Master of Information Security

MIS4203 – Independent Studies in Information Security

Index Number – 16770217 | Reg. Number – 2016MIS021

Study Number – 04 – Tor Hidden Services

December 08, 2018

University of Colombo School of Computing

Table of Contents

Problem

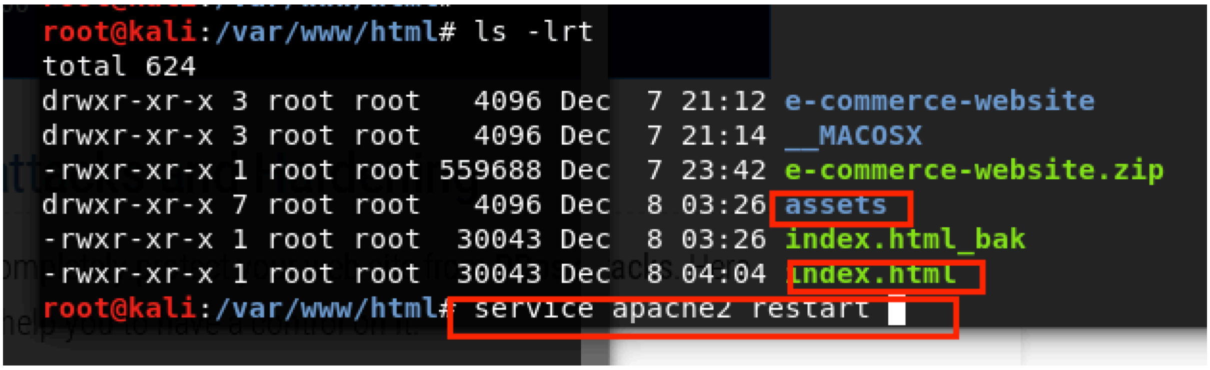
Given E-Commerce website and need to host that website as a Tor hidden service. As well as need to secure webserver and provide the improvements with validations.

Approach

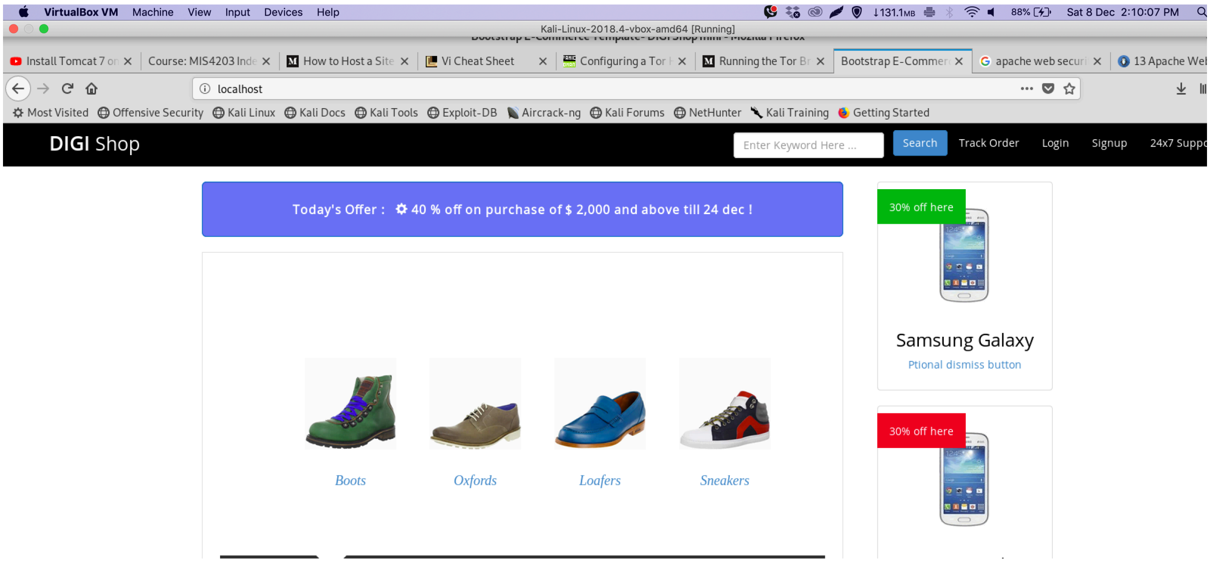
1. Setup E-Commerce website static website in web server.

   Setting up the web service on Apache server

   - Install apache server and copy static website to the www/html folder and restart the apache server.



```
root@kali:/var/www/html# ls -lrt
total 624
drwxr-xr-x 3 root root   4096 Dec  7 21:12 e-commerce-website
drwxr-xr-x 3 root root   4096 Dec  7 21:14 __MACOSX
-rwxr-xr-x 1 root root 559688 Dec  7 23:42 e-commerce-website.zip
drwxr-xr-x 7 root root   4096 Dec  8 03:26 assets
-rwxr-xr-x 1 root root  30043 Dec  8 03:26 index.html_bak
-rwxr-xr-x 1 root root  30043 Dec  8 04:04 index.html
root@kali:/var/www/html# service apache2 restart
```



Today's Offer : ⚙ 40 % off on purchase of $ 2,000 and above till 24 dec !

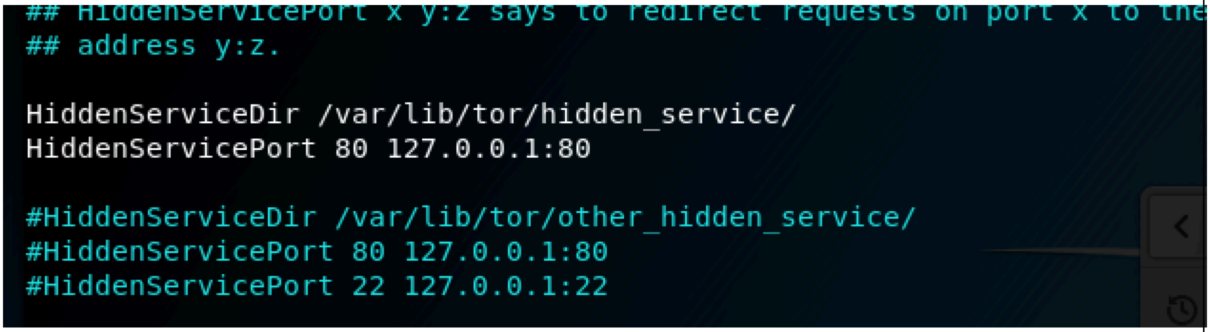
2. Convert E-Commerce website to a tor hidden service:

   Deploy furniture store site as a Tor Hidden Services (https://www.torproject.org/docs/tor-onion-service.html.en) and provide the .onion url.

