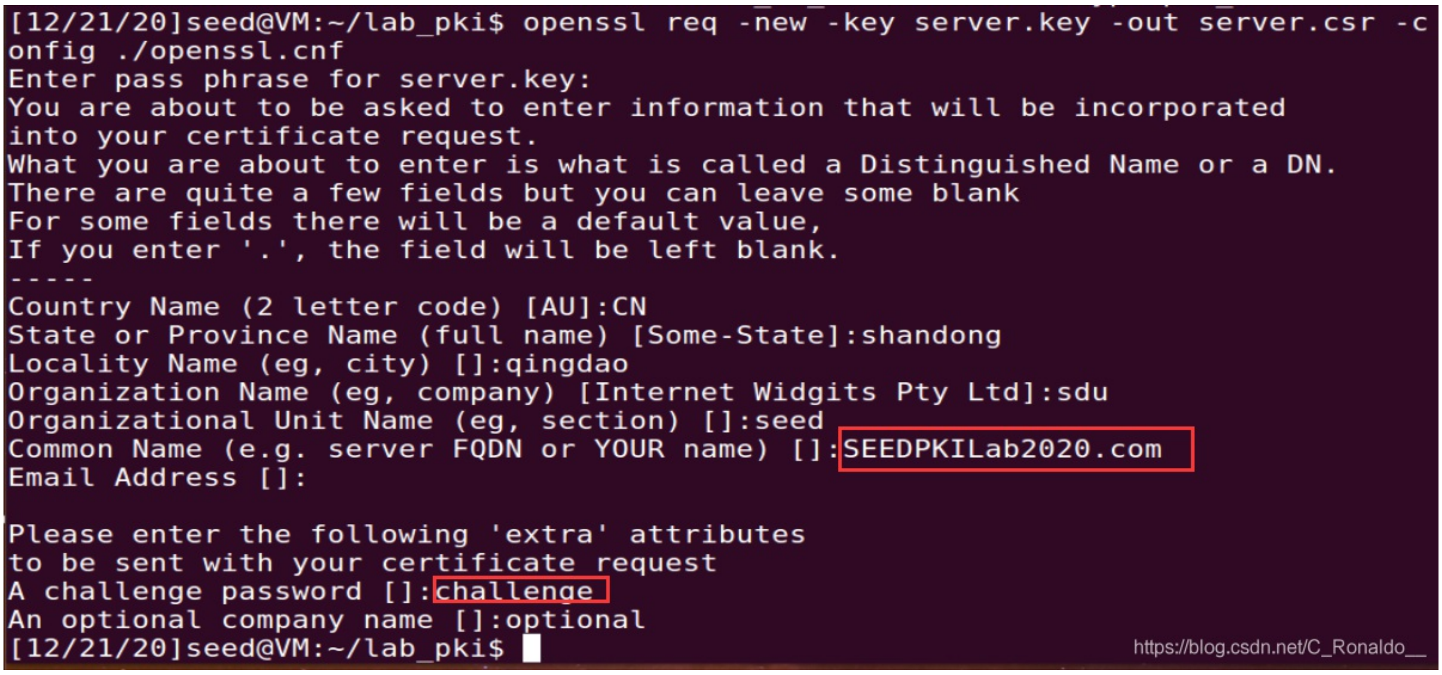
```
openssl genrsa -aes128 -out server.key 1024
```

将输入的密钥存储到server.key文件中

2. 生成证书签字请求.csr文件

```
openssl req -new -key server.key -out server.csr -config openssl.cnf
```

相关配置信息如下:



```
[12/21/20]seed@VM:~/lab_pki$ openssl req -new -key server.key -out server.csr -c
onfig ./openssl.cnf
Enter pass phrase for server.key:
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]:CN
State or Province Name (full name) [Some-State]:shandong
Locality Name (eg, city) []:qingdao
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sdu
Organizational Unit Name (eg, section) []:seed
Common Name (e.g. server FQDN or YOUR name) []:SEEDPKILab2020.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:challenge
An optional company name []:optional
[12/21/20]seed@VM:~/lab_pki$
```

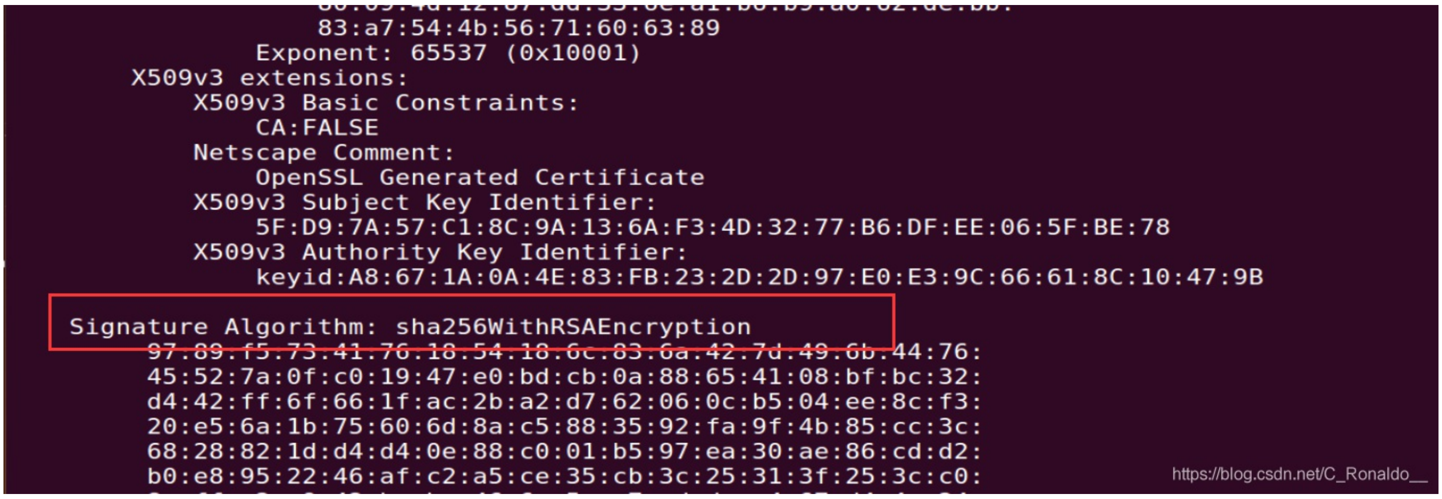
3. 与root CA进行验证与签名

```
openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key
-config openssl.cnf
```

将SEEDPKILab2020.com提交的server.csr文件给CA,CA验证完csr文件后,会给SEEDPKILab2020.com签发一个X509版本的证书,本实验忽略验证这一步,上面命令直接将server.csr,ca.crt 以及ca.key文件生成一个证书server.crt,注意openssl默认使用SHA256算法了,与课本上所说默认算法不同,不同openssl版本,可以使用如下命令查看:

```
openssl x509 -in server.crt -text
```

发现签名算法为:



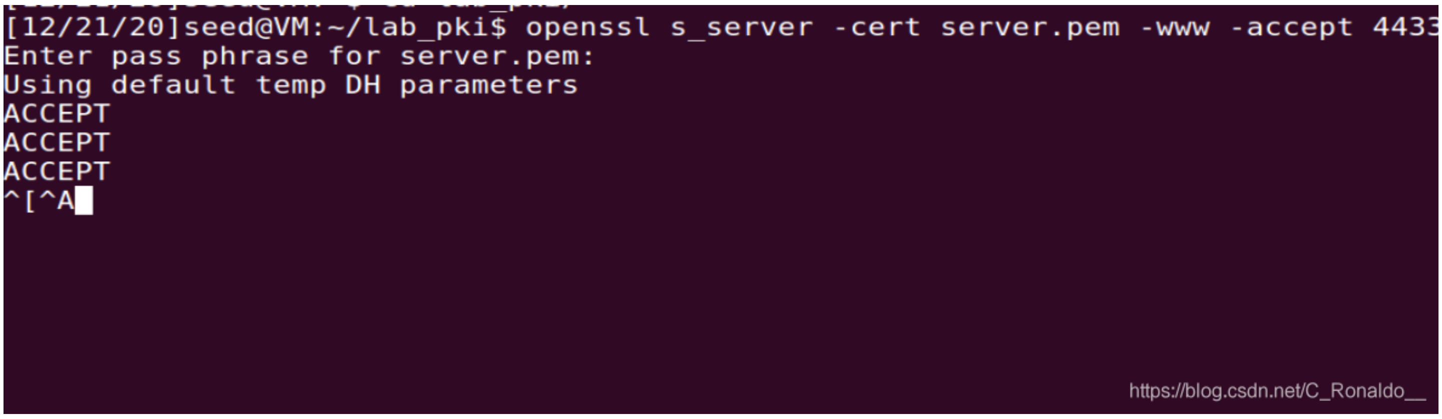
```
                    83:a7:54:4b:56:71:60:63:89
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                5F:D9:7A:57:C1:8C:9A:13:6A:F3:4D:32:77:B6:DF:EE:06:5F:BE:78
            X509v3 Authority Key Identifier:
                keyid:A8:67:1A:0A:4E:83:FB:23:2D:2D:97:E0:E3:9C:66:61:8C:10:47:9B

    Signature Algorithm: sha256WithRSAEncryption
         97:89:f5:73:41:76:18:54:18:6c:83:6a:42:7d:49:6b:44:76:
         45:52:7a:0f:c0:19:47:e0:bd:cb:0a:88:65:41:08:bf:bc:32:
         d4:42:ff:6f:66:1f:ac:2b:a2:d7:62:06:0c:b5:04:ee:8c:f3:
         20:e5:6a:1b:75:60:6d:8a:c5:88:35:92:fa:9f:4b:85:cc:3c:
         68:28:82:1d:d4:d4:0e:88:c0:01:b5:97:ea:30:ae:86:cd:d2:
         b0:e8:95:22:46:af:c2:a5:ce:35:cb:3c:25:31:3f:25:3c:c0:
```

task 3: 使用openssl自带服务器进行配置

使用openssl自带服务器可以进行配置HTTPS,但是首先需要将SEEDPKILab2020.com的私钥文件与公钥文件合并到一个文件`*`.pem中,使用如下命令(注意使用顺序,即文件的合并顺序需要注意):

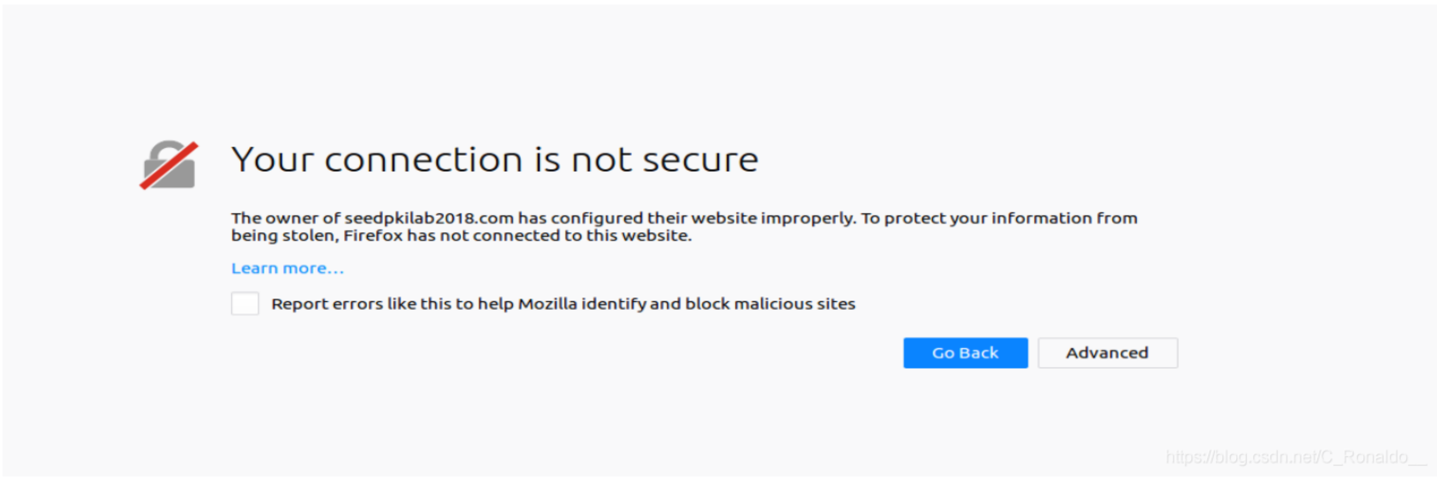
```
cp server.key server.pem
cat server.crt >> server.pem
```

随后,使用openssl s_server命令启动服务器,服务器默认监听4433端口,注意需要一直开着:



```
[12/21/20]seed@VM:~/lab_pki$ openssl s_server -cert server.pem -www -accept 443
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
ACCEPT
ACCEPT
^[^A
```

才能进行访问指定网站,会得到如下失败的结果:

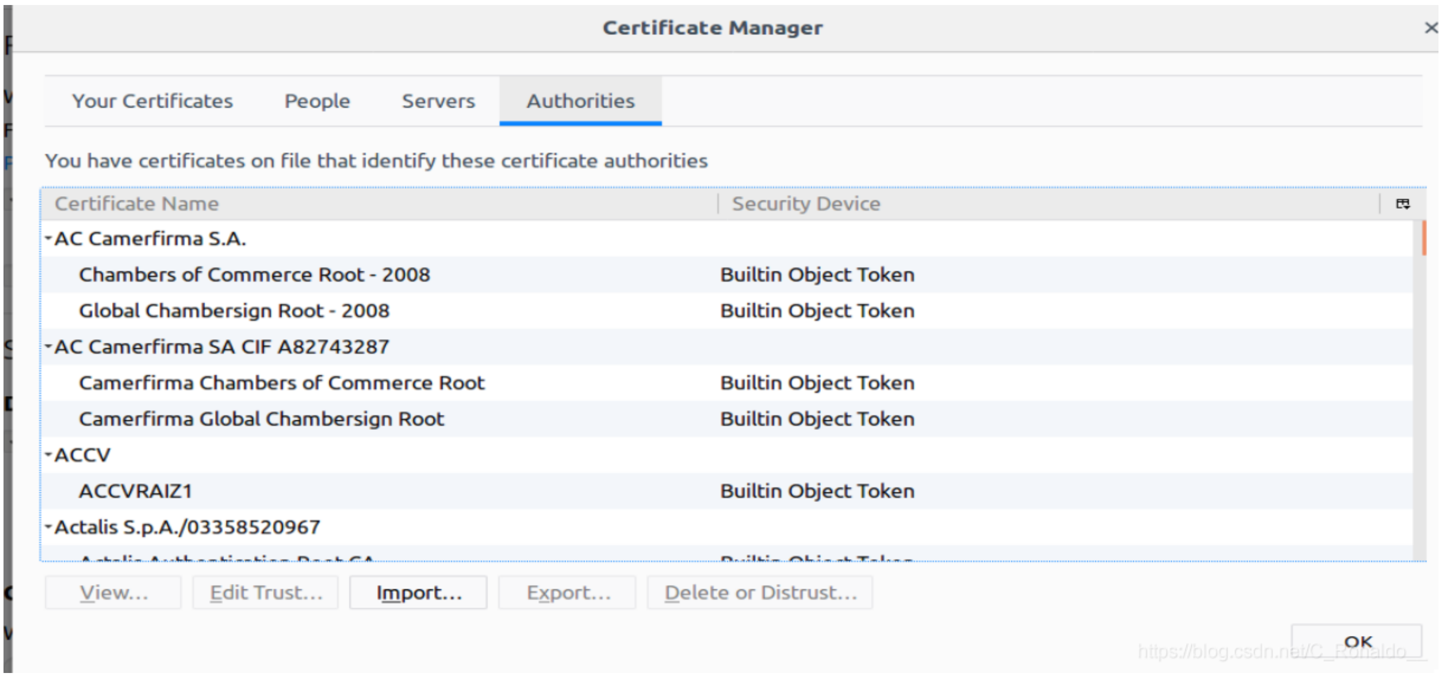


Your connection is not secure

The owner of seedpkilab2018.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…
Report errors like this to help Mozilla identify and block malicious sites
Go Back
Advanced

