

# **Отчёт по лабораторной работе №6**

**Мандатное разграничение прав в Linux**

Гаглов Олг НПИБд-01-20

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
2.1	Подготовка . . . . .	5
2.2	Изучение механики SetUID . . . . .	6
<b>3</b>	<b>Выводы</b>	<b>19</b>
	<b>Список литературы</b>	<b>20</b>

## Список иллюстраций

2.1	Настройка httpd . . . . .	5
2.2	Проверка SELinux . . . . .	6
2.3	Запуск сервера 1 . . . . .	7
2.4	Запуск сервера 2 . . . . .	7
2.5	Поиск процессов . . . . .	8
2.6	Просмотр состояний переключателей . . . . .	9
2.7	Статистика seinfo . . . . .	10
2.8	Просмотр директории . . . . .	10
2.9	Работа с файлом . . . . .	11
2.10	Запуск файла . . . . .	12
2.11	Работа с файлом . . . . .	13
2.12	Работа с файлом . . . . .	13
2.13	Перепроверка сайта . . . . .	14
2.14	Анализ логов . . . . .	14
2.15	Анализ логов . . . . .	15
2.16	Настройка конфига . . . . .	15
2.17	Перезапуск httpd . . . . .	16
2.18	Лог файлы . . . . .	16
2.19	Лог файлы . . . . .	17
2.20	Выполнение команды . . . . .	17
2.21	Запуск сервера . . . . .	18
2.22	Доработка файла . . . . .	18

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache

## 2 Выполнение лабораторной работы

### 2.1 Подготовка

1. Установили httpd
2. Задали имя сервера
3. Открыли порты для работы с протоколом http

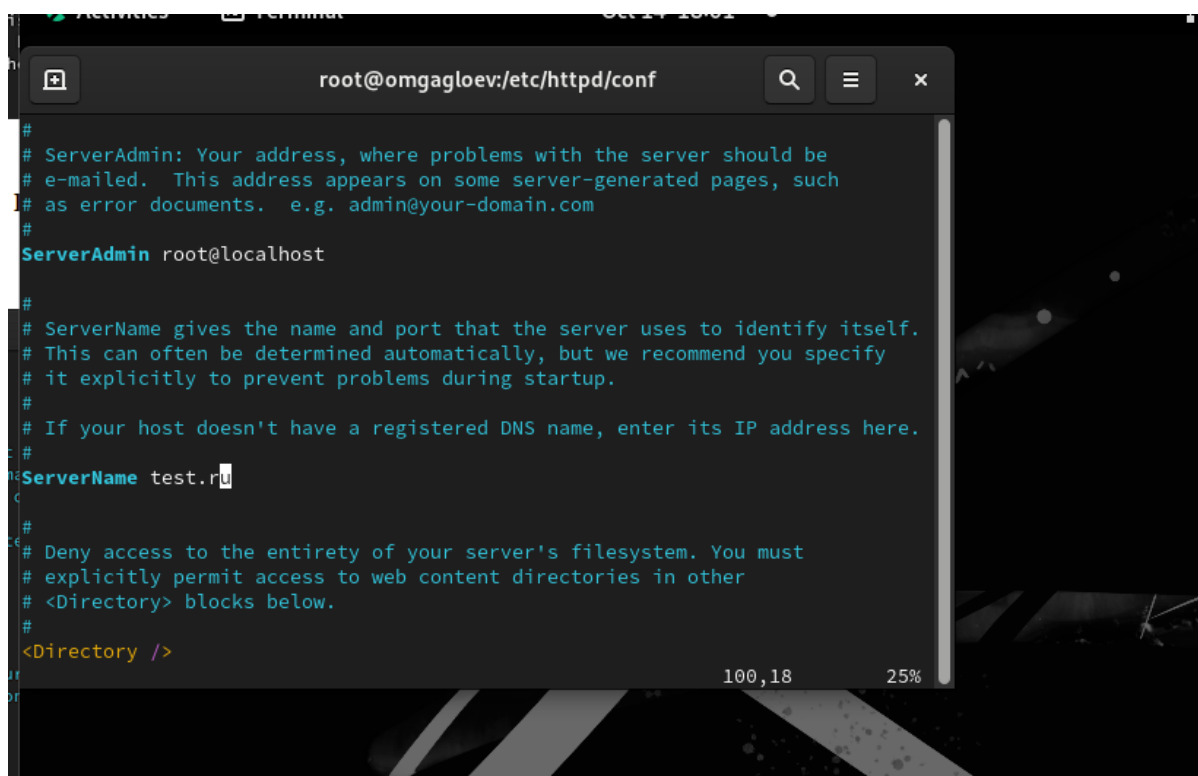
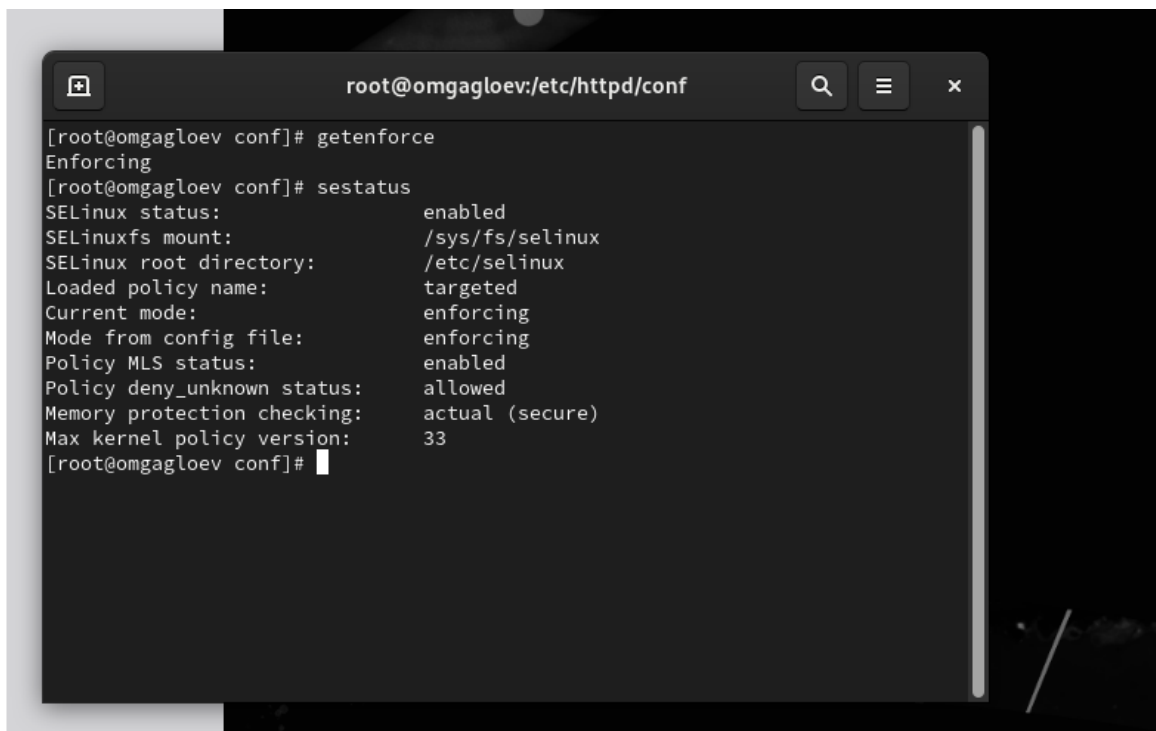


