INSTITUTO TECNOLOGICO DE CULIACAN

INGENIERIA EN SISTEMAS COMPUTACIONALES

ADMINISTRACION DE REDES

INSTALACION SERVICIOS HTTP

ALUMNO*:*

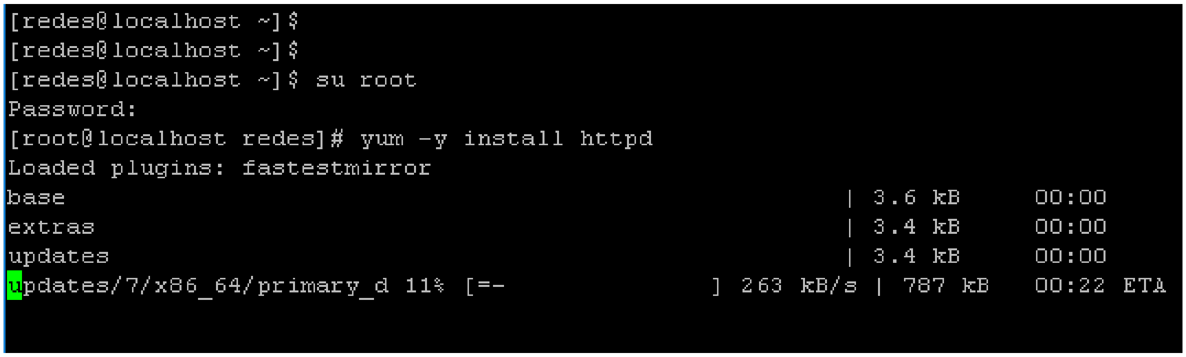
ROSALES CORVERA HERNAN ENRIQUE

DOCENTE*: LUIS ERNESTO LIZARRAGA BOLAÑOS*

CULIACAN SINALOA, 02 DE JULIO DEL 2019

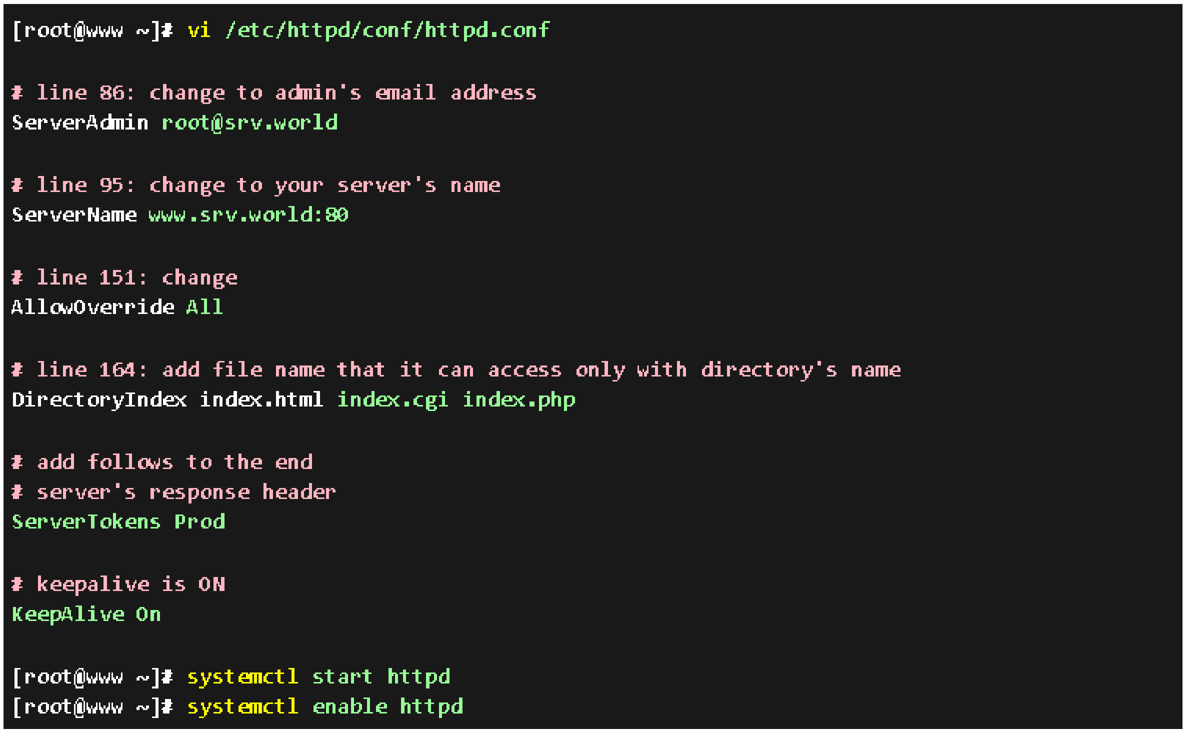
APACHE HTTPD : INSTALL HTTPD

Paso 1.- procederemos a instalar HTTPD directamente en el servidor:

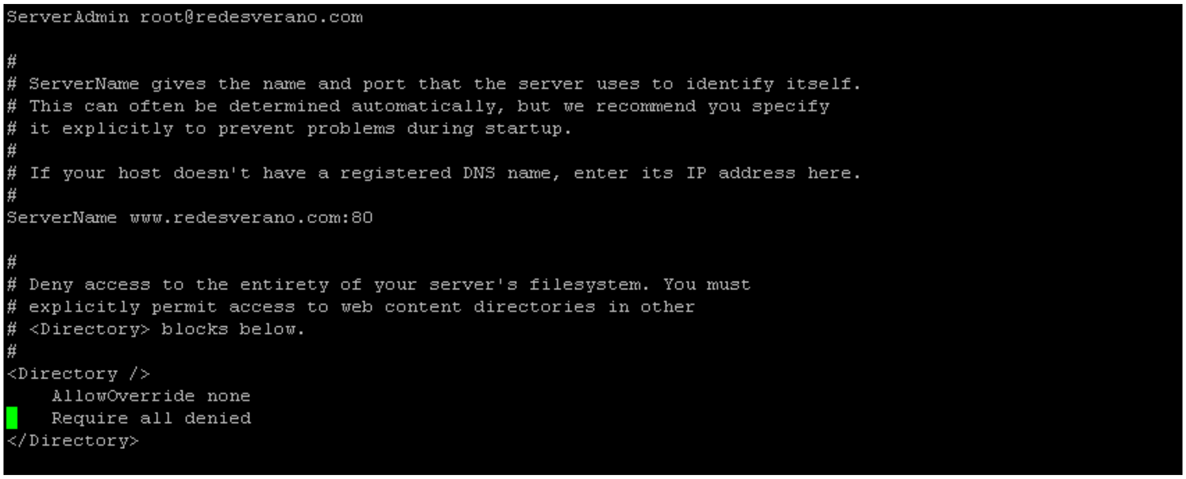


```
[redes@localhost ~]$
[redes@localhost ~]$
[redes@localhost ~]$ su root
Password:
[root@localhost redes]# yum -y install httpd
Loaded plugins: fastestmirror
base                                                     | 3.6 kB     00:00
extras                                                   | 3.4 kB     00:00
updates                                                  | 3.4 kB     00:00
updates/7/x86_64/primary_d 11% [=-               ] 263 kB/s | 787 kB   00:22 ETA
```

Procederemos a Configurar el HTTPD utilizaremos el comando nano /etc/httpd/conf/httpd.conf

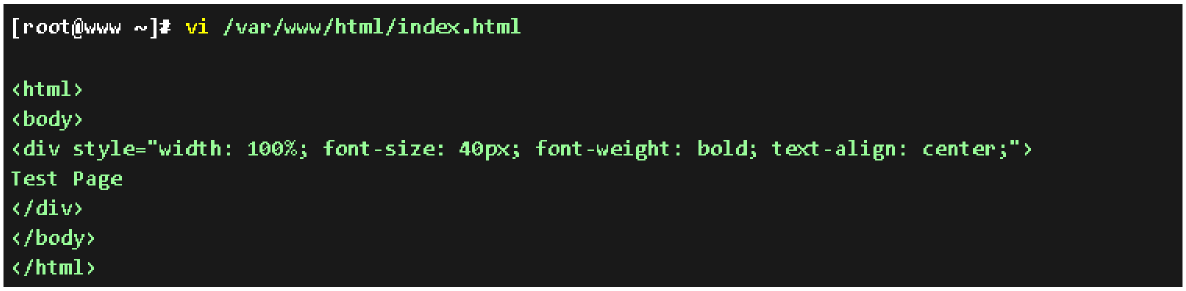


```
[root@www ~]# vi /etc/httpd/conf/httpd.conf

# line 86: change to admin's email address
ServerAdmin root@srv.world

# line 95: change to your server's name
ServerName www.srv.world:80

# line 151: change
AllowOverride All

# line 164: add file name that it can access only with directory's name
DirectoryIndex index.html index.cgi index.php

# add follows to the end
# server's response header
ServerTokens Prod

# keepalive is ON
KeepAlive On

[root@www ~]# systemctl start httpd
[root@www ~]# systemctl enable httpd
```



