Practical 9

Configuring Apache

(Basic, Secure & Password Protected)

Basic Web Hosting

We will host a website www.student.com on Apache web server. Create a document root directory for this website and an index page.

1) Check the IP address of machine.

```
File  Edit  View  Search  Terminal  Help
[root@localhost ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.100  netmask 255.0.0.0  broadcast 10.255.255.255
        inet6 fe80::20c:29ff:feaf:d3cb  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:af:d3:cb  txqueuelen 1000  (Ethernet)
        RX packets 95  bytes 8277 (8.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35  bytes 4752 (4.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2) Check for httpd package.

```
[root@localhost ~]# rpm -q httpd
httpd-2.4.6-67.el7.x86_64
```

3) Document root directory is /var/www/html and index page is to be save in this directory. Change the directory to /var/www/html and open index.html in vi editor.

```
[root@localhost ~]# cd /var/www/html
[root@localhost html]# vi index.html
```

4) Enter the following contents in the file.

```
<html>
<head>
<title> Hello Title </title>
<body>
<h1> Hello Page </h1>
<p> This is a hello page </p>
</body>
</html>
```

Press **esc :wq** to save and exit from vi editor.

5) Now, change the directory to /etc/httpd/conf and list down its contents.

```
[root@localhost html]# cd /etc/httpd/conf
[root@localhost conf]# ls
httpd.conf  magic
```

6) Copy the httpd.conf file to httpd.conf.sample and open the httpd.conf file using vi editor.

```
[root@localhost conf]# cp httpd.conf httpd.conf.sample
[root@localhost conf]# vi httpd.conf
```

7) Now add the following lines at the end of the file.

```
<VirtualHost 10.0.0.102:80>
ServerAdmin root@www.student.com
ErrorLog logs/student.com_access_error_log
CustomLog logs/student.com_access_log common
</VirtualHost>
```

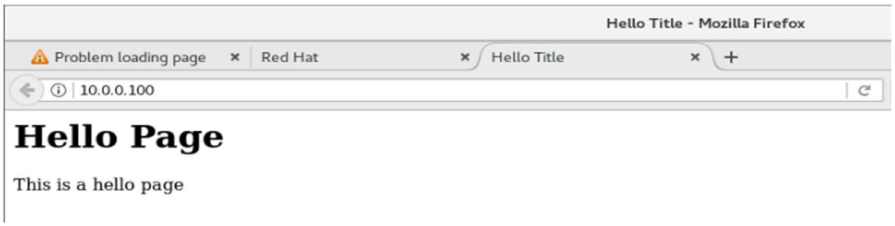
Press **esc :wq** to save and exit from vi editor.

8) Now, restart the httpd service, check status and disable firewall.

```
[root@localhost conf]# systemctl restart httpd
[root@localhost conf]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2024-09-23 13:46:17 IST; 4s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 3498 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 3506 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─3506 /usr/sbin/httpd -DFOREGROUND
           ├─3507 /usr/libexec/nss_pcache 327682 off
           ├─3508 /usr/sbin/httpd -DFOREGROUND
           ├─3509 /usr/sbin/httpd -DFOREGROUND
           ├─3510 /usr/sbin/httpd -DFOREGROUND
           ├─3511 /usr/sbin/httpd -DFOREGROUND
           └─3512 /usr/sbin/httpd -DFOREGROUND