Рис. 2.1: Настройка httpd

## 2.2 Изучение механики SetUID

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

A screenshot of a terminal window titled 'root@omgagloev:/etc/httpd/conf'. The terminal shows the output of the 'getenforce' and 'sestatus' commands. The 'getenforce' command returns 'Enforcing'. The 'sestatus' command returns a detailed status report: SELinux status: enabled, SELinuxfs mount: /sys/fs/selinux, SELinux root directory: /etc/selinux, Loaded policy name: targeted, Current mode: enforcing, Mode from config file: enforcing, Policy MLS status: enabled, Policy deny\_unknown status: allowed, Memory protection checking: actual (secure), and Max kernel policy version: 33.

```
root@omgagloev:/etc/httpd/conf
[root@omgagloev conf]# getenforce
Enforcing
[root@omgagloev conf]# sestatus
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                    enforcing
Mode from config file:           enforcing
Policy MLS status:               enabled
Policy deny_unknown status:      allowed
Memory protection checking:      actual (secure)
Max kernel policy version:       33
[root@omgagloev conf]#
```

Рис. 2.2: Проверка SELinux

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status`. Если не работает, запустите его так же, но с параметром `start`.

```
[root@omgagloev conf]# service httpd status
Redirecting to /bin/systemctl status httpd.service
○ httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset:
   Active: inactive (dead)
   Docs: man:httpd.service(8)
lines 1-4/4 (END)
```

