Отчёт по лабораторной работе №5

Дисциплина: Администрирование сетевых подсистем

Мишина Анастасия Алексеевна

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

## 2.1 Конфигурирование HTTP-сервера для работы через протокол HTTPS

Запускаем ВМ через рабочий каталог. На ВМ server входим под собственным пользователем и переходим в режим суперпользователя. В каталоге /etc/ssl создаем каталог private: mkdir -p /etc/pki/tls/private, ln -s /etc/pki/tls/private /etc/ssl/private, cd /etc/pki/tls/private. Генерируем ключ и сертификат (рис. 1), введя следующую команду: openssl req -x509 -nodes -newkey rsa:2048 -keyout www.aamishina.net.key -out www.aamishina.net.crt

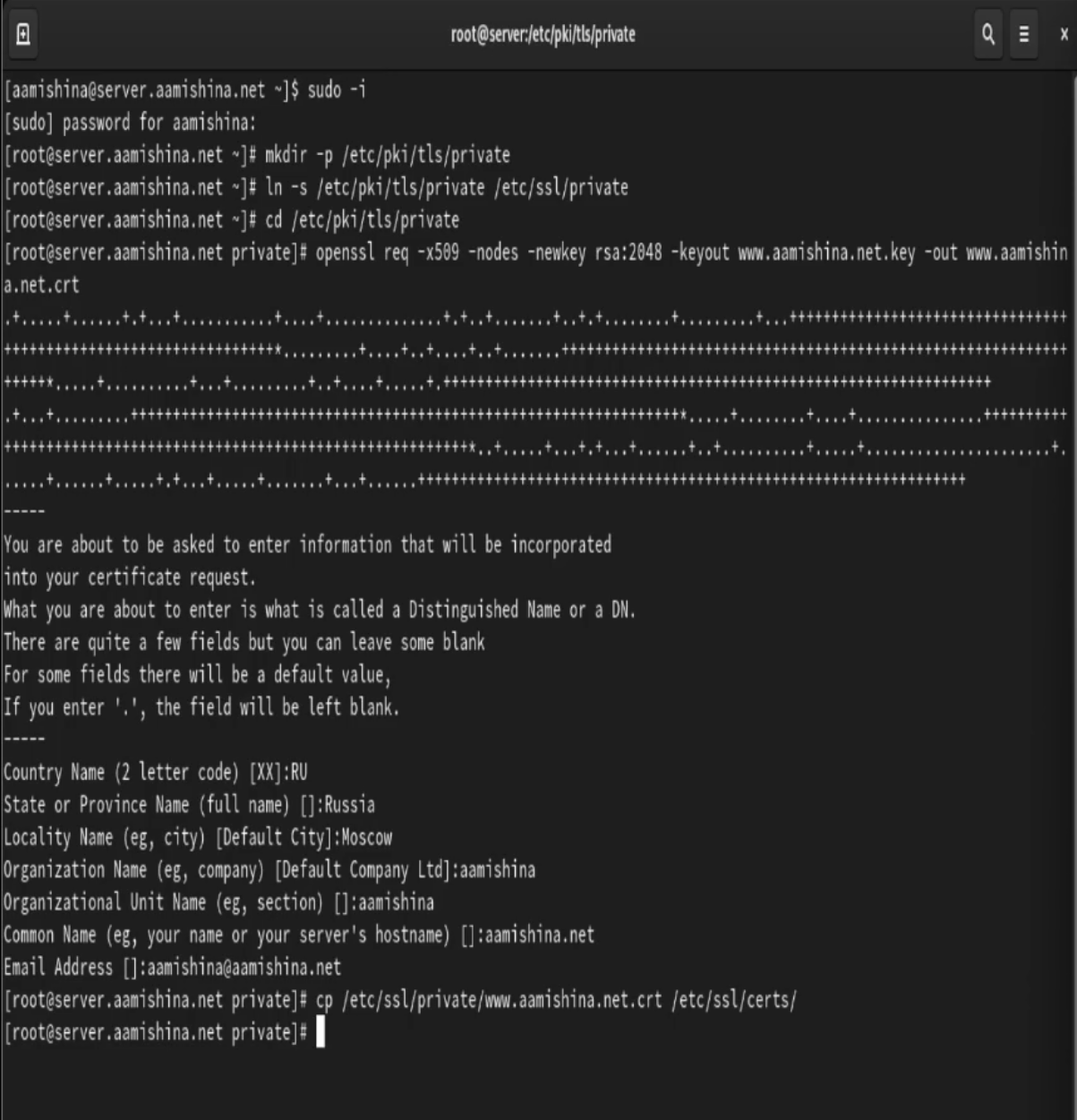


Рис. 1: Генерация ключа и заполнение сертификата

Сгенерированные ключ и сертификат появляются в соответствующем каталоге /etc/ssl/private. Копируем сертификат в каталог /etc/ssl/certs (рис. 2)