Sep 23 13:46:17 localhost.localdomain systemd[1]: Starting The Apache HTTP Se...
Sep 23 13:46:17 localhost.localdomain httpd[3506]: AH00558: httpd: Could not ...
Sep 23 13:46:17 localhost.localdomain httpd[3506]: [Mon Sep 23 13:46:17.08416...
Sep 23 13:46:17 localhost.localdomain systemd[1]: Started The Apache HTTP Ser...
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost conf]# systemctl stop firewalld
```

9) Go to browser and enter http://10.0.0.10 to test the apache service. If it runs successfully, you will get the following output.



Source Web Hosting

1) Install the utilities to create a self-signed certificate.

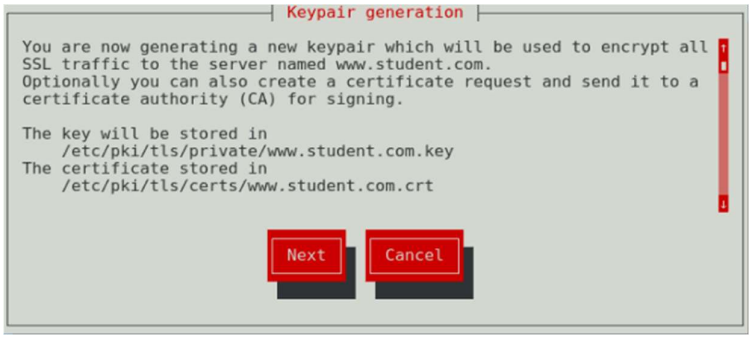
```
[root@localhost conf]# yum install -y crypto-utils mod_ssl
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager
Resolving Dependencies
--> Running transaction check
---> Package crypto-utils.x86_64 0:2.4.1-42.el7 will be installed
--> Processing Dependency: perl(Newt) for package: crypto-utils-2.4.1-42.el7.x86_64
---> Package mod_ssl.x86_64 1:2.4.6-67.el7 will be installed
--> Running transaction check
---> Package perl-Newt.x86_64 0:1.08-36.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved
```

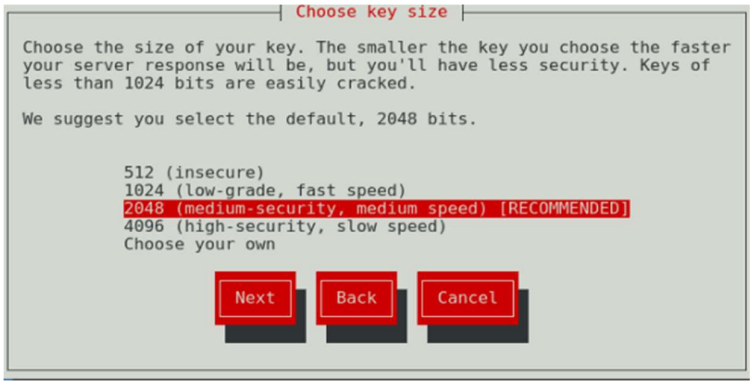
2) Create a certificate for 365 days for the website.

```
[root@localhost ~]# genkey --days 365 www.student.com
```

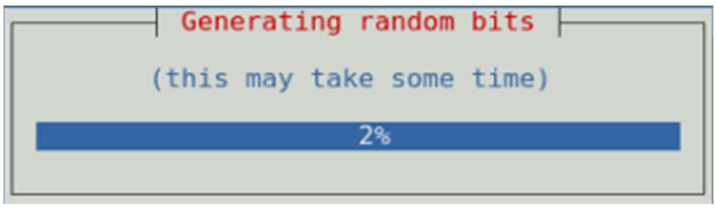
3) The following window appears for Keypair generation. Click on Next.



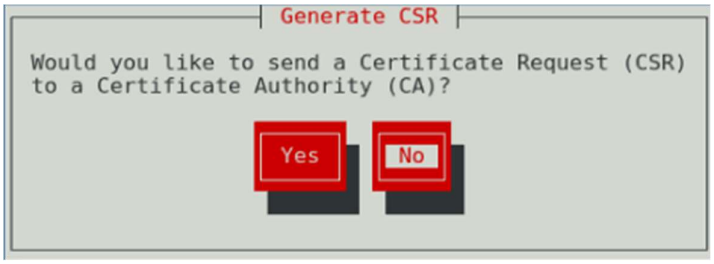
4) Choose the key size as 2048 and click on Next.



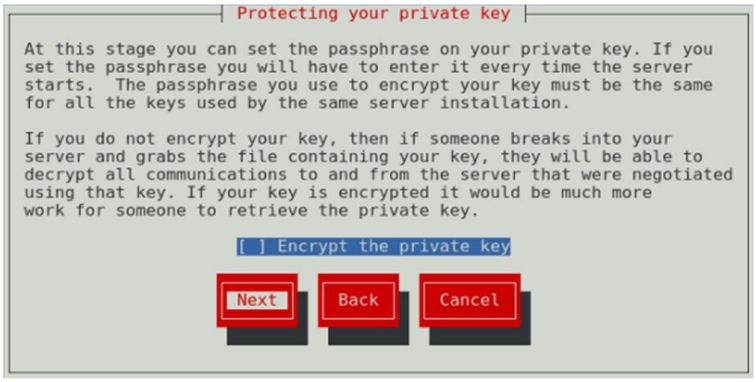
5) It will now start generating random bits.



6) It will now ask to Generate CSR. Click on No.



7) Now, a window for protecting your private key appears. Click on Next.



8) Enter the details for certificate as follows:

9) Now, click on Next and it takes you back to prompt.