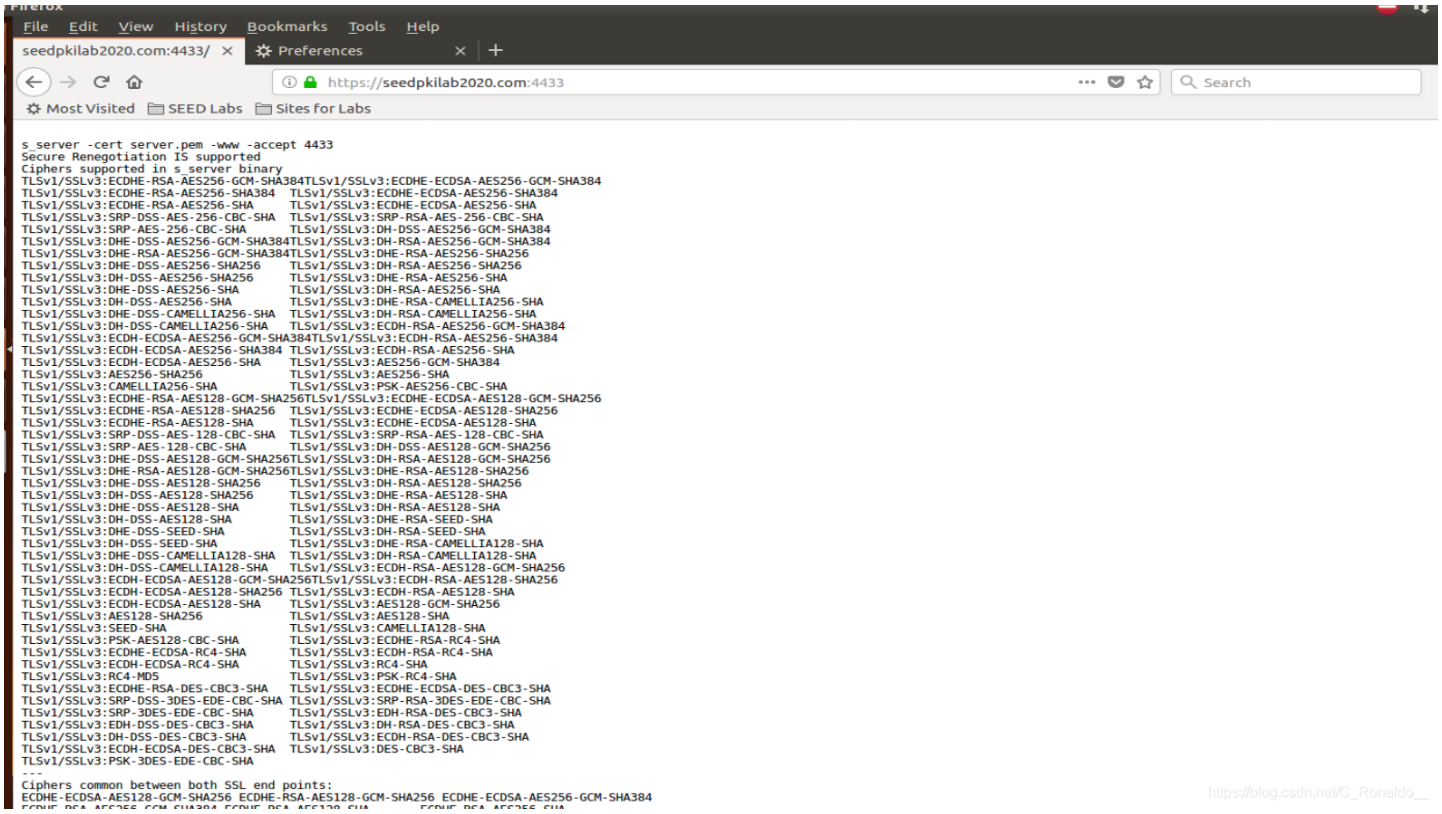
这是因为root CA为我们自己创建的,浏览器不会信任,所以需要手动添加之前任务创建的ca.crt文件到浏览器CA列表中:



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	

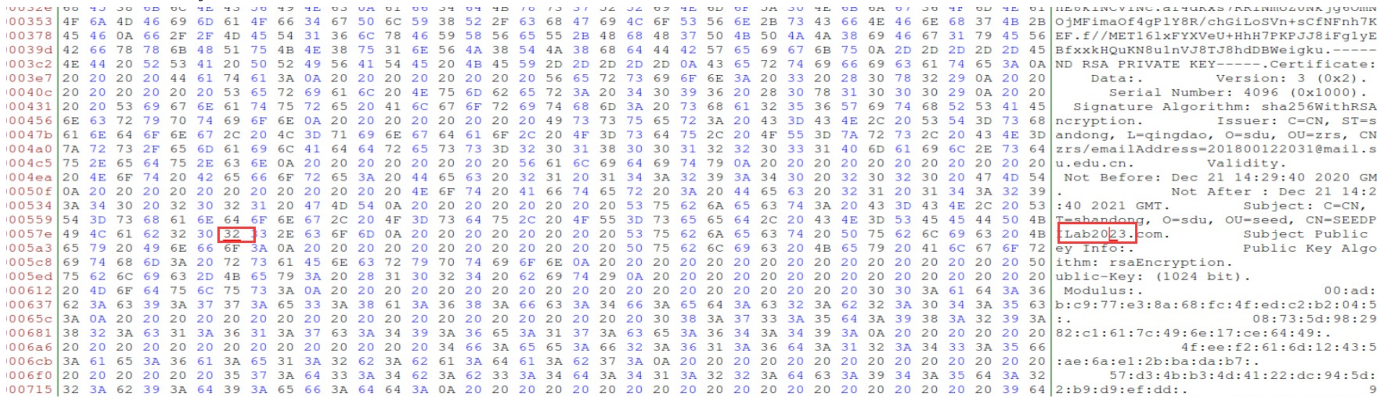
随后进行测试,可以正常运行:



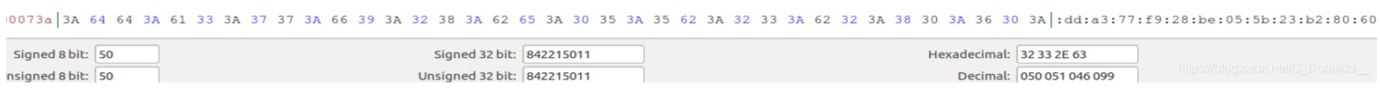
```
s_server -cert server.pem -www -accept 4433
Secure Renegotiation IS supported
Ciphers supported in s_server binary
TLSv1/SSLv3:ECDHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA384  TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA
TLSv1/SSLv3:SRP-DSS-AES-256-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-256-CBC-SHA
TLSv1/SSLv3:SRP-AES-256-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-DSS-AES256-GCM-SHA384TLSv1/SSLv3:DH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:DHE-RSA-AES256-SHA256
TLSv1/SSLv3:DHE-DSS-AES256-SHA256    TLSv1/SSLv3:DH-RSA-AES256-SHA256
TLSv1/SSLv3:DH-DSS-AES256-SHA256     TLSv1/SSLv3:DHE-RSA-AES256-SHA
TLSv1/SSLv3:DHE-DSS-AES256-SHA       TLSv1/SSLv3:DH-RSA-AES256-SHA
TLSv1/SSLv3:DH-DSS-AES256-SHA        TLSv1/SSLv3:DHE-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA256-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA256-SHA   TLSv1/SSLv3:ECDH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDH-RSA-AES256-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA384 TLSv1/SSLv3:ECDH-RSA-AES256-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA    TLSv1/SSLv3:AES256-GCM-SHA384
TLSv1/SSLv3:AES256-SHA256            TLSv1/SSLv3:AES256-SHA
TLSv1/SSLv3:CAMELLIA256-SHA          TLSv1/SSLv3:PSK-AES256-CBC-SHA
TLSv1/SSLv3:ECDHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA256  TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA
TLSv1/SSLv3:SRP-DSS-AES-128-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-128-CBC-SHA
TLSv1/SSLv3:SRP-AES-128-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-GCM-SHA256TLSv1/SSLv3:DH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:DHE-RSA-AES128-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-SHA256    TLSv1/SSLv3:DH-RSA-AES128-SHA256
TLSv1/SSLv3:DH-DSS-AES128-SHA256     TLSv1/SSLv3:DHE-RSA-AES128-SHA
TLSv1/SSLv3:DHE-DSS-AES128-SHA       TLSv1/SSLv3:DH-RSA-AES128-SHA
TLSv1/SSLv3:DH-DSS-AES128-SHA        TLSv1/SSLv3:DHE-RSA-SEED-SHA
TLSv1/SSLv3:DHE-DSS-SEED-SHA         TLSv1/SSLv3:DH-RSA-SEED-SHA
TLSv1/SSLv3:DH-DSS-SEED-SHA          TLSv1/SSLv3:DHE-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA128-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA128-SHA   TLSv1/SSLv3:ECDH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDH-RSA-AES128-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA256 TLSv1/SSLv3:ECDH-RSA-AES128-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA    TLSv1/SSLv3:AES128-GCM-SHA256
TLSv1/SSLv3:AES128-SHA256            TLSv1/SSLv3:AES128-SHA
TLSv1/SSLv3:SEED-SHA                 TLSv1/SSLv3:CAMELLIA128-SHA
TLSv1/SSLv3:PSK-AES128-CBC-SHA       TLSv1/SSLv3:ECDHE-RSA-RC4-SHA
TLSv1/SSLv3:ECDHE-ECDSA-RC4-SHA      TLSv1/SSLv3:ECDH-RSA-RC4-SHA
TLSv1/SSLv3:ECDH-ECDSA-RC4-SHA       TLSv1/SSLv3:RC4-SHA
TLSv1/SSLv3:RC4-MD5                  TLSv1/SSLv3:PSK-RC4-SHA
TLSv1/SSLv3:ECDHE-RSA-DES-CBC3-SHA   TLSv1/SSLv3:ECDHE-ECDSA-DES-CBC3-SHA
TLSv1/SSLv3:SRP-DSS-3DES-EDE-CBC-SHA TLSv1/SSLv3:SRP-RSA-3DES-EDE-CBC-SHA
TLSv1/SSLv3:SRP-3DES-EDE-CBC-SHA     TLSv1/SSLv3:EDH-RSA-DES-CBC3-SHA
TLSv1/SSLv3:EDH-DSS-DES-CBC3-SHA     TLSv1/SSLv3:DH-RSA-DES-CBC3-SHA
TLSv1/SSLv3:DH-DSS-DES-CBC3-SHA      TLSv1/SSLv3:ECDH-RSA-DES-CBC3-SHA
TLSv1/SSLv3:ECDH-ECDSA-DES-CBC3-SHA  TLSv1/SSLv3:DES-CBC3-SHA
TLSv1/SSLv3:PSK-3DES-EDE-CBC-SHA
---
Ciphers common between both SSL end points:
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384
```

Q1:

修改一个位于subject域的Common Name字节信息:

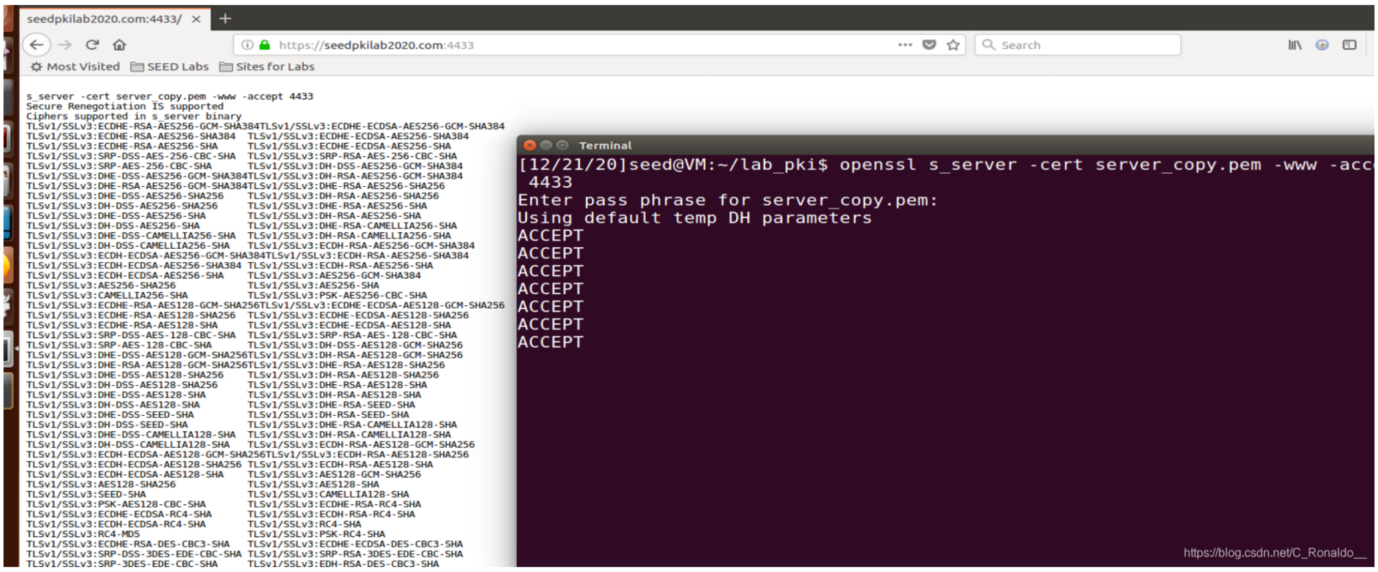


```
00353 4F 6A 4D 46 69 6D 61 4F 66 34 67 50 6C 59 38 52 2F 63 68 47 69 4C 6F 53 56 6E 2B 73 43 66 4E 46 6E 68 37 4B 2B OjMFimaOf4gPlY8R/chGiLoSVn+sCfNFnh7K
00378 45 46 0A 66 2F 2F 4D 45 54 31 36 6C 78 46 59 58 56 65 55 2B 48 68 48 37 50 4B 50 4A 4A 38 69 46 67 31 79 45 56 EF.f//MET16lxFYXVeU+HhH7PKPJJ8iFg1yE
0039d 42 66 78 78 6B 48 51 75 4B 4E 38 75 31 6E 56 4A 38 54 4A 38 68 64 44 42 57 65 69 67 6B 75 0A 2D 2D 2D 2D 2D 45 BfxxkHQuKN8u1nVJ8TJ8hdDBWeigku.-----
003c2 4E 44 20 52 53 41 20 50 52 49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D 2D 0A 43 65 72 74 69 66 69 63 61 74 65 3A 0A ND RSA PRIVATE KEY-----.Certificate:
003e7 20 20 20 20 44 61 74 61 3A 0A 20 20 20 20 20 20 20 20 56 65 72 73 69 6F 6E 3A 20 33 20 28 30 78 32 29 0A 20 20     Data:.        Version: 3 (0x2).
0040c 20 20 20 20 20 20 53 65 72 69 61 6C 20 4E 75 6D 62 65 72 3A 20 34 30 39 36 20 28 30 78 31 30 30 30 29 0A 20 20       Serial Number: 4096 (0x1000).
00431 20 20 53 69 67 6E 61 74 75 72 65 20 41 6C 67 6F 72 69 74 68 6D 3A 20 73 68 61 32 35 36 57 69 74 68 52 53 41 45   Signature Algorithm: sha256WithRSA
00456 6E 63 72 79 70 74 69 6F 6E 0A 20 20 20 20 20 20 20 20 49 73 73 75 65 72 3A 20 43 3D 43 4E 2C 20 53 54 3D 73 68 ncryption.        Issuer: C=CN, ST=s
0047b 61 6E 64 6F 6E 67 2C 20 4C 3D 71 69 6E 67 64 61 6F 2C 20 4F 3D 73 64 75 2C 20 4F 55 3D 7A 72 73 2C 20 43 4E 3D andong, L=qingdao, O=sdu, OU=zrs, CN
004a0 7A 72 73 2F 65 6D 61 69 6C 41 64 64 72 65 73 73 3D 32 30 31 38 30 30 31 32 32 30 33 31 40 6D 61 69 6C 2E 73 64 zrs/emailAddress=201800122031@mail.s
004c5 75 2E 65 64 75 2E 63 6E 0A 20 20 20 20 20 20 20 20 56 61 6C 69 64 69 74 79 0A 20 20 20 20 20 20 20 20 20 20 20 u.edu.cn.        Validity.
004ea 20 4E 6F 74 20 42 65 66 6F 72 65 3A 20 44 65 63 20 32 31 20 31 34 3A 32 39 3A 34 30 20 32 30 32 30 20 47 4D 54  Not Before: Dec 21 14:29:40 2020 GM
0050f 0A 20 20 20 20 20 20 20 20 20 20 20 20 4E 6F 74 20 41 66 74 65 72 20 3A 20 44 65 63 20 32 31 20 31 34 3A 32 39 .            Not After : Dec 21 14:2
00534 3A 34 30 20 32 30 32 31 20 47 4D 54 0A 20 20 20 20 20 20 20 20 53 75 62 6A 65 63 74 3A 20 43 3D 43 4E 2C 20 53 :40 2021 GMT.        Subject: C=CN,
00559 54 3D 73 68 61 6E 64 6F 6E 67 2C 20 4F 3D 73 64 75 2C 20 4F 55 3D 73 65 65 64 2C 20 43 4E 3D 53 45 45 44 50 4B T=shandong, O=sdu, OU=seed, CN=SEEDP
0057e 49 4C 61 62 32 30 32 33 2E 63 6F 6D 0A 20 20 20 20 20 20 20 20 53 75 62 6A 65 63 74 20 50 75 62 6C 69 63 20 4B ILab2023.com.        Subject Public
005a3 65 79 20 49 6E 66 6F 3A 0A 20 20 20 20 20 20 20 20 20 20 20 20 50 75 62 6C 69 63 20 4B 65 79 20 41 6C 67 6F 72 ey Info:.            Public Key Algo
005c8 69 74 68 6D 3A 20 72 73 61 45 6E 63 72 79 70 74 69 6F 6E 0A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 50 ithm: rsaEncryption.
005ed 75 62 6C 69 63 2D 4B 65 79 3A 20 28 31 30 32 34 20 62 69 74 29 0A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ublic-Key: (1024 bit).
00612 20 4D 6F 64 75 6C 75 73 3A 0A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 30 30 3A 61 64 3A 36  Modulus:.                    00:ad:
00637 62 3A 63 39 3A 37 37 3A 65 33 3A 38 61 3A 36 38 3A 66 63 3A 34 66 3A 65 64 3A 63 32 3A 62 32 3A 30 34 3A 35 63 b:c9:77:e3:8a:68:fc:4f:ed:c2:b2:04:5
0065c 3A 0A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 30 38 3A 37 33 3A 35 64 3A 39 38 3A 32 39 3A :.                    08:73:5d:98:29
00681 38 32 3A 63 31 3A 36 31 3A 37 63 3A 34 39 3A 36 65 3A 31 37 3A 63 65 3A 36 34 3A 34 39 3A 0A 20 20 20 20 20 20 82:c1:61:7c:49:6e:17:ce:64:49:.
006a6 20 20 20 20 20 20 20 20 20 20 20 20 20 20 34 66 3A 65 65 3A 66 32 3A 36 31 3A 36 64 3A 31 32 3A 34 33 3A 35 66               4f:ee:f2:61:6d:12:43:5
006cb 3A 61 65 3A 36 61 3A 65 31 3A 32 62 3A 62 61 3A 64 61 3A 62 37 3A 0A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 :ae:6a:e1:2b:ba:da:b7:.
006f0 20 20 20 20 20 20 35 37 3A 64 33 3A 34 62 3A 62 33 3A 34 64 3A 34 31 3A 32 32 3A 64 63 3A 39 34 3A 35 64 3A 32       57:d3:4b:b3:4d:41:22:dc:94:5d:
00715 32 3A 62 39 3A 64 39 3A 65 66 3A 64 64 3A 0A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 39 64 2:b9:d9:ef:dd:.                    9
```



```
0073a|3A 64 64 3A 61 33 3A 37 37 3A 66 39 3A 32 38 3A 62 65 3A 30 35 3A 35 62 3A 32 33 3A 62 32 3A 38 30 3A 36 30 3A|:dd:a3:77:f9:28:be:05:5b:23:b2:80:60
```