Рис. 2: Копирование сертификата в каталог /etc/ssl/certs

Редактируем конфигурационный файл /etc/httpd/conf.d/www.aamishina.net (рис. 3)

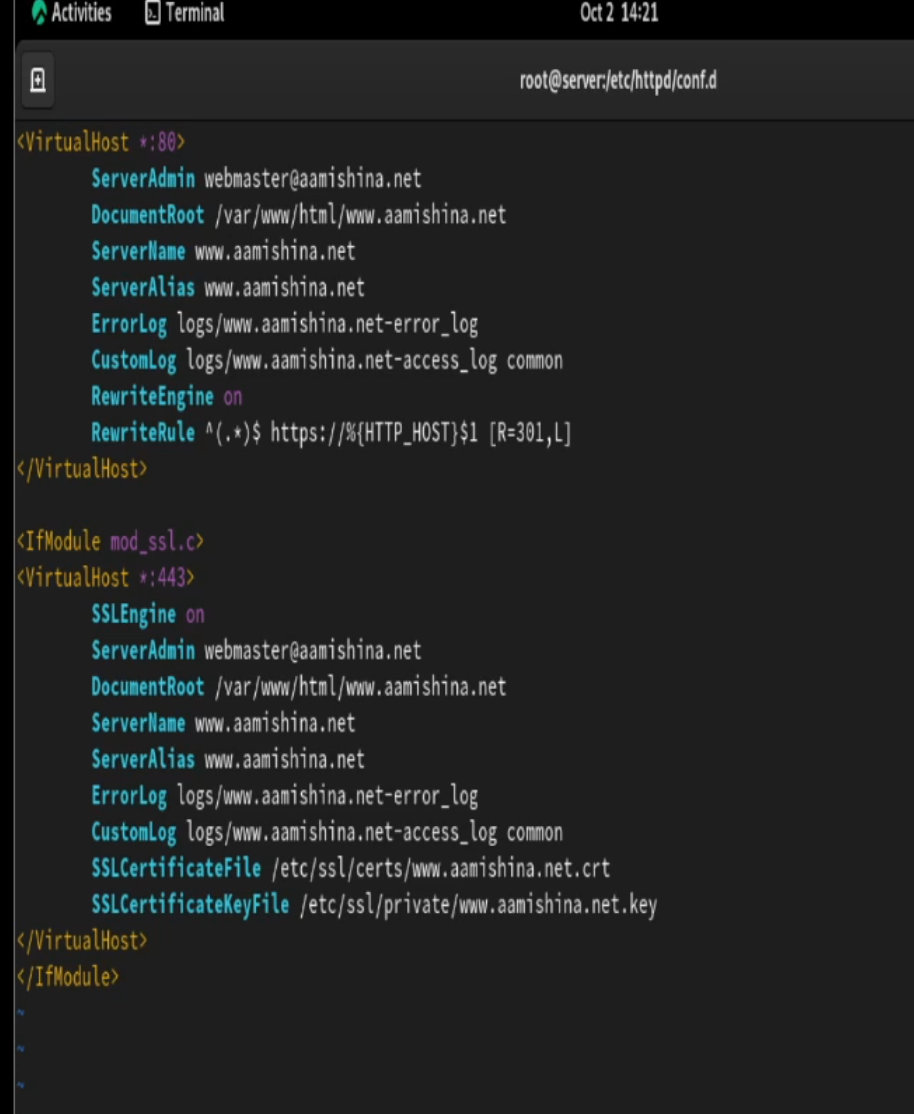


Рис. 3: Редактирование файла /etc/httpd/conf.d/www.aamishina.net

Вносим изменения в настройки межсетевого экрана на сервере, перезапускаем веб-сервер (рис. 4)