   - Install Tor in linux VM and configure hidden service and make .onion url
   - Configure apache virtual hosts to accept .onion url

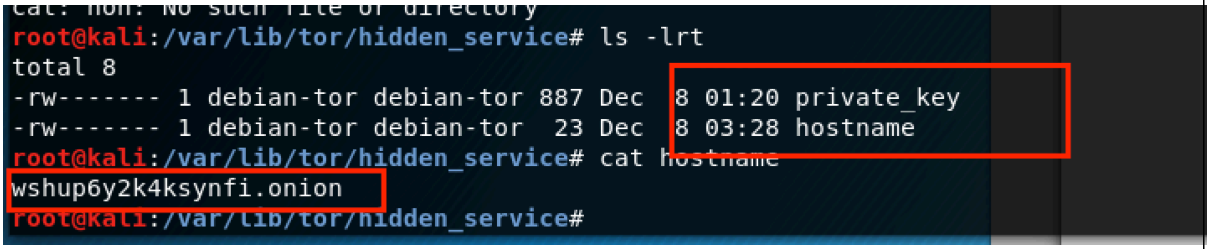
Reference: https://famicoman.com/2018/01/05/configuring-a-tor-hidden-service/

Make configs on /etc/tor/torrc file:



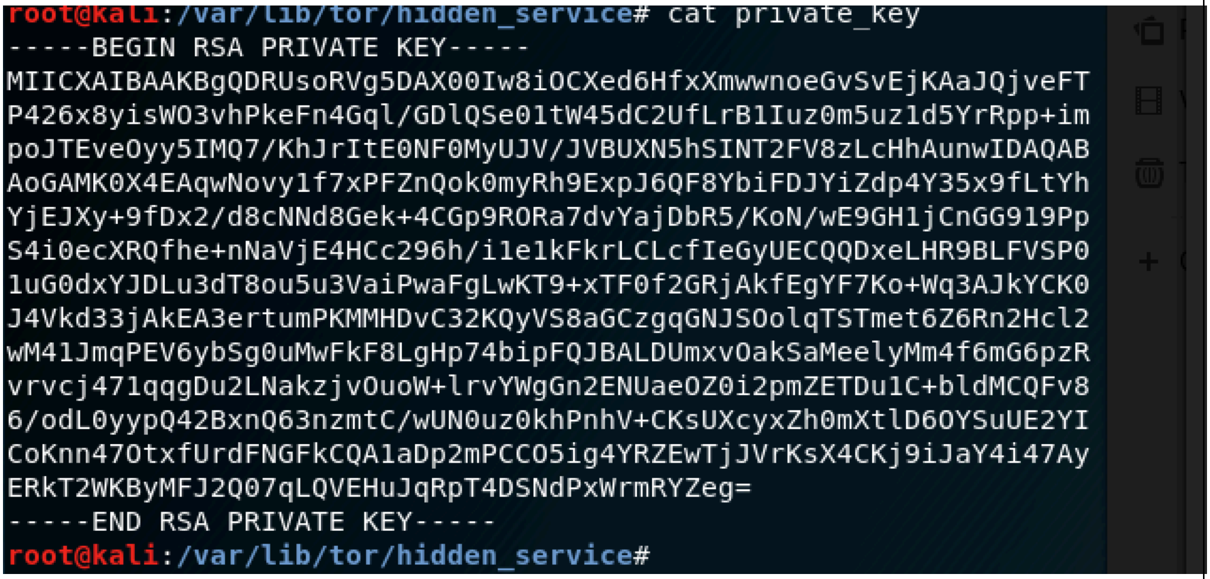
```
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22
```

After restart the tor service, below files are created:



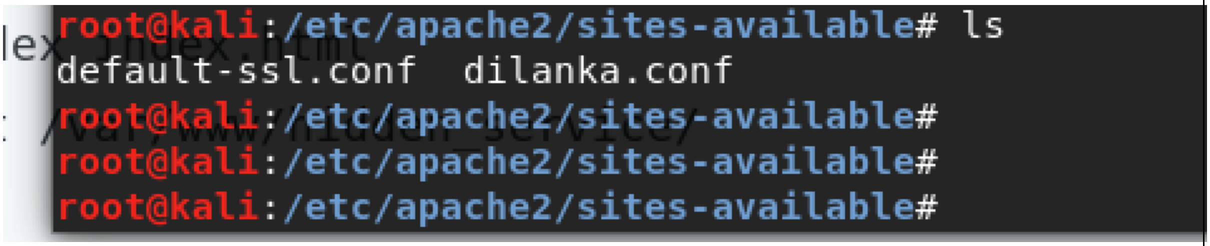
```
cat: non: No such file or directory
root@kali:/var/lib/tor/hidden_service# ls -lrt
total 8
-rw------- 1 debian-tor debian-tor 887 Dec  8 01:20 private_key
-rw------- 1 debian-tor debian-tor  23 Dec  8 03:28 hostname
root@kali:/var/lib/tor/hidden_service# cat hostname
wshup6y2k4ksynfi.onion
root@kali:/var/lib/tor/hidden_service#
```

Private key:

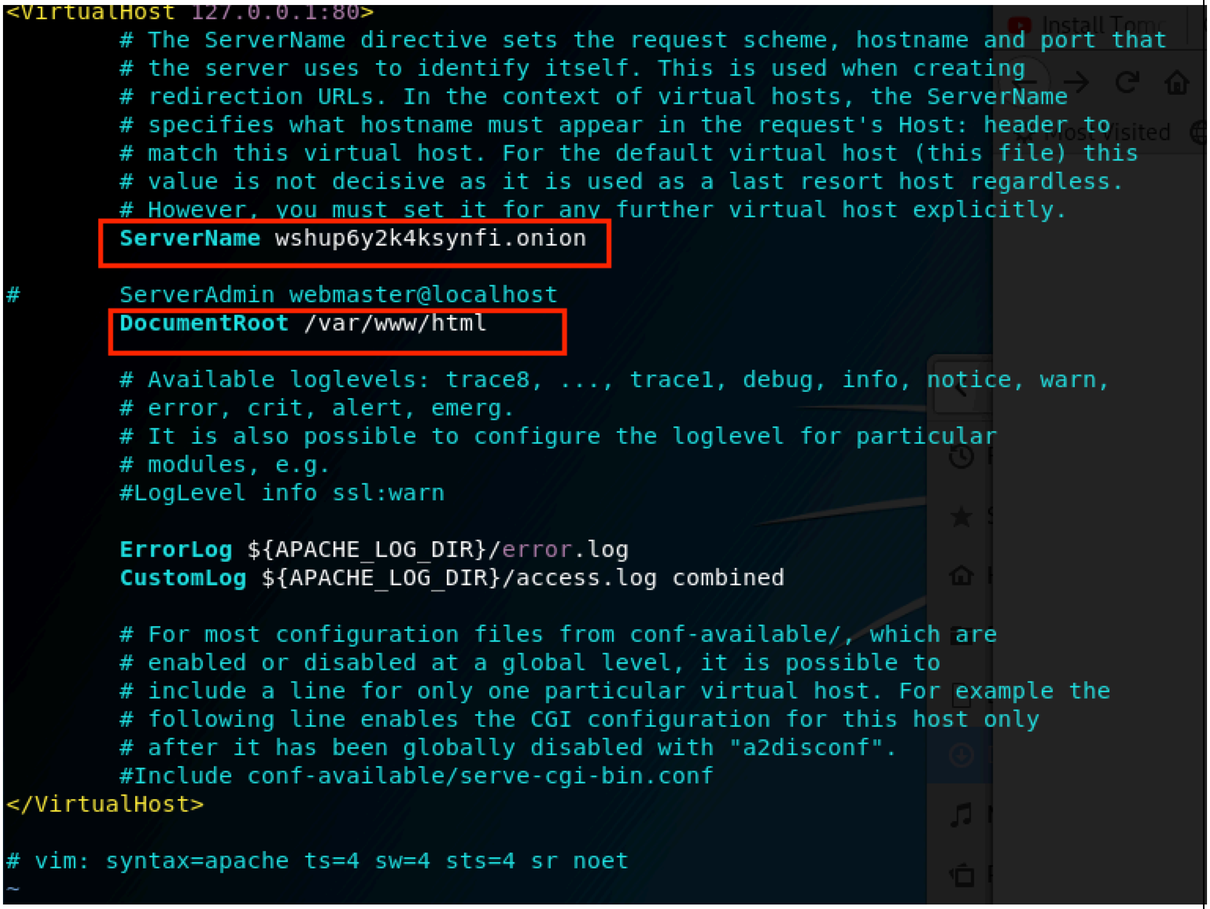


```
root@kali:/var/lib/tor/hidden_service# cat private_key
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDRUsoRVg5DAX00Iw8iOCXed6HfxXmwwnoeGvSvEjKAaJQjveFT
P426x8yisWO3vhPkeFn4Gql/GDlQSe01tW45dC2UfLrB1Iuz0m5uz1d5YrRpp+im
poJTEveOyy5IMQ7/KhJrItE0NF0MyUJV/JVBUXN5hSINT2FV8zLcHhAunwIDAQAB
AoGAMK0X4EAqwNovy1f7xPFZnQok0myRh9ExpJ6QF8YbiFDJYiZdp4Y35x9fLtYh
YjEJXy+9fDx2/d8cNNd8Gek+4CGp9RORa7dvYajDbR5/KoN/wE9GH1jCnGG919Pp
S4i0ecXRQfhe+nNaVjE4HCc296h/i1e1kFkrLCLcfIeGyUECQQDxeLHR9BLFVSP0
1uG0dxYJDLu3dT8ou5u3VaiPwaFgLwKT9+xTF0f2GRjAkfEgYF7Ko+Wq3AJkYCK0
J4Vkd33jAkEA3ertumPKMMHDvC32KQyVS8aGCzgqGNJSOolqTSTmet6Z6Rn2Hcl2
wM41JmqPEV6ybSg0uMwFkF8LgHp74bipFQJBALDUmxvOakSaMeelyMm4f6mG6pzR
vrvcj471qqgDu2LNakzjvOuoW+lrvYWgGn2ENUaeOZ0i2pmZETDu1C+bldMCQFv8
6/odL0yypQ42BxnQ63nzmtC/wUN0uz0khPnhV+CKsUXcyxZh0mXtlD6OYSuUE2YI
CoKnn47OtxfUrdFNGFkCQA1aDp2mPCCO5ig4YRZEwTjJVrKsX4CKj9iJaY4i47Ay
ERkT2WKByMFJ2Q07qLQVEHuJqRpT4DSNdPxWrmRYZeg=
-----END RSA PRIVATE KEY-----
root@kali:/var/lib/tor/hidden_service#
```

Apache Configurations:

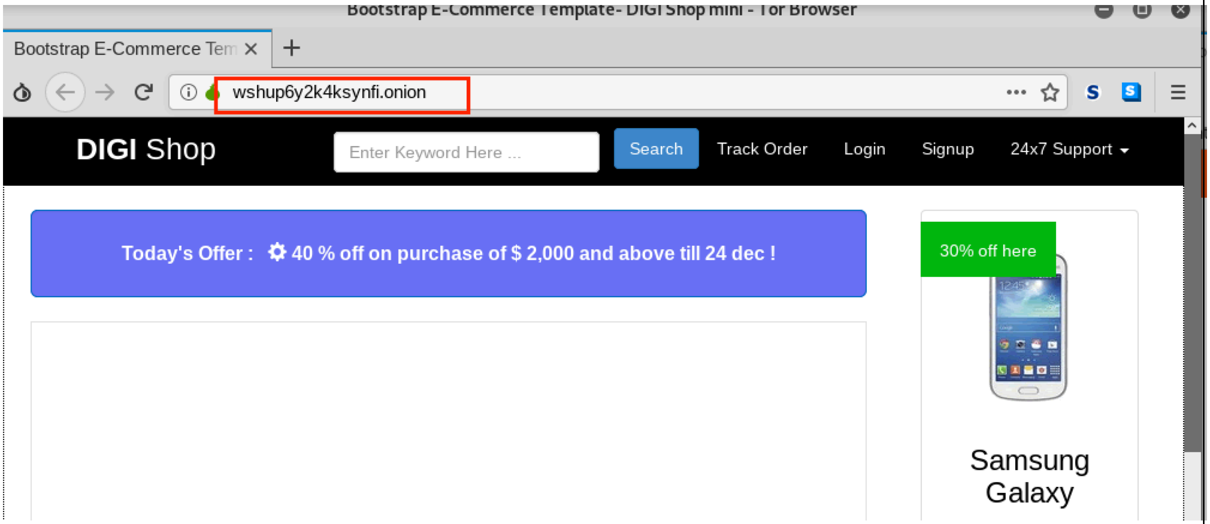


```
root@kali:/etc/apache2/sites-available# ls
default-ssl.conf  dilanka.conf
root@kali:/etc/apache2/sites-available#
root@kali:/etc/apache2/sites-available#
root@kali:/etc/apache2/sites-available#
```



```
<VirtualHost 127.0.0.1:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        ServerName wshup6y2k4ksynfi.onion

#       ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
~
```

After successful restart of apache and tor service, we can see website is running as hidden service.