保存后继续运行得到结果如下:

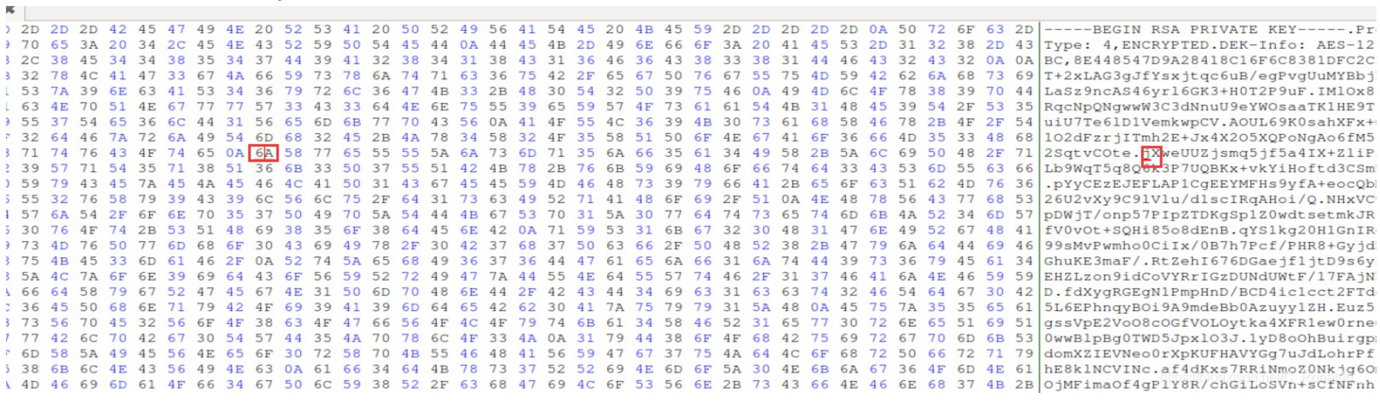


```
s_server -cert server_copy.pem -www -accept 4433
Secure Renegotiation IS supported
Ciphers supported in s_server binary
TLSv1/SSLv3:ECDHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA384  TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA
TLSv1/SSLv3:SRP-DSS-AES-256-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-256-CBC-SHA
TLSv1/SSLv3:SRP-AES-256-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-DSS-AES256-GCM-SHA384TLSv1/SSLv3:DH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:DHE-RSA-AES256-SHA256
TLSv1/SSLv3:DHE-DSS-AES256-SHA256    TLSv1/SSLv3:DH-RSA-AES256-SHA256
TLSv1/SSLv3:DH-DSS-AES256-SHA256     TLSv1/SSLv3:DHE-RSA-AES256-SHA
TLSv1/SSLv3:DHE-DSS-AES256-SHA       TLSv1/SSLv3:DH-RSA-AES256-SHA
TLSv1/SSLv3:DH-DSS-AES256-SHA        TLSv1/SSLv3:DHE-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA256-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA256-SHA   TLSv1/SSLv3:ECDH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDH-RSA-AES256-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA384 TLSv1/SSLv3:ECDH-RSA-AES256-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA    TLSv1/SSLv3:AES256-GCM-SHA384
TLSv1/SSLv3:AES256-SHA256            TLSv1/SSLv3:AES256-SHA
TLSv1/SSLv3:CAMELLIA256-SHA          TLSv1/SSLv3:PSK-AES256-CBC-SHA
TLSv1/SSLv3:ECDHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA256  TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA
TLSv1/SSLv3:SRP-DSS-AES-128-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-128-CBC-SHA
TLSv1/SSLv3:SRP-AES-128-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-GCM-SHA256TLSv1/SSLv3:DH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:DHE-RSA-AES128-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-SHA256    TLSv1/SSLv3:DH-RSA-AES128-SHA256
TLSv1/SSLv3:DH-DSS-AES128-SHA256     TLSv1/SSLv3:DHE-RSA-AES128-SHA
TLSv1/SSLv3:DHE-DSS-AES128-SHA       TLSv1/SSLv3:DH-RSA-AES128-SHA
TLSv1/SSLv3:DH-DSS-AES128-SHA        TLSv1/SSLv3:DHE-RSA-SEED-SHA
TLSv1/SSLv3:DHE-DSS-SEED-SHA         TLSv1/SSLv3:DH-RSA-SEED-SHA
TLSv1/SSLv3:DH-DSS-SEED-SHA          TLSv1/SSLv3:DHE-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA128-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA128-SHA   TLSv1/SSLv3:ECDH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDH-RSA-AES128-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA256 TLSv1/SSLv3:ECDH-RSA-AES128-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA    TLSv1/SSLv3:AES128-GCM-SHA256
TLSv1/SSLv3:AES128-SHA256            TLSv1/SSLv3:AES128-SHA
TLSv1/SSLv3:SEED-SHA                 TLSv1/SSLv3:CAMELLIA128-SHA
TLSv1/SSLv3:PSK-AES128-CBC-SHA       TLSv1/SSLv3:ECDHE-RSA-RC4-SHA
TLSv1/SSLv3:ECDHE-ECDSA-RC4-SHA      TLSv1/SSLv3:ECDH-RSA-RC4-SHA
TLSv1/SSLv3:ECDH-ECDSA-RC4-SHA       TLSv1/SSLv3:RC4-SHA
TLSv1/SSLv3:RC4-MD5                  TLSv1/SSLv3:PSK-RC4-SHA
TLSv1/SSLv3:ECDHE-RSA-DES-CBC3-SHA   TLSv1/SSLv3:ECDHE-ECDSA-DES-CBC3-SHA
TLSv1/SSLv3:SRP-DSS-3DES-EDE-CBC-SHA TLSv1/SSLv3:SRP-RSA-3DES-EDE-CBC-SHA
TLSv1/SSLv3:SRP-3DES-EDE-CBC-SHA     TLSv1/SSLv3:EDH-RSA-DES-CBC3-SHA
```

```
[12/21/20]seed@VM:~/lab_pki$ openssl s_server -cert server_copy.pem -www -acc
 4433
Enter pass phrase for server_copy.pem:
Using default temp DH parameters
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
```

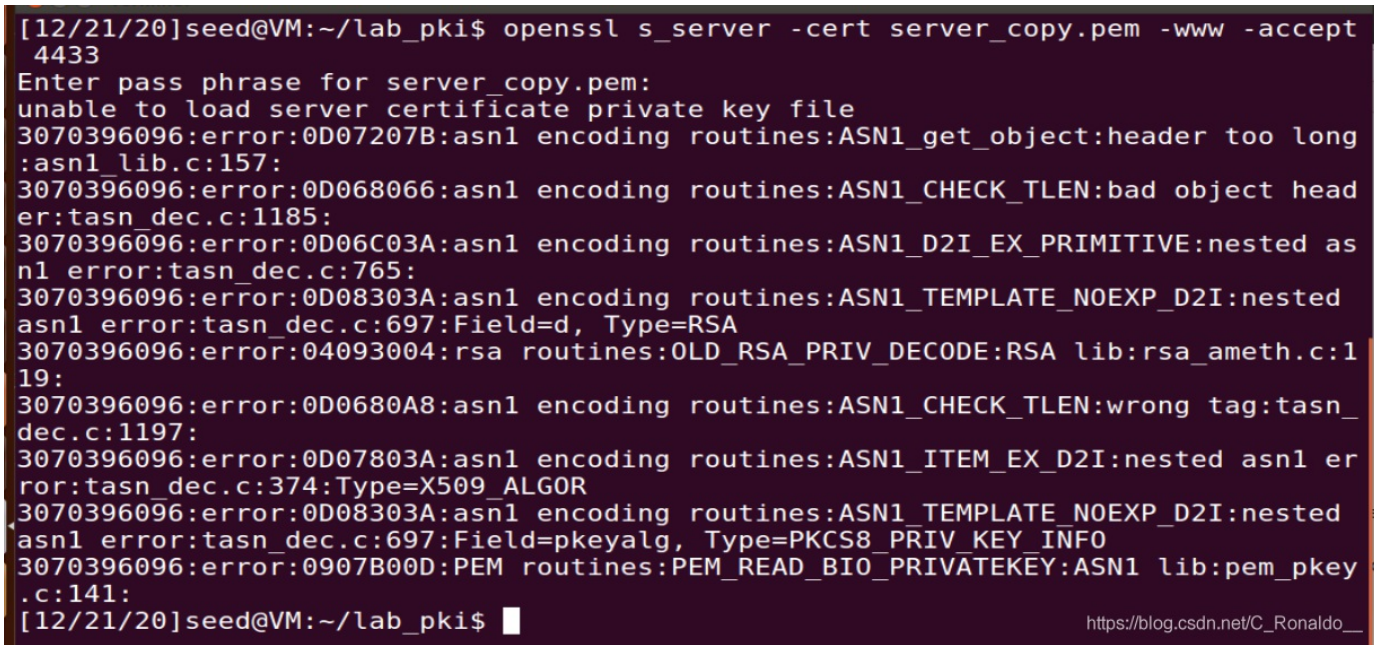
仍然可以正常运行.

修改一个位于Private Key的字节:



```
2D 2D 2D 42 45 47 49 4E 20 52 53 41 20 50 52 49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D 2D 0A 50 72 6F 63 2D |-----BEGIN RSA PRIVATE KEY-----.Pr
70 65 3A 20 34 2C 45 4E 43 52 59 50 54 45 44 0A 44 45 4B 2D 49 6E 66 6F 3A 20 41 45 53 2D 31 32 38 2D 43 |Type: 4,ENCRYPTED.DEK-Info: AES-12
2C 38 45 34 34 38 35 34 37 44 39 41 32 38 34 31 38 43 31 36 46 36 43 38 33 38 31 44 46 43 32 43 32 0A 0A |BC,8E448547D9A28418C16F6C8381DFC2C
32 78 4C 41 47 33 67 4A 66 59 73 78 6A 74 71 63 36 75 42 2F 65 67 50 76 67 55 75 4D 59 42 62 6A 68 73 69 |T+2xLAG3gJfYsxjtqc6uB/egPvgUuMYBbj
53 7A 39 6E 63 41 53 34 36 79 72 6C 36 47 4B 33 2B 48 30 54 32 50 39 75 46 0A 49 4D 6C 4F 78 38 39 70 44 |LaSz9ncAS46yrl6GK3+H0T2P9uF.IMlOx8
63 4E 70 51 4E 67 77 77 57 33 43 33 64 4E 6E 75 55 39 65 59 57 4F 73 61 61 54 4B 31 48 45 39 54 2F 53 35 |RqcNpQNgwwW3C3dNnuU9eYWOsaaTKlHE9T
55 37 54 65 36 6C 44 31 56 65 6D 6B 77 70 43 56 0A 41 4F 55 4C 36 39 4B 30 73 61 68 58 46 78 2B 4F 2F 54 |uiU7Te6lD1VemkwpCV.AOUL69K0sahXFx+
32 64 46 7A 72 6A 49 54 6D 68 32 45 2B 4A 78 34 58 32 4F 35 58 51 50 6F 4E 67 41 6F 36 66 4D 35 33 48 68 |lO2dFzrjITmh2E+Jx4X2O5XQPoNgAo6fM5
71 74 76 43 4F 74 65 0A 6A 58 77 65 55 55 5A 6A 73 6D 71 35 6A 66 35 61 34 49 58 2B 5A 6C 69 50 48 2F 71 |2SqtvCOte.jXweUUZjsmq5jf5a4IX+ZliP
39 57 71 54 35 71 38 51 36 6B 33 50 37 55 51 42 4B 78 2B 76 6B 59 69 48 6F 66 74 64 33 43 53 6D 55 63 66 |Lb9WqT5q8Q6k3P7UQBKx+vkYiHoftd3CSm
59 79 43 45 7A 45 4A 45 46 4C 41 50 31 43 67 45 45 59 4D 46 48 73 39 79 66 41 2B 65 6F 63 51 62 4D 76 36 |.pYyCEzEJEFLAP1CgEEYMFHs9yfA+eocQb
55 32 76 58 79 39 43 39 6C 56 6C 75 2F 64 31 73 63 49 52 71 41 48 6F 69 2F 51 0A 4E 48 78 56 43 77 68 53 |26U2vXy9C9lVlu/d1scIRqAHoi/Q.NHxVC
57 6A 54 2F 6F 6E 70 35 37 50 49 70 5A 54 44 4B 67 53 70 31 5A 30 77 64 74 73 65 74 6D 6B 4A 52 34 6D 57 |pDWjT/onp57PIpZTDKgSp1Z0wdtsetmkJR
30 76 4F 74 2B 53 51 48 69 38 35 6F 38 64 45 6E 42 0A 71 59 53 31 6B 67 32 30 48 31 47 6E 49 52 67 48 41 |fV0vOt+SQHi85o8dEnB.qYS1kg20H1GnIR
73 4D 76 50 77 6D 68 6F 30 43 69 49 78 2F 30 42 37 68 37 50 63 66 2F 50 48 52 38 2B 47 79 6A 64 44 69 46 |99sMvPwmho0CiIx/0B7h7Pcf/PHR8+Gyjd
75 4B 45 33 6D 61 46 2F 0A 52 74 5A 65 68 49 36 37 36 44 47 61 65 6A 66 31 6A 74 44 39 73 36 79 45 61 34 |GhuKE3maF/.RtZehI676DGaejf1jtD9s6y
5A 4C 7A 6F 6E 39 69 64 43 6F 56 59 52 72 49 47 7A 44 55 4E 64 55 57 74 46 2F 31 37 46 41 6A 4E 46 59 59 |EHZLzon9idCoVYRrIGzDUNdUWtF/17FAjN
66 64 58 79 67 52 47 45 67 4E 31 50 6D 70 48 6E 44 2F 42 43 44 34 69 63 31 63 63 74 32 46 54 64 67 30 42 |D.fdXygRGEgN1PmpHnD/BCD4ic1cct2FTd
36 45 50 68 6E 71 79 42 4F 69 39 41 39 6D 64 65 42 62 30 41 7A 75 79 79 31 5A 48 0A 45 75 7A 35 35 65 61 |5L6EPhnqyBOi9A9mdeBb0Azuyy1ZH.Euz5
73 56 70 45 32 56 6F 4F 38 63 4F 47 66 56 4F 4C 4F 79 74 6B 61 34 58 46 52 31 65 77 30 72 6E 65 51 69 51 |gssVpE2VoO8cOGfVOLOytka4XFR1ew0rne
77 42 6C 70 42 67 30 54 57 44 35 4A 70 78 6C 4F 33 4A 0A 31 79 44 38 6F 4F 68 42 75 69 72 67 70 6D 6B 53 |0wwBlpBg0TWD5Jpxl03J.1yD8oOhBuirgp
6D 58 5A 49 45 56 4E 65 6F 30 72 58 70 4B 55 46 48 41 56 59 47 67 37 75 4A 64 4C 6F 68 72 50 66 72 71 79 |domXZIEVNeo0rXpKUFHAVYGg7uJdLohrPf
38 6B 6C 4E 43 56 49 4E 63 0A 61 66 34 64 4B 78 73 37 52 52 69 4E 6D 6F 5A 30 4E 6B 6A 67 36 4F 6D 4E 61 |hE8klNCVINc.af4dKxs7RRiNmoZ0Nkjg6O
4D 46 69 6D 61 4F 66 34 67 50 6C 59 38 52 2F 63 68 47 69 4C 6F 53 56 6E 2B 73 43 66 4E 46 6E 68 37 4B 2B |OjMFimaOf4gPlY8R/chGiLoSVn+sCfNFnh
```