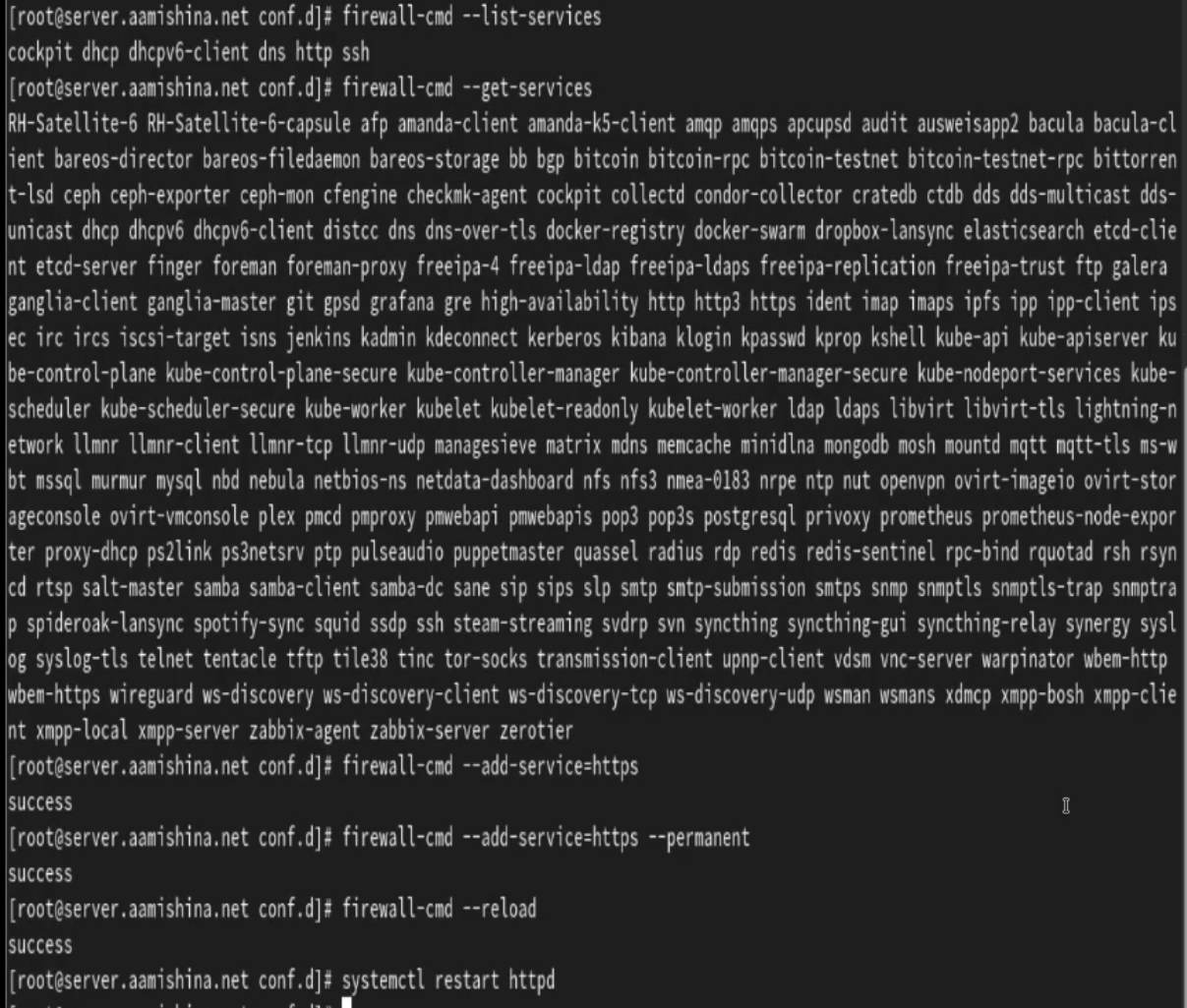


Рис. 4: Внесение изменений в настройки межсетевого экрана, перезапуск веб-сервера

На ВМ client открываем в браузере страницу www.aamishina.net с сообщением о незащищенности соединения (рис. 5). Добавив страницу в исключения, просматриваем информацию о сертификате (рис. 6).