3. Improve security in the sites. (Eg: Apache Web Server Hardening and etc)

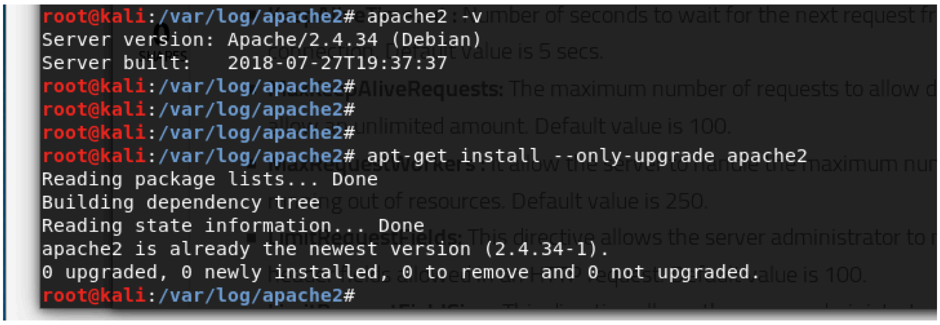
   ○ Configure hardening methods on Apache web server

4. Validate your security improvements.

   ○ Validation by comparing before and after hardening the server.

Hardening Methods and Validations

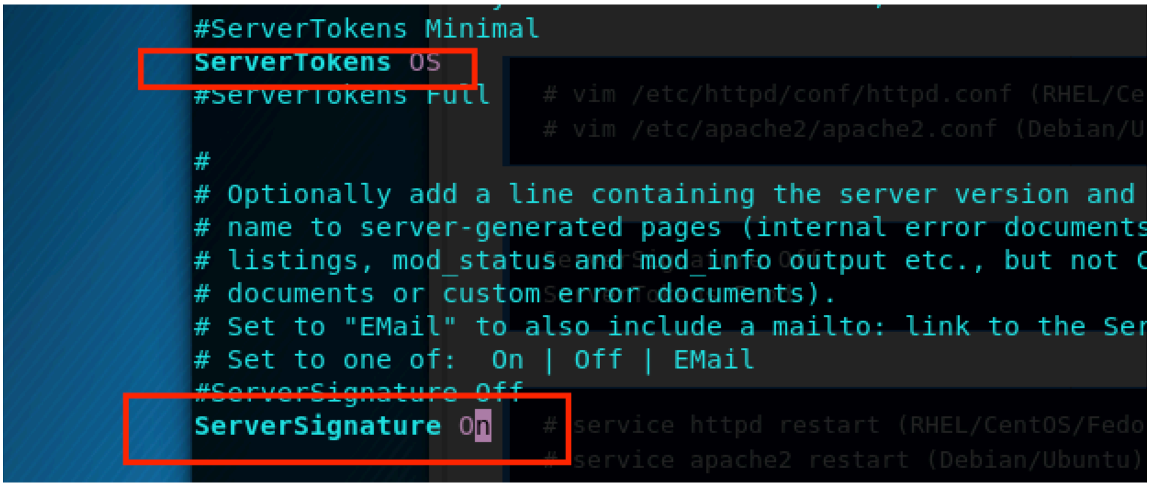
1. Update apache and get new patches and security implementations.



```
root@kali:/var/log/apache2# apache2 -v
Server version: Apache/2.4.34 (Debian)
Server built:   2018-07-27T19:37:37
root@kali:/var/log/apache2#
root@kali:/var/log/apache2#
root@kali:/var/log/apache2#
root@kali:/var/log/apache2# apt-get install --only-upgrade apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.34-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:/var/log/apache2#
```

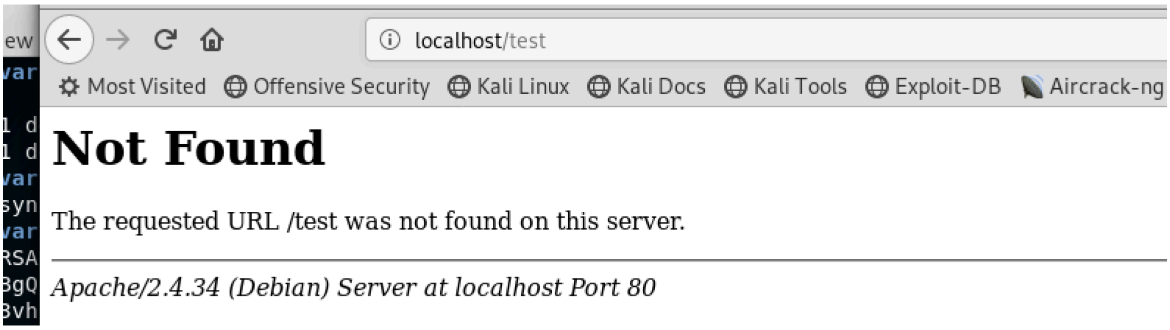
2. Hide OS identity and Apache version.

Before:



```
#ServerTokens Minimal
ServerTokens OS
#ServerTokens Full

#
# Optionally add a line containing the server version and
# name to server-generated pages (internal error documents
# listings, mod_status and mod_info output etc., but not C
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the Ser
# Set to one of:  On | Off | EMail
#ServerSignature Off
ServerSignature On
```

```
# vim /etc/httpd/conf/httpd.conf (RHEL/Ce
# vim /etc/apache2/apache2.conf (Debian/U
# service httpd restart (RHEL/CentOS/Fedo
# service apache2 restart (Debian/Ubuntu)
```