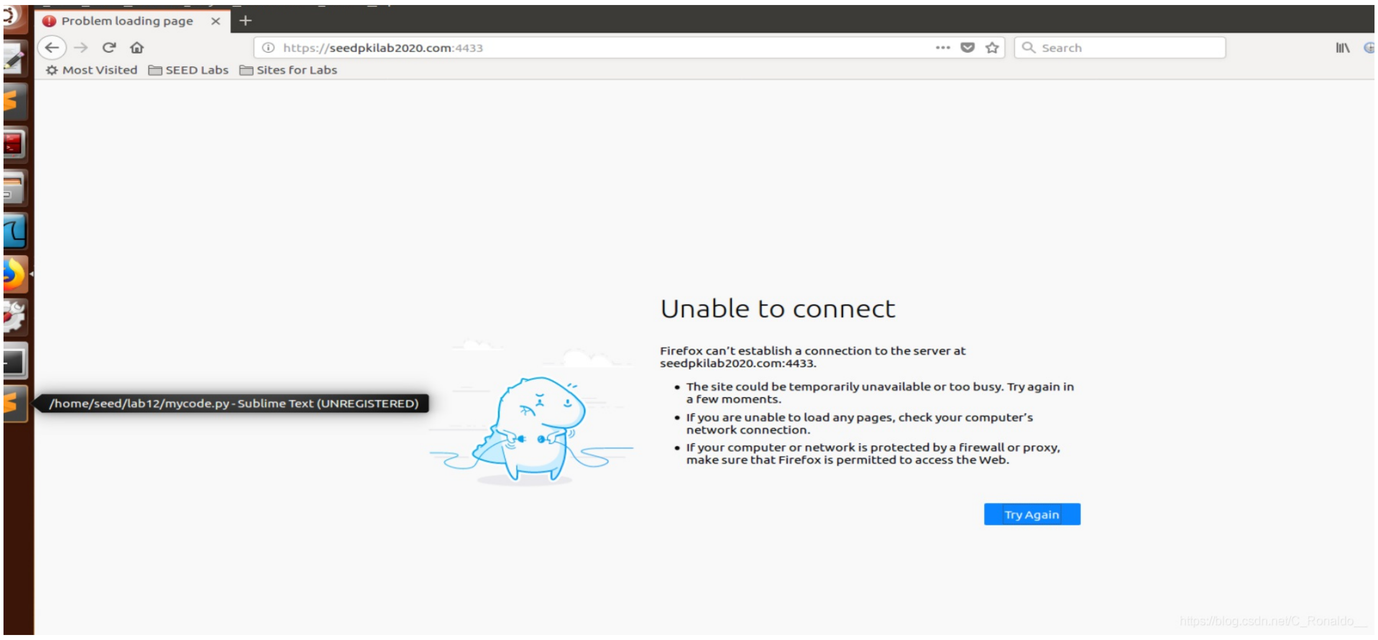
保存后继续运行得到结果如下:



```
[12/21/20]seed@VM:~/lab_pki$ openssl s_server -cert server_copy.pem -www -accept
 4433
Enter pass phrase for server_copy.pem:
unable to load server certificate private key file
3070396096:error:0D07207B:asn1 encoding routines:ASN1_get_object:header too long
:asn1_lib.c:157:
3070396096:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object head
er:tasn_dec.c:1185:
3070396096:error:0D06C03A:asn1 encoding routines:ASN1_D2I_EX_PRIMITIVE:nested as
n1 error:tasn_dec.c:765:
3070396096:error:0D08303A:asn1 encoding routines:ASN1_TEMPLATE_NOEXP_D2I:nested
asn1 error:tasn_dec.c:697:Field=d, Type=RSA
3070396096:error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib:rsa_ameth.c:1
19:
3070396096:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_
dec.c:1197:
3070396096:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 er
ror:tasn_dec.c:374:Type=X509_ALGOR
3070396096:error:0D08303A:asn1 encoding routines:ASN1_TEMPLATE_NOEXP_D2I:nested
asn1 error:tasn_dec.c:697:Field=pkeyalg, Type=PKCS8_PRIV_KEY_INFO
3070396096:error:0907B00D:PEM routines:PEM_READ_BIO_PRIVATEKEY:ASN1 lib:pem_pkey
.c:141:
[12/21/20]seed@VM:~/lab_pki$ 
```

浏览器不可以访问:

blem loading page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
En
10:43


Problem loading page

https://seedpkilab2020.com:4433

/home/seed/lab12/mycode.py - Sublime Text (UNREGISTERED)

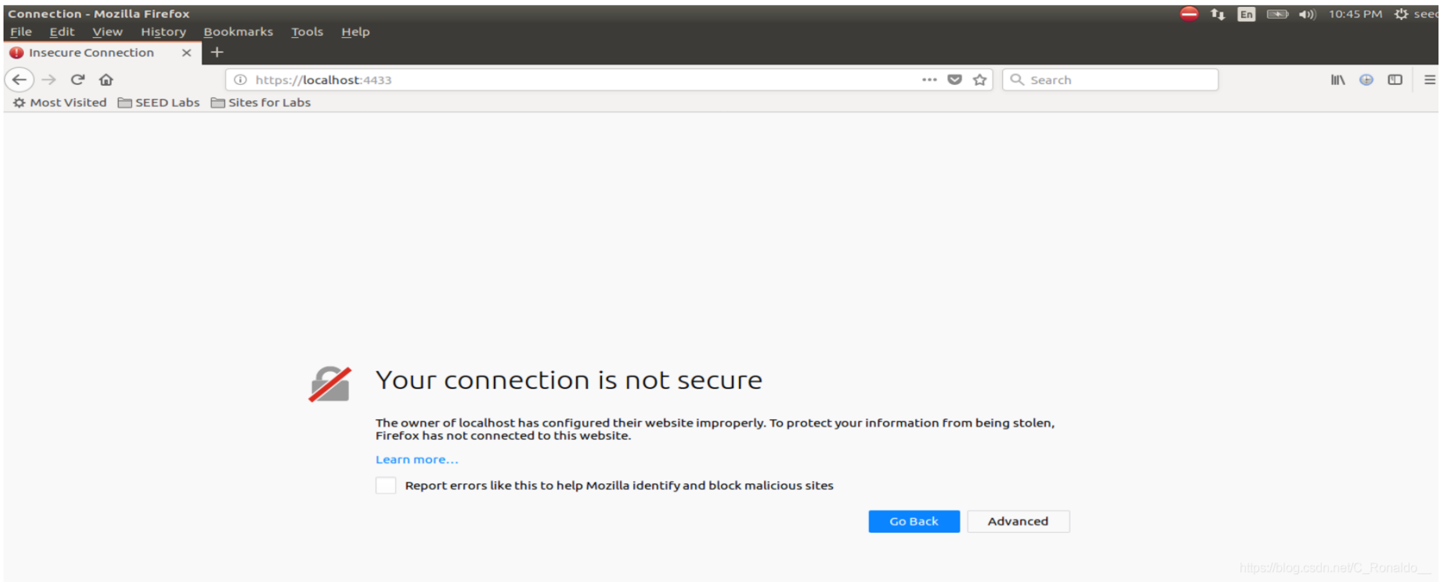
Unable to connect

Firefox can't establish a connection to the server at seedpkilab2020.com:4433.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

结果分析:CA拥有私钥,可以进行验证server_copy.pem文件是否合法,但是为什么修改subject域信息可以通过??
这个原因我也不太清楚…
可能是在此过程中SSL验证证书的合法性但是浏览器没有验证证书Commoon Name与域名的是否匹配问题,TLS有这个使用上的问题…
不太确定…

Q2


Connection - Mozilla Firefox

Insecure Connection

https://localhost:4433

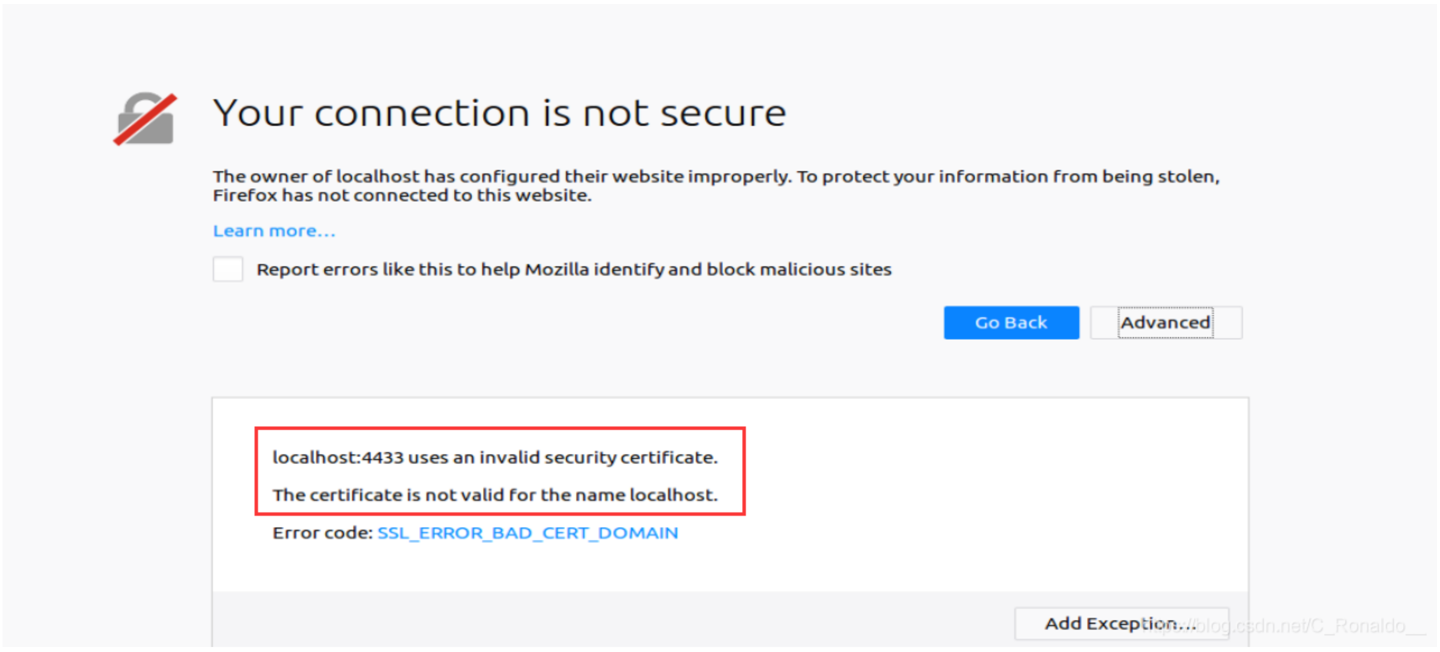
Your connection is not secure

The owner of localhost has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

Report errors like this to help Mozilla identify and block malicious sites

由于浏览器会检查URL中名称域证书中Subject域信息中域名条目Common Name是否一致,此时并不一致所以失败,浏览器给出了原因,与分析基本一致:


Your connection is not secure

The owner of localhost has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

Report errors like this to help Mozilla identify and block malicious sites

localhost:4433 uses an invalid security certificate.

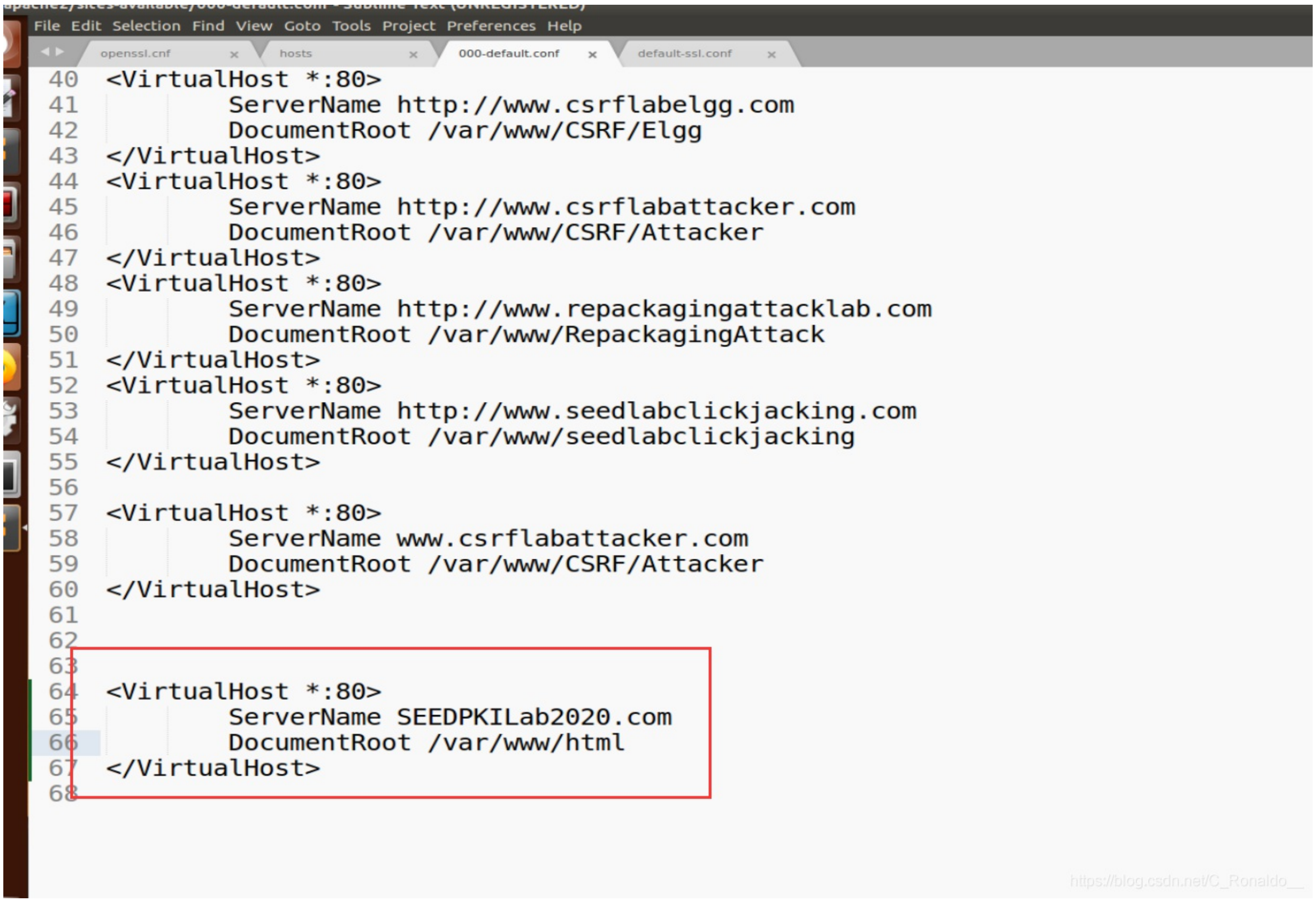
The certificate is not valid for the name localhost.

Error code: SSL_ERROR_BAD_CERT_DOMAIN

task 4: 使用Apache配置HTTPS服务器

在task3中,我们使用openssl的s_server命令设置HTTPS服务器,主要用于调试和演示目的。
在这个实验中，我们基于Apache服务器建立一个真正的HTTPS web服务器。Apache服务器(已经安装在我们的VM中)且支持HTTPS协议。
要创建一个HTTPS网站，我们只需要配置Apache服务器，这样它就知道从哪里获得私钥和证书。

- 对000-default.conf使用如下配置:

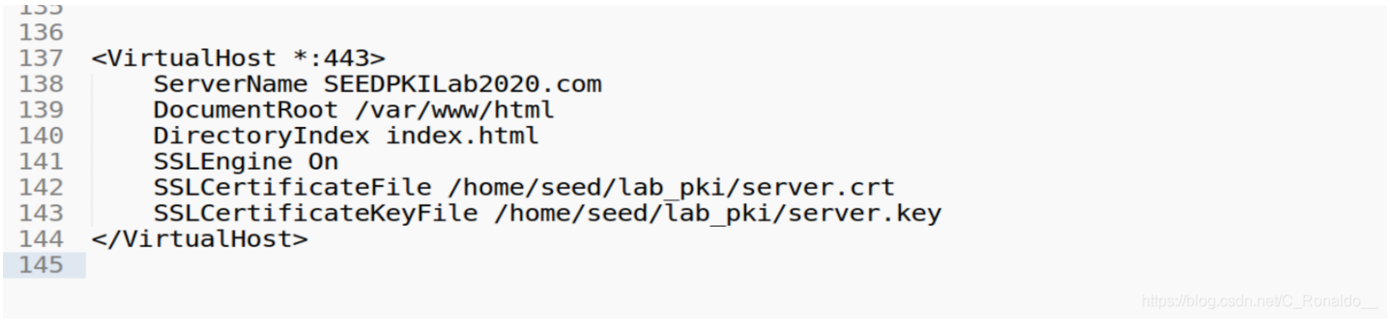


File Edit Selection Find View Goto Tools Project Preferences Help
openssl.cnf
hosts
000-default.conf
default-ssl.conf

```
<VirtualHost *:80>
        ServerName http://www.csrflabelgg.com
        DocumentRoot /var/www/CSRF/Elgg
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.csrflabattacker.com
        DocumentRoot /var/www/CSRF/Attacker
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.repackagingattacklab.com
        DocumentRoot /var/www/RepackagingAttack
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.seedlabclickjacking.com
        DocumentRoot /var/www/seedlabclickjacking
</VirtualHost>

<VirtualHost *:80>
        ServerName www.csrflabattacker.com
        DocumentRoot /var/www/CSRF/Attacker
</VirtualHost>



<VirtualHost *:80>
        ServerName SEEDPKILab2020.com
        DocumentRoot /var/www/html
</VirtualHost>

```

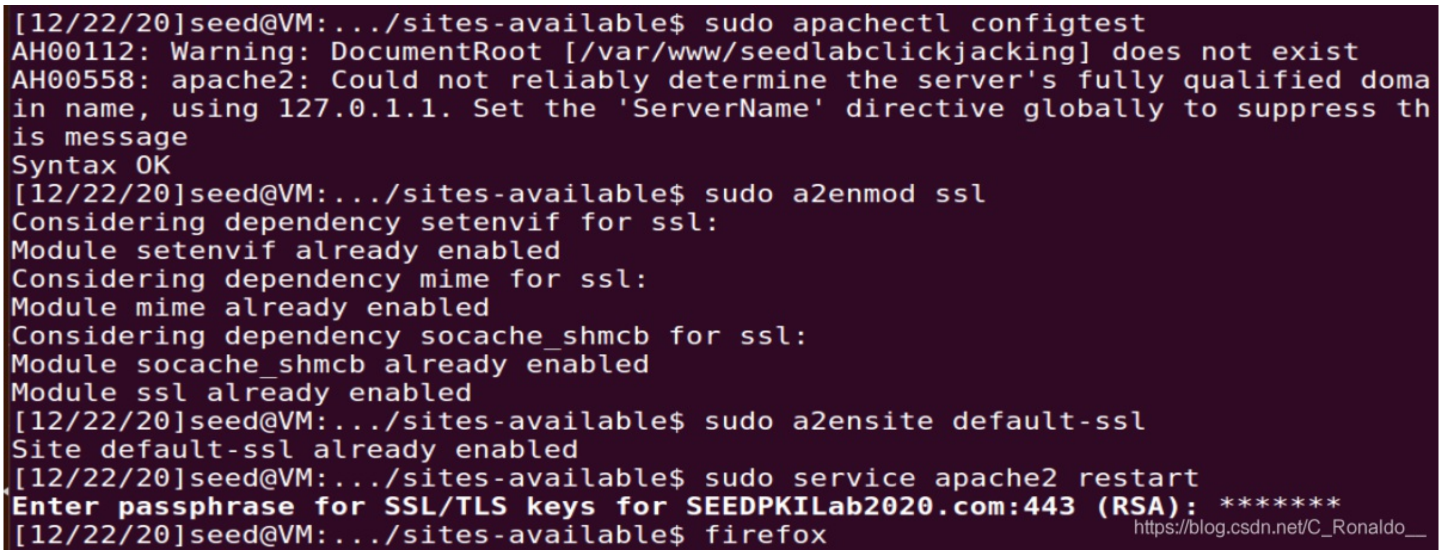
需要进行此配置, 不设置也没有影响,因为会显示默认网站,也就是我们设置的网页界面,但是在task5任务中,网站不同,必须进行配置.