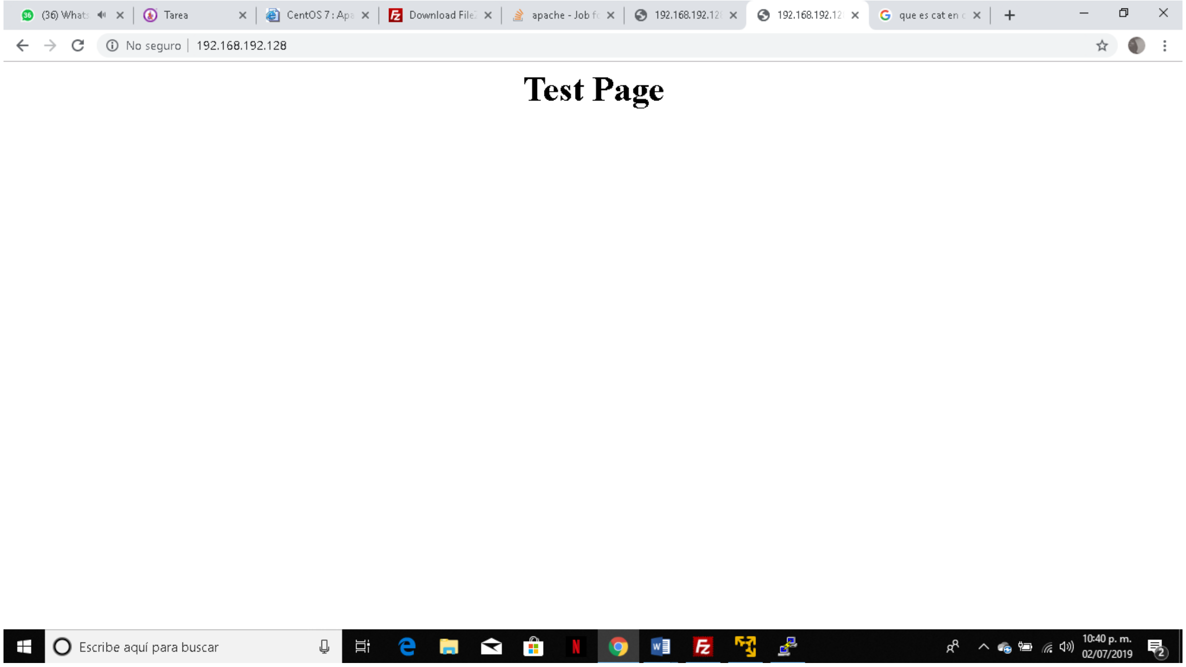
```
ServerAdmin root@redesverano.com

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName www.redesverano.com:80

#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>
```

En el siguiente paso, procederemos a crear una página de prueba en html, esto para acceder a ella después desde el navegador la computadora misma.



