

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5

дисциплина: Администрирование сетевых подсистем

Расширенная настройка HTTP-сервера Apache

Студент: Танрибергенов Эльдар

Группа: НПИбд-02-20

МОСКВА

2023 г.

Цель работы:

Приобретение практических навыков по расширенному конфигурированию HTTP-сервера Apache в части безопасности и возможности использования PHP.

Ход работы:

1. Конфигурирование HTTP-сервера для работы через протокол HTTPS

1. Загрузите вашу операционную систему и перейдите в рабочий каталог с проектом

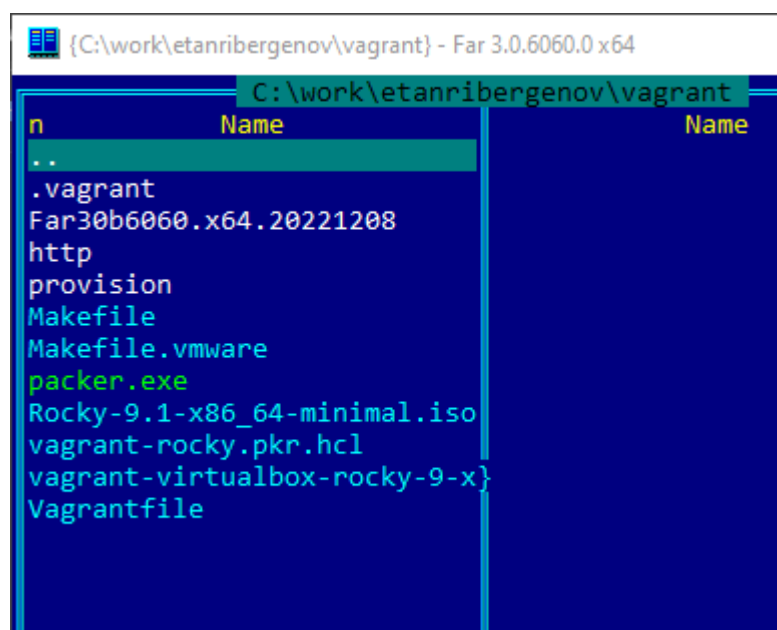
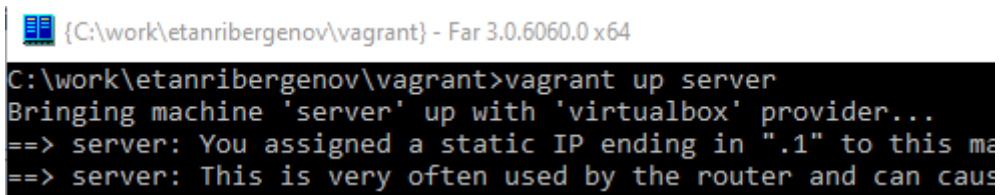


Рис. 1. Рабочий каталог

2. Запустите виртуальную машину server



```
{C:\work\etanribergenov\vagrant} - Far 3.0.6060.0 x64
C:\work\etanribergenov\vagrant>vagrant up server
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".1" to this ma
==> server: This is very often used by the router and can caus
```

Рис. 2. Запуск ВМ server.

3. На виртуальной машине server войдите под вашим пользователем и откройте терминал.
Перейдите в режим суперпользователя

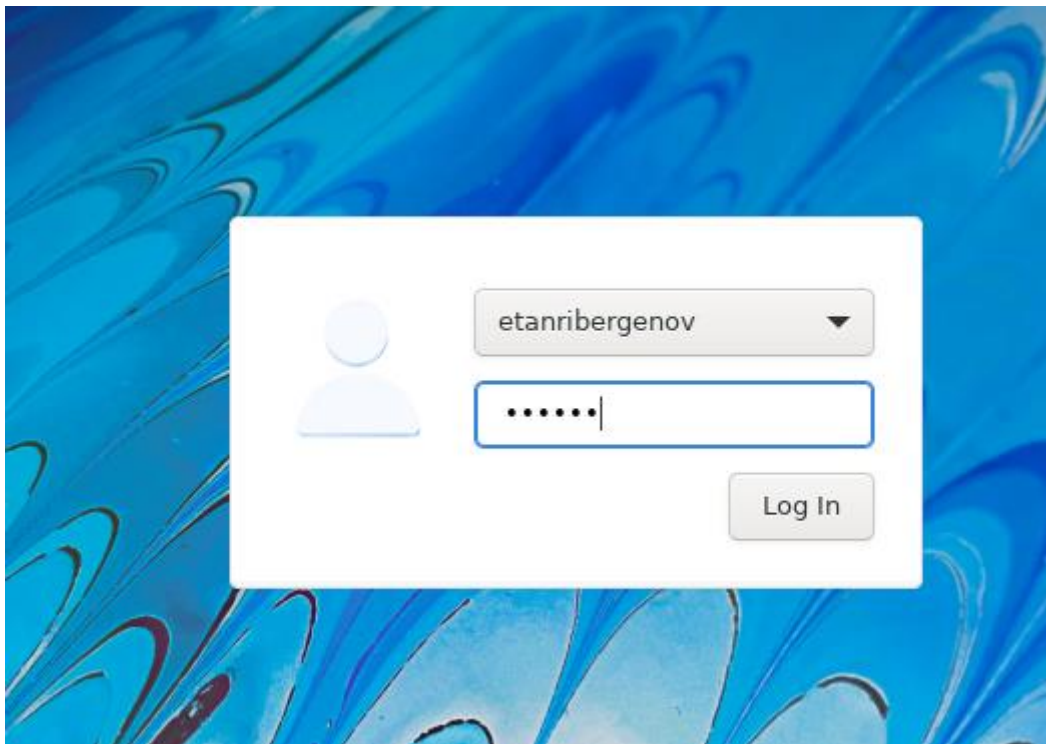
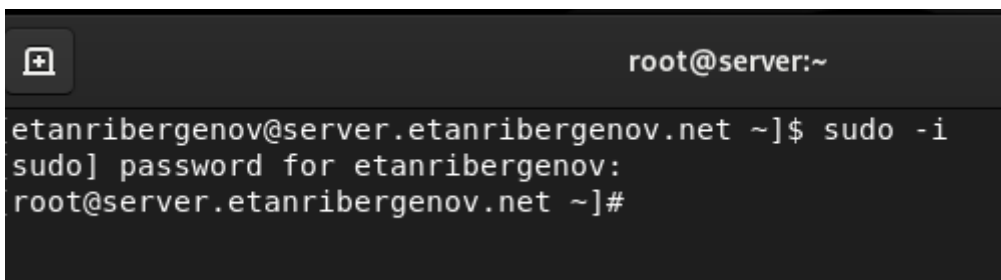


Рис. 3. Вход в систему



```
root@server:~
etanribergenov@server.etanribergenov.net ~]$ sudo -i
[sudo] password for etanribergenov:
root@server.etanribergenov.net ~]#
```

Рис. 4. Переход в режим суперпользователя

4. В каталоге /etc/ssl создайте каталог private

```
[root@server.etanribergenov.net ~]# mkdir -p /etc/ssl/private
[root@server.etanribergenov.net ~]#
```

Рис. 5. Создание каталога /etc/ssl/private

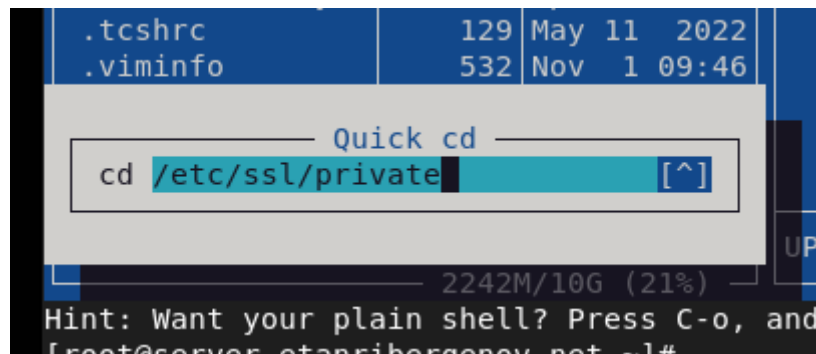


Рис. 6. Переход в каталог /etc/ssl/private

Сгенерируйте ключ и сертификат, используя следующую команду

```
openssl req -x509 -nodes -newkey rsa:2048 -keyout www.user.net.key -out www.user.net.crt
```