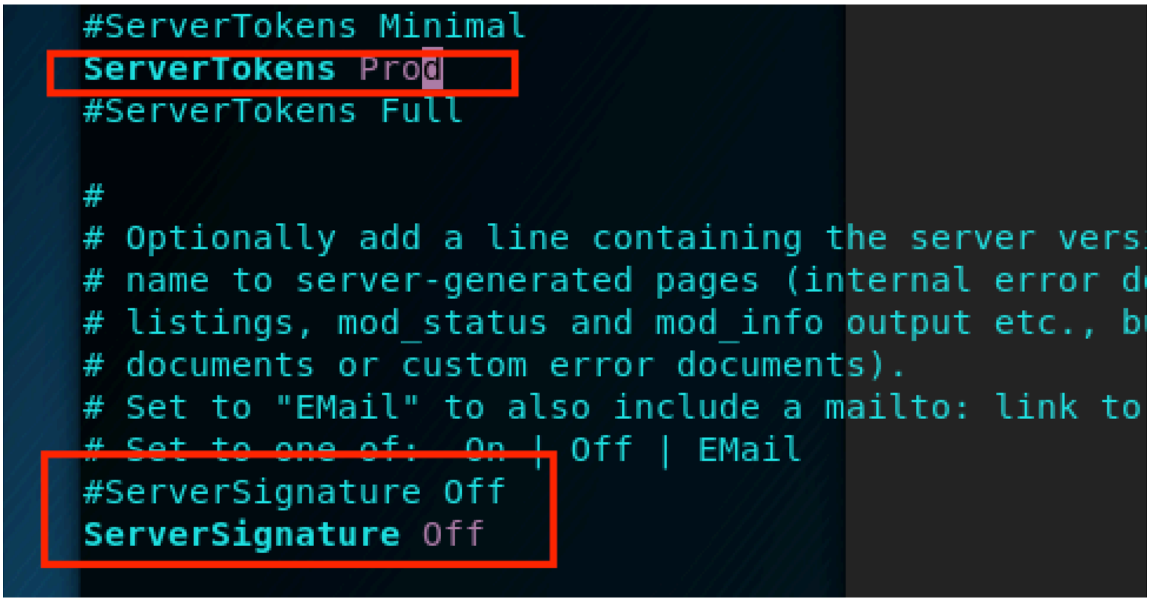


Not Found

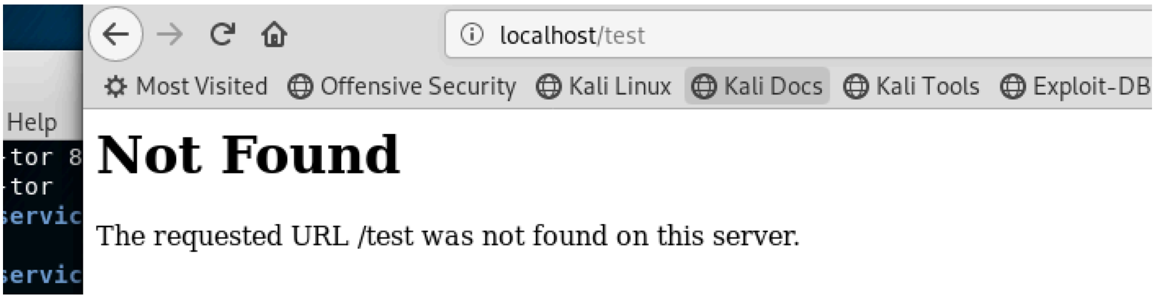
The requested URL /test was not found on this server.

Apache/2.4.34 (Debian) Server at localhost Port 80

After:



```
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full

#
# Optionally add a line containing the server vers
# name to server-generated pages (internal error do
# listings, mod_status and mod_info output etc., bu
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to
# Set to one of:  On | Off | EMail
#ServerSignature Off
ServerSignature Off
```

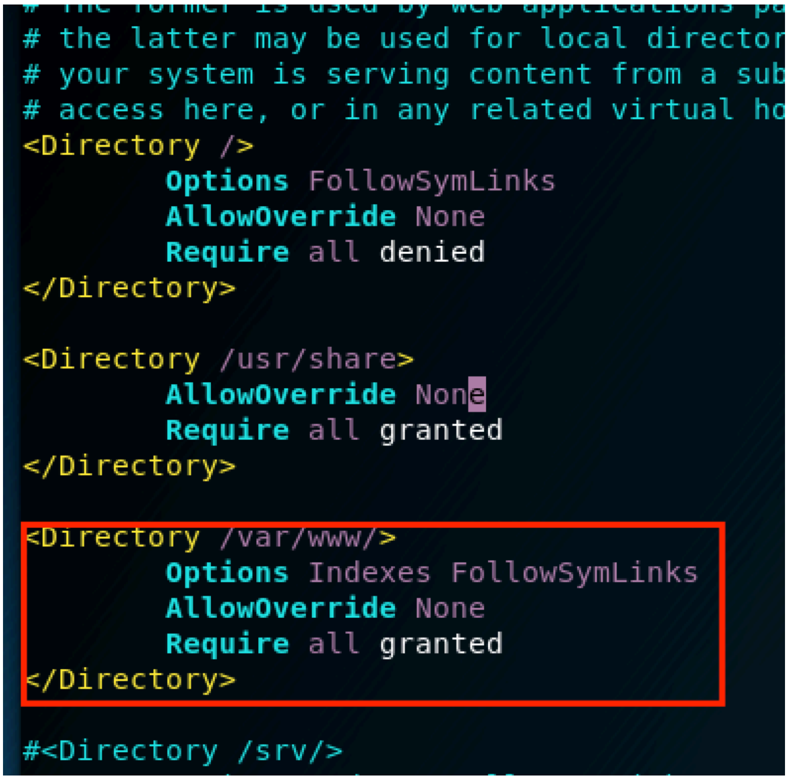


Not Found

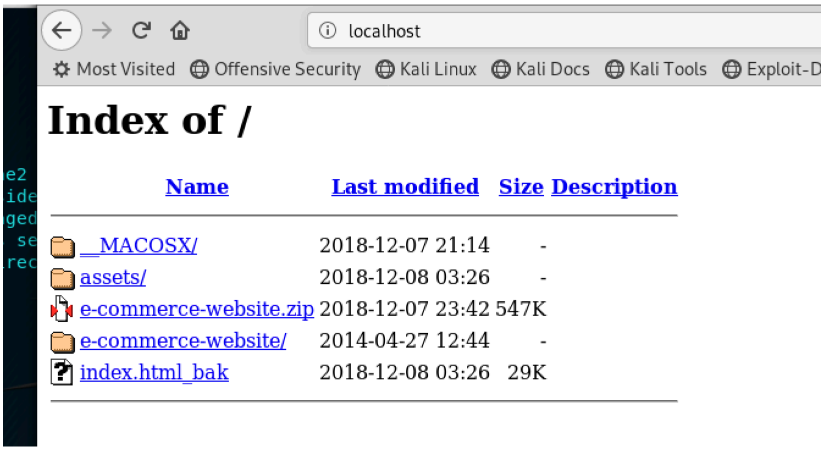
The requested URL /test was not found on this server.

3. Disable directory listing

Before:



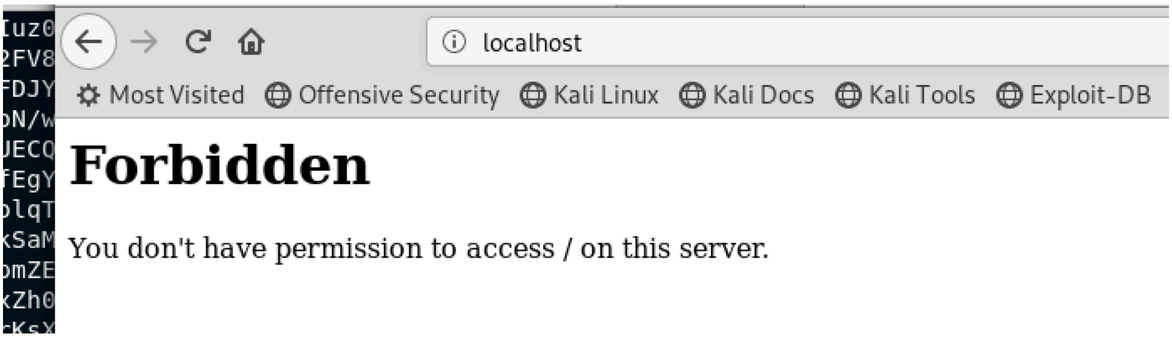
```
# The former is used by web applications pa
# the latter may be used for local director
# your system is serving content from a sub
# access here, or in any related virtual ho
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

#<Directory /srv/>
```