```
Generating key. This may take a few moments...

Made a key
Opened tmprequest for writing
/usr/bin/keyutil Copying the cert pointer
Created a certificate
Wrote 1682 bytes of encoded data to /etc/pki/tls/private/www.student.com.key
Wrote the key to:
/etc/pki/tls/private/www.student.com.key
```

10) Open the certificate using following command.

```
[root@localhost ~]# openssl x509 -text < /etc/pki/tls/certs/www.student.com.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3294144037 (0xc458a625)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=IN, ST=Maharashtra, L=Dombivli, O=student.com, CN=www.student.com
        Validity
            Not Before: Sep 23 08:29:49 2024 GMT
            Not After : Sep 23 08:29:49 2025 GMT
        Subject: C=IN, ST=Maharashtra, L=Dombivli, O=student.com, CN=www.student.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e0:b8:0c:97:f5:46:ee:66:6b:e9:7c:d6:aa:29:
                    38:02:48:de:83:71:0e:3a:e1:97:65:f6:88:55:90:
                    18:f5:b9:1d:77:ce:72:d1:7e:8d:b1:80:2d:31:55:
                    ec:0a:35:72:1d:7d:8a:c3:00:07:77:e5:e6:6d:40:
                    71:37:c5:9d:1e:b6:d6:4c:c2:0f:d5:b8:be:60:bd:
                    1d:58:eb:e8:f4:d3:b8:ee:06:9a:a3:c7:3b:ec:3f:
                    a3:4f:d2:49:b4:bf:7f:5c:ab:22:f9:34:f3:42:b7:
                    35:1b:3a:8d:3f:62:34:63:b0:7b:9c:55:d8:00:3f:
                    dc:3c:db:55:14:64:9f:50:90:6e:f4:82:ed:a3:c7:
                    99:03:9f:53:47:78:d0:dd:57:f2:b1:b8:75:66:32:
                    cc:07:fe:b3:97:32:38:de:00:1a:7a:2c:81:e1:7a:
                    66:a4:29:33:fd:d8:93:08:fe:63:3a:c3:ef:8f:4c:
                    42:e7:56:73:ce:9a:5e:77:e6:e9:6a:03:32:9b:75:
                    63:7c:73:50:c1:a1:c7:1d:eb:d0:1a:1e:d3:00:8a:
                    d3:3f:60:dd:78:ee:0b:19:ba:ba:dc:34:b3:75:63:
                    89:23:2e:c8:d1:a0:5f:33:6e:c7:82:8d:bc:3f:82:
                    31:1c:77:c6:de:fa:bc:e5:3c:51:da:bb:65:2f:87:
                    9d:ff
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
         41:50:ce:12:bf:ca:8c:e9:44:a2:92:8f:f1:9a:99:ec:b5:a6:
         0b:40:3e:40:d0:be:ce:1d:e7:94:eb:8d:2c:7a:d0:32:16:f6:
         8d:e1:f4:6d:d3:f1:02:26:81:e0:84:0a:b0:29:17:f4:80:0a:
         62:1f:ca:68:b2:57:6f:0c:99:65:18:f2:b3:91:6c:b8:ed:e4:
         c7:80:96:c2:2a:f7:c4:b7:fd:9a:88:4d:ca:c2:25:34:65:54:
         d3:78:86:25:20:51:35:16:6e:1a:2e:b0:66:c5:af:0d:2a:c9:
         ad:a4:13:37:82:f2:59:72:7d:ea:cf:84:06:da:f8:45:c3:83:
         2c:5e:68:96:67:97:20:57:a5:99:c0:41:bd:78:e3:1b:e3:51:
         fd:3f:1e:26:dd:9d:ff:76:b6:01:64:30:53:2f:6e:bf:44:97:
         d9:58:db:d8:90:1e:7e:3e:39:15:b2:a0:f2:f9:75:de:bb:8c:
         6e:d1:ec:00:26:78:c9:27:b1:5f:f2:a9:a4:2e:53:4b:37:52:
         01:08:de:de:74:3b:51:19:ba:45:3b:c2:a9:3f:79:a7:f3:fa:
         8d:6a:cf:ec:88:b3:12:af:a5:57:0e:c0:f7:e2:15:0f:82:d4:
         87:d6:b3:0f:44:cb:79:f0:5d:7e:e3:16:3f:c6:47:d3:3c:c8:
         e1:ec:b4:68
-----BEGIN CERTIFICATE-----
MIIDSTCCAjGgAwIBAgIFAMRYpiUwDQYJKoZIhvcNAQEFBQAwZjELMAkGA1UEBhMC
SU4xFDASBgNVBAgTC01haGFyYXNodHJhMREwDwYDVQQHEwhEb21iaXZsaTEUMBIG
A1UEChMLc3R1ZGVudC5jb20xGDAWBgNVBAMTD3d3dy5zdHVkZW50LmNvbTAeFw0y
NDA5MjMwODI5NDlaFw0yNTA5MjMwODI5NDlaMGYxCzAJBgNVBAYTAklOMRQwEgYD
VQQIEwtNYWhhcmFzaHRyYTERMA8GA1UEBxMIRG9tYml2bGkxFDASBgNVBAoTC3N0
dWRlbnQuY29tMRgwFgYDVQQDEw93d3cuc3R1ZGVudC5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDguAyX9UbuZmvpfNaqKTgCSN6DcQ464Zdl9ohV
kBj1uR13znLRfo2xgC0xVewKNXIdfYrDAAd35eZtQHE3xZ0ettZMwg/VuL5gvR1Y
6+j007juBpqjxzvsP6NP0km0v39cqyL5NPNCtzUbOo0/YjRjsHucVdgAP9w821UU
ZJ9QkG70gu2jx5kDn1NHeNDdV/KxuHVmMswH/rOXMjjeABp6LIHhemakKTP92JMI
/mM6w++PTELnVnPOml535ulqAzKbdWN8c1DBoccd69AaHtMAitM/YN147gsZurrc
NLN1Y4kjLsjRoF8zbseCjbw/gjEcd8be+rzlPFHau2Uvh53/AgMBAAEwDQYJKoZI
hvcNAQEFBQADggEBAEFQzhK/yozpRKKSj/Gamey1pgtAPkDQvs4d55TrjSx60DIW
9o3h9G3T8QImgeCECrApF/SACmIfymiyV28MmWUY8rORbLjt5MeAlsIq98S3/ZqI
TcrCJTRlVNN4hiUgUTUWbhousGbFrw0qya2kEzeC8llyferPhAba+EXDgyxeaJZn
lyBXpZnAQb144xvjUf0/Hibdnf92tgFkMFMvbr9El9lY29iQHn4+ORWyoPL5dd67
jG7R7AAmeMknsV/yqaQuU0s3UgEI3t50O1EZukU7wqk/eafz+o1qz+yIsxKvpVcO
wPfiFQ+C1IfWsw9Ey3nwXX7jFj/GR9M8yOHstGg=
-----END CERTIFICATE-----
```

11) Change the directory to etc/httpd/conf.d and list down its contents. Copy the ssl.conf to ssl.conf.sample and open the ssl.conf using vi editor.