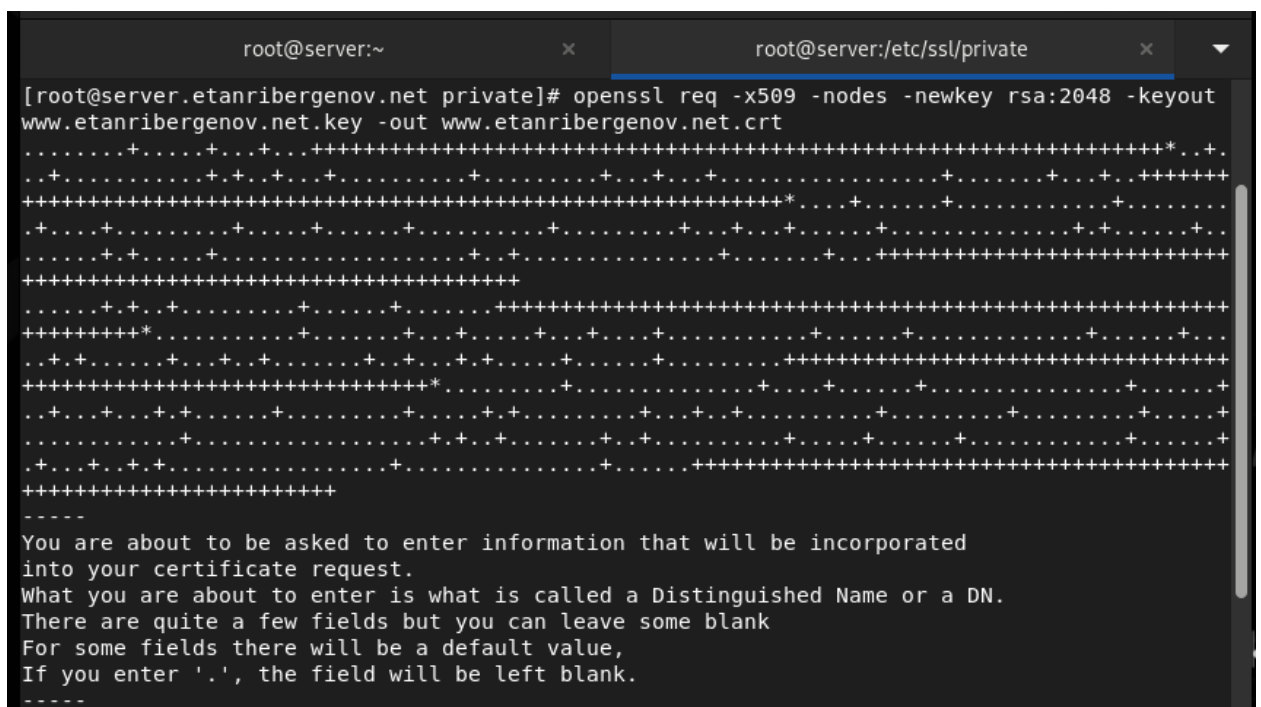


Рис. 7. Генерация ключа и сертификата

```
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:Russia
Locality Name (eg, city) [Default City]:Moscow
Organization Name (eg, company) [Default Company Ltd]:etanribergenov
Organizational Unit Name (eg, section) []:etanribergenov
Common Name (eg, your name or your server's hostname) []:etanribergenov.net
Email Address []:etanribergenov@etanribergenov.net
```

Рис. 7. Генерация ключа и сертификата: ввод данных

File	Command	Options	Size	Modify time
..	UP	--DIR		Apr 4 17:19
www.etanrib~ov.net.crt			1537	Apr 4 17:31
www.etanrib~ov.net.key			1704	Apr 4 17:24

Рис. 8. Сгенерированные ключ и сертификат появились в каталоге

- Для перехода веб-сервера `www.user.net` на функционирование через протокол HTTPS требуется изменить его конфигурационный файл. Перейдите в каталог с конфигурационными файлами

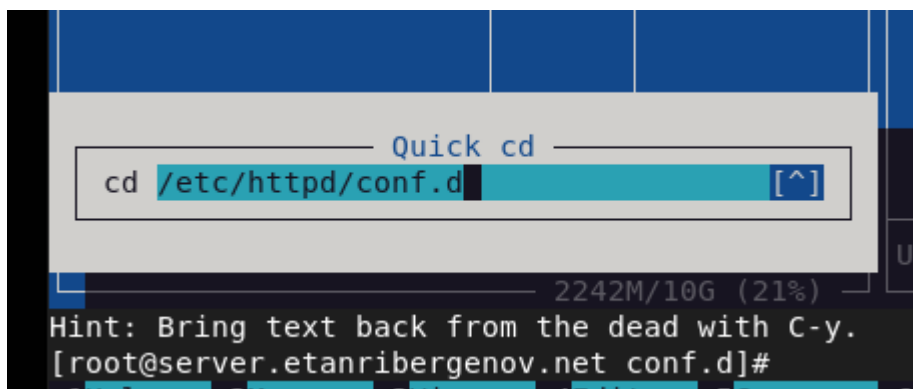


Рис. 9. Переход в каталог с конф. файлами веб-серверов

```

/etc/httpd/conf.d/www.etanribergenov.net.conf
<VirtualHost *:80>
    ServerAdmin webmaster@etanribergenov.net
    DocumentRoot /var/www/html/www.etanribergenov.net
    ServerName www.etanribergenov.net
    ServerAlias www.etanribergenov.net
    ErrorLog logs/www.etanribergenov.net-error_log
    CustomLog logs/www.etanribergenov.net-access_log common
    RewriteEngine on
    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
</VirtualHost>

<IfModule mod_ssl.c>
<VirtualHost *:443>
    SSLEngine on
    ServerAdmin webmaster@etanribergenov.net
    DocumentRoot /var/www/html/www.etanribergenov.net
    ServerName www.etanribergenov.net
    ServerAlias www.etanribergenov.net
    ErrorLog logs/www.etanribergenov.net-error_log
    CustomLog logs/www.etanribergenov.net-access_log common
    SSLCertificateFile /etc/ssl/private/www.etanribergenov.net.crt
    SSLCertificateKeyFile /etc/ssl/private/www.etanribergenov.net.key
</VirtualHost>
</IfModule>

```

*Рис. 10. Редактирование файла конфигурации веб-сервера **www.etanribergenov.net***

Здесь был добавлен псевдоним сервера (ServerAlias), включение механизма переписи домена и добавлено к нему правило переписи. Далее добавлен модуль ssl.c в котором указаны пути к ключу и сертификату.

6. Внесите изменения в настройки межсетевого экрана на сервере, разрешив работу с https

```

[root@server.etanribergenov.net ~]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http ssh
[root@server.etanribergenov.net ~]# firewall-cmd --get-services

```

Рис. 11. Просмотр разрешённых для работы с межсетевым экраном служб

```
[root@server.etanribergenov.net ~]# firewall-cmd --get-services | grep https
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audi
t bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bitto
rent-bsd ceph ceph-mon cfengine cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6-cl
ient distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd
-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeip
a-replication freeipa-trust ftp galera ganglia-client ganglia-master git grafana gre high-av
ailability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kad
min kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-cont
rol-plane kube-controller-manager kube-scheduler kubelet-worker ldap ldaps libvirt libvirt-t
ls lightning-network llmnr managesieve matrix mdns memcache minidlna mongodb mosh mountd mqt
t mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn
ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3
pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster quassel radius r
dp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client sam
a-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync spotify-sy
nc squid sssd ssh steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tl
s telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsms vnc-server
wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-ser
ver zabbix-agent zabbix-server
[root@server.etanribergenov.net ~]#
```

Рис. 12. Просмотр всех доступных служб

Использовал grep для выделения искомой службы среди остальных для удобной и быстрой проверки наличия.

```
[root@server.etanribergenov.net ~]# firewall-cmd --add-service=https
success
[root@server.etanribergenov.net ~]# firewall-cmd --add-service=https --permanent
success
```

Рис. 13. Разрешение работы межсетевого экрана с https

```
[root@server.etanribergenov.net ~]# firewall-cmd --reload
success
[root@server.etanribergenov.net ~]# █
```

Рис. 14. Перезагрузка межсетевого экрана

7. Перезапустите веб-сервер

```
[root@server.etanribergenov.net ~]# systemctl restart httpd
[root@server.etanribergenov.net ~]# █
```

Рис. 15. Перезапуск веб-сервера

8. На виртуальной машине client в строке браузера введите название веб-сервера .net и убедитесь, что произойдёт автоматическое переключение на работу по протоколу HTTPS. На открывшейся странице с сообщением о незащищённости соединения нажмите кнопку «Дополнительно», затем добавьте адрес вашего сервера в постоянные исключения. Затем просмотрите содержание сертификата (нажмите на значок с замком в адресной строке и кнопку «Подробнее»).