Рис. 2.3: Запуск сервера 1

```
[root@omgagloev conf]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@omgagloev conf]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: active (running) since Sat 2023-10-14 18:11:23 MSK; 3s ago
   Docs: man:httpd.service(8)
  Main PID: 86334 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 37116)
    Memory: 37.4M
       CPU: 107ms
    CGroup: /system.slice/httpd.service
            └─86334 /usr/sbin/httpd -DFOREGROUND
              └─86335 /usr/sbin/httpd -DFOREGROUND
                └─86336 /usr/sbin/httpd -DFOREGROUND
                  └─86337 /usr/sbin/httpd -DFOREGROUND
                    └─86338 /usr/sbin/httpd -DFOREGROUND

Oct 14 18:11:23 omgagloev.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 18:11:23 omgagloev.localdomain httpd[86334]: Server configured, listening on: port 80
Oct 14 18:11:23 omgagloev.localdomain systemd[1]: Started The Apache HTTP Server.
[root@omgagloev conf]#
```

Рис. 2.4: Запуск сервера 2

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`

```
Oct 17 10:11:23 omgagloev.localdomain systemd[1]: Started the Apache HTTP Server.
[root@omgagloev conf]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      86334  0.0  0.1  20116 11532 ?        Ss   18:11
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  86335  0.0  0.1  21600  7516 ?        S    18:11
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  86336  0.0  0.2  2259020 15208 ?       Sl   18:11
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  86337  0.1  0.3  2455692 19292 ?       Sl   18:11
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  86338  0.0  0.2  2259020 15200 ?       Sl   18:11
0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 86582 0.0  0.0  221664 2448 pts/0 S+
18:13  0:00 grep --color=auto httpd
[root@omgagloev conf]#
```

Рис. 2.5: Поиск процессов

- Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся в положении «off».



```
Without options, show SELinux status.
[root@omgagloev conf]# sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_manage_courier_spool off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
```

Рис. 2.6: Просмотр состояний переключателей

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.

```
[root@omgagloev conf]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 135      Permissions:          457
Sensitivities:           1        Categories:           1024
Types:                   5100     Attributes:            258
Users:                   8         Roles:                 14
Booleans:                 353     Cond. Expr.:          384
Allow:                   65008    Neverallow:            0
Auditallow:              170     Dontaudit:             8572
Type_trans:              265344   Type_change:           87
Type_member:              35      Range_trans:           6164
Role allow:               38      Role_trans:            420
Constraints:              70     Validatetrans:          0
MLS Constrain:            72     MLS Val. Tran:          0
Permissives:              2       Polcap:                 6
Defaults:                 7       Typebounds:            0
Allowxperm:               0       Neverallowxperm:        0
Auditallowxperm:          0       Dontauditxperm:         0
Ibendportcon:             0       Ibpkeycon:              0
Initial SIDs:             27      Fs_use:                 35
Genfscon:                 109     Portcon:                660
Netifcon:                 0       Nodecon:                0
[root@omgagloev conf]#
```