```
[root@localhost ~]# cd /etc/httpd/conf.d
[root@localhost conf.d]# ls
autoindex.conf  lookup_identity.conf  nss.conf  README  ssl.conf  userdir.conf  welcome.conf
[root@localhost conf.d]# cp ssl.conf ssl.conf.sample
[root@localhost conf.d]# vi ssl.conf
```

12) Make following changes in the file.

```
<VirtualHost 10.0.0.100:443>

# General setup for the virtual host, inherited from global configuration
DocumentRoot "/var/www/html"
ServerName www.student.com:443

# Use separate log files for the SSL virtual host; note that LogLevel
# is not inherited from httpd.conf.
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

#   SSL Protocol support:
# List the enable protocol levels with which clients will be able to
# connect.  Disable SSLv2 access by default:
SSLProtocol all -SSLv2
```

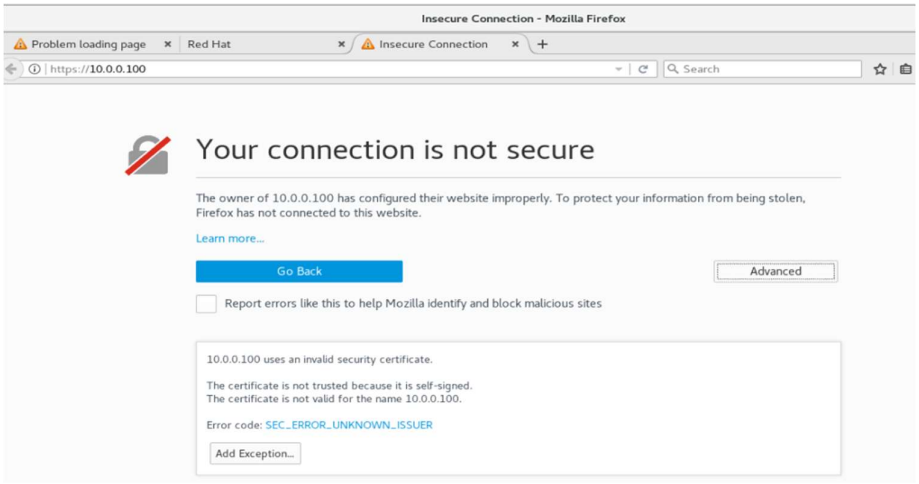
Press **esc :wq** to save and exit from vi editor.

13) Restart the httpd service, check its status and disable firewall.

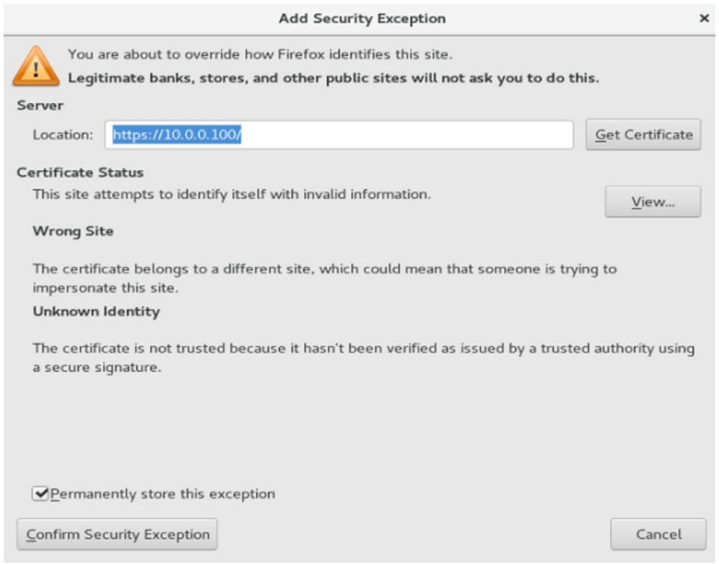
```
[root@localhost conf.d]# systemctl restart httpd
[root@localhost conf.d]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: d:
   Active: active (running) since Mon 2024-09-23 14:21:48 IST; 40s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 4976 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 4983 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─4983 /usr/sbin/httpd -DFOREGROUND
           ├─4985 /usr/libexec/nss_pcache 622595 off
           ├─4986 /usr/sbin/httpd -DFOREGROUND
           ├─4987 /usr/sbin/httpd -DFOREGROUND
           ├─4988 /usr/sbin/httpd -DFOREGROUND
           ├─4989 /usr/sbin/httpd -DFOREGROUND
           └─4990 /usr/sbin/httpd -DFOREGROUND