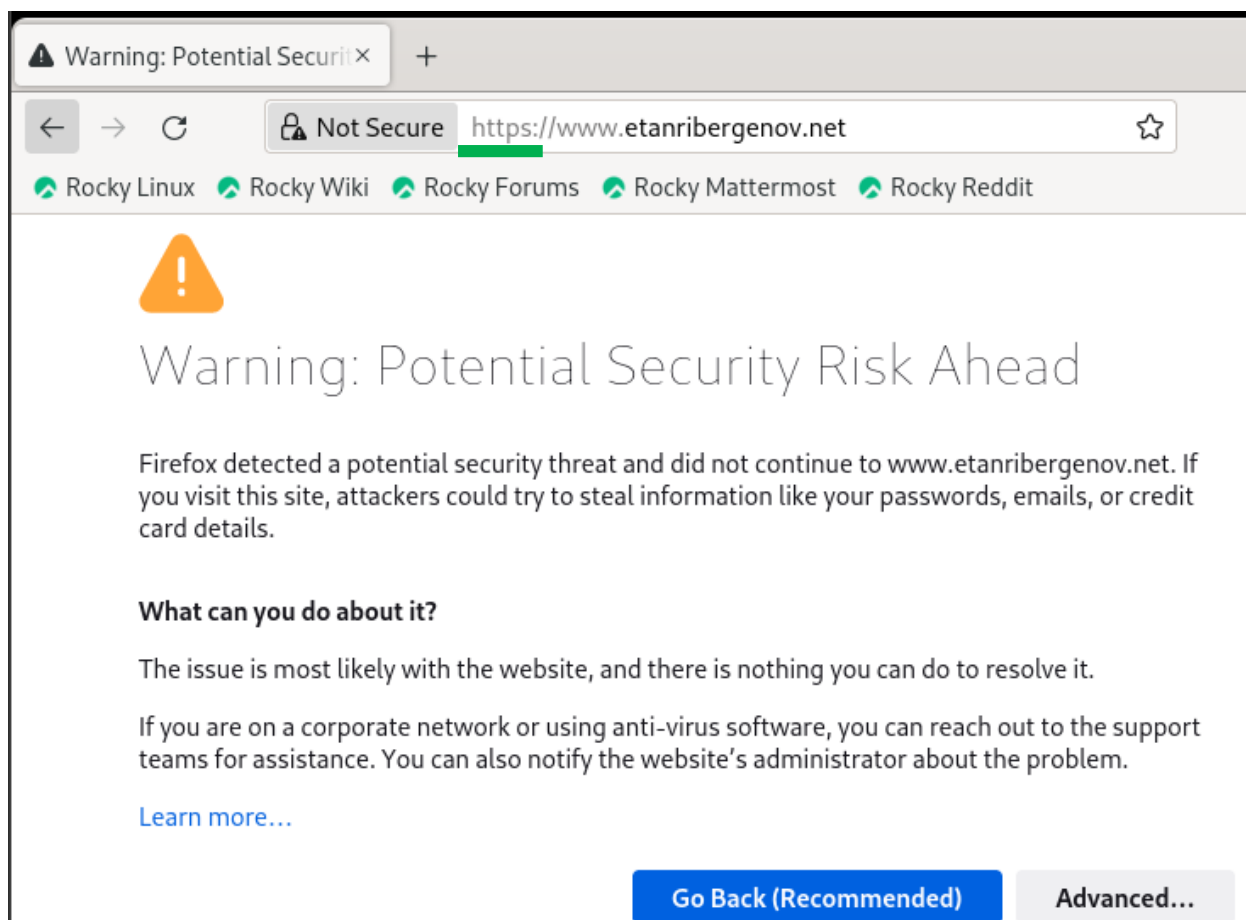


Рис. 16. Ввод названия веб-сервера в поисковую строку браузера

Убедился, что http заменяется на https. Нажал кнопку «Дополнительно» (Advanced) – появилось сообщение снизу. Нажал на кнопку «Accept the Risk and Continue» чтобы сделать исключения для данного сервера.

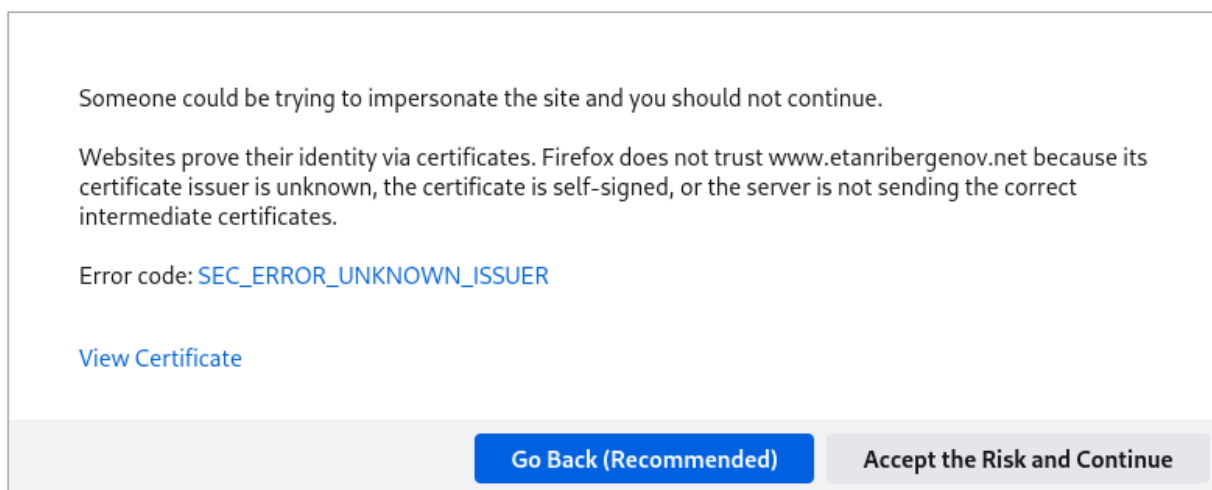


Рис. 17. Принятие исключения (Accept the Risk and Continue)