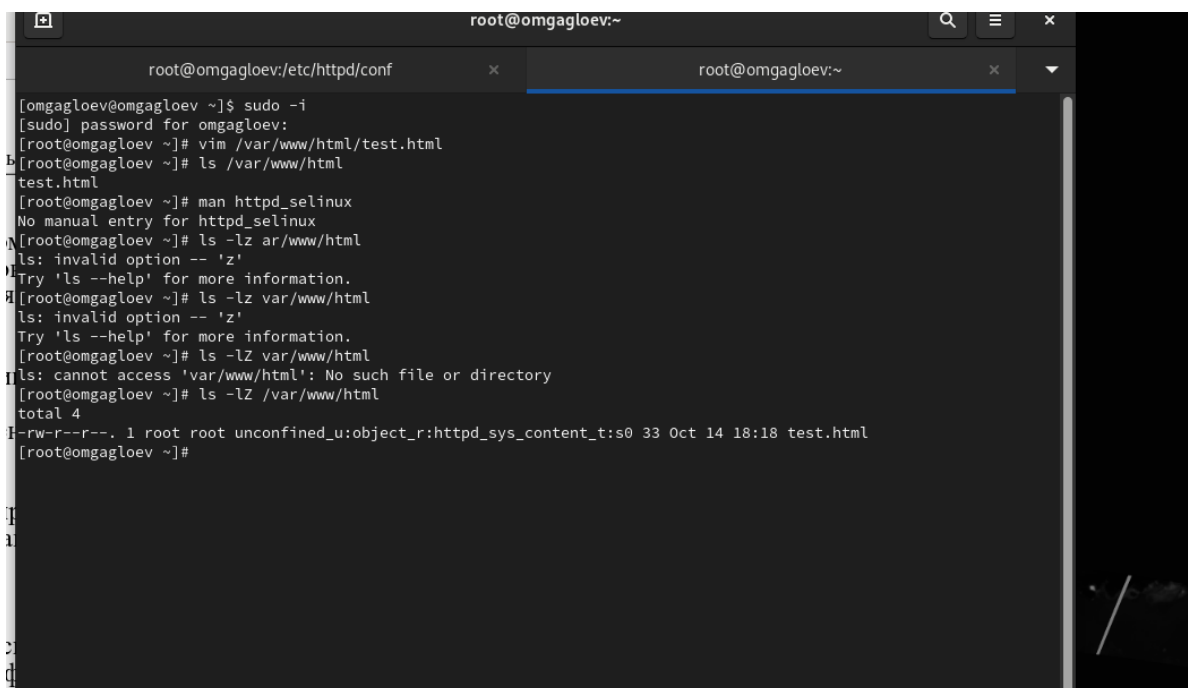
Рис. 2.7: Статистика seinfo

6. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www`. В поддиректориях могут располагаться системные скрипты и контент для http.
7. Определите тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html`. В директории изначально нет файлов.
8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html. Создавать файлы может только root.

```
[root@omgagloev conf]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 23:21 html
[root@omgagloev conf]# ls -lZ /var/www/html
total 0
[root@omgagloev conf]# ls /var/www/html
[root@omgagloev conf]#
```

Рис. 2.8: Просмотр директории

9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания: Test
10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.



```
root@omgagloev:~  
root@omgagloev:/etc/httpd/conf  
[omgagloev@omgagloev ~]$ sudo -i  
[sudo] password for omgagloev:  
[root@omgagloev ~]# vim /var/www/html/test.html  
[root@omgagloev ~]# ls /var/www/html  
test.html  
[root@omgagloev ~]# man httpd_selinux  
No manual entry for httpd_selinux  
[root@omgagloev ~]# ls -lz ar/www/html  
ls: invalid option -- 'z'  
Try 'ls --help' for more information.  
[root@omgagloev ~]# ls -lz var/www/html  
ls: invalid option -- 'z'  
Try 'ls --help' for more information.  
[root@omgagloev ~]# ls -lZ var/www/html  
ls: cannot access 'var/www/html': No such file or directory  
[root@omgagloev ~]# ls -lZ /var/www/html  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 14 18:18 test.html  
[root@omgagloev ~]#
```

Рис. 2.9: Работа с файлом

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён.

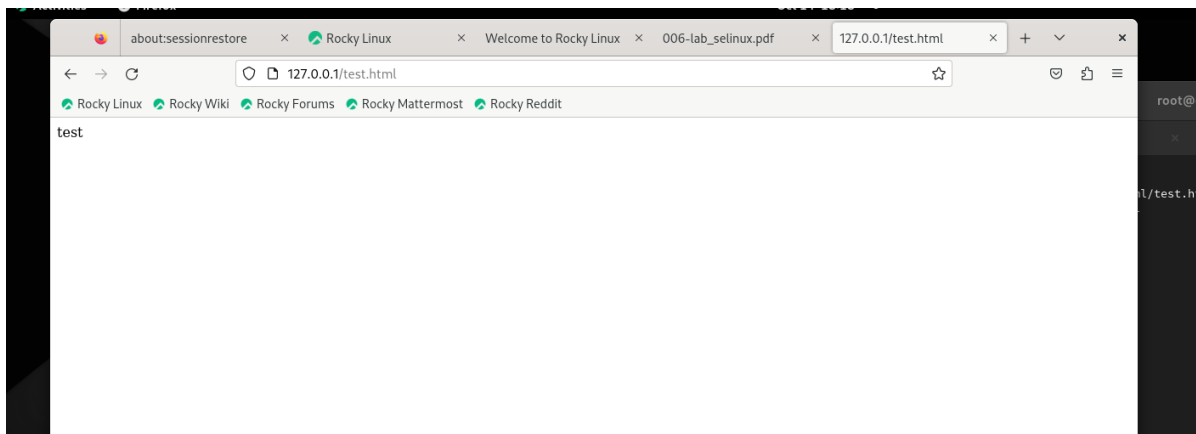


Рис. 2.10: Запуск файла

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`. `ls -Z /var/www/html/test.html`. Основным контекстом является `httpd_sys_content_t`, его мы и увидели в выводе команды.
13. Измените контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` После этого проверьте, что контекст поменялся.