- 对default-ssl.conf文件使用如下配置:



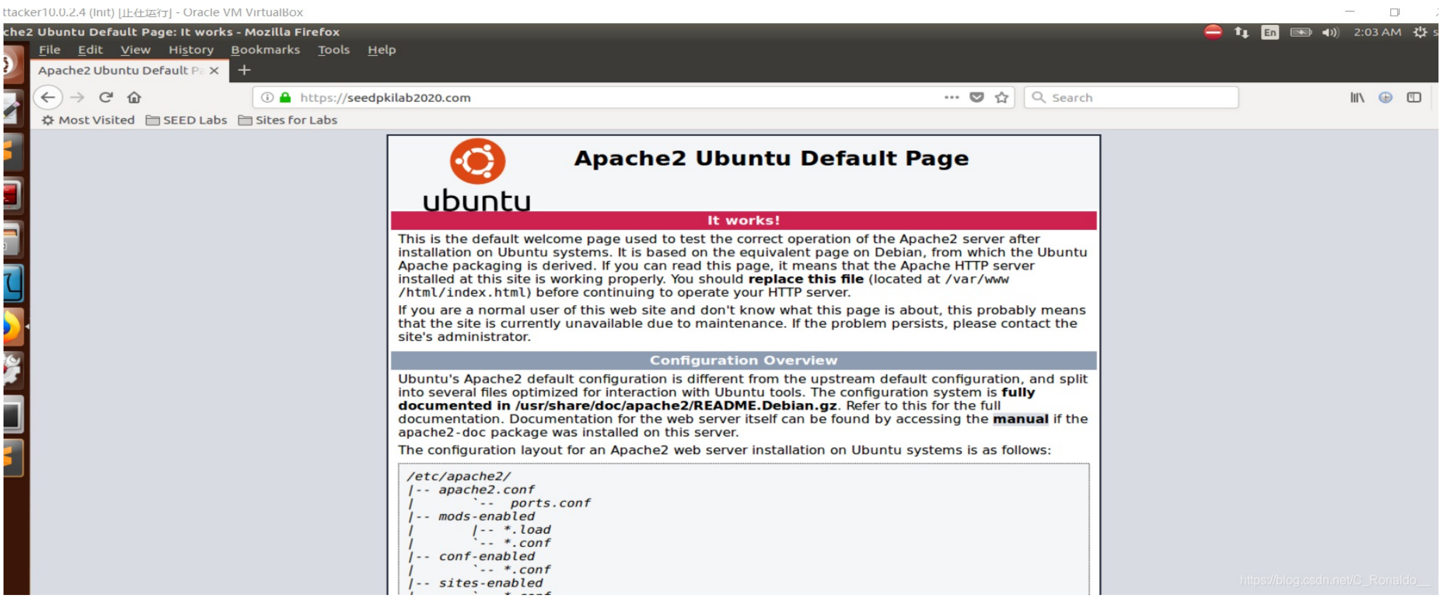
```

<VirtualHost *:443>
    ServerName SEEDPKILab2020.com
    DocumentRoot /var/www/html
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /home/seed/lab_pki/server.crt
    SSLCertificateKeyFile /home/seed/lab_pki/server.key
</VirtualHost>

```

其中ServerName条目指定网站的名称，而DocumentRoot条目指定网站文件存储的位置。同时我们需要告诉Apache服务器证书和私钥存储在哪里,后两行为task2中证书和私钥文件的位置.
随后运行一系列命令得到如下:



```
[12/22/20]seed@VM:.../sites-available$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickjacking] does not exist
AH00558: apache2: Could not reliably determine the server's fully qualified doma
in name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress th
is message
Syntax OK
[12/22/20]seed@VM:.../sites-available$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
[12/22/20]seed@VM:.../sites-available$ sudo a2ensite default-ssl
Site default-ssl already enabled
[12/22/20]seed@VM:.../sites-available$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for SEEDPKILab2020.com:443 (RSA): *******
[12/22/20]seed@VM:.../sites-available$ firefox
```

此时可以正常访问:



Apache2 Ubuntu Default Page: It works - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://seedpkilab2020.com
Most Visited
SEED Labs
Sites for Labs

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

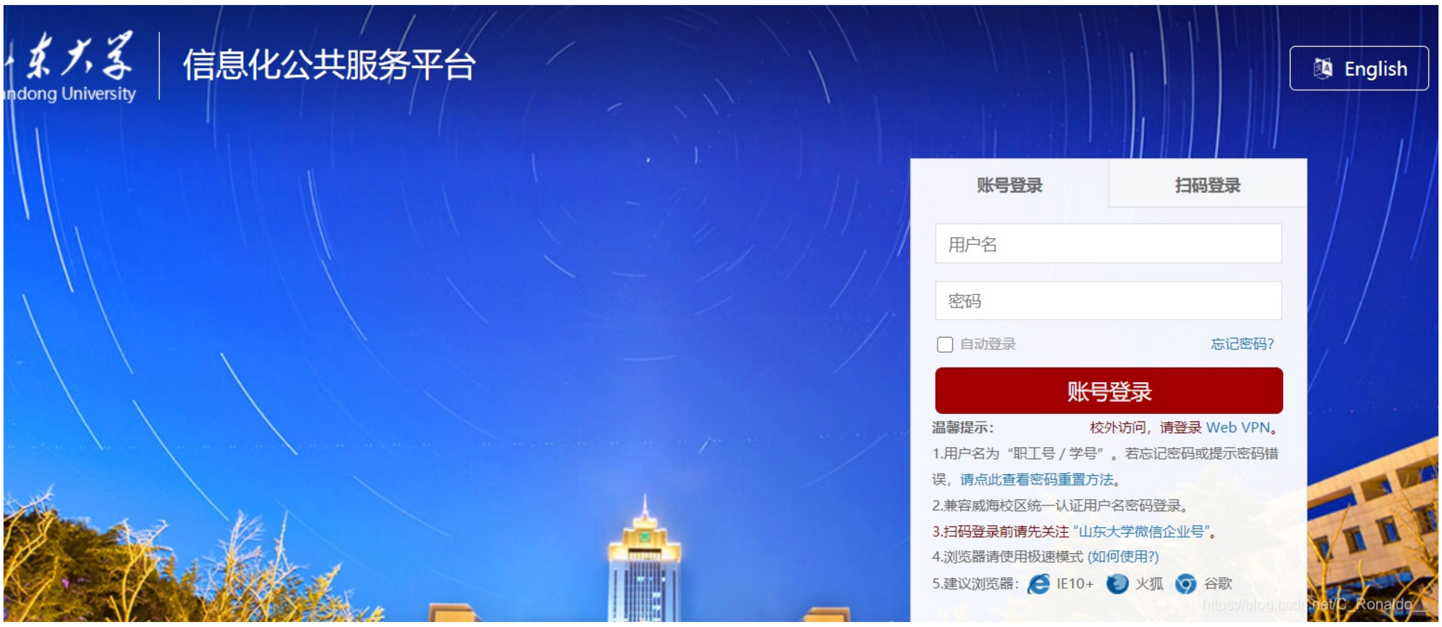
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
```

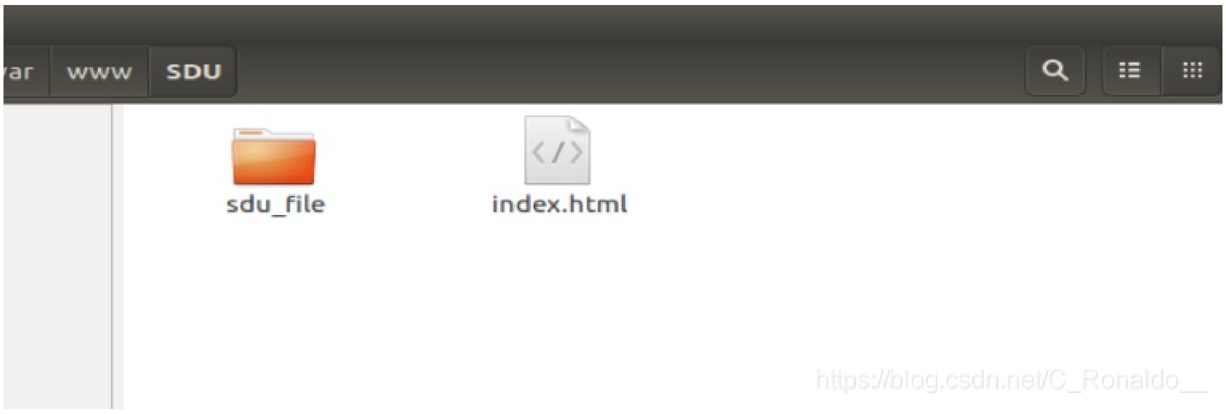
Task 5: Launching a Man-In-The-Middle Attack

本次实验中,我们进行伪造一个pass.sdu.edu.cn网站,真实网站信息:

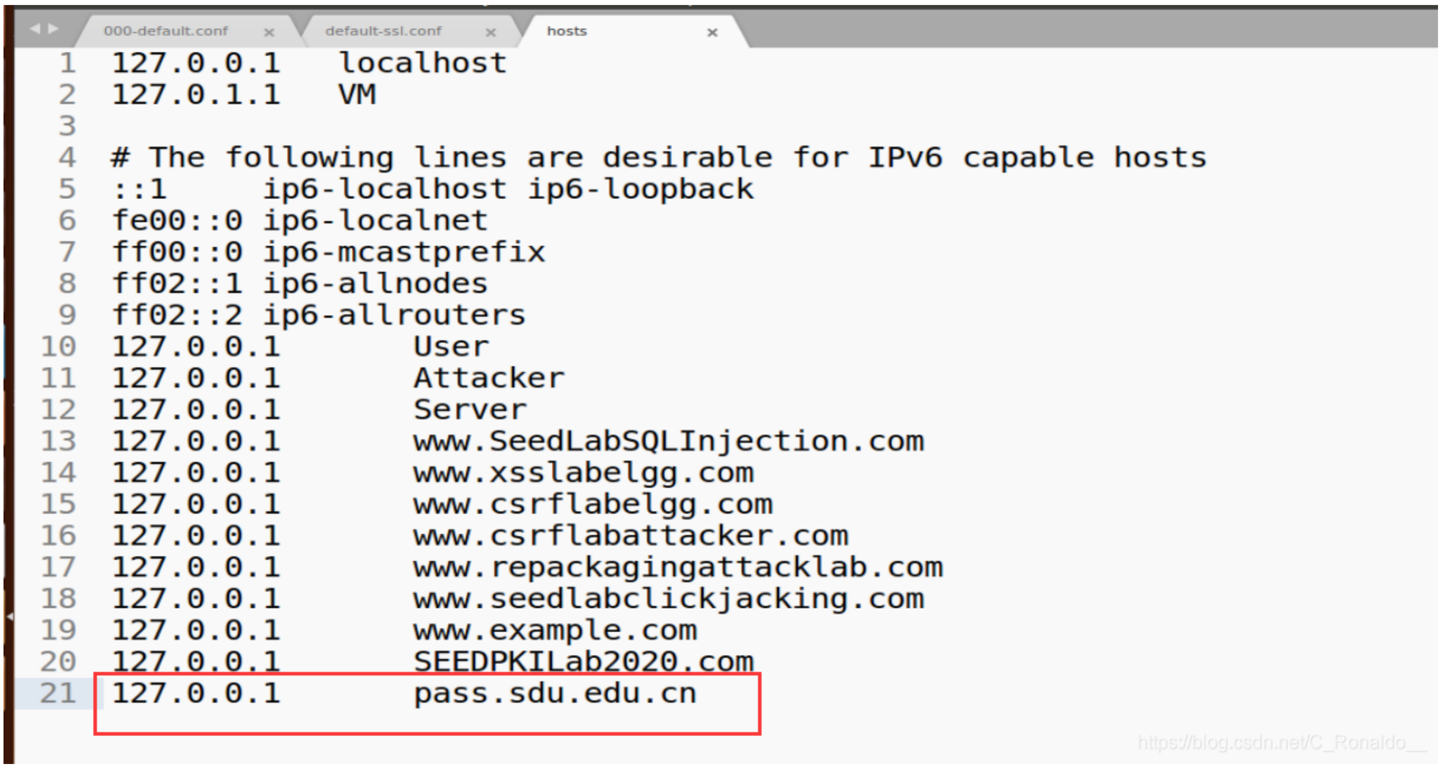


温馨提示: 校外访问，请登录 Web VPN。
1.用户名为“职工号 / 学号”。若忘记密码或提示密码错误，请点此查看密码重置方法。
2.兼容威海校区统一认证用户名密码登录。
3.扫码登录前请先关注“山东大学微信企业号”。
4.浏览器请使用极速模式 (如何使用?)
5.建议浏览器: IE10+ 火狐 谷歌

首先下载网站信息,将网站相关文件该名称(为了方便操作,修改成英文名称),移动到网页指定存储位置,一般为/var/www/目录,创建一个SDU目录,将网站相关信息移动到此目录中:



为了可以在本地访问到,在/etc/hosts配置静态映射:

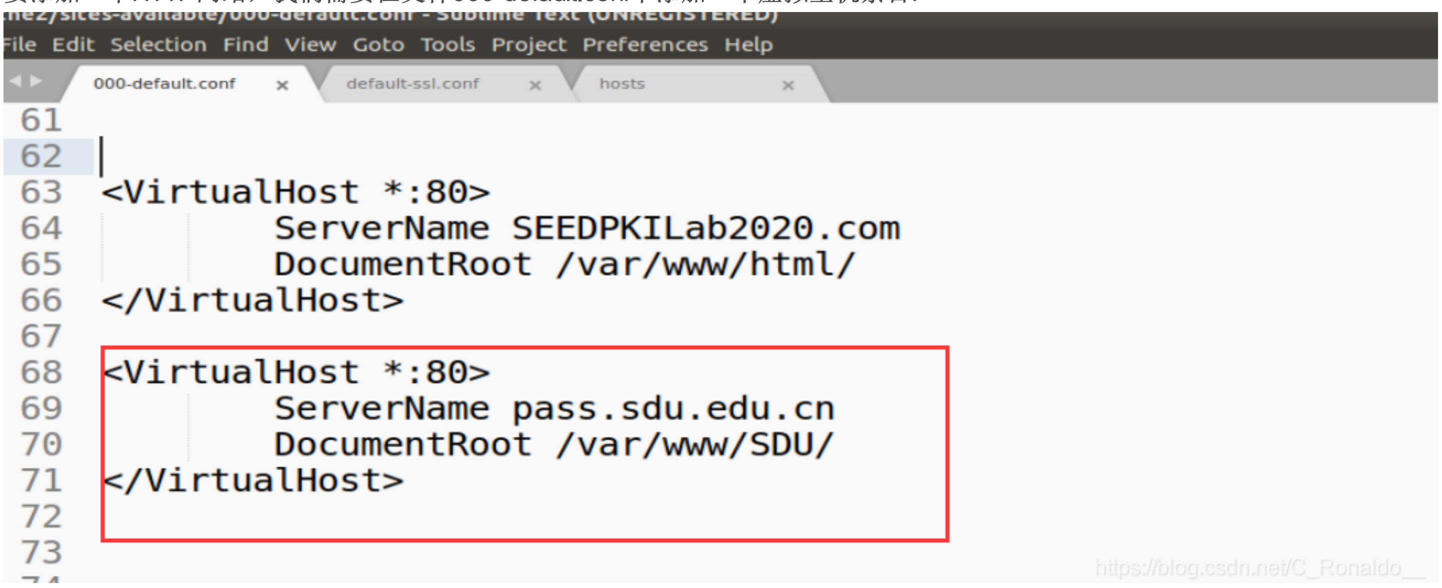


```
127.0.0.1	localhost
127.0.1.1	VM

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
127.0.0.1       www.example.com
127.0.0.1       SEEDPKILab2020.com
127.0.0.1       pass.sdu.edu.cn
```

随后需要到apache2服务器位置进行配置文件配置,文件位置:/etc/apache2/sites-available/:

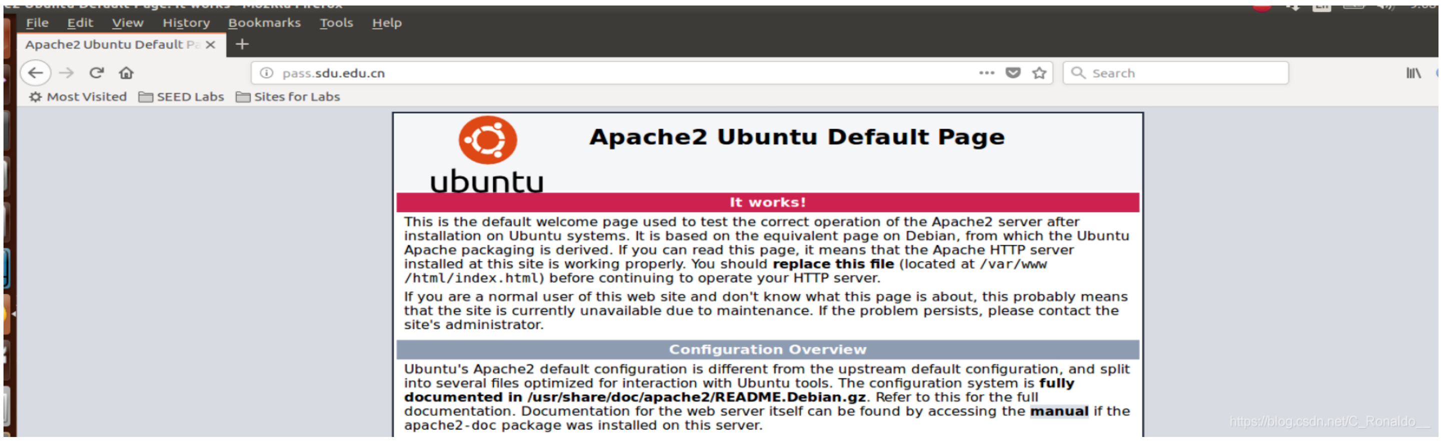
文件000-default.conf:

要添加一个HTTP网站，我们需要在文件000-default.conf中添加一个虚拟主机条目:


ne2/sites-available/000-default.conf - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
000-default.conf
default-ssl.conf
hosts