Index of /

Name	Last modified	Size	Description
__MACOSX/	2018-12-07 21:14	-	
assets/	2018-12-08 03:26	-	
e-commerce-website.zip	2018-12-07 23:42	547K	
e-commerce-website/	2014-04-27 12:44	-	
index.html_bak	2018-12-08 03:26	29K	

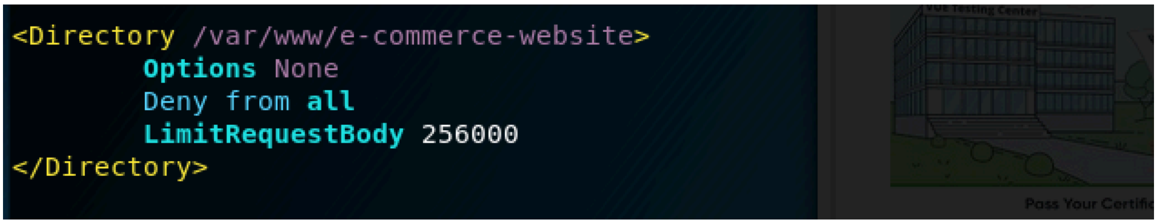
After:



Forbidden

You don't have permission to access / on this server.

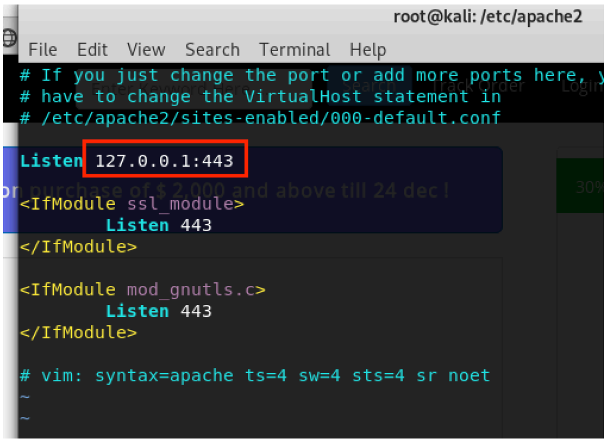
4. If there is uploads, we can limit the upload file size according to the requirement rather than keep default value which is 2GB. Which may cause to resource starvation problem in server. Below is 256K



```
<Directory /var/www/e-commerce-website>
        Options None
        Deny from all
        LimitRequestBody 256000
</Directory>
```

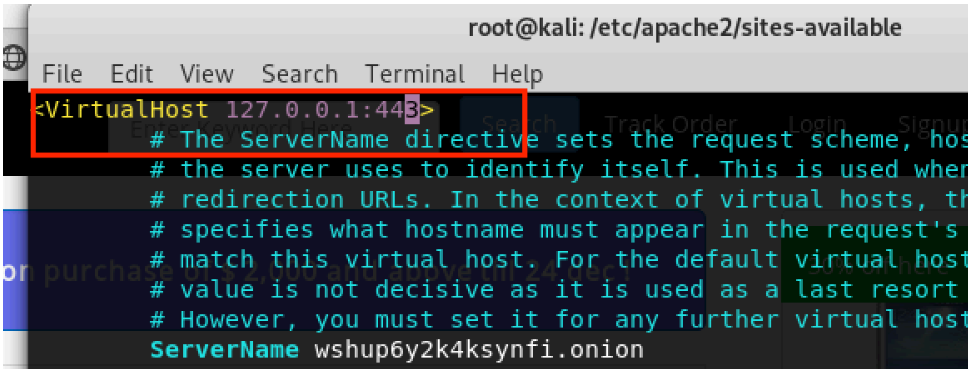
5. Run applications specific port and disable other ports from the firewall. Change running port to secure port which is 443 below locations:

Port.conf file

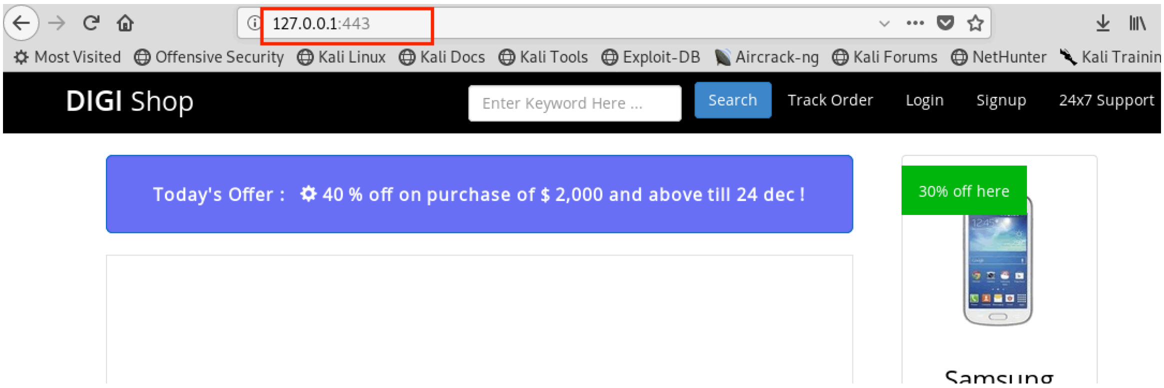


```
# If you just change the port or add more ports here, y
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 127.0.0.1:443

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
~
~
```

Virtual host conf file

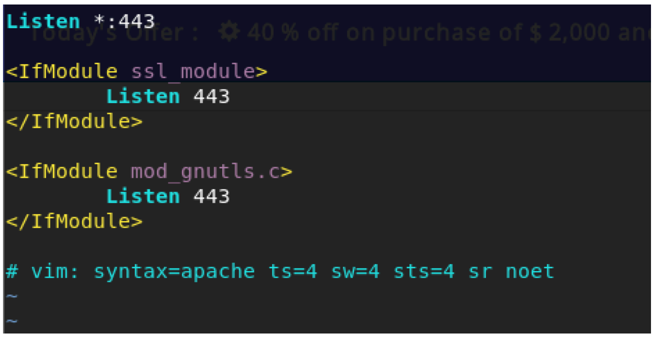

root@kali: /etc/apache2/sites-available
File Edit View Search Terminal Help

```
<VirtualHost 127.0.0.1:443>
        # The ServerName directive sets the request scheme, hos
        # the server uses to identify itself. This is used when
        # redirection URLs. In the context of virtual hosts, th
        # specifies what hostname must appear in the request's
        # match this virtual host. For the default virtual host
        # value is not decisive as it is used as a last resort
        # However, you must set it for any further virtual host
        ServerName wshup6y2k4ksynfi.onion
```