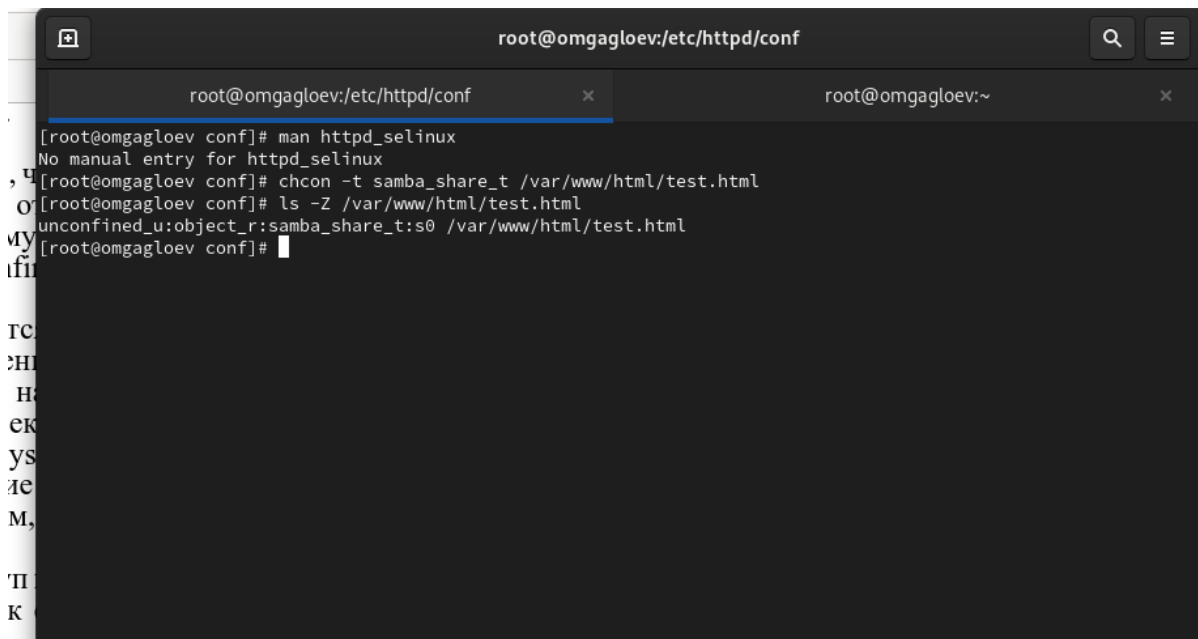


Рис. 2.11: Работа с файлом

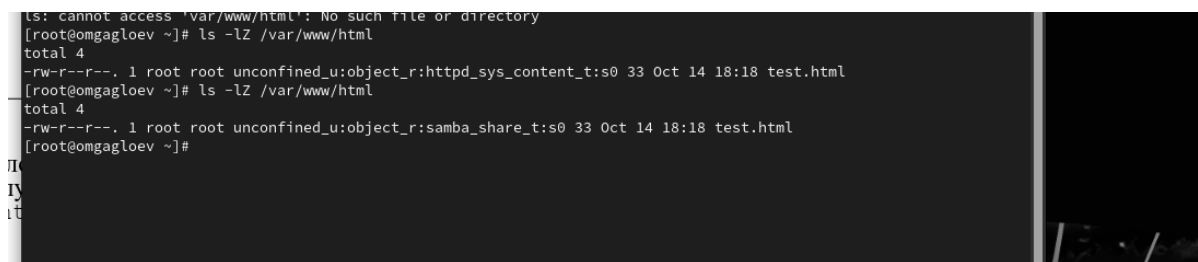


Рис. 2.12: Работа с файлом

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.` При изменении контекста файл стал считаться чужим для http и программа не может его прочитать.