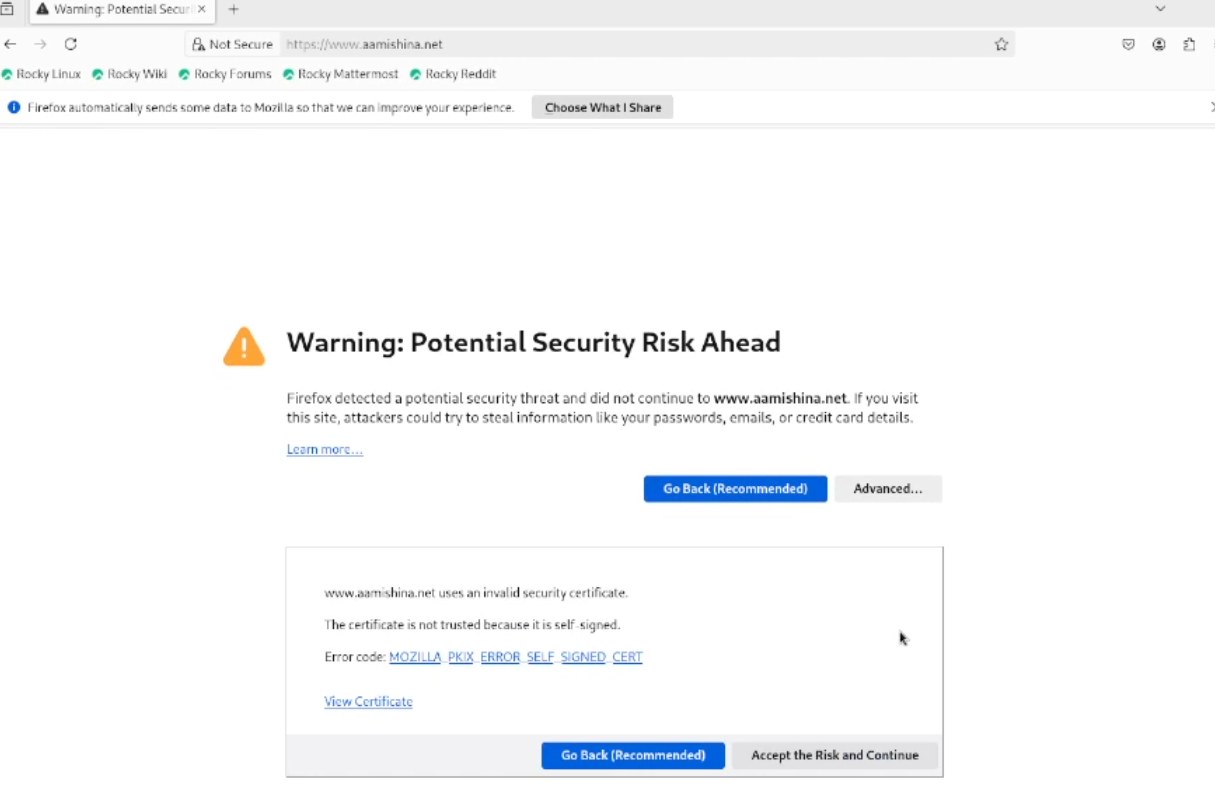


Рис. 5: Сообщение о незащищенности соединения

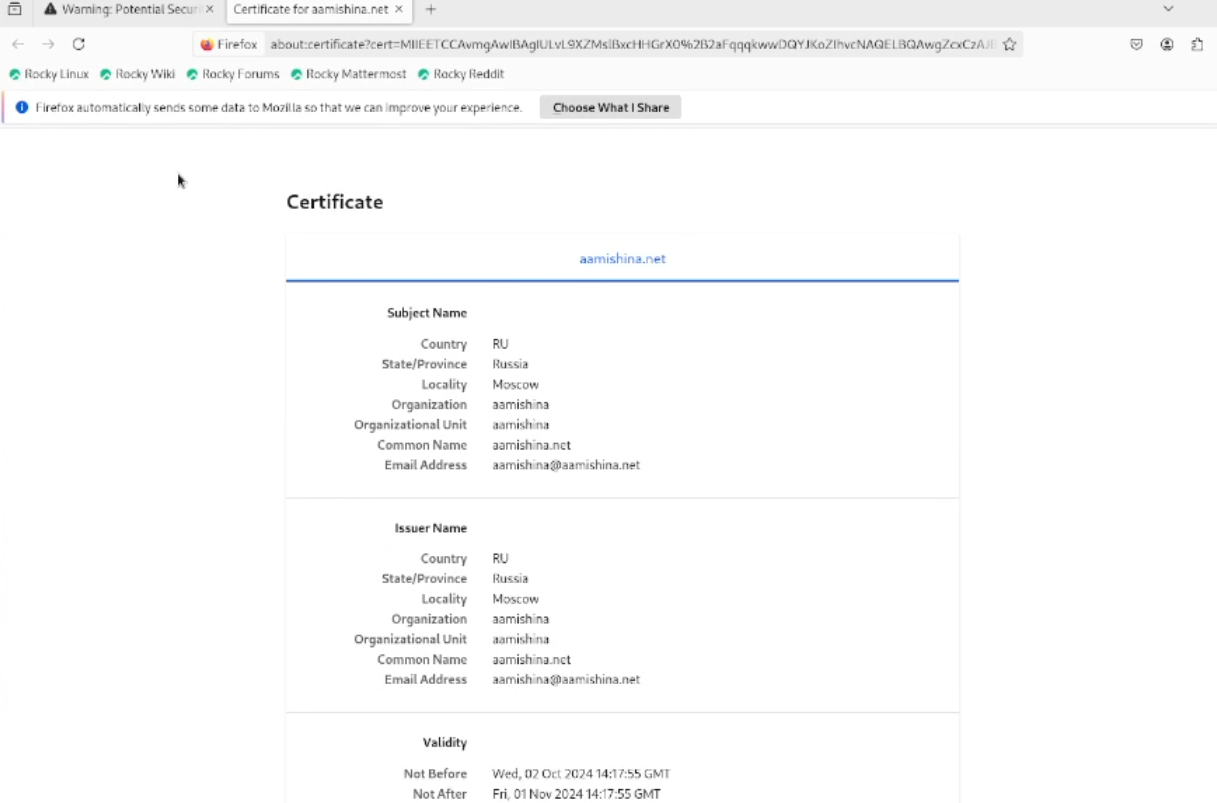


Рис. 6: Содержимое сертификата

## 2.2 Конфигурирование HTTP-сервера для работы с PHP

Устанавливаем пакеты для работы с PHP: dnf -y install php.

В каталоге /var/www/html/www.aamishina.net заменяем index.html на index.php (рис. 7).

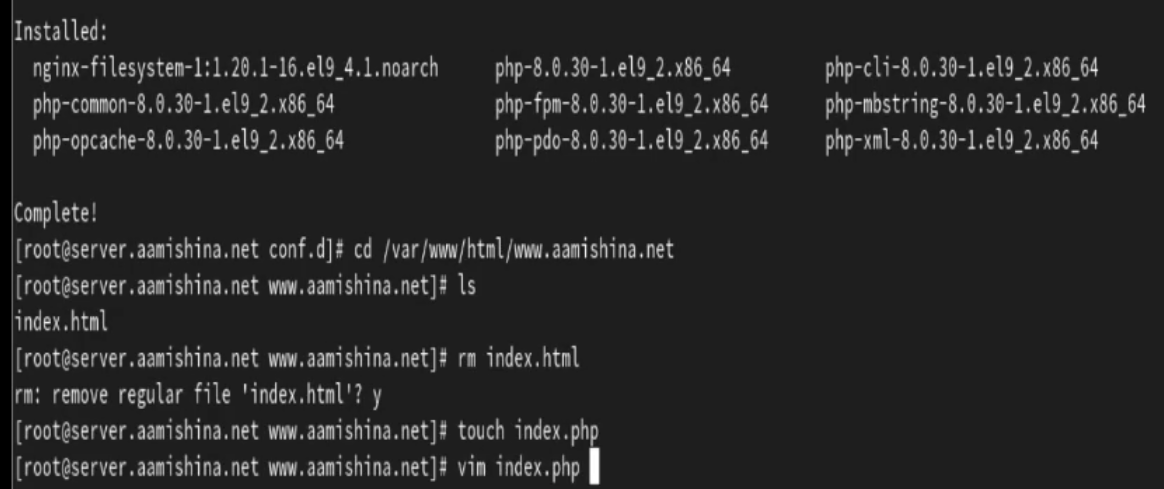


Рис. 7: Замена файла /var/www/html/www.aamishina.net/index.html на index.php

Редактируем index.php (рис. 8).

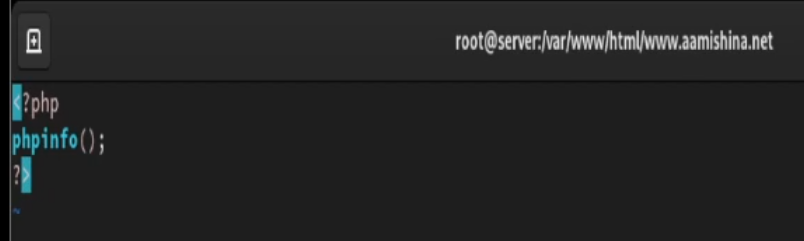


Рис. 8: Редактирование index.php

Корректируем права доступа в каталог с веб-контентом, восстанавливаем контекст безопасности в SELinux, перезагружаем HTTP-сервер: chown -R apache:apache /var/www, restorecon -vR /etc, restorecon -vR /var/www и systemctl restart httpd (рис. 9).