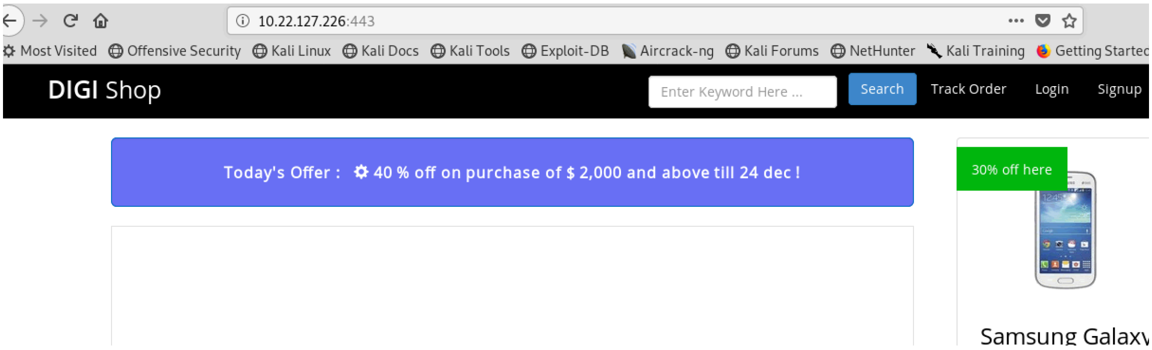


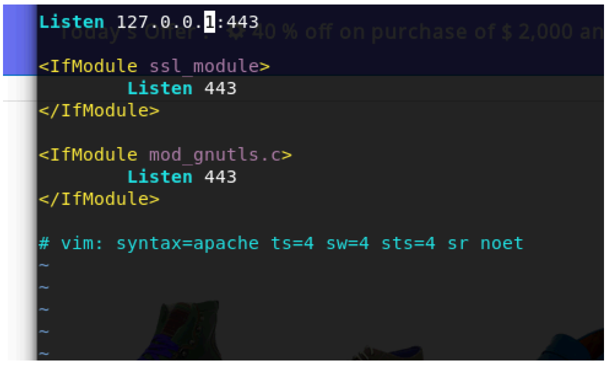
6. Listen to localhost only or specific IP address only.

Configure on port.conf

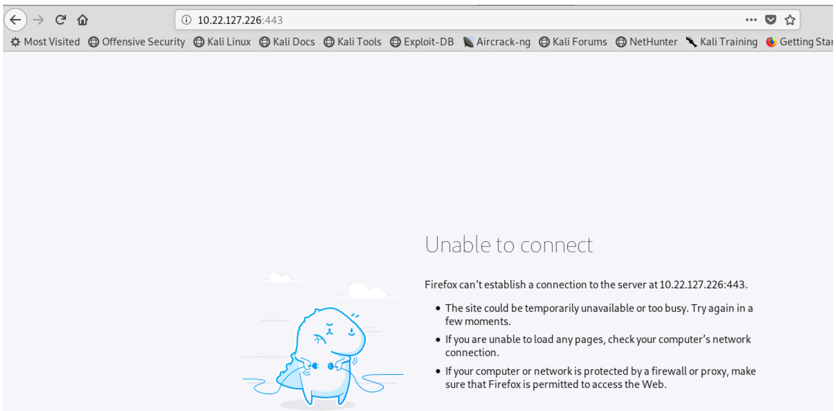


```
Listen *:443

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
~
~
```





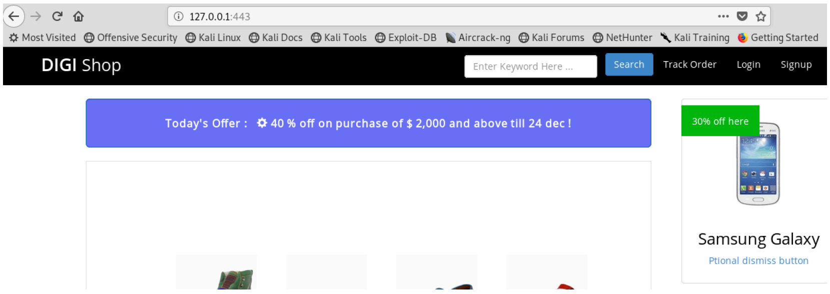
```
Listen 127.0.0.1:443

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
~
~
~
~
~
```



Unable to connect

Firefox can't establish a connection to the server at 10.22.127.226:443.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

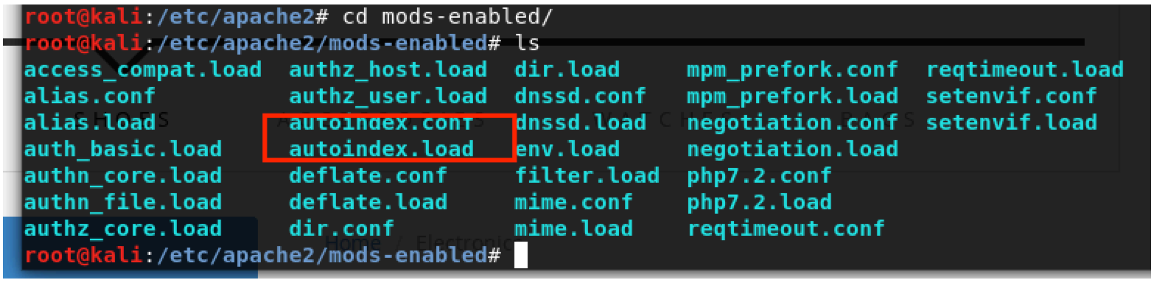


Today's Offer : 40 % off on purchase of $ 2,000 and above till 24 dec !