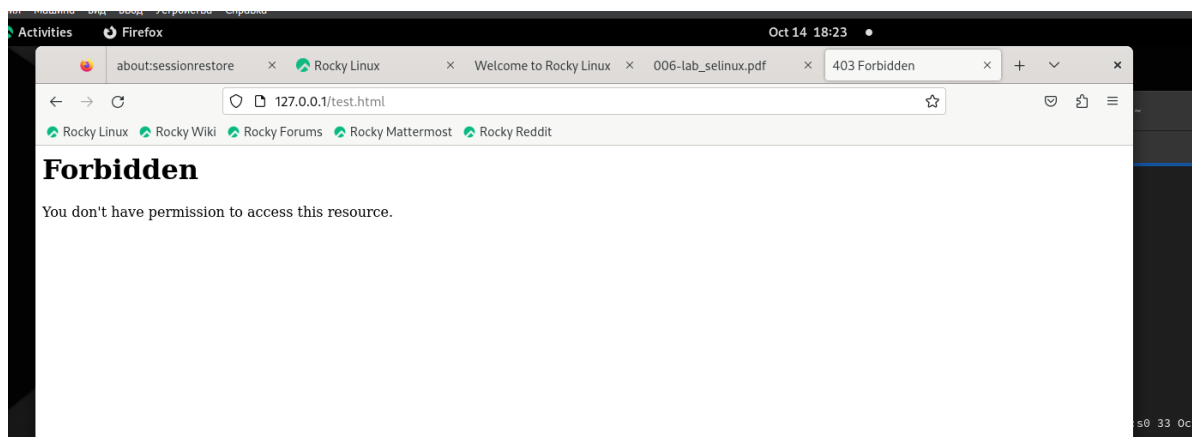
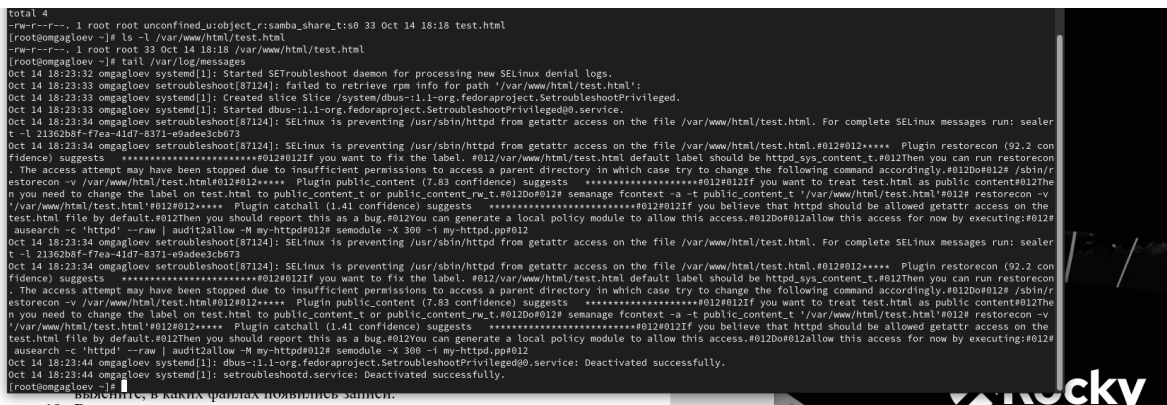


Рис. 2.13: Перепроверка сайта

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы `setroubleshootd` и `auditd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.



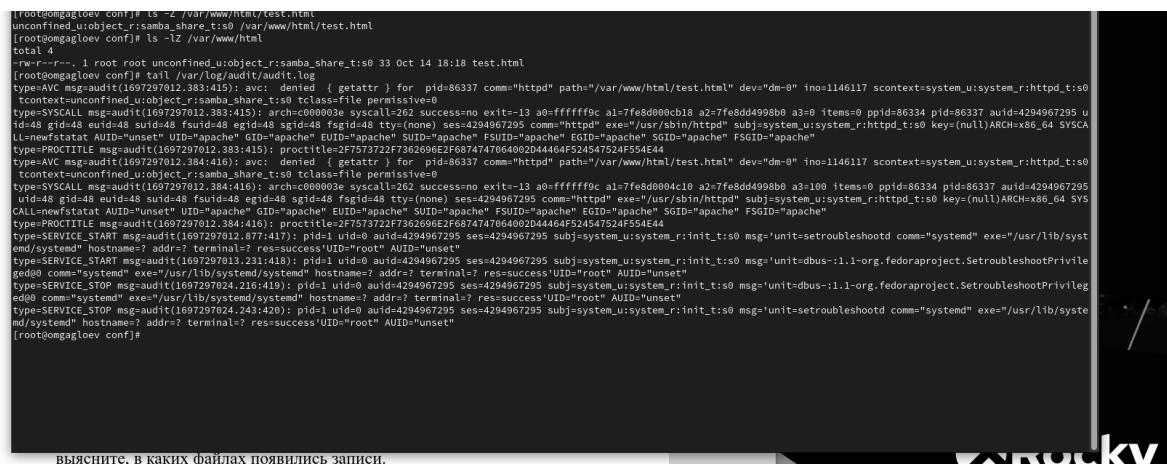


Рис. 2.15: Анализ логов

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.