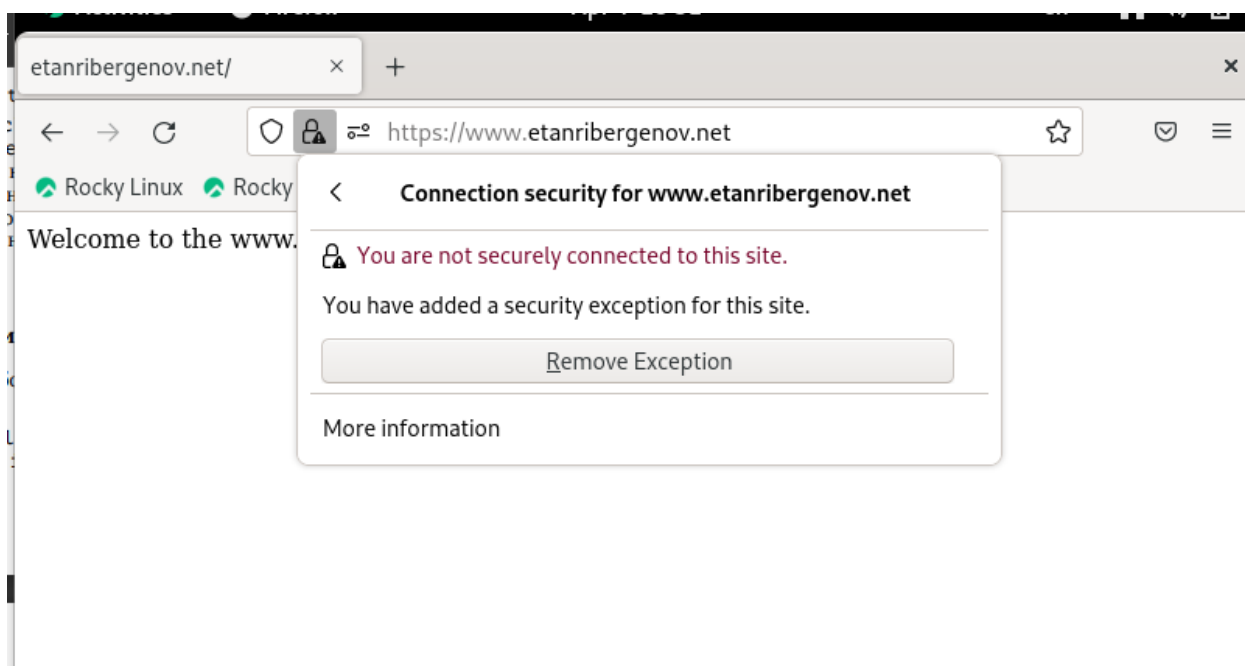


Рис. 18. Кнопка «замок»: уведомляет, что сайт был добавлен в исключения – далее кнопка «More information»

Нажал на «Подробнее» (More information) – открылась страница с информацией о сайте (веб-сервере).

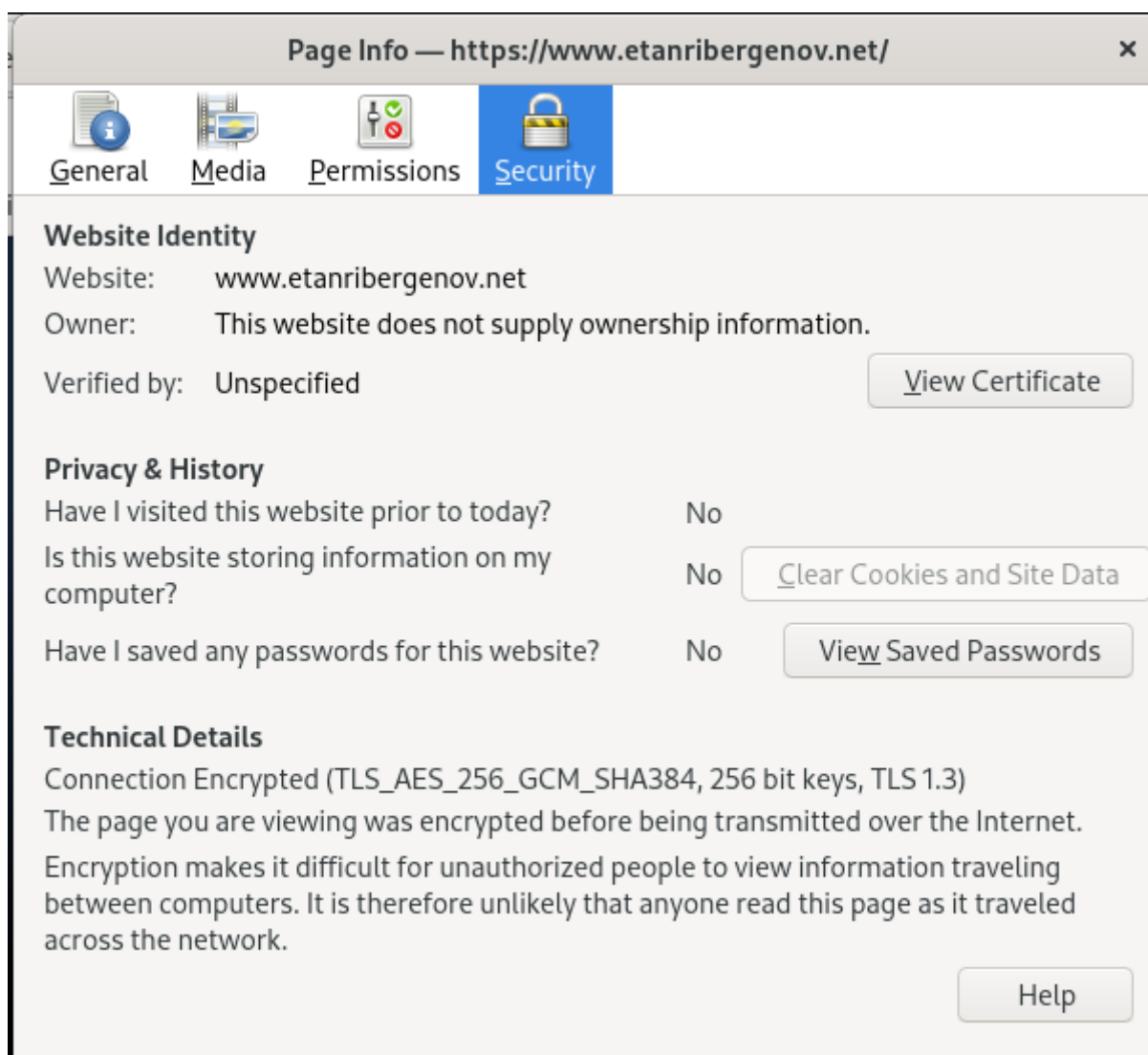


Рис. 19. Просмотр информации о сайте (нажатие на кнопку «View Certificate»)

Открыл на просмотр сертификат: убедился, что отображаются введённые мной ранее данные.