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

<html>
<body>
<div style="width: 100%; font-size: 40px; font-weight: bold; text-align: center;">
Test Page
</div>
</body>
</html>
```

Ahora pasaremos a probar lo realizado, accediendo desde un navegador de la computadora al nombre del servidor en nuestro caso es www.redesverano.com:80

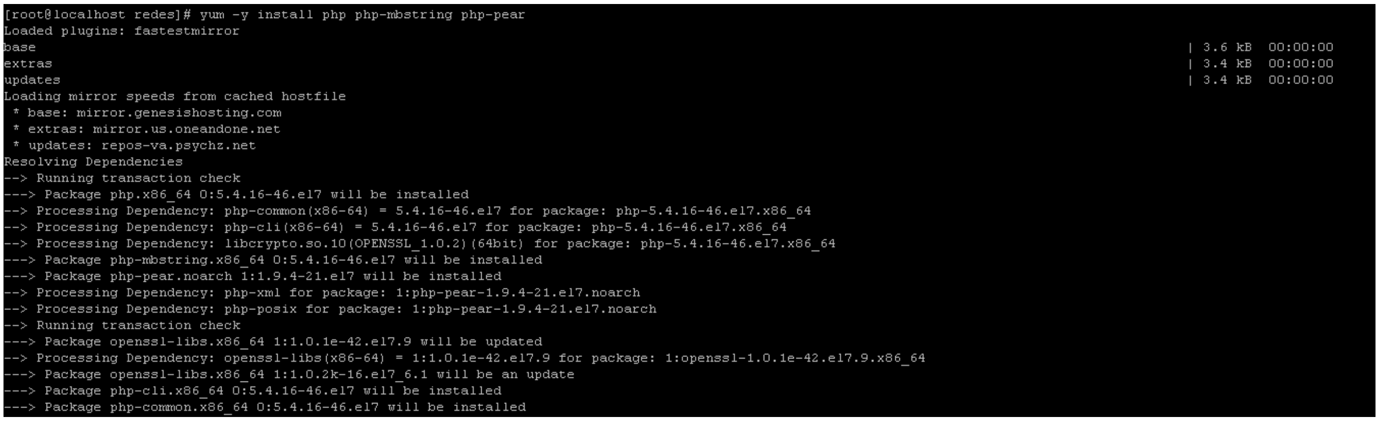


192.168.192.128

Test Page

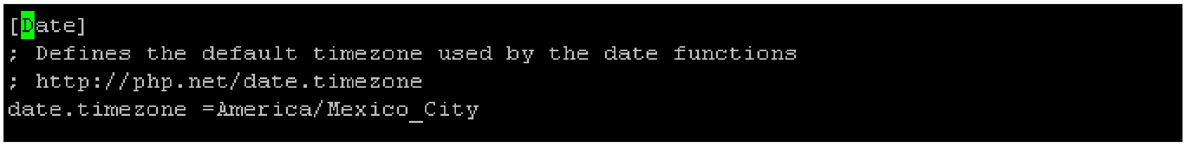
APACHE HTTPD : USE PHP SCRIPTS

En este punto usaremos ahora un script realizado en php para accede desde el navegador web, el primer paso a realizar es el instalar el php mediante el comando yum -y install php php-mbstring php-pear



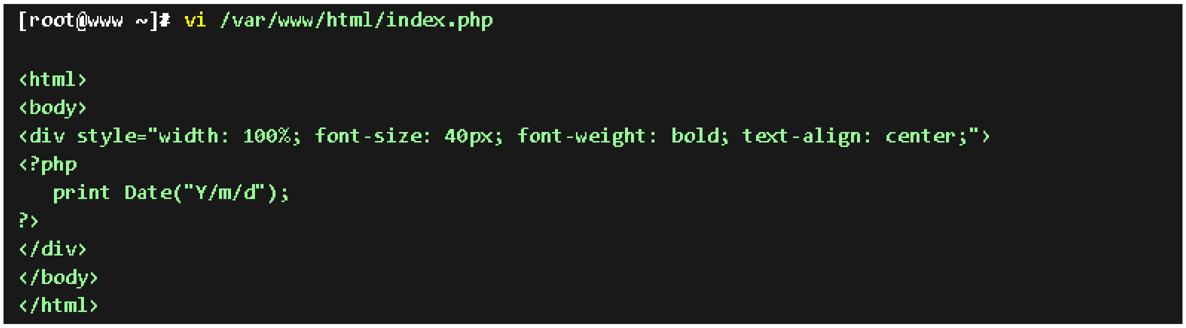
```
[root@localhost redes]# yum -y install php php-mbstring php-pear
Loaded plugins: fastestmirror
base                                                                                                                                             | 3.6 kB  00:00:00
extras                                                                                                                                           | 3.4 kB  00:00:00
updates                                                                                                                                          | 3.4 kB  00:00:00
Loading mirror speeds from cached hostfile
 * base: mirror.genesishosting.com
 * extras: mirror.us.oneandone.net
 * updates: repos-va.psychz.net
Resolving Dependencies
--> Running transaction check
---> Package php.x86_64 0:5.4.16-46.el7 will be installed
--> Processing Dependency: php-common(x86-64) = 5.4.16-46.el7 for package: php-5.4.16-46.el7.x86_64
--> Processing Dependency: php-cli(x86-64) = 5.4.16-46.el7 for package: php-5.4.16-46.el7.x86_64
--> Processing Dependency: libcrypto.so.10(OPENSSL_1.0.2)(64bit) for package: php-5.4.16-46.el7.x86_64
---> Package php-mbstring.x86_64 0:5.4.16-46.el7 will be installed
---> Package php-pear.noarch 1:1.9.4-21.el7 will be installed
--> Processing Dependency: php-xml for package: 1:php-pear-1.9.4-21.el7.noarch
--> Processing Dependency: php-posix for package: 1:php-pear-1.9.4-21.el7.noarch
--> Running transaction check
---> Package openssl-libs.x86_64 1:1.0.1e-42.el7.9 will be updated
--> Processing Dependency: openssl-libs(x86-64) = 1:1.0.1e-42.el7.9 for package: 1:openssl-1.0.1e-42.el7.9.x86_64
---> Package openssl-libs.x86_64 1:1.0.2k-16.el7_6.1 will be an update
---> Package php-cli.x86_64 0:5.4.16-46.el7 will be installed
---> Package php-common.x86_64 0:5.4.16-46.el7 will be installed
```

Ahora pondremos el comando nano /etc/php.ini, para buscar la línea 878 y configurar la zona horaria ala nuestra:



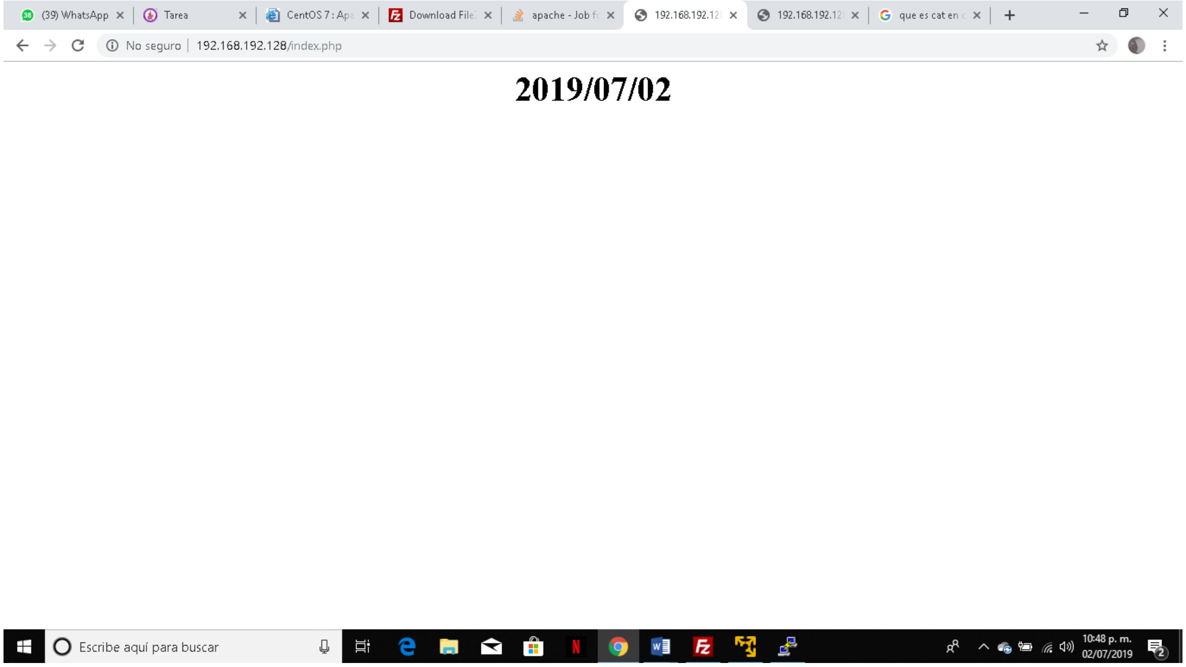
```
[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
date.timezone =America/Mexico_City
```

Ahora, pasaremos a crear una pagina sencilla en php, en donde mostraremos la hora actual del equipo:



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

<html>
<body>
<div style="width: 100%; font-size: 40px; font-weight: bold; text-align: center;">
<?php
   print Date("Y/m/d");
?>
</div>
</body>
</html>
```