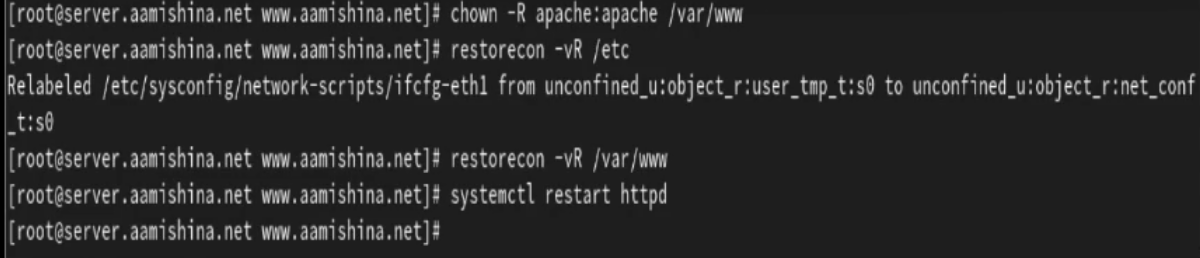


Рис. 9: Корректирование прав доступа, восстановление контекста безопасности SELinux, перезагрузка HTTP-сервера

На ВМ client вводим в адресную строку браузера www.aamishina.net и видим веб-страницу с информацией об используемой версии PHP (рис. 10).