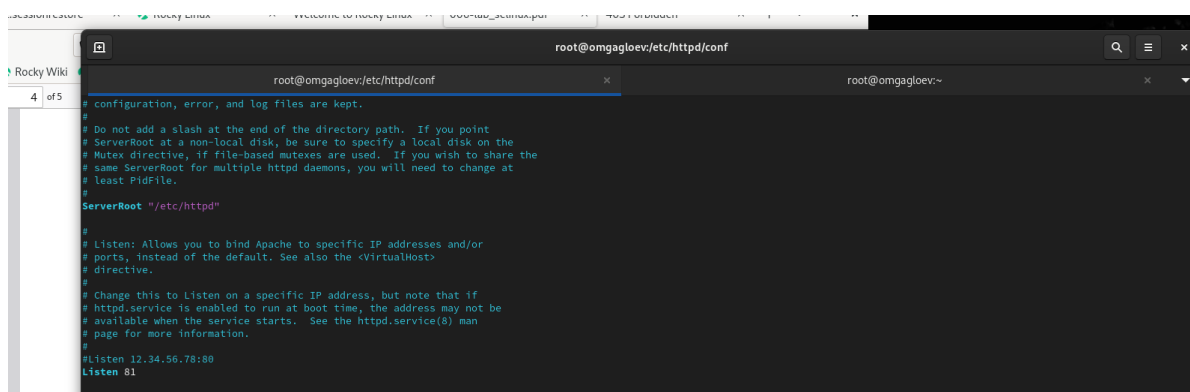


Рис. 2.16: Настройка конфига

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? Сбой не происходит, порт 81 уже вписан в разрешенные

```
root@omgagloev:/etc/httpd/conf

[root@omgagloev conf]# ls
httpd.conf  magic
[root@omgagloev conf]# vim httpd.conf
[root@omgagloev conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@omgagloev conf]#
```

Рис. 2.17: Перезапуск httpd

18. Проанализируйте лог-файлы: `tail -nl /var/log/messages` Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи.

```
[root@omgagloev conf]# tail -nl /var/log/messages
Oct 14 18:23:44 omgagloev systemd[1]: setroubleshoot.service: Deactivated successfully.
Oct 14 18:28:12 omgagloev gnome-shell[1968]: Window manager warning: last_user_time (2448524) is greater than comparison timestamp (2448494). This most likely represents a buggy client
sending inaccurate timestamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Oct 14 18:28:12 omgagloev gnome-shell[1968]: Window manager warning: W1 appears to be one of the offending windows with a timestamp of 2448524. Working around...
Oct 14 18:28:56 omgagloev systemd[1]: Stopping The Apache HTTP Server...
Oct 14 18:28:57 omgagloev systemd[1]: httpd.service: Deactivated successfully.
Oct 14 18:28:57 omgagloev systemd[1]: Stopped The Apache HTTP Server.
Oct 14 18:28:57 omgagloev systemd[1]: httpd.service: Consumed 3.669s CPU time.
Oct 14 18:28:57 omgagloev systemd[1]: Starting The Apache HTTP Server...
Oct 14 18:28:57 omgagloev httpd[87202]: Server configured, listening on: port 81
Oct 14 18:28:57 omgagloev systemd[1]: Started The Apache HTTP Server.
[root@omgagloev conf]# cat /var/log/http/error_log
cat: /var/log/http/error_log: No such file or directory
[root@omgagloev conf]# cat /var/log/httpd/error_log
[Sat Oct 14 18:11:23.487696 2023] [core:notice] [pid 86334:tid 86334] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 14 18:11:23.488144 2023] [suexec:notice] [pid 86334:tid 86334] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 14 18:11:23.497553 2023] [lbmethod_heartbeat:notice] [pid 86334:tid 86334] AH02282: No slotmem from mod_heartbeat
[Sat Oct 14 18:11:23.501932 2023] [mpm_event:notice] [pid 86334:tid 86334] AH00489: Apache/2.4.53 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 14 18:11:23.501953 2023] [core:notice] [pid 86334:tid 86334] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Oct 14 18:23:32.384722 2023] [core:error] [pid 86337:tid 86519] (13)Permission denied: [client 127.0.0.1:48798] AH00035: access to /test.html denied (filesystem path '/var/www/html
/test.html') because search permissions are missing on a component of the path
[Sat Oct 14 18:28:56.481446 2023] [mpm_event:notice] [pid 86334:tid 86334] AH00492: caught SIGWINCH, shutting down gracefully
[Sat Oct 14 18:28:57.532182 2023] [core:notice] [pid 87202:tid 87202] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 14 18:28:57.532668 2023] [suexec:notice] [pid 87202:tid 87202] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 14 18:28:57.540595 2023] [lbmethod_heartbeat:notice] [pid 87202:tid 87202] AH02282: No slotmem from mod_heartbeat
[Sat Oct 14 18:28:57.543439 2023] [mpm_event:notice] [pid 87202:tid 87202] AH00489: Apache/2.4.53 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 14 18:28:57.543458 2023] [core:notice] [pid 87202:tid 87202] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[root@omgagloev conf]#
semanage port -l | grep http_port_t
```