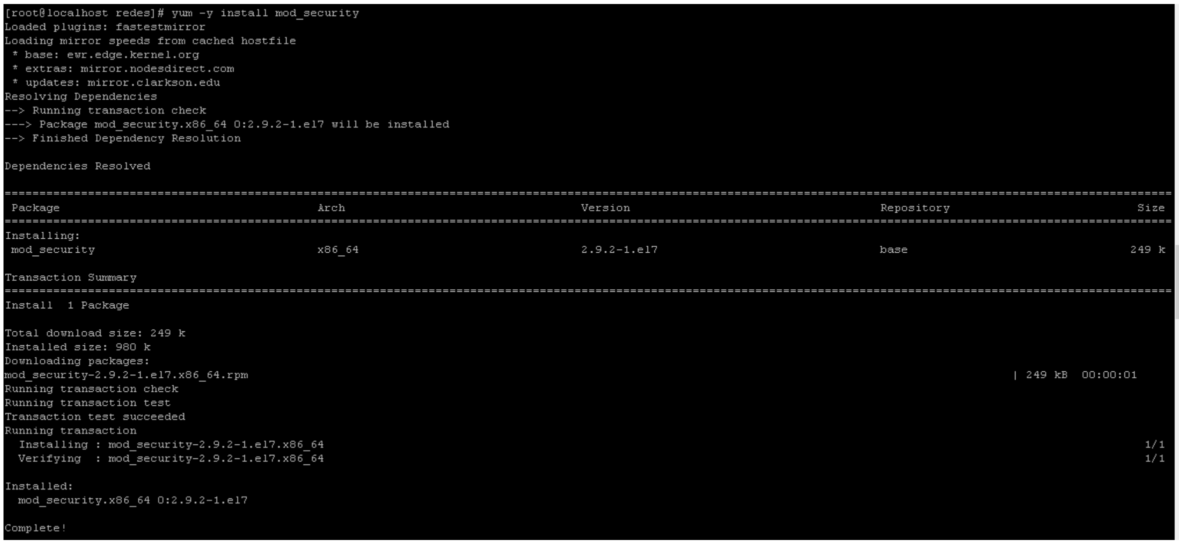
Y al final, al acceder desde el navegador, debe de verse asi