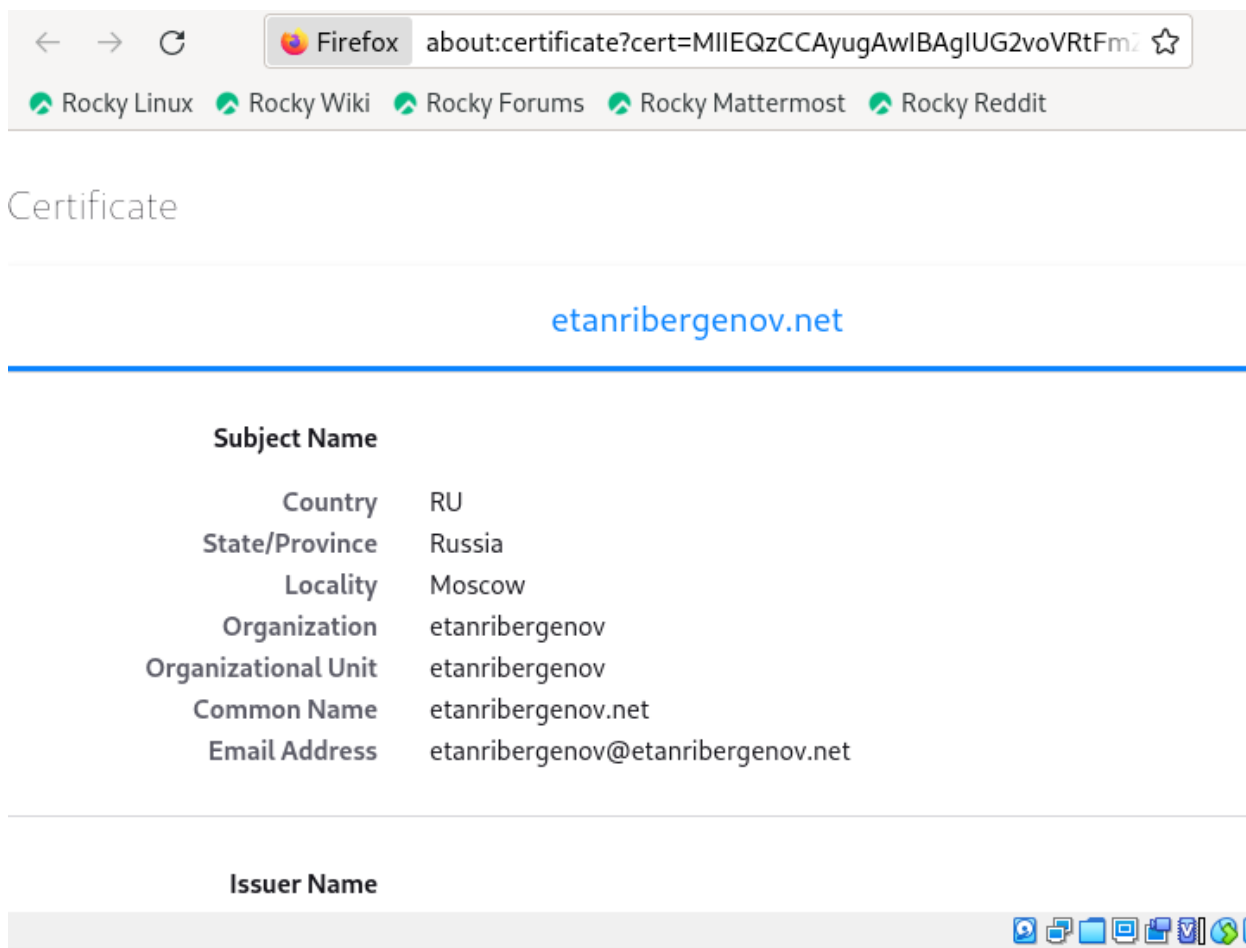


Рис. 20. Сертификат (1)

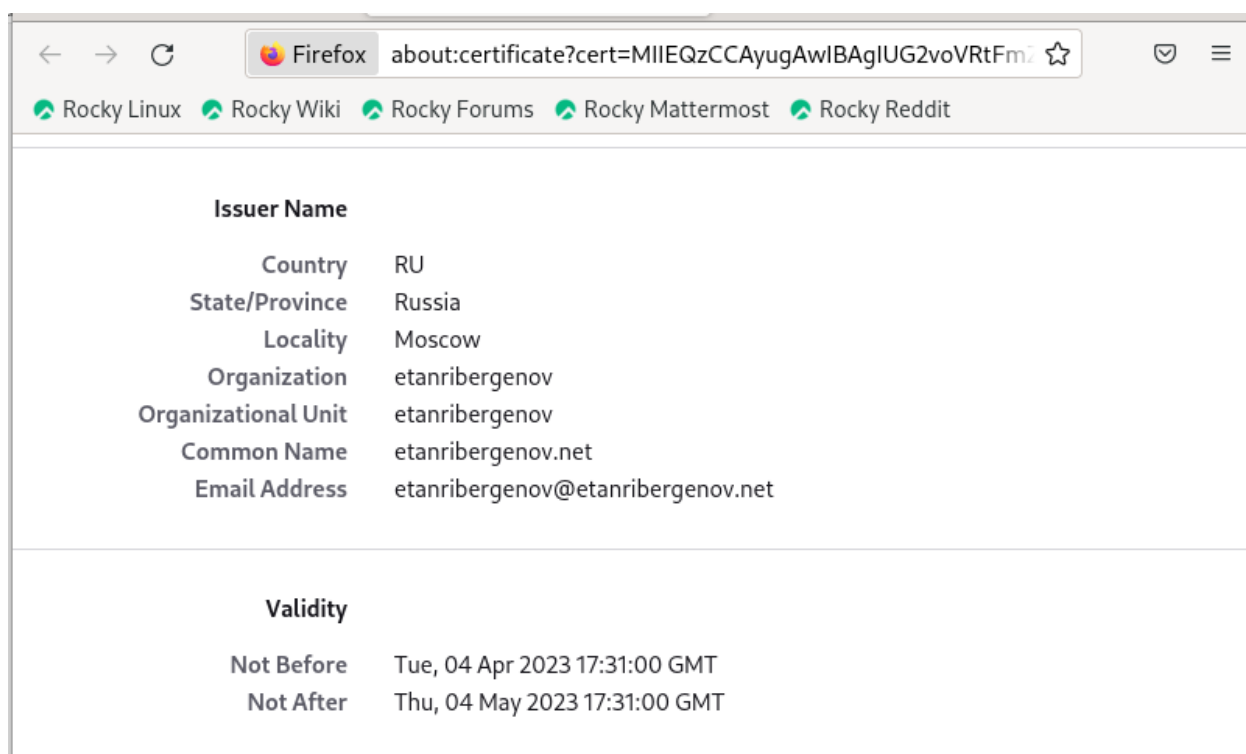


Рис. 21. Сертификат (2)

← → ↻ Firefox about:certificate?cert=MIIEQzCCAyugAwIBAgIUUG2voVRtFmZ ☆

Rocky Linux Rocky Wiki Rocky Forums Rocky Mattermost Rocky Reddit

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	AF:40:83:06:F6:E9:2B:9D:81:04:80:E2:40:A4:BF:45:19:A7:85:DB:C7:2B:E7:C...

Miscellaneous

Serial Number	1B:6B:E8:55:1B:45:99:93:B4:5B:AD:5F:3D:0B:1D:29:60:88:14:55
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Рис. 22. Сертификат (3)

etanribergenov.net/ × Certificate for etanribergenov × + ×

← → ↻ Firefox about:certificate?cert=MIIEQzCCAyugAwIBAgIUUG2voVRtFmZ ☆

Rocky Linux Rocky Wiki Rocky Forums Rocky Mattermost Rocky Reddit

Fingerprints

SHA-256	48:C4:80:60:2B:24:7C:C6:F0:81:1D:98:16:37:48:AC:F5:E2:8B:82:3A:E6:24:4D:...
SHA-1	BB:F0:08:5F:D4:C2:FD:06:E7:4D:71:2A:E2:48:BA:2F:2D:D8:A0:FF

Basic Constraints

Certificate Authority	Yes
-----------------------	-----

Subject Key ID

Key ID	1C:A2:62:05:C4:D0:AF:39:4A:BE:9F:3E:30:5C:F3:71:B3:63:08:D7
--------	---

Authority Key ID

Key ID	1C:A2:62:05:C4:D0:AF:39:4A:BE:9F:3E:30:5C:F3:71:B3:63:08:D7
--------	---

Right Ctrl

Рис. 23. Сертификат (4)

2. Конфигурирование HTTP-сервера для работы с PHP

1. Установите пакеты для работы с PHP

```
[root@server.etanribergenov.net ~]# dnf -y install php
Last metadata expiration check: 1:01:58 ago on Tue 04 Apr 2023 05:26:41 PM UTC.
Dependencies resolved.
=====
Package                Architecture Version                Repository            Size
=====
Installing:
php                    x86_64          8.0.27-1.el9_1        appstream              10 k
Installing dependencies:
nginx-filessystem      noarch          1:1.20.1-13.el9        appstream              11 k
php-common             x86_64          8.0.27-1.el9_1        appstream             667 k
Installing weak dependencies:
php-cli               x86_64          8.0.27-1.el9_1        appstream             3.1 M
php-fpm               x86_64          8.0.27-1.el9_1        appstream             1.6 M
php-mbstring          x86_64          8.0.27-1.el9_1        appstream             470 k
php-opcache            x86_64          8.0.27-1.el9_1        appstream             512 k
php-pdo                x86_64          8.0.27-1.el9_1        appstream              83 k
php-xml                x86_64          8.0.27-1.el9_1        appstream             131 k
=====
Transaction Summary
=====
Install 9 Packages

Total download size: 6.5 M
Installed size: 35 M
Downloading Packages:
```

Рис. 25. Установка PHP

2. В каталоге /var/www/html/www.etanribergenov.net замените файл index.html на index.php следующего содержания:

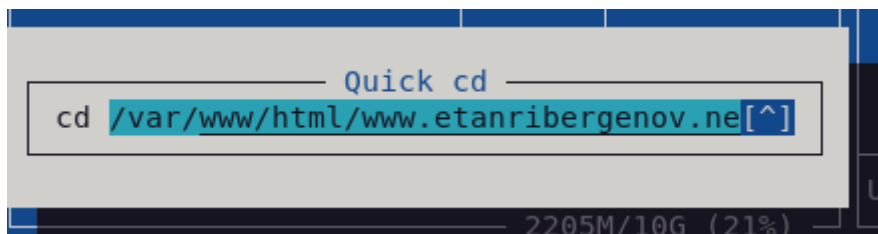


Рис. 26. Переход в каталог с содержимым веб-сервера

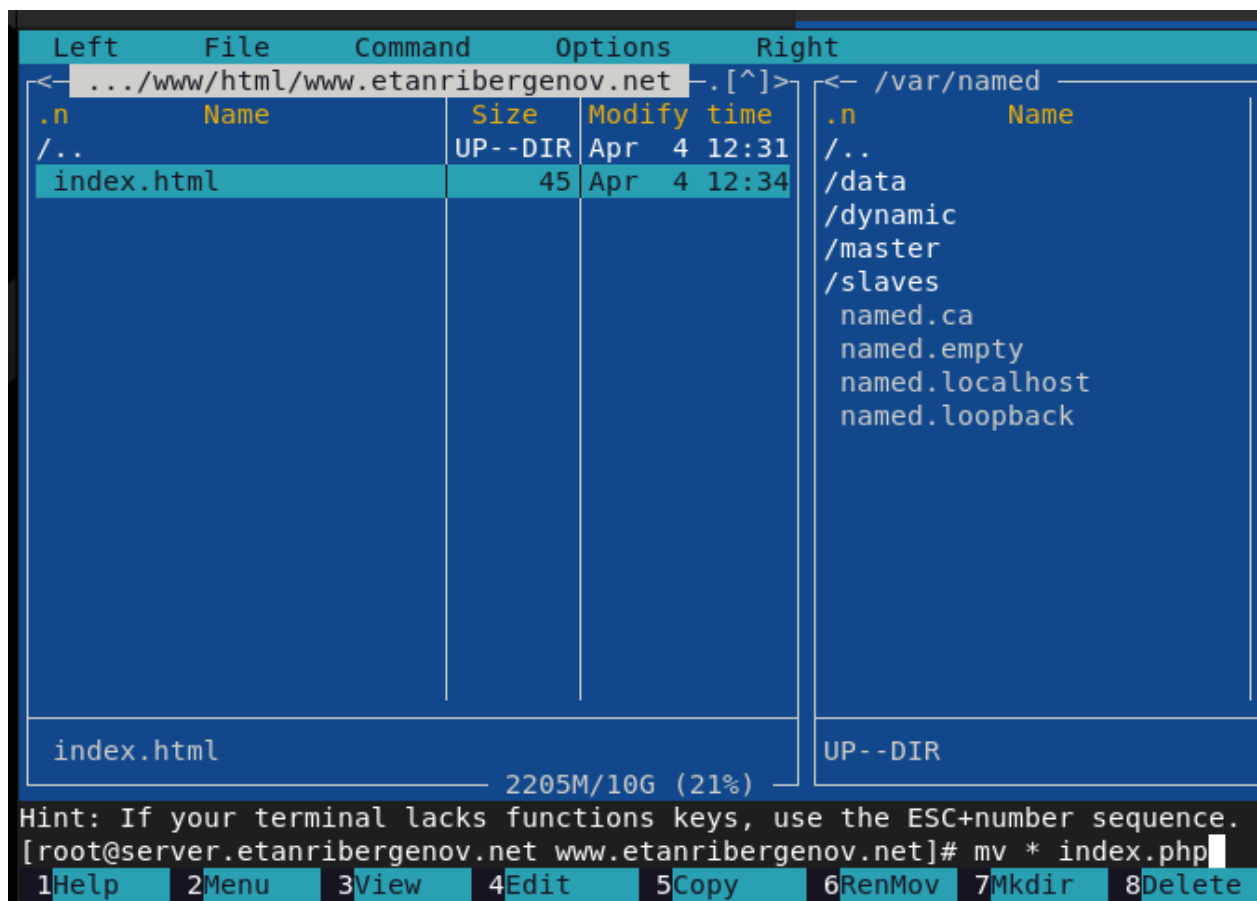


Рис. 27. Переименование файла .html в .php

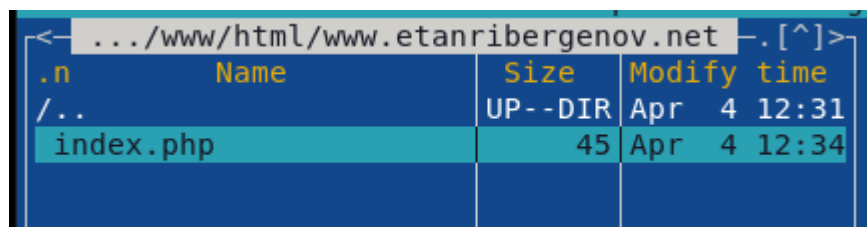


Рис. 28. Результат пред. действия

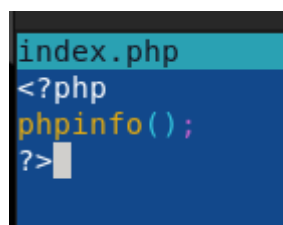


Рис. 29. Содержимое файла index.php

3. Скорректируйте права доступа в каталог с веб-контентом:

```
chown -R apache:apache /var/www
```

```
Complete!  
[root@server.etanribergenov.net ~]# chown -R apache:apache /var/www  
[root@server.etanribergenov.net ~]#
```

Рис. 30. Изменение прав доступа в каталог с веб-контентом

4. Восстановите контекст безопасности в SELinux

```
[root@server.etanribergenov.net ~]# restorecon -vR /etc  
Relabeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r:user_tmp_t:s0 to  
unconfined_u:object_r:net_conf_t:s0  
[root@server.etanribergenov.net ~]# restorecon -vR /var/www  
[root@server.etanribergenov.net ~]#
```

Рис. 31. Восстановление контекста безопасности в SELinux

5. Перезапустите HTTP-сервер

```
[root@server.etanribergenov.net ~]# systemctl restart httpd  
[root@server.etanribergenov.net ~]#
```

Рис. 32. Перезапуск HTTP-сервера

6. На виртуальной машине client в строке браузера введите название веб-сервера `www.etanribergenov.net` и убедитесь, что будет выведена страница с информацией об используемой на веб-сервере версии PHP.