Sep 23 14:21:47 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
Sep 23 14:21:48 localhost.localdomain httpd[4983]: AH00558: httpd: Could not reliabl
Sep 23 14:21:48 localhost.localdomain httpd[4983]: [Mon Sep 23 14:21:48.006364 2024]
Sep 23 14:21:48 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost conf.d]# systemctl stop firewalld
```

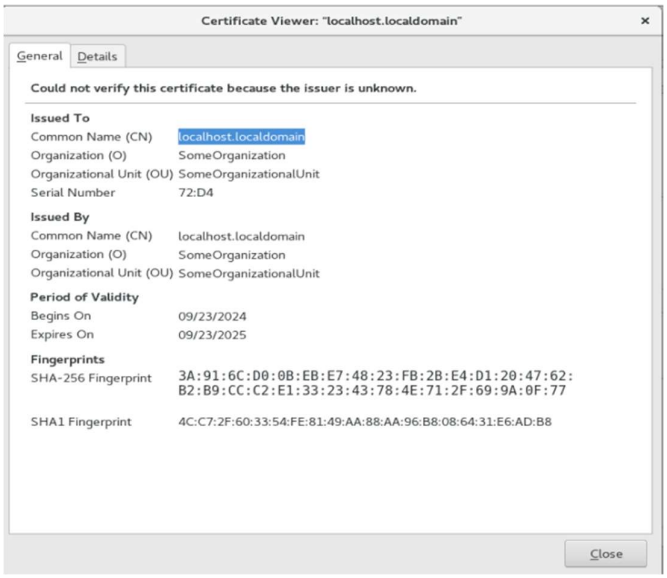
14) Go to browser and type https://10.0.0.100 It shows that the connection is not secure.



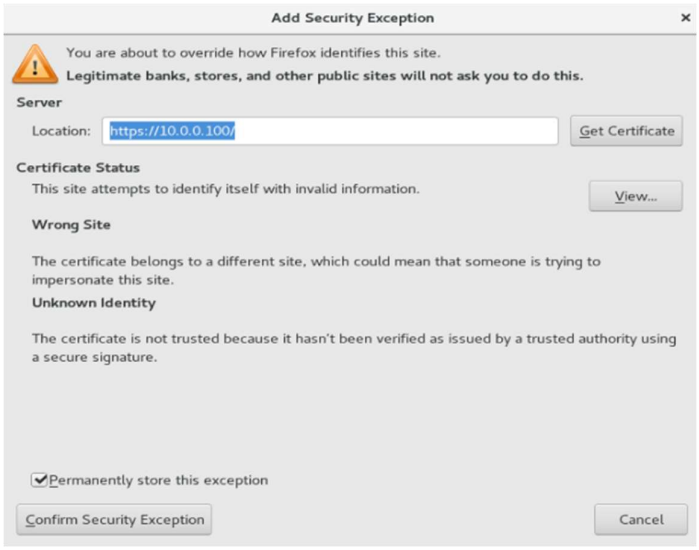
15) Click on Advanced and then Click on Add Exception.



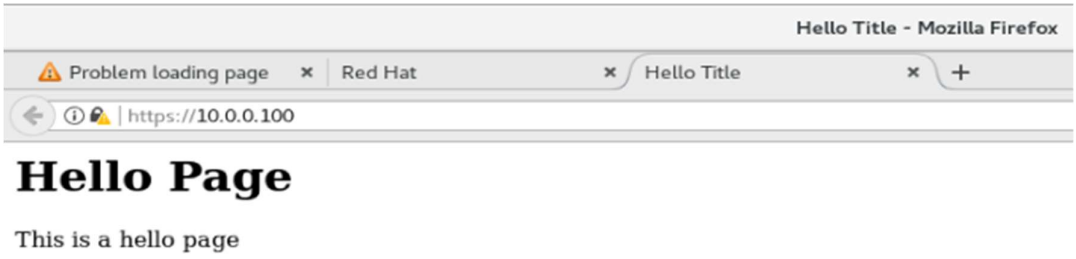
16) Click on View.



17) Close it and go back to previous window and click on Confirm Security Exception.



18) Your website will now be visible.



Password Protected Web Hosting

1) Open the httpd.conf file in the /etc/httpd/conf directory.