2019/07/02

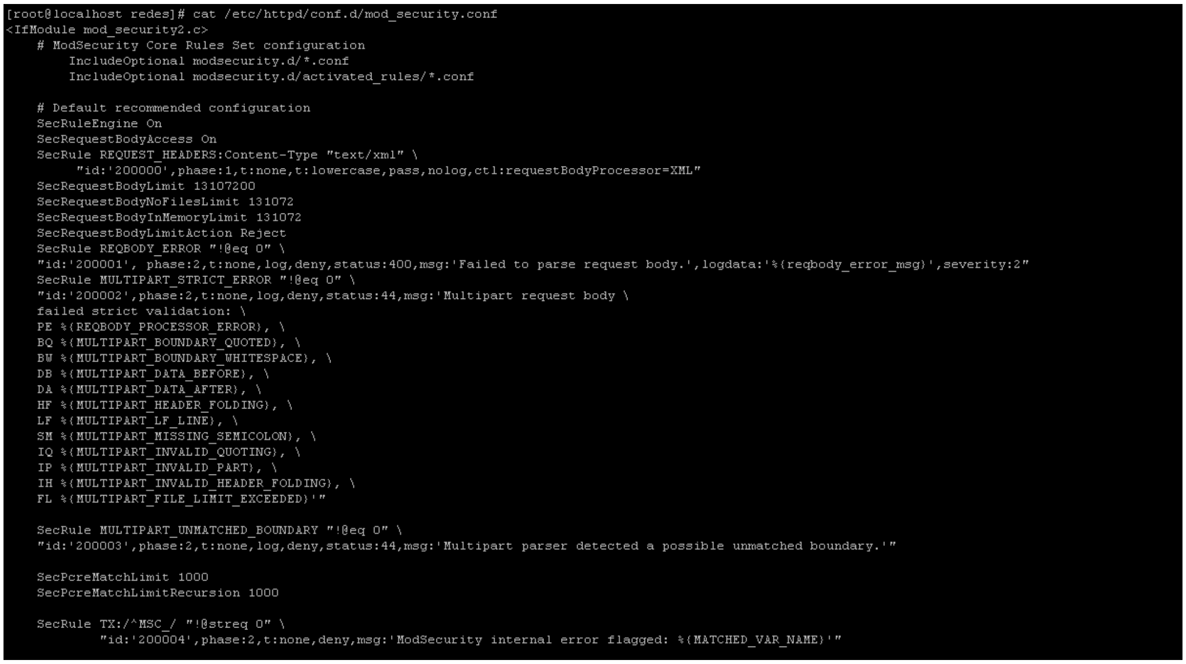
APACHE HTTPD : USE MOD_SECURITY

Procederemos a instalar mod_security.



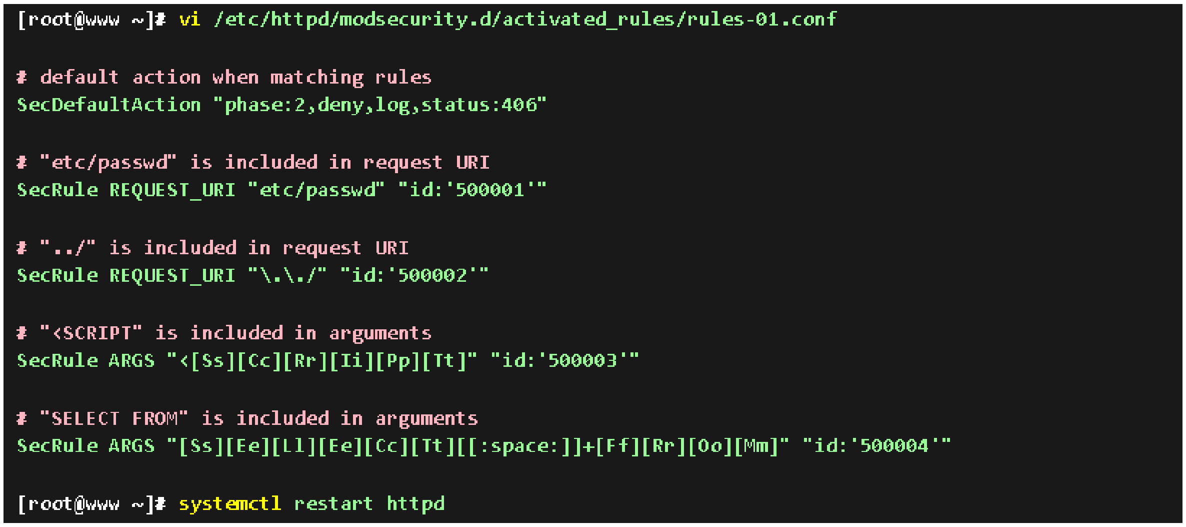
```
[root@localhost redes]# yum -y install mod_security
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ewr.edge.kernel.org
 * extras: mirror.nodesdirect.com
 * updates: mirror.clarkson.edu
Resolving Dependencies
--> Running transaction check
---> Package mod_security.x86_64 0:2.9.2-1.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

========================================================================================================================================================================
 Package                                     Arch                                  Version                                    Repository                           Size
========================================================================================================================================================================
Installing:
 mod_security                                x86_64                                2.9.2-1.el7                                base                                249 k

Transaction Summary
========================================================================================================================================================================
Install  1 Package

Total download size: 249 k
Installed size: 980 k
Downloading packages:
mod_security-2.9.2-1.el7.x86_64.rpm                                                                                                              | 249 kB  00:00:01
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : mod_security-2.9.2-1.el7.x86_64                                                                                                                      1/1
  Verifying  : mod_security-2.9.2-1.el7.x86_64                                                                                                                      1/1

Installed:
  mod_security.x86_64 0:2.9.2-1.el7

Complete!
```

Despues de instalar , podemos ver que la configuraciones iniciales están situadas en el siguiente directorio. A su vez, podemos también modificar reglas para nuestros beneficios:



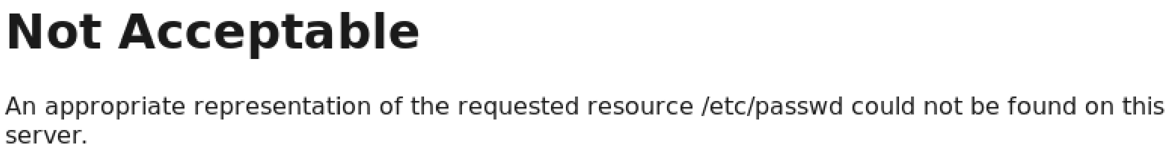
```
[root@localhost redes]# cat /etc/httpd/conf.d/mod_security.conf
<IfModule mod_security2.c>
    # ModSecurity Core Rules Set configuration
        IncludeOptional modsecurity.d/*.conf
        IncludeOptional modsecurity.d/activated_rules/*.conf

    # Default recommended configuration
    SecRuleEngine On
    SecRequestBodyAccess On
    SecRule REQUEST_HEADERS:Content-Type "text/xml" \
         "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"
    SecRequestBodyLimit 13107200
    SecRequestBodyNoFilesLimit 131072
    SecRequestBodyInMemoryLimit 131072
    SecRequestBodyLimitAction Reject
    SecRule REQBODY_ERROR "!@eq 0" \
    "id:'200001', phase:2,t:none,log,deny,status:400,msg:'Failed to parse request body.',logdata:'%{reqbody_error_msg}',severity:2"
    SecRule MULTIPART_STRICT_ERROR "!@eq 0" \
    "id:'200002',phase:2,t:none,log,deny,status:44,msg:'Multipart request body \
    failed strict validation: \
    PE %{REQBODY_PROCESSOR_ERROR}, \
    BQ %{MULTIPART_BOUNDARY_QUOTED}, \
    BW %{MULTIPART_BOUNDARY_WHITESPACE}, \
    DB %{MULTIPART_DATA_BEFORE}, \
    DA %{MULTIPART_DATA_AFTER}, \
    HF %{MULTIPART_HEADER_FOLDING}, \
    LF %{MULTIPART_LF_LINE}, \
    SM %{MULTIPART_MISSING_SEMICOLON}, \
    IQ %{MULTIPART_INVALID_QUOTING}, \
    IP %{MULTIPART_INVALID_PART}, \
    IH %{MULTIPART_INVALID_HEADER_FOLDING}, \
    FL %{MULTIPART_FILE_LIMIT_EXCEEDED}'"

    SecRule MULTIPART_UNMATCHED_BOUNDARY "!@eq 0" \
    "id:'200003',phase:2,t:none,log,deny,status:44,msg:'Multipart parser detected a possible unmatched boundary.'"

    SecPcreMatchLimit 1000
    SecPcreMatchLimitRecursion 1000

    SecRule TX:/^MSC_/ "!@streq 0" \
            "id:'200004',phase:2,t:none,deny,msg:'ModSecurity internal error flagged: %{MATCHED_VAR_NAME}'"
```

Vamos a cambiar algunas reglas, para probar que todo funcione correctamente (o tal vez no)



```
[root@www ~]# vi /etc/httpd/modsecurity.d/activated_rules/rules-01.conf

# default action when matching rules
SecDefaultAction "phase:2,deny,log,status:406"

# "etc/passwd" is included in request URI
SecRule REQUEST_URI "etc/passwd" "id:'500001'"

# "../" is included in request URI
SecRule REQUEST_URI "\.\./" "id:'500002'"

# "<SCRIPT" is included in arguments
SecRule ARGS "<[Ss][Cc][Rr][Ii][Pp][Tt]" "id:'500003'"

# "SELECT FROM" is included in arguments
SecRule ARGS "[Ss][Ee][Ll][Ee][Cc][Tt][[:space:]]+[Ff][Rr][Oo][Mm]" "id:'500004'"

[root@www ~]# systemctl restart httpd
```

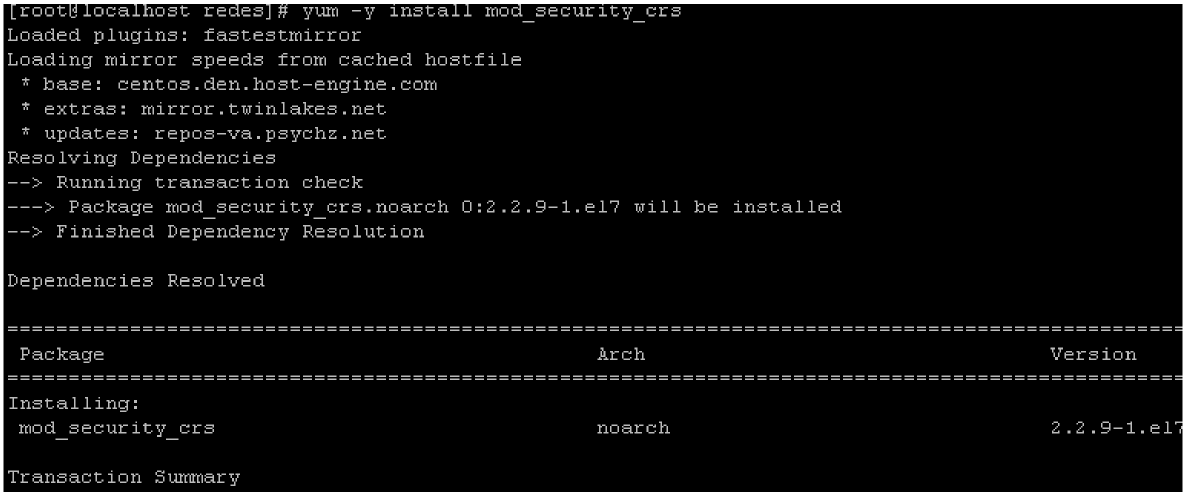
Accederemos a la URL y comprobaremos si podemos acceder normalmente ala URL y se obtiene el siguiente pantallazo