```


<VirtualHost *:80>
        ServerName SEEDPKILab2020.com
        DocumentRoot /var/www/html/
</VirtualHost>

<VirtualHost *:80>
        ServerName pass.sdu.edu.cn
        DocumentRoot /var/www/SDU/
</VirtualHost>


```

否则显示的网站仍然会是默认配置,显示如下结果:


File Edit View History Bookmarks Tools Help
Apache2 Ubuntu Default Page
pass.sdu.edu.cn
Most Visited SEED Labs Sites for Labs

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

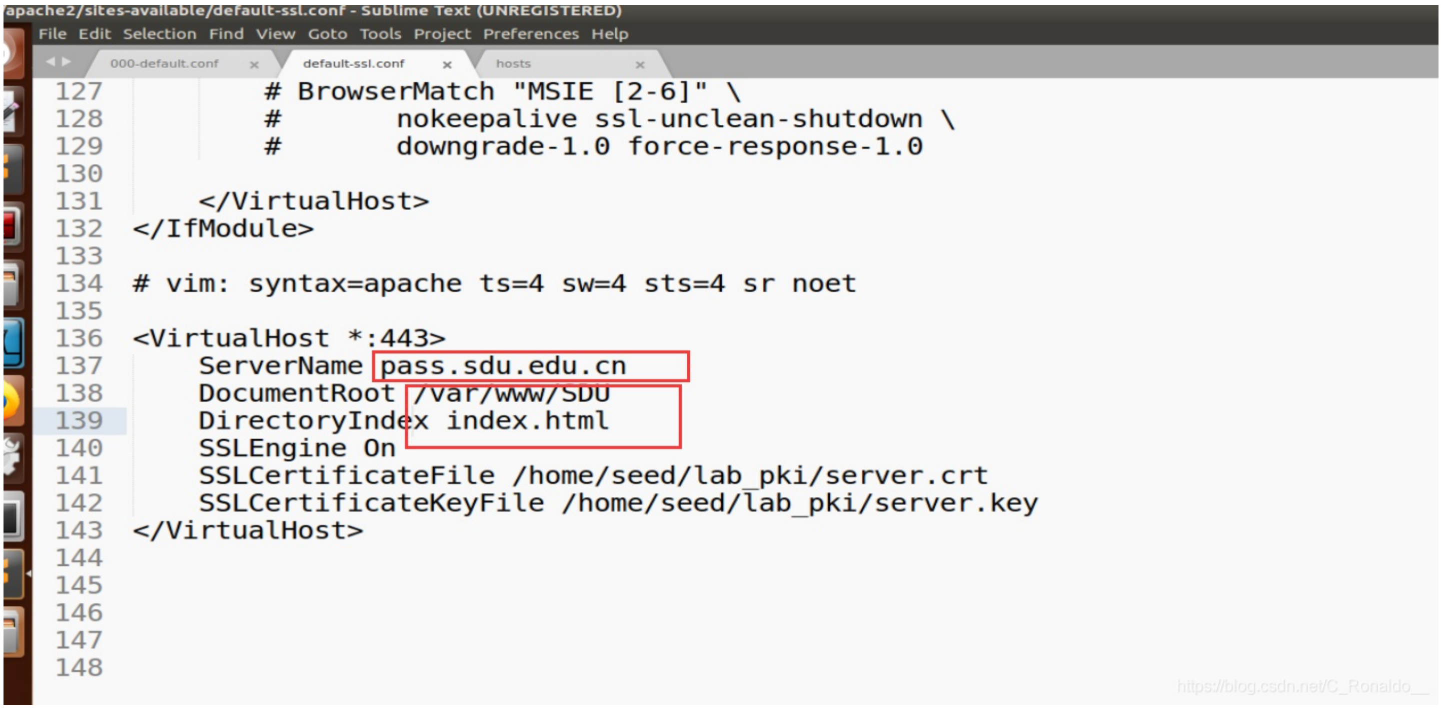
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

就不会显示我们自己配置的网站页面了.

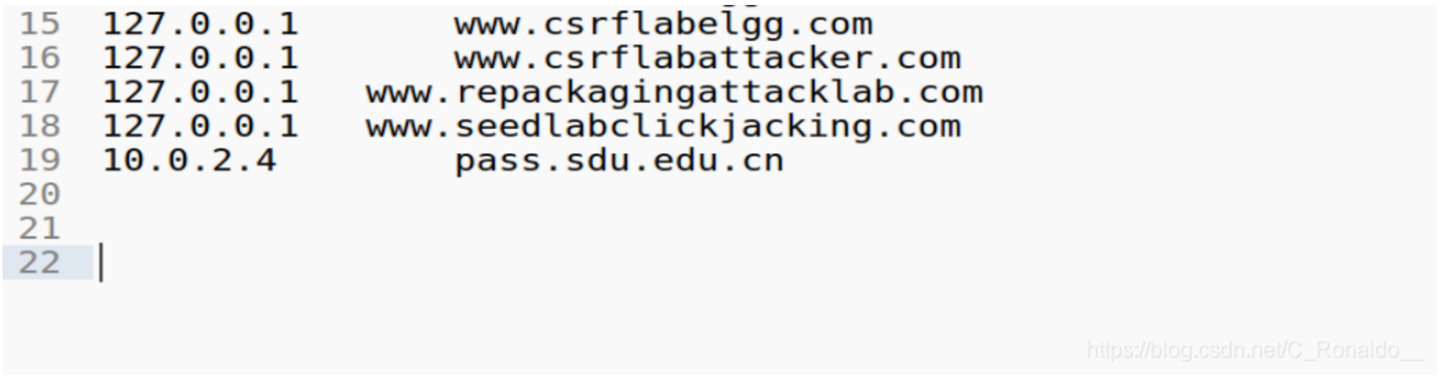
文件**default-ssl.conf**:而要添加一个HTTPS网站，我们则需要在同一个文件夹的default-ssl.conf文件中添加一个VirtualHost条目:


apache2/sites-available/default-ssl.conf - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
000-default.conf default-ssl.conf hosts

```
		#   BrowserMatch "MSIE [2-6]" \
		#		nokeepalive ssl-unclean-shutdown \
		#		downgrade-1.0 force-response-1.0

	</VirtualHost>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

<VirtualHost *:443>
	ServerName pass.sdu.edu.cn
	DocumentRoot /var/www/SDU
	DirectoryIndex index.html
	SSLEngine On
	SSLCertificateFile /home/seed/lab_pki/server.crt
	SSLCertificateKeyFile /home/seed/lab_pki/server.key
</VirtualHost>
```

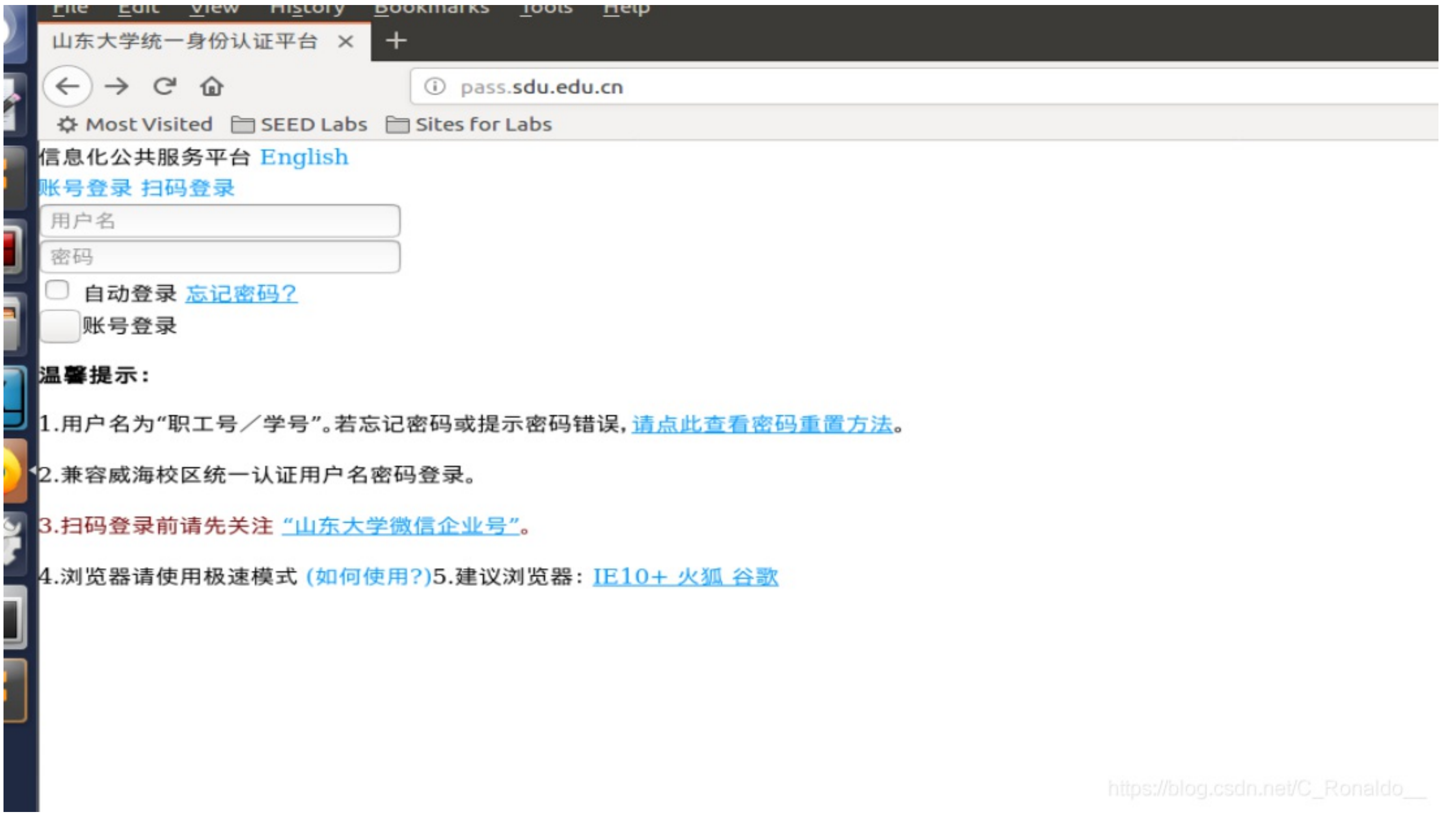
使用10.0.2.5主机进行测试,访问(https://)pass.sdu.edu.cn

在10.0.2.5主机,首先配置/etc/hosts静态映射:



```
127.0.0.1         www.csrflabelgg.com
127.0.0.1         www.csrflabattacker.com
127.0.0.1     www.repackagingattacklab.com
127.0.0.1     www.seedlabclickjacking.com
10.0.2.4          pass.sdu.edu.cn
```

访问pass.sdu.edu.cn得到如下结果:



信息化公共服务平台 English

账号登录 扫码登录

用户名

密码

自动登录 忘记密码?

账号登录

温馨提示:

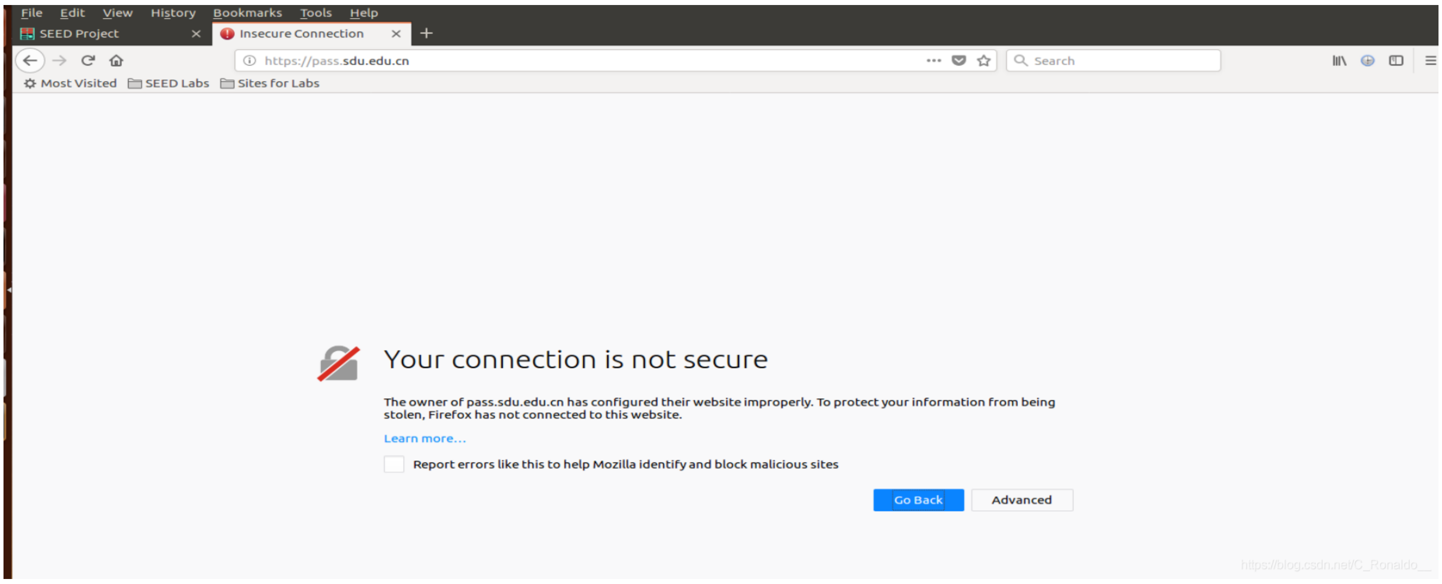
1.用户名为"职工号/学号"。若忘记密码或提示密码错误,请点此查看密码重置方法。

2.兼容威海校区统一认证用户名密码登录。

3.扫码登录前请先关注 "山东大学微信企业号"。

4.浏览器请使用极速模式 (如何使用?)5.建议浏览器: IE10+ 火狐 谷歌

而访问https://pass.sdu.edu.cn 时,会得到如下结果:



Your connection is not secure

The owner of pass.sdu.edu.cn has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

Report errors like this to help Mozilla identify and block malicious sites

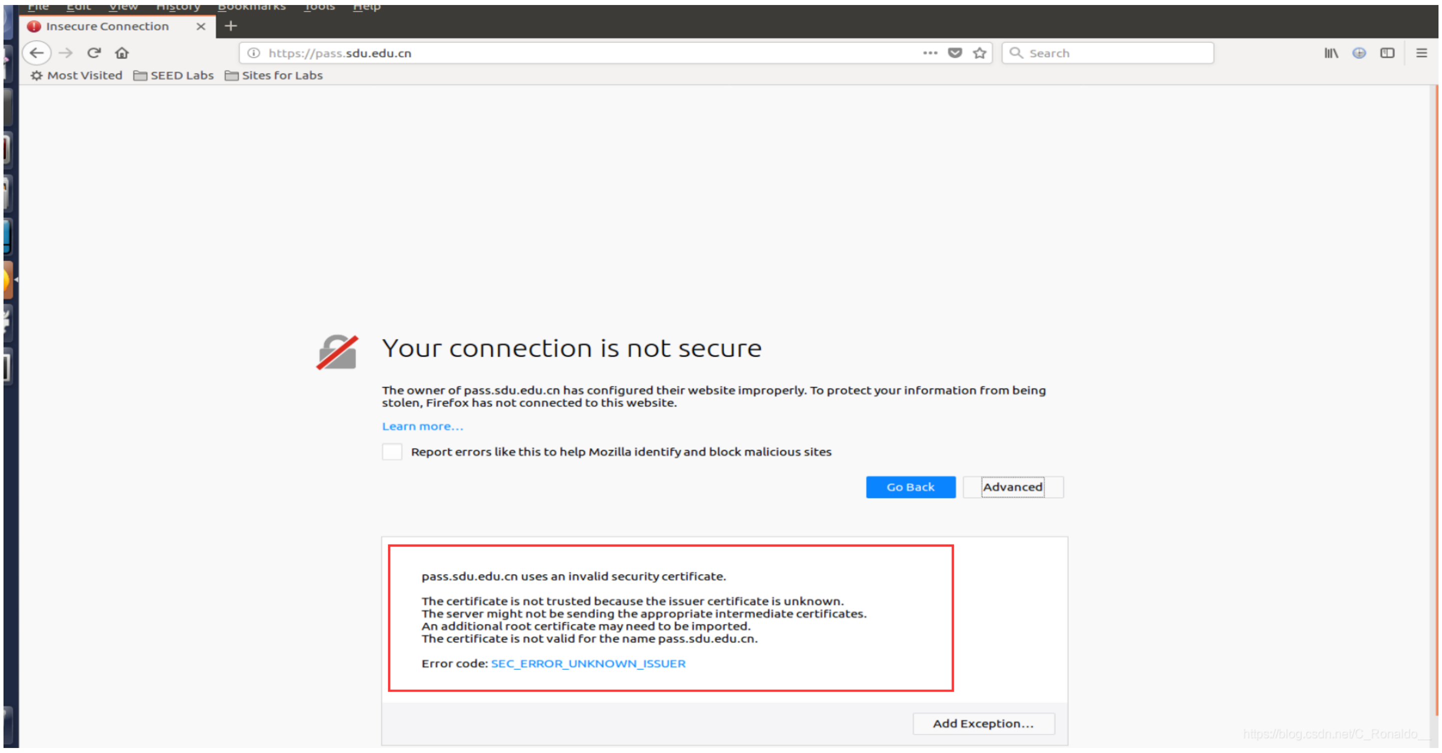
Go Back Advanced

原因分析:

经查阅资料:我们找到浏览器会验证通用名称域,在SSL握手期间,会进行两个重要的验证:

1. 核对接收到的证书是否有效,即确保证书中的公钥属于Subject域描述的主体,但不能说明证书域正在访问的网站是否匹配.SSL库执行
2. 浏览器验证证书通用名称是否与访问的网站名称匹配.浏览器等应用程序执行.
   在上面的实验中:,验证过程:

- 第一条,由于测试主机的浏览器未配置ca.crt,浏览器不会信任此ca发布的证书,不会通过验证.
- 第二条,由于Common Name与访问的pass.sdu.edu.cn不匹配,也不会通过,所以出现警告信息.


Your connection is not secure

The owner of pass.sdu.edu.cn has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

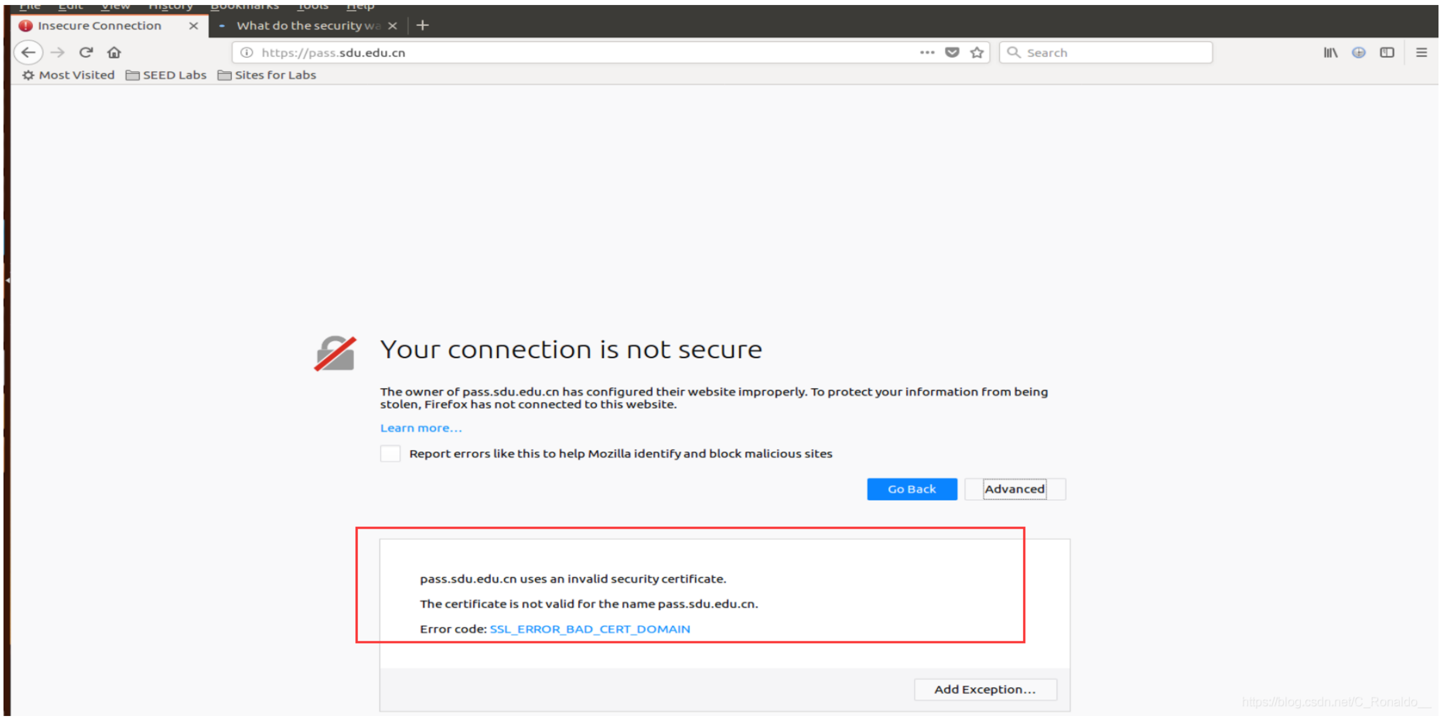
Report errors like this to help Mozilla identify and block malicious sites

pass.sdu.edu.cn uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.
The certificate is not valid for the name pass.sdu.edu.cn.

Error code: SEC_ERROR_UNKNOWN_ISSUER

为了进一步验证上面两条SSL握手规则,我们回到配置Apache服务器主机(10.0.2.4)进行访问pass.sdu.edu.cn,可以正常访问,当时访问https://pass.sdu.edu.cn 时,会失败,得到如下结果:


Your connection is not secure

The owner of pass.sdu.edu.cn has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

Report errors like this to help Mozilla identify and block malicious sites

pass.sdu.edu.cn uses an invalid security certificate.

The certificate is not valid for the name pass.sdu.edu.cn.

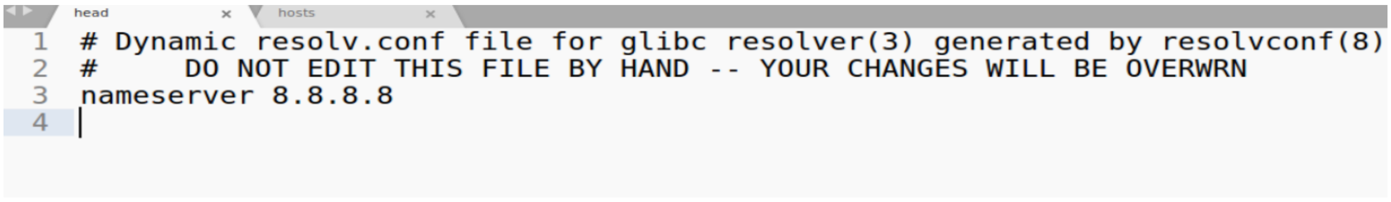
Error code: SSL_ERROR_BAD_CERT_DOMAIN

即第一条通过SSL验证证书成功,但是第二条不通过,浏览器检查发现证书Common Name域访问域名不匹配,出现上面的警告信息.

实验过程中小Tips

在使用10.0.2.5主机进行测试,访问apache文件信息时,我们发现网络断开

- 用wireshark抓包,就发现会出现许多ARP请求报文,最后导致超时错误发生.
- 无法进行ping www.baidu.com , 出现unknown host错误警告信息
- ping 8.8.8.8有回应.
  所以应该是DNS服务器配置错误,不是网络问题,配置dns,由于使用的是DHCP分配协议,所以配置dns的nameserver需要进入/etc/resolvconf/resolv.conf.d/head文件,修改nameserver 127.0.1.1为nameserver 8.8.8.8



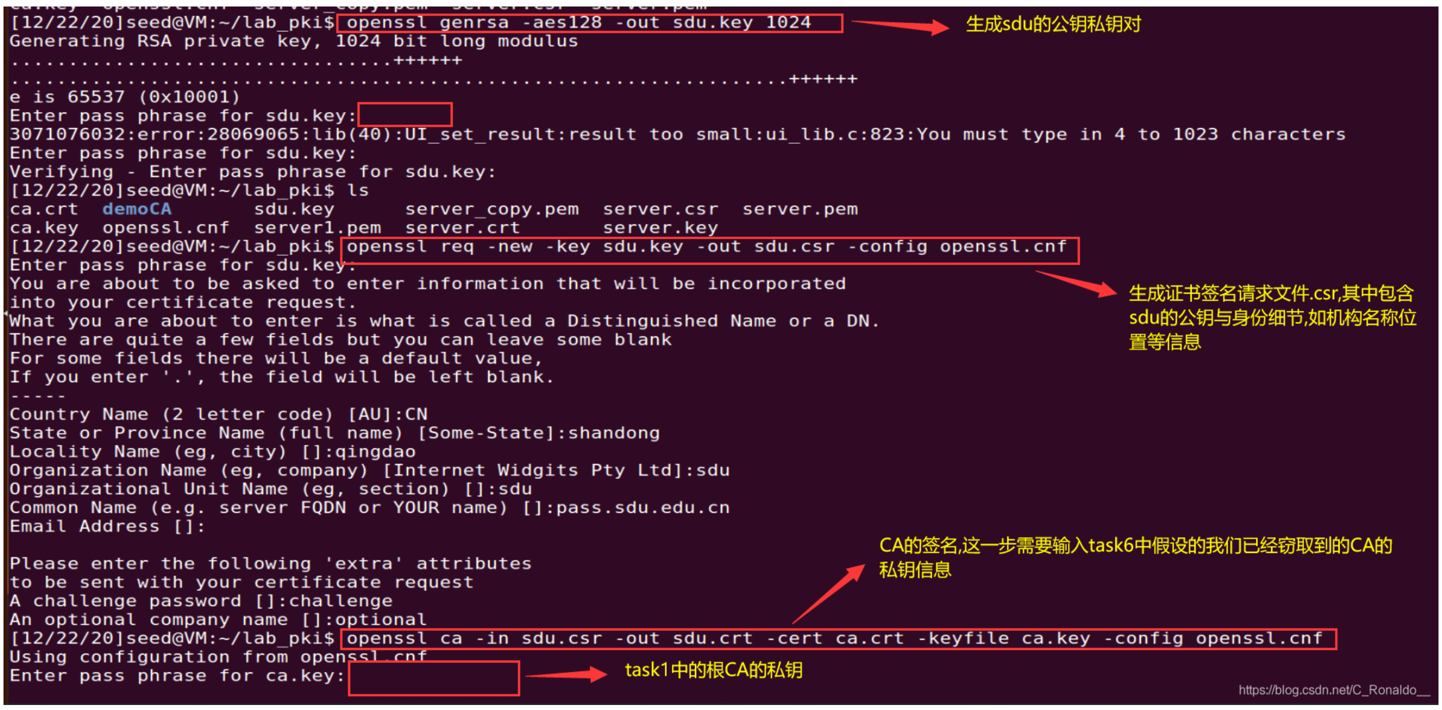
```
# Dynamic resolv.conf file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRN
nameserver 8.8.8.8

```

再运行sudo resolvconf -u即可上网.
但是为什么127.0.1.1不行?可是这个在其他虚拟机是可以上网的,**不知道原因.???,欢迎解答**

Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA

服务器主机:10.0.2.4
测试用户主机:10.0.2.5

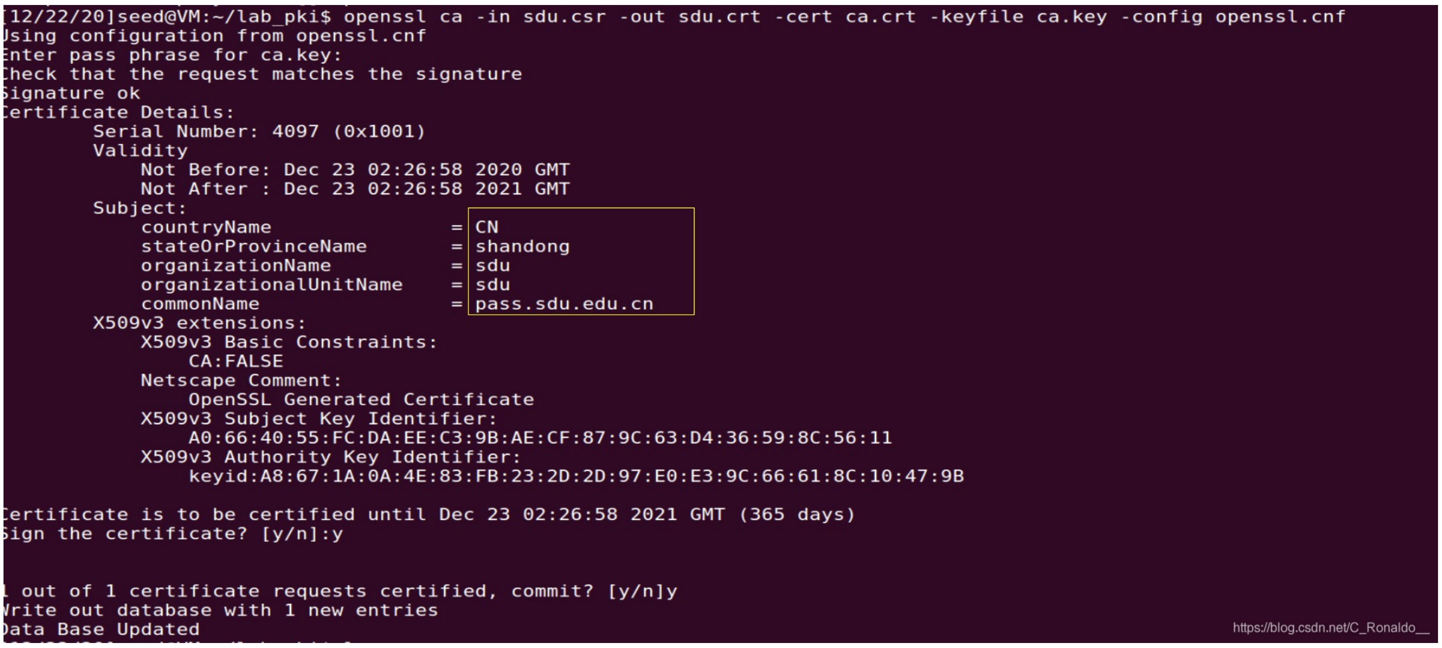
此实验中,我们假设攻击者已经知道根CA的私钥,所以攻击者可以通过CA的私钥伪造一个pass.sdu.edu.cn网站的证书,具体过程如下:



```
[12/22/20]seed@VM:~/lab_pki$ openssl genrsa -aes128 -out sdu.key 1024
Generating RSA private key, 1024 bit long modulus
.................................++++++
...................................................................++++++
e is 65537 (0x10001)
Enter pass phrase for sdu.key:
3071076032:error:28069065:lib(40):UI_set_result:result too small:ui_lib.c:823:You must type in 4 to 1023 characters
Enter pass phrase for sdu.key:
Verifying - Enter pass phrase for sdu.key:
[12/22/20]seed@VM:~/lab_pki$ ls
ca.crt  demoCA       sdu.key      server_copy.pem  server.csr  server.pem
ca.key  openssl.cnf  server1.pem  server.crt       server.key
[12/22/20]seed@VM:~/lab_pki$ openssl req -new -key sdu.key -out sdu.csr -config openssl.cnf
Enter pass phrase for sdu.key:
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]:CN
State or Province Name (full name) [Some-State]:shandong
Locality Name (eg, city) []:qingdao
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sdu
Organizational Unit Name (eg, section) []:sdu
Common Name (e.g. server FQDN or YOUR name) []:pass.sdu.edu.cn
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:challenge
An optional company name []:optional
[12/22/20]seed@VM:~/lab_pki$ openssl ca -in sdu.csr -out sdu.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
```

生成sdu的公钥私钥对
生成证书签名请求文件.csr,其中包含sdu的公钥与身份细节,如机构名称位置等信息
CA的签名,这一步需要输入task6中假设的我们已经窃取到的CA的私钥信息
task1中的根CA的私钥
https://blog.csdn.net/C_Ronaldo__

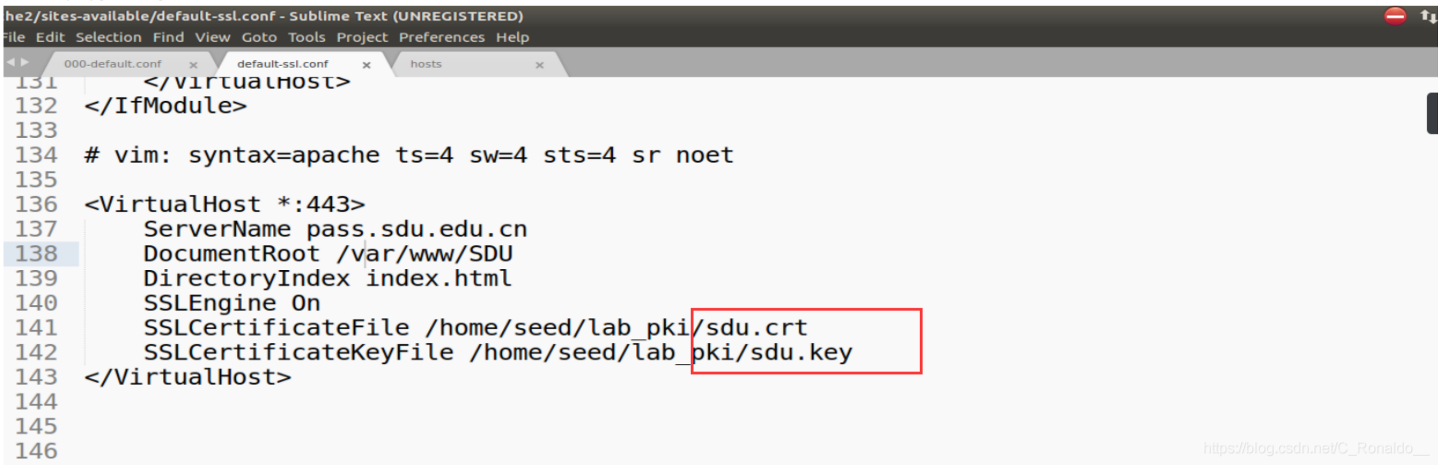
在CA验证与签名过程中,我们需要输入CA的密钥:



```
[12/22/20]seed@VM:~/lab_pki$ openssl ca -in sdu.csr -out sdu.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Dec 23 02:26:58 2020 GMT
            Not After : Dec 23 02:26:58 2021 GMT
        Subject:
            countryName               = CN
            stateOrProvinceName       = shandong
            organizationName          = sdu
            organizationalUnitName    = sdu
            commonName                = pass.sdu.edu.cn
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                A0:66:40:55:FC:DA:EE:C3:9B:AE:CF:87:9C:63:D4:36:59:8C:56:11
            X509v3 Authority Key Identifier:
                keyid:A8:67:1A:0A:4E:83:FB:23:2D:2D:97:E0:E3:9C:66:61:8C:10:47:9B