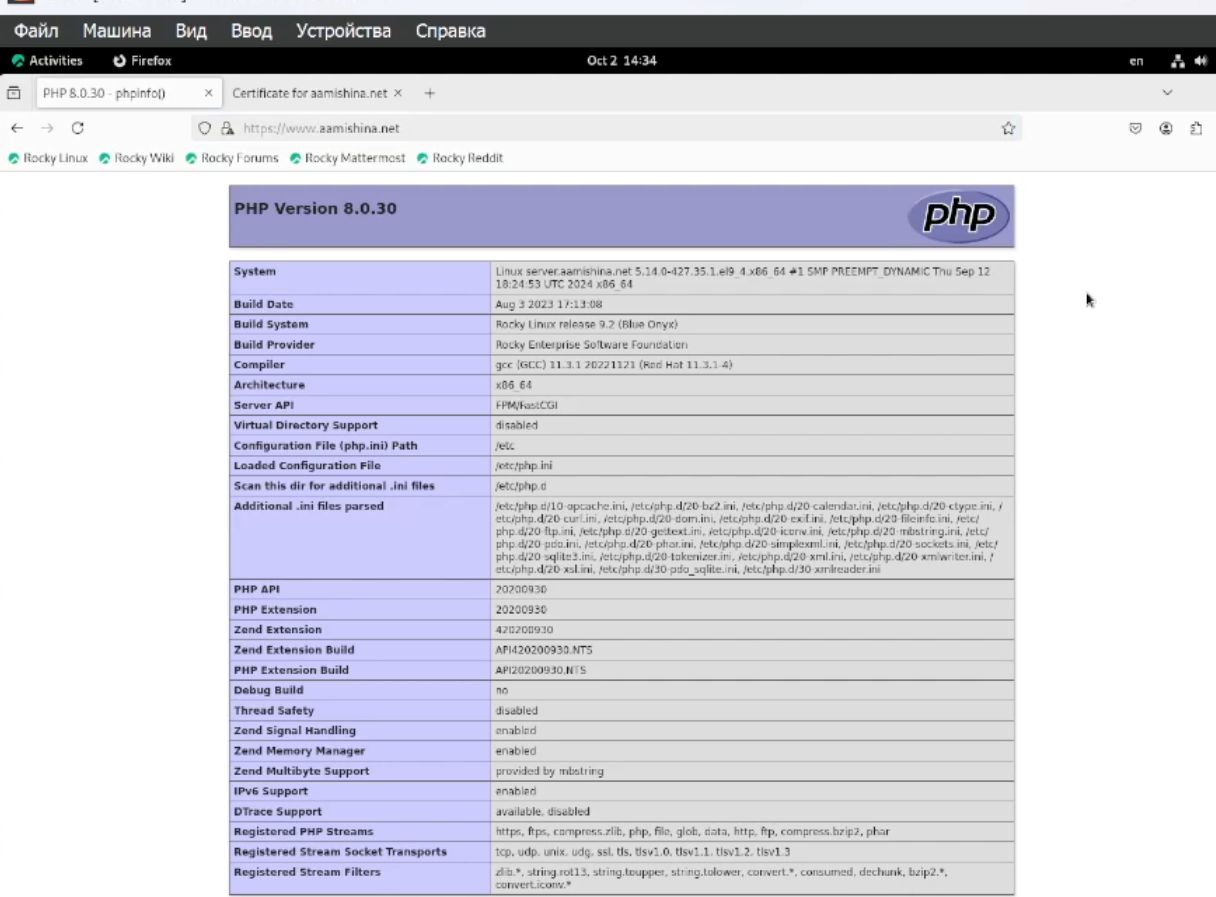


Рис. 10: Веб-страница с информацией об используемой версии PHP

## 2.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

На ВМ server переходим в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копируем в соответствующие каталоги конфигурационные файлы (рис. 11).

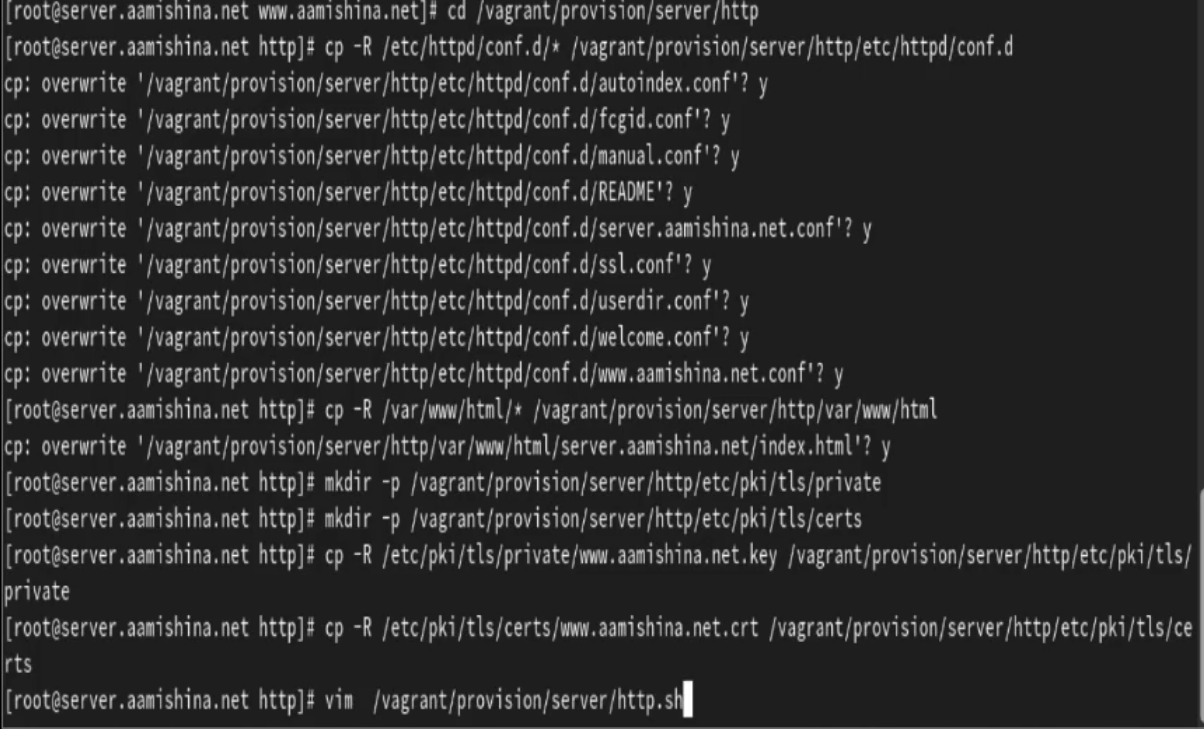


Рис. 11: Копируем в каталоги конфигурационные файлы

В скрипт /vagrant/provision/server/http.sh вносим изменения, добавив установку PHP и настройку межсетевого экрана для работы с https (рис. 12).