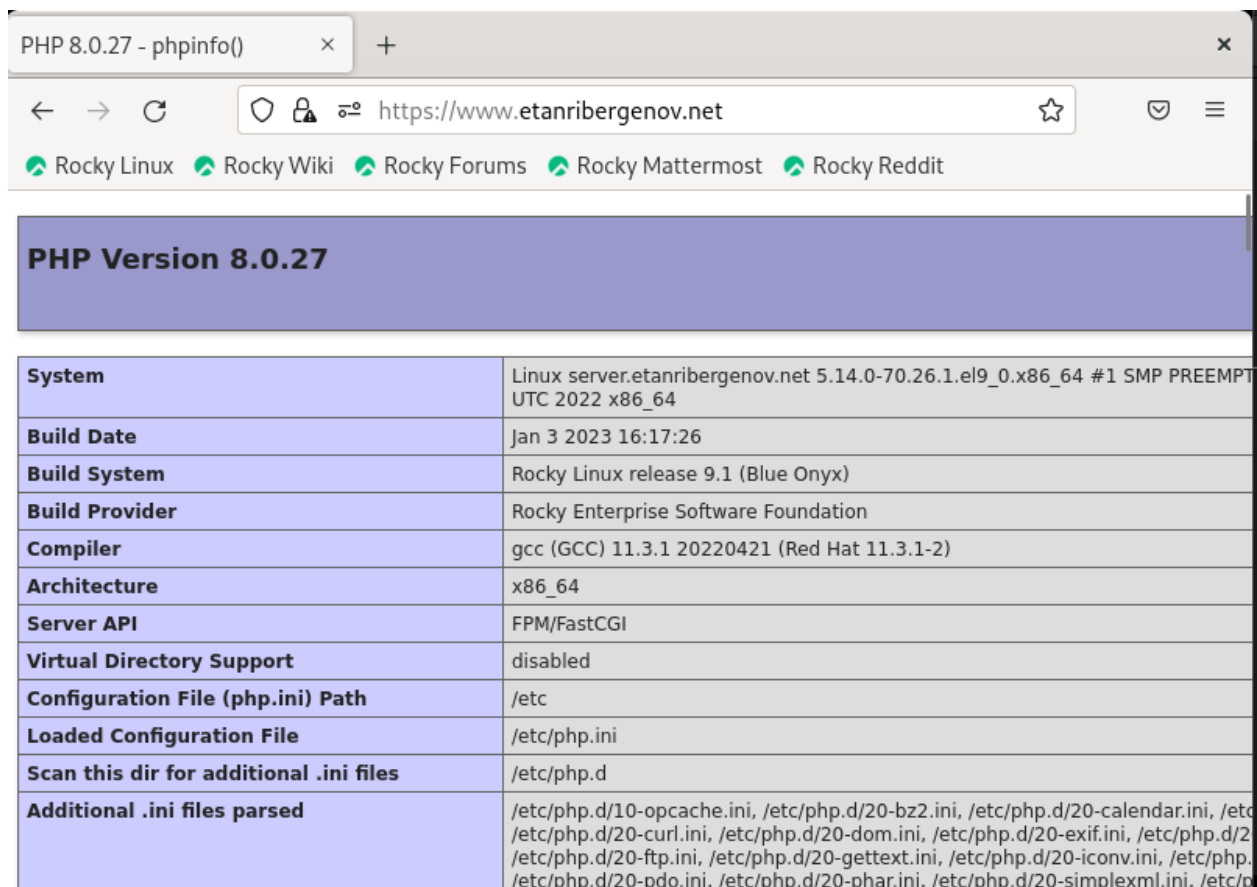


Рис. 33. Проверка отображения страницы с информацией о версии php в браузере

3. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/http` и в соответствующие каталоги скопируйте конфигурационные файлы