Certificate is to be certified until Dec 23 02:26:58 2021 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

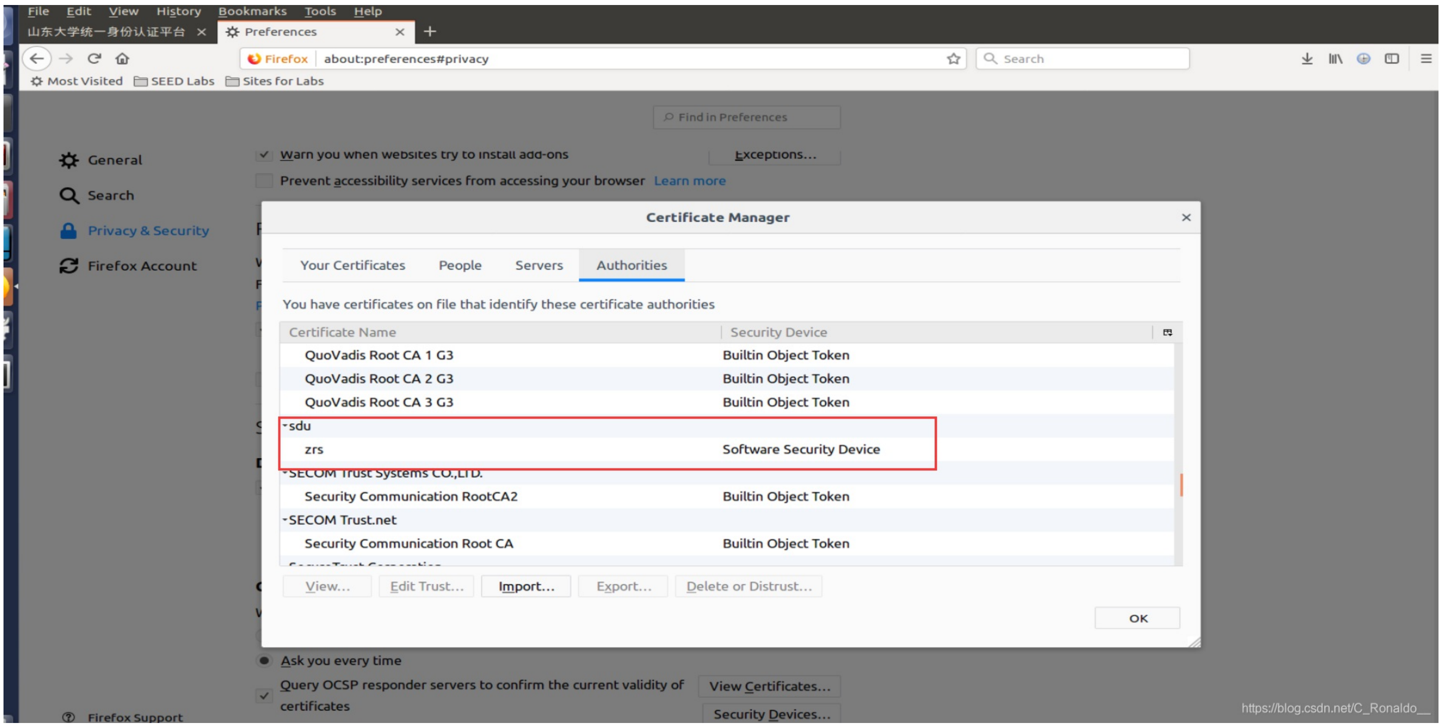
需要注意的是,我们在生成证书过程中对Common Name字段要填写pass.sdu.edu.cn,这样才可以通过task5中写到的浏览器验证阶段.

得到证书文件sdu.crt和私钥文件sdu.key,随后我们需要在apache服务器文件中进行配置相关文件,需要将域名与证书文件进行一一对应处理:


he2/sites-available/default-ssl.conf - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
000-default.conf
default-ssl.conf
hosts

```
    </VirtualHost>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

<VirtualHost *:443>
    ServerName pass.sdu.edu.cn
    DocumentRoot /var/www/SDU
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /home/seed/lab_pki/sdu.crt
    SSLCertificateKeyFile /home/seed/lab_pki/sdu.key
</VirtualHost>
```

随后,我们更换主机,使用另一台主机即10.0.2.5,首先需要在此主机的浏览器中添加CA证书:



Warn you when websites try to install add-ons Exceptions…

Prevent accessibility services from accessing your browser Learn more

Certificate Manager

Your Certificates | People | Servers | Authorities

You have certificates on file that identify these certificate authorities

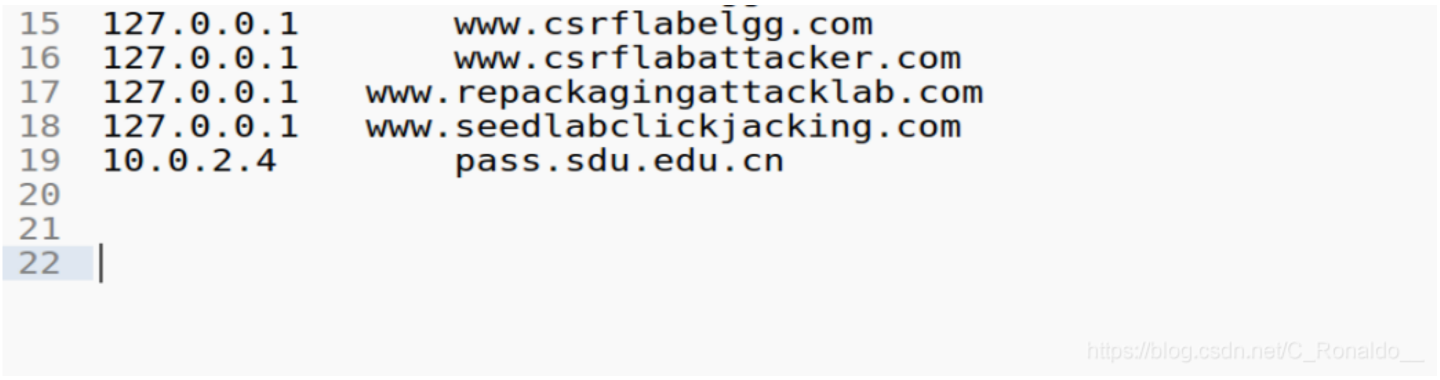
Certificate Name	Security Device
QuoVadis Root CA 1 G3	Builtin Object Token
QuoVadis Root CA 2 G3	Builtin Object Token
QuoVadis Root CA 3 G3	Builtin Object Token
˅sdu	
zrs	Software Security Device
˅SECOM Trust Systems CO.,LTD.	
Security Communication RootCA2	Builtin Object Token
˅SECOM Trust.net	
Security Communication Root CA	Builtin Object Token

View… | Edit Trust… | Import… | Export… | Delete or Distrust… | OK

Ask you every time

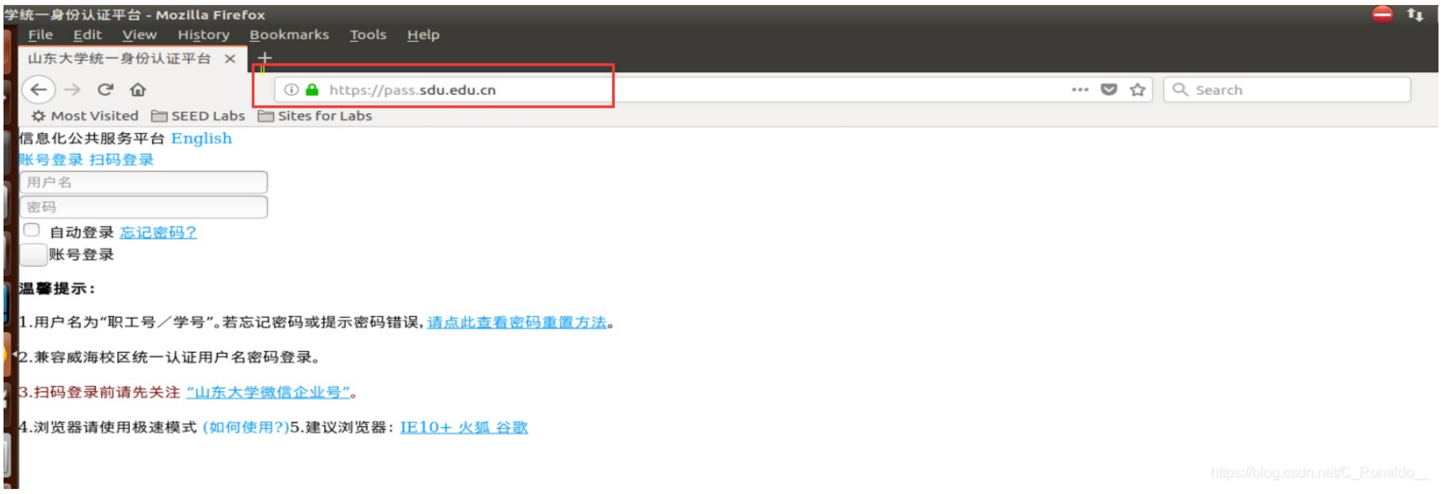
Query OCSP responder servers to confirm the current validity of certificates View Certificates… Security Devices…

同时,在task5中已经设置了etc/hosts中静态IP地址主机名映射关系:



```
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1   www.repackagingattacklab.com
127.0.0.1   www.seedlabclickjacking.com
10.0.2.4        pass.sdu.edu.cn
```

此时,我们就可以进行实验测试了,在task5中访问https://pass.sdu.edu.cn 会出现访问警告问题,由于访问的URL域名与证书中subject域中的Common Name不匹配,而修改了Apache中证书后,可以匹配,所以会成功访问,不会出现安全警告问题:



信息化公共服务平台 English

账号登录 扫码登录

用户名

密码

自动登录 忘记密码?

账号登录

温馨提示:

1.用户名为"职工号/学号"。若忘记密码或提示密码错误,请点此查看密码重置方法。

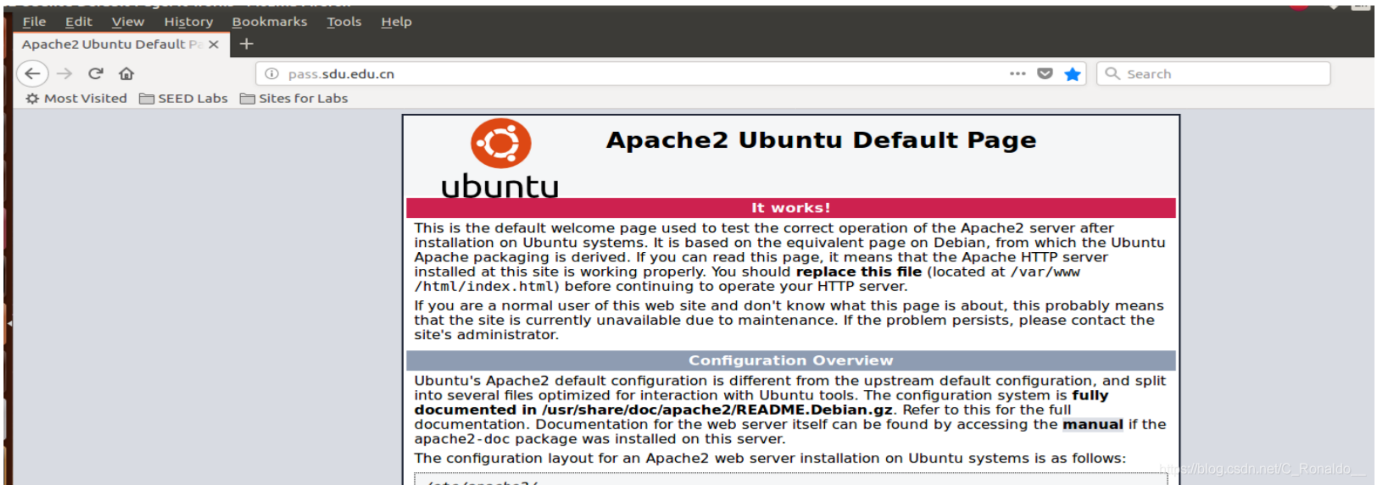
2.兼容威海校区统一认证用户名密码登录。

3.扫码登录前请先关注 "山东大学微信企业号"。

4.浏览器请使用极速模式 (如何使用?)5.建议浏览器: IE10+ 火狐 谷歌

实验总结

1. 本次实验是在期末考试临近期间完成的,时间有些紧迫,写的仓促.虽然任务不太复杂,但由于对Apache服务器了解不是很深,在配置Apache过程遇到了一些问题,呃…其实按照步骤走也没出现问题,主要不理解过程,所以进行了修改部分文件测试,才一步一步地搞明白一点Apache各个文件配置的作用与文件存储位置等信息.
2. 两个配置文件/etc/apache2/sites-available/:
   000-default.conf:HTTP网站默认位置,当访问不带https的网站地址时,apache会到这个文件寻找域名以及对应的网站文件根目录DocumentRoot /var/www/`**`(一般为此位置),然后到网站文件根目录寻找网站页面等相关文件,返回到发送请求的浏览器器中.
   一个网站如果没有对应配置信息,则会显示默认界面,即:



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

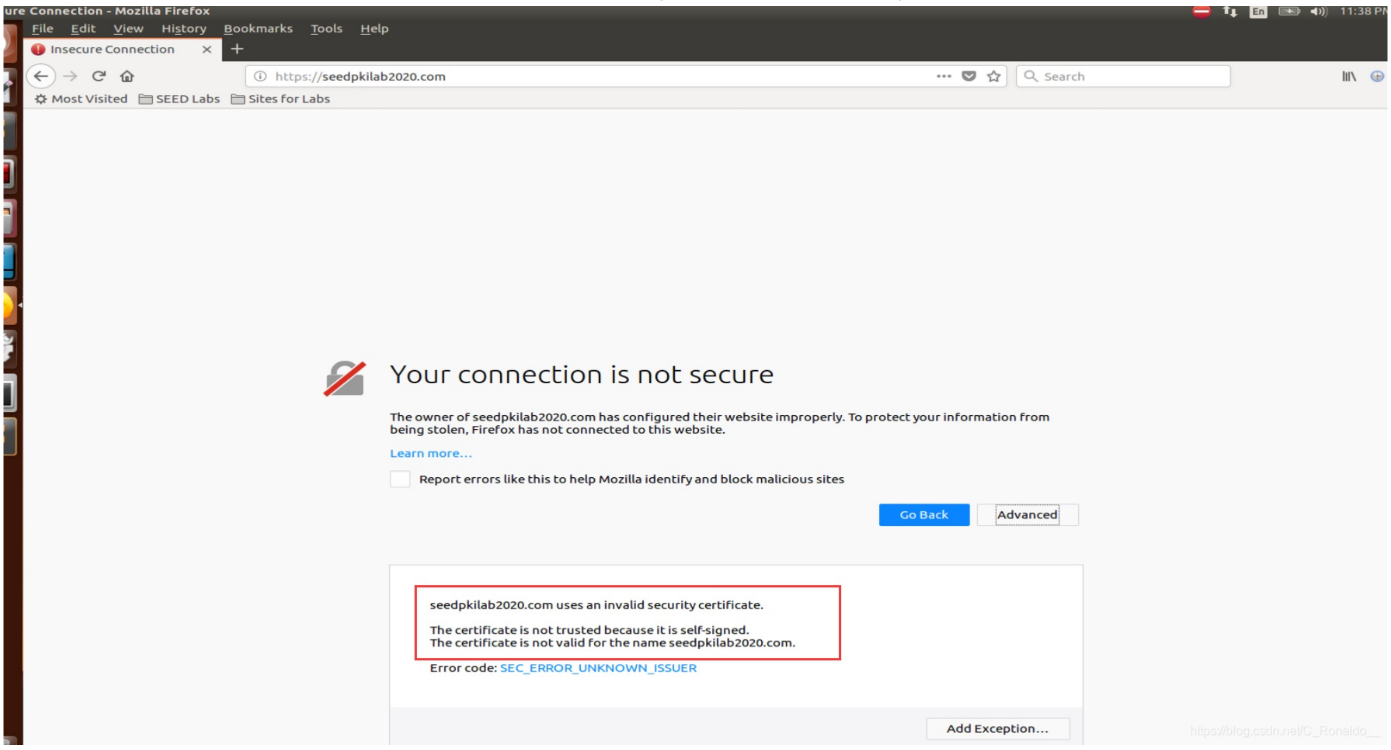
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

   (罗嗦了,前面已经写过这个了…自己摸索好久才搞明白的,就再写一次吧…)
   default-ssl.conf:HTTPS网站配置文件,当访问带有https的网站时,到此文件寻找相关域名,以及这个网站的证书,网页显示相关文件的存储位置根目录DocumentRoot等信息,并返回给发送请求的主机的浏览器中,浏览器再进行验证证书,域名等信息…

如果一个网站配置了default-ssl.conf但没有配置000-default.conf,则访问https可以,访问非https则会显示默认网页,不显示指定网页,这也很符合逻辑.

配置了000-default却没有配置default-ssl.conf,则访问不带https可以正常显示,带https则会出现安全警告:



ure Connection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Insecure Connection
https://seedpkilab2020.com
Search
Most Visited
SEED Labs
Sites for Labs

Your connection is not secure

The owner of seedpkilab2020.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

Report errors like this to help Mozilla identify and block malicious sites

Go Back Advanced

seedpkilab2020.com uses an invalid security certificate.

The certificate is not trusted because it is self-signed.
The certificate is not valid for the name seedpkilab2020.com.

Error code: SEC_ERROR_UNKNOWN_ISSUER

Add Exception…

显示证书验证失败信息,其实压根没有配置证书文件,也符合逻辑.

一个小小实验,使用了快2天时间,还是了解的东西太少,太慢,特别时Web相关信息,不过总算搞明白了apache文件工作机理的一点头绪…