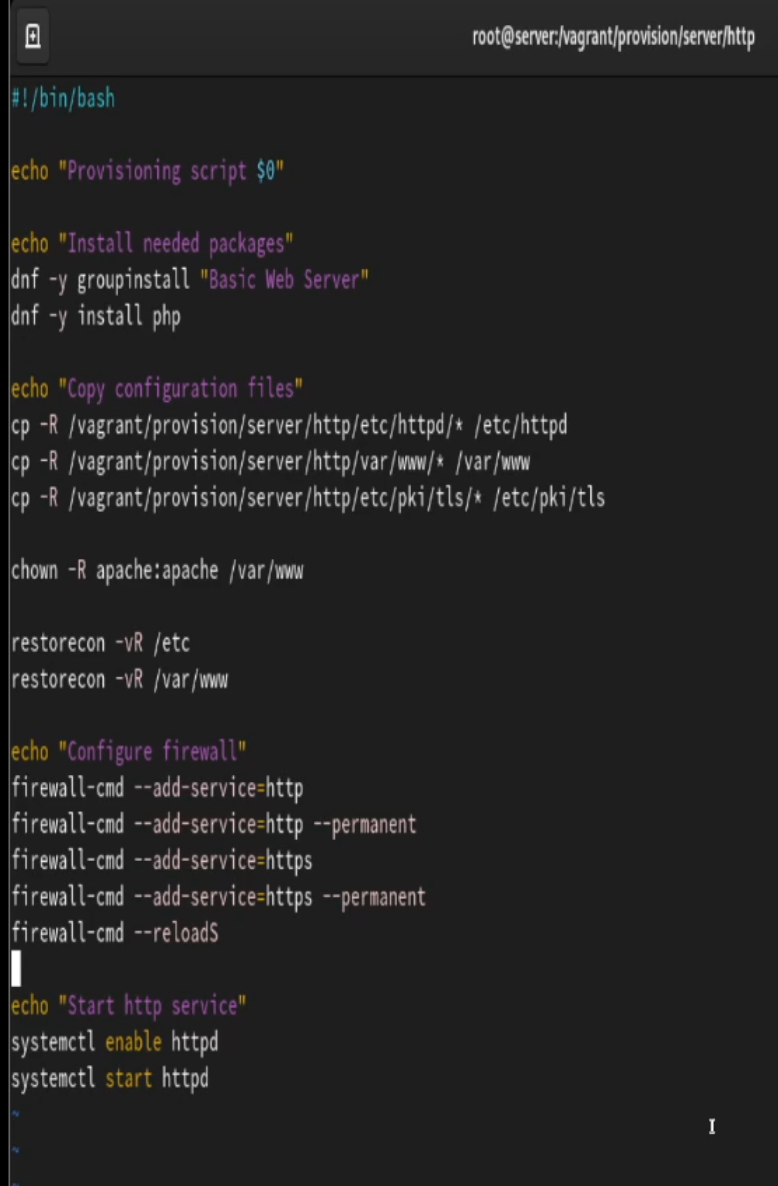


Рис. 12: Внесение изменений в скрипт http.sh

# 3 Выводы

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

# 4 Ответы на контрольные вопросы

1. В чём отличие HTTP от HTTPS?

* **HTTP** (HyperText Transfer Protocol) – это протокол передачи данных, который используется для передачи информации между клиентом (например, веб-браузером) и сервером. Однако он не обеспечивает шифрование данных, что делает их уязвимыми к перехвату злоумышленниками.
* **HTTPS** (HyperText Transfer Protocol Secure) - это расширение протокола HTTP с добавлением шифрования, обеспечивающее безопасную передачу данных между клиентом и сервером. Протокол HTTPS использует SSL (Secure Sockets Layer) или более современный TLS (Transport Layer Security) для шифрования данных.

1. Каким образом обеспечивается безопасность контента веб-сервера при работе через HTTPS?

* Шифрование данных: при использовании HTTPS данные, передаваемые между клиентом и сервером, шифруются, что делает их невозможными для прочтения злоумышленниками, перехватывающими трафик.
* Идентификация сервера: сервер предоставляет цифровой сертификат, подтверждающий его легитимность. Этот сертификат выдается сертификационным центром и содержит информацию о владельце сертификата, публичный ключ для шифрования и подпись, подтверждающую подлинность сертификата.

1. Что такое сертификационный центр?

* Сертификационный центр (Центр сертификации) - это доверенная сторона, которая выдает цифровые сертификаты, подтверждающие подлинность владельца сертификата. Пример: Одним из известных сертификационных центров является “Let’s Encrypt”. Он предоставляет бесплатные SSL-сертификаты, которые используются для обеспечения безопасного соединения на множестве веб-сайтов. Владельцы веб-сайтов могут получить сертификат от Let’s Encrypt, чтобы обеспечить шифрование и подтвердить свою легитимность в онлайн-среде.