Рис. 2.18: Лог файлы



```
root@omgagloev:/etc/httpd/conf
root@omgagloev:/etc/httpd/conf
root@omgagloev:~
[root@omgagloev conf]# cat /var/log/httpd/access_log
127.0.0.1 - - [14/Oct/2023:18:18:43 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [14/Oct/2023:18:18:43 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [14/Oct/2023:18:21:34 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [14/Oct/2023:18:23:32 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
[root@omgagloev conf]# cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1694256886.346:113): op=start ver=3.0.7 format=enriched kernel=5.14.0-284.11.1.el9_2.x86_64 auid=4294967295 pid=739 uid=0 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=successAUID="unset" UID="root"
type=SERVICE_START msg=audit(1694256886.352:5): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-journal-catalog-update comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=successUID="root" AUID="unset"'
type=CONFIG_CHANGE msg=audit(1694256886.405:6): op=set audit_backlog_limit=8192 old=64 auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_service_t:s0 res=IAUID="unset"
type=SYSCALL msg=audit(1694256886.405:6): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffef966c1f0 a2=3c a3=0 items=0 ppid=744 pid=754 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUI
type=PROCTITLE msg=audit(1694256886.405:6): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1694256886.405:7): op=set audit_failure=1 old=1 auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_service_t:s0 res=IAUID="unset"
type=SYSCALL msg=audit(1694256886.405:7): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffef966c1f0 a2=3c a3=0 items=0 ppid=744 pid=754 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUI
type=PROCTITLE msg=audit(1694256886.405:7): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1694256886.407:8): op=set audit_backlog_wait_time=60000 old=60000 auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_service_t:s0 res=IAUID="u
type=SYSCALL msg=audit(1694256886.407:8): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffef966c1f0 a2=3c a3=0 items=0 ppid=744 pid=754 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUI
type=PROCTITLE msg=audit(1694256886.407:8): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=SERVICE_START msg=audit(1694256886.410:9): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=successUID="root" AUID="unset"'
type=SYSTEM_BOOT msg=audit(1694256886.419:10): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='comm="systemd-update-utmp" exe="/usr/lib/systemd/systemd-update-utmp" hostname=? addr=? terminal=? res=successUID="root" AUID="unset"'
type=SERVICE_START msg=audit(1694256886.424:11): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-update-utmp comm="systemd" exe="/usr/lib/systemd/systemd-update-utmp" hostname=? addr=? terminal=? res=successUID="root" AUID="unset"'
type=SERVICE_START msg=audit(1694256887.104:12): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=ldconfig comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=successUID="root" AUID="unset"'
type=SERVICE_START msg=audit(1694256887.114:13): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-update-done comm="systemd" exe="/usr/lib/systemd/systemd-update-done" hostname=? addr=? terminal=? res=successUID="root" AUID="unset"'
```

Рис. 2.19: Лог файлы

19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` Убедитесь, что порт 81 появился в списке.

```
defaults to s0.
1:81 -p PROTO, --proto PROTO
Protocol for the specified port (tcp|udp|dccp|sctp) or internet protocol version for the
a — C [root@omgagloev conf]# semmanage port -l | grep http_port_t
i файл http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000
y: pegasus_http_port_t tcp 5988
[root@omgagloev conf]#
```

Рис. 2.20: Выполнение команды

20. Попробуйте запустить веб-сервер Apache ещё раз.

```
-p pegasus_http_port_t tcp 5988
[root@omgagloev conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@omgagloev conf]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: active (running) since Sat 2023-10-14 18:35:36 MSK; 6s ago
     Docs: man:httpd.service(8)
    Main PID: 87510 (httpd)
   Status: "Started, listening on: port 81"
     Tasks: 213 (limit: 37116)
    Memory: 49.0M
       CPU: 81ms
    CGroup: /system.slice/httpd.service
            └─87510 /usr/sbin/httpd -DFOREGROUND
              └─87511 /usr/sbin/httpd -DFOREGROUND
                └─87512 /usr/sbin/httpd -DFOREGROUND
                  └─87513 /usr/sbin/httpd -DFOREGROUND
                    └─87514 /usr/sbin/httpd -DFOREGROUND

Oct 14 18:35:36 omgagloev.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 18:35:36 omgagloev.localdomain httpd[87510]: Server configured, listening on: port 81
Oct 14 18:35:36 omgagloev.localdomain systemd[1]: Started The Apache HTTP Server.
[root@omgagloev conf]#
```

Рис. 2.21: Запуск сервера

21. Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`:  
`chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Вы должны увидеть содержимое файла — слово «test».
22. Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`.
23. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
24. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

```
[root@omgagloev conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@omgagloev conf]# vim httpd.conf
[root@omgagloev conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@omgagloev conf]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@omgagloev conf]#
```

Рис. 2.22: Доработка файла

## **3 Выводы**

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux и apache

# Список литературы

1. SELinux в CentOS
2. Веб-сервер Apache