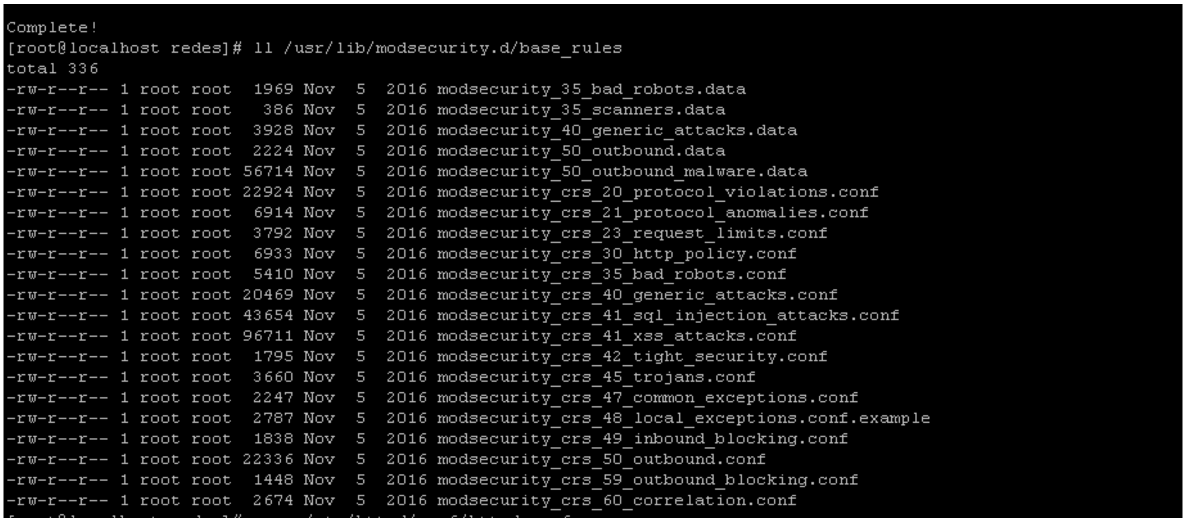
Not Acceptable

An appropriate representation of the requested resource /etc/passwd could not be found on this server.

Por último, procederemos a instalar el mod security crs con el siguiente comando:



```
[root@localhost redes]# yum -y install mod_security_crs
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.den.host-engine.com
 * extras: mirror.twinlakes.net
 * updates: repos-va.psychz.net
Resolving Dependencies
--> Running transaction check
---> Package mod_security_crs.noarch 0:2.2.9-1.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

==========================================================================================================================
 Package                                               Arch                                      Version
==========================================================================================================================
Installing:
 mod_security_crs                                      noarch                                    2.2.9-1.el7

Transaction Summary
```



```
Complete!
[root@localhost redes]# ll /usr/lib/modsecurity.d/base_rules
total 336
-rw-r--r-- 1 root root  1969 Nov  5  2016 modsecurity_35_bad_robots.data
-rw-r--r-- 1 root root   386 Nov  5  2016 modsecurity_35_scanners.data
-rw-r--r-- 1 root root  3928 Nov  5  2016 modsecurity_40_generic_attacks.data
-rw-r--r-- 1 root root  2224 Nov  5  2016 modsecurity_50_outbound.data
-rw-r--r-- 1 root root 56714 Nov  5  2016 modsecurity_50_outbound_malware.data
-rw-r--r-- 1 root root 22924 Nov  5  2016 modsecurity_crs_20_protocol_violations.conf
-rw-r--r-- 1 root root  6914 Nov  5  2016 modsecurity_crs_21_protocol_anomalies.conf
-rw-r--r-- 1 root root  3792 Nov  5  2016 modsecurity_crs_23_request_limits.conf
-rw-r--r-- 1 root root  6933 Nov  5  2016 modsecurity_crs_30_http_policy.conf
-rw-r--r-- 1 root root  5410 Nov  5  2016 modsecurity_crs_35_bad_robots.conf
-rw-r--r-- 1 root root 20469 Nov  5  2016 modsecurity_crs_40_generic_attacks.conf
-rw-r--r-- 1 root root 43654 Nov  5  2016 modsecurity_crs_41_sql_injection_attacks.conf
-rw-r--r-- 1 root root 96711 Nov  5  2016 modsecurity_crs_41_xss_attacks.conf
-rw-r--r-- 1 root root  1795 Nov  5  2016 modsecurity_crs_42_tight_security.conf
-rw-r--r-- 1 root root  3660 Nov  5  2016 modsecurity_crs_45_trojans.conf
-rw-r--r-- 1 root root  2247 Nov  5  2016 modsecurity_crs_47_common_exceptions.conf
-rw-r--r-- 1 root root  2787 Nov  5  2016 modsecurity_crs_48_local_exceptions.conf.example
-rw-r--r-- 1 root root  1838 Nov  5  2016 modsecurity_crs_49_inbound_blocking.conf
-rw-r--r-- 1 root root 22336 Nov  5  2016 modsecurity_crs_50_outbound.conf
-rw-r--r-- 1 root root  1448 Nov  5  2016 modsecurity_crs_59_outbound_blocking.conf
-rw-r--r-- 1 root root  2674 Nov  5  2016 modsecurity_crs_60_correlation.conf
```