```
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf
[root@localhost ~]#
```

2) Make following changes in the file.

```
102 <Directory /var/www/html>
103     AllowOverride AuthConfig
104     Require valid-user
105 </Directory>
```

3) Create a hidden file httpasswd in the /etc/httpd directory and create a user apache01.

```
[root@localhost ~]# htpasswd -c /etc/httpd/.htpasswd apache01
New password:
Re-type new password:
Adding password for user apache01
[root@localhost ~]#
```

4) Display the contents of hidden file.

```
[root@localhost ~]# cat /etc/httpd/.htpasswd
apache01:$apr1$WrZs9HDc$asGiL8o./6NvgTVc7Hp0X1
[root@localhost ~]#
```

5) Create a hidden file with name htaccess in /var/www/html directory.

```
[root@localhost ~]# vi /var/www/html/.htaccess
```

6) Enter following contents in the file.

```
AuthType Basic
AuthName "Password Protected Website, Please provide valid credentials"
AuthUserFile /etc/httpd/.htpasswd
Require valid-user
```

Press **esc :wq** to save and exit from vi editor.

7) Go to /etc/httpd/conf.d directory and make changes in the ssl.conf file.

```
[root@localhost ~]# cd /etc/httpd/conf.d
[root@localhost conf.d]# ls
autoindex.conf  lookup_identity.conf  nss.conf  README  ssl.conf  ssl.conf.sample  userdir.conf  welcome.conf
[root@localhost conf.d]# vi ssl.conf
```

8) Add following lines in the file.

```
178 <Directory "/var/www/html">
179     AllowOverride AuthConfig
180 </Directory>
181
```

Press **esc :wq** to save and exit from vi editor.

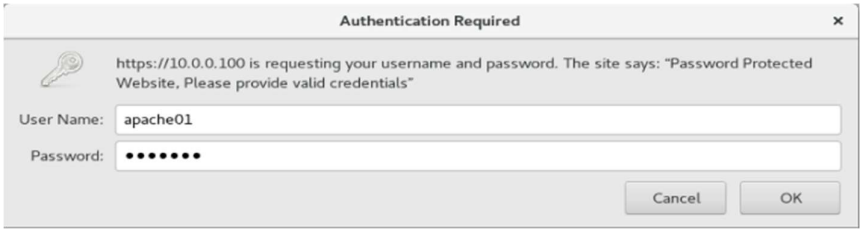
9) Restart httpd service, check its status and disable firewall.

```
[root@localhost conf.d]# systemctl restart httpd
[root@localhost conf.d]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled
   Active: active (running) since Mon 2024-09-23 15:12:11 IST; 15s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 6118 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 6125 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─6125 /usr/sbin/httpd -DFOREGROUND
           ├─6127 /usr/libexec/nss_pcache 917507 off
           ├─6128 /usr/sbin/httpd -DFOREGROUND
           ├─6129 /usr/sbin/httpd -DFOREGROUND
           ├─6130 /usr/sbin/httpd -DFOREGROUND
           ├─6131 /usr/sbin/httpd -DFOREGROUND
           └─6132 /usr/sbin/httpd -DFOREGROUND

Sep 23 15:12:10 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
Sep 23 15:12:10 localhost.localdomain httpd[6125]: AH00558: httpd: Could not reliably deter
Sep 23 15:12:10 localhost.localdomain httpd[6125]: [Mon Sep 23 15:12:10.932371 2024] [core:
Sep 23 15:12:11 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost conf.d]# systemctl stop firewalld
```

(clear history before accessing the website)

10) Access the website from the browser. You will get the following window. Enter user name and password and click on ok.



11) Now the website is visible.