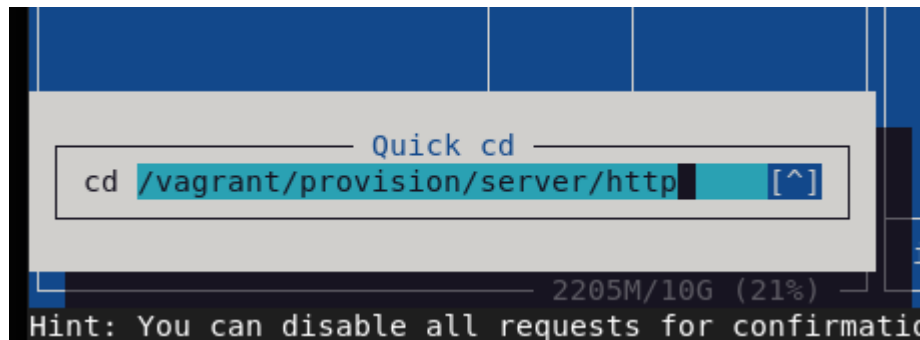


Рис. 34. Переход в подкаталог с веб-контентом в каталоге настройки VM server

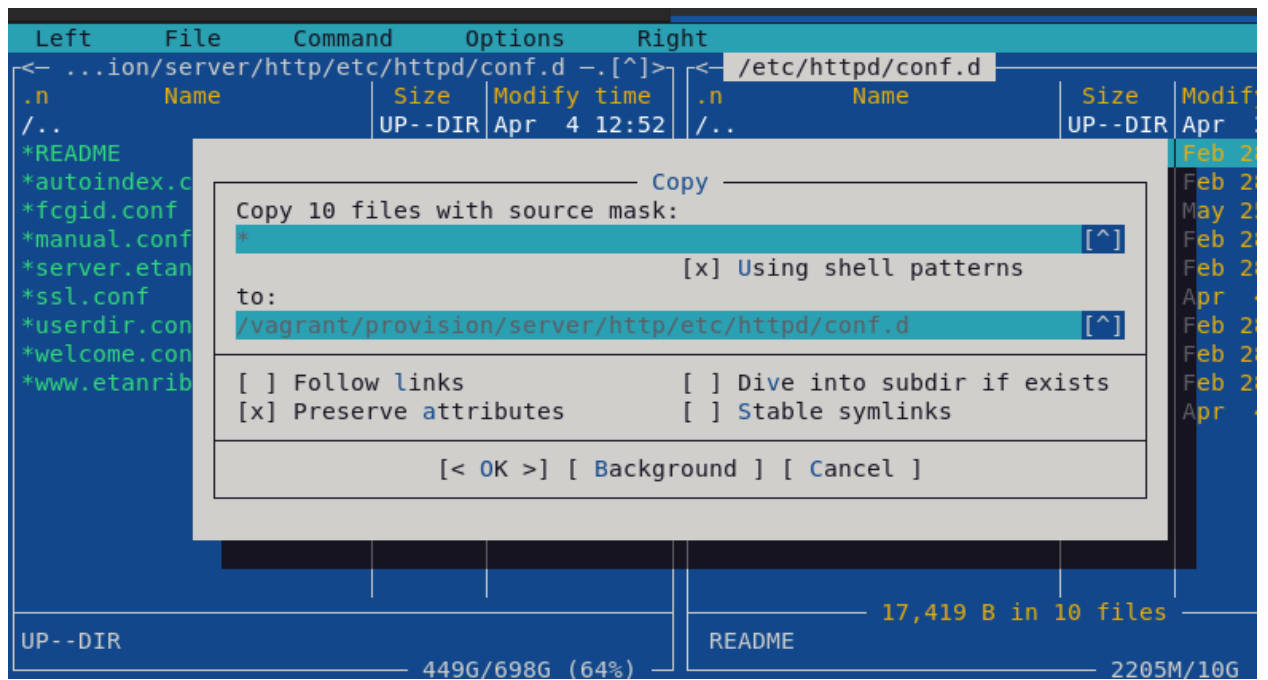


Рис. 35. Копирование конфигурационных файлов

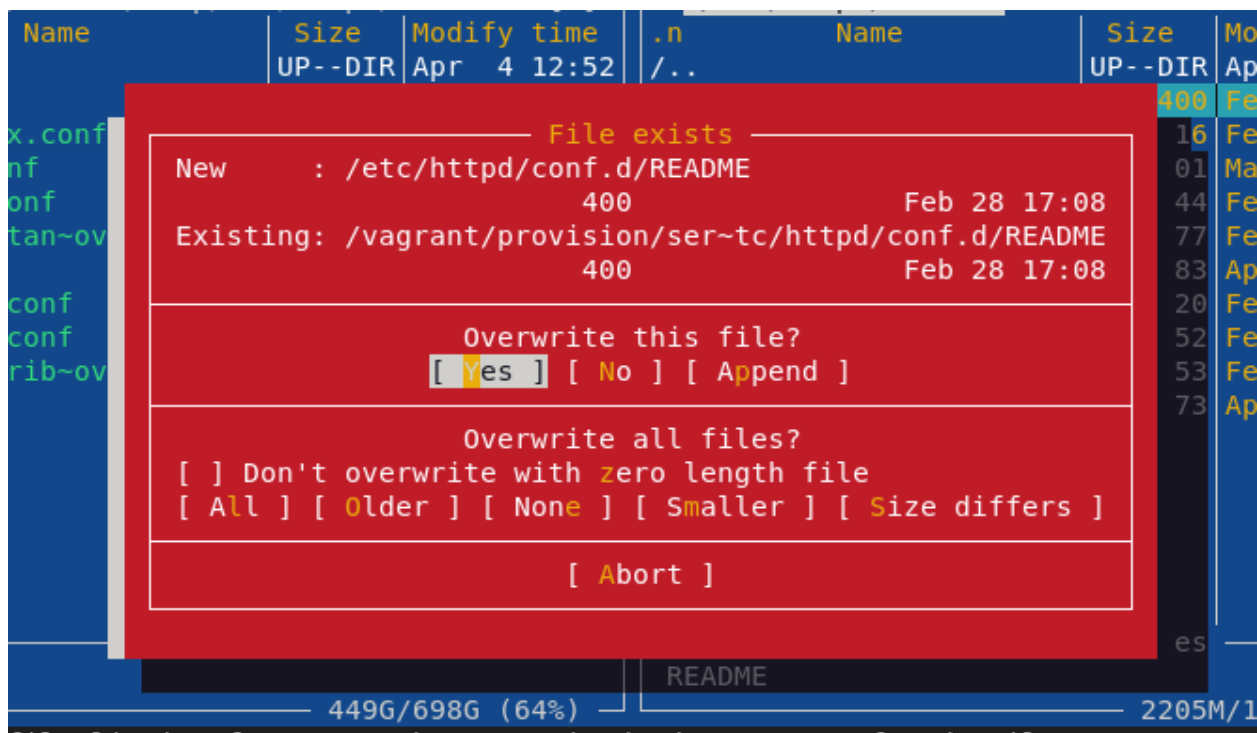


Рис. 36. Подтверждение перезаписи файлов

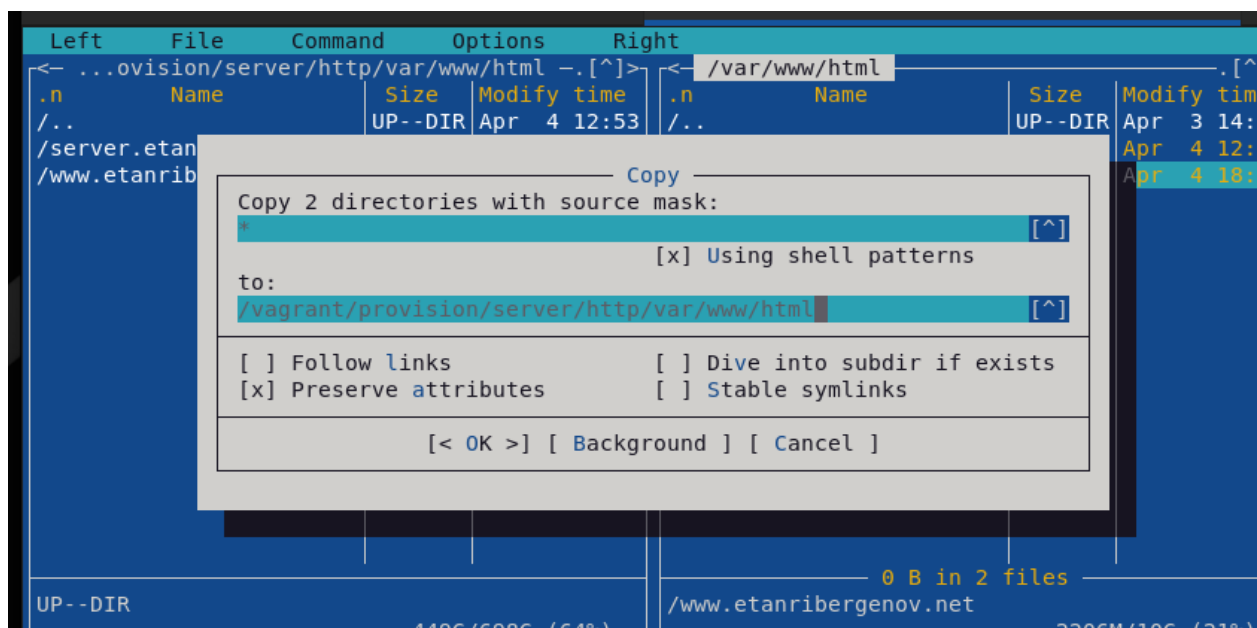


Рис. 37. Копирование каталогов с веб-контентом

```
[root@server.etanribergenov.net etc]# mkdir -p ssl/private
[root@server.etanribergenov.net etc]#
```

Рис. 38. Создание подкаталога для хранения ключа и сертификата

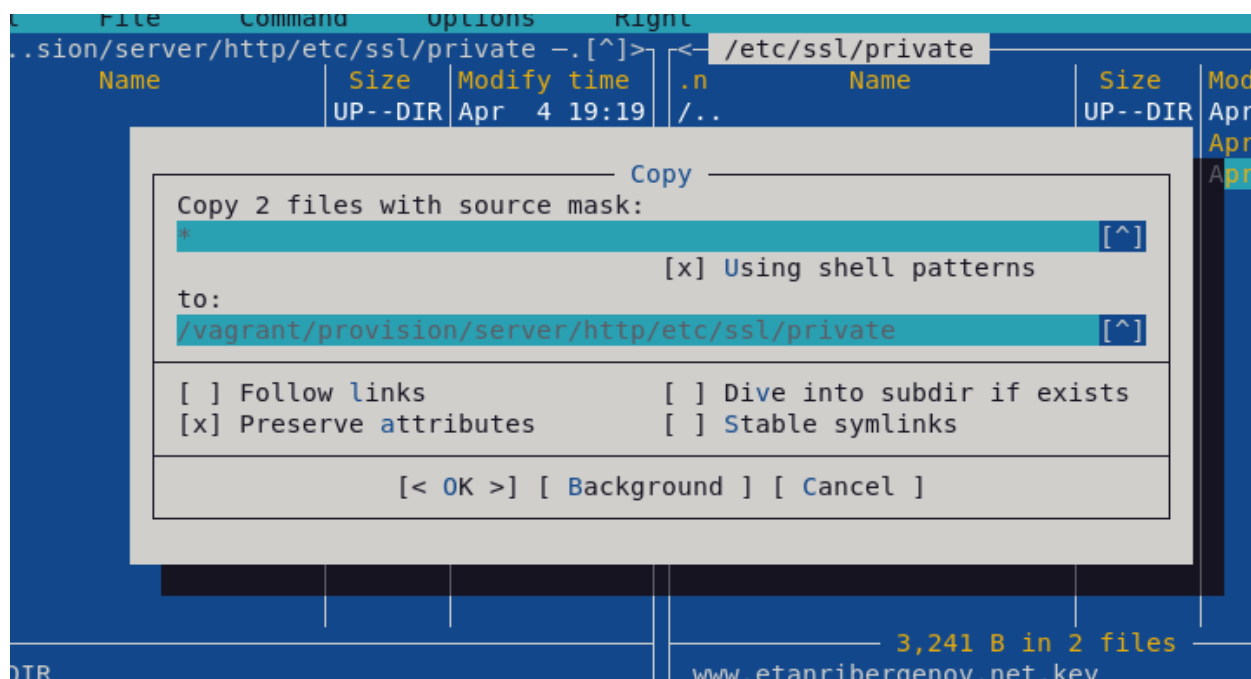


Рис. 39. Копирование ключа и сертификата в каталог настройки

2. В имеющийся скрипт `/vagrant/provision/server/http.sh` внесите изменения, добавив установку PHP и настройку межсетевого экрана, разрешающую работать с https.

```
http.sh [-M--] 25 L:[ 1+17 18/ 27] *(386 / 613b
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y groupinstall "Basic Web Server"
dnf -y install php

echo "Copy configuration files"
cp -R /vagrant/provision/server/http/etc/httpd/* /etc/httpd
cp -R /vagrant/provision/server/http/var/www/* /var/www

chown -R apache:apache /var/www

restorecon -vR /etc
restorecon -vR /var/www

echo "Configure firewall"
firewall-cmd --add-service=http
firewall-cmd --add-service=http --permanent
firewall-cmd --add-service=https
firewall-cmd --add-service=https --permanent

echo "Start http service"
1Help 2Save 3Mark 4Replac 5Copy 6Move 7S
```

Рис. 40. Скрипт http.sh (изменённый)

Вывод

В результате выполнения лабораторной работы я приобрёл практические навыки по расширенному конфигурированию HTTP-сервера Apache в части безопасности и возможности использования PHP.

Ответы на контрольные вопросы

1. HTTPS – это расширение протокола HTTP для поддержки шифрования в целях повышения безопасности.
2. Достигается за счёт использования криптографических протоколов при организации HTTP-соединения и передачи по нему данных. Для шифрования может применяться протокол SSL или протокол TLS. Оба протокола используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.
3. Сертификационный центр (Certification authority, CA), технически, представляет собой компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Это организация, чей открытый ключ широко известен общественности и не вызывает сомнений в подлинности. Пример: AlphaSSL.