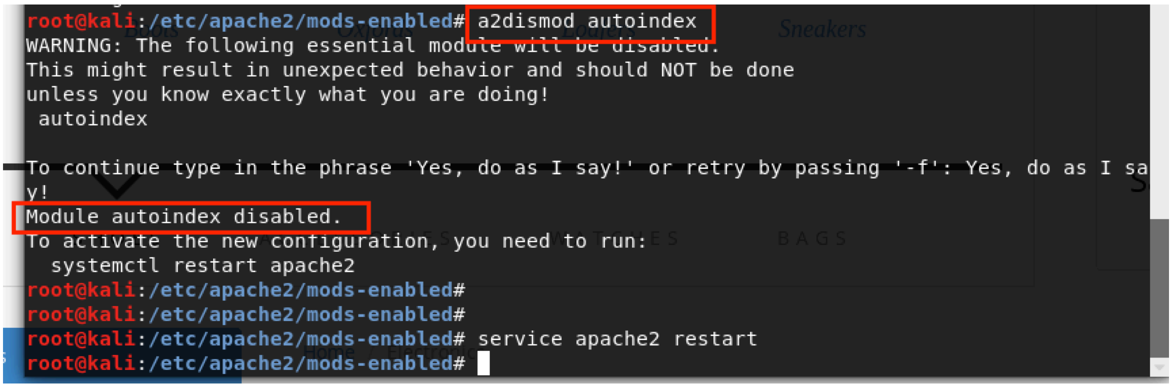
Samsung Galaxy

Ptional dismiss button

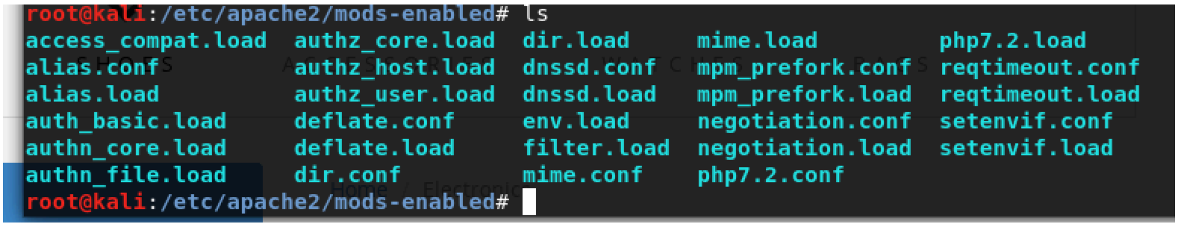
7. Disable unwanted modules.



```
root@kali:/etc/apache2# cd mods-enabled/
root@kali:/etc/apache2/mods-enabled# ls
access_compat.load  authz_host.load  dir.load      mpm_prefork.conf  reqtimeout.load
alias.conf          authz_user.load  dnssd.conf    mpm_prefork.load  setenvif.conf
alias.load          autoindex.conf   dnssd.load    negotiation.conf  setenvif.load
auth_basic.load     autoindex.load   env.load      negotiation.load
authn_core.load     deflate.conf     filter.load   php7.2.conf
authn_file.load     deflate.load     mime.conf     php7.2.load
authz_core.load     dir.conf         mime.load     reqtimeout.conf
root@kali:/etc/apache2/mods-enabled# 
```



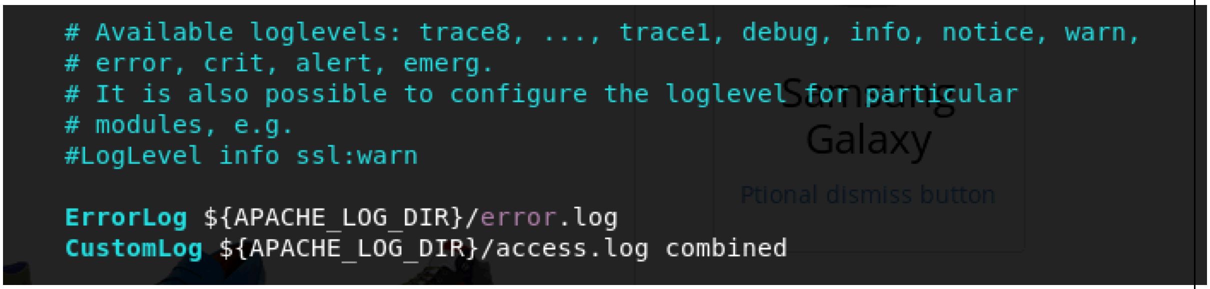
```
root@kali:/etc/apache2/mods-enabled# a2dismod autoindex
WARNING: The following essential module will be disabled.
This might result in unexpected behavior and should NOT be done
unless you know exactly what you are doing!
 autoindex

To continue type in the phrase 'Yes, do as I say!' or retry by passing '-f': Yes, do as I sa
y!
Module autoindex disabled.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@kali:/etc/apache2/mods-enabled#
root@kali:/etc/apache2/mods-enabled#
root@kali:/etc/apache2/mods-enabled# service apache2 restart
root@kali:/etc/apache2/mods-enabled# 
```



```
root@kali:/etc/apache2/mods-enabled# ls
access_compat.load  authz_core.load  dir.load     mime.load           php7.2.load
alias.conf          authz_host.load  dnssd.conf   mpm_prefork.conf    reqtimeout.conf
alias.load          authz_user.load  dnssd.load   mpm_prefork.load    reqtimeout.load
auth_basic.load     deflate.conf     env.load     negotiation.conf    setenvif.conf
authn_core.load     deflate.load     filter.load  negotiation.load    setenvif.load
authn_file.load     dir.conf         mime.conf    php7.2.conf
root@kali:/etc/apache2/mods-enabled# 
```

8. Enable logging whenever necessary.

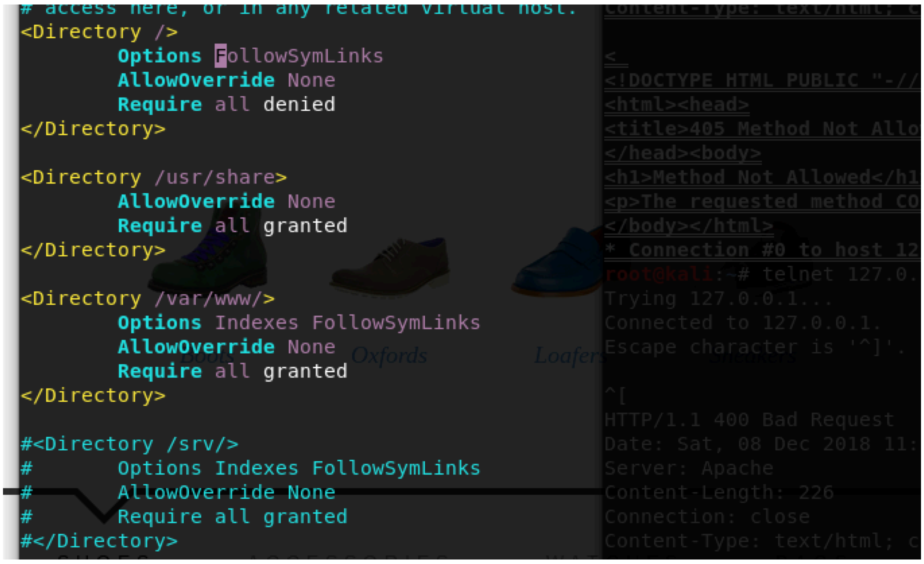
Edit the virtualhost config file and custom logs.



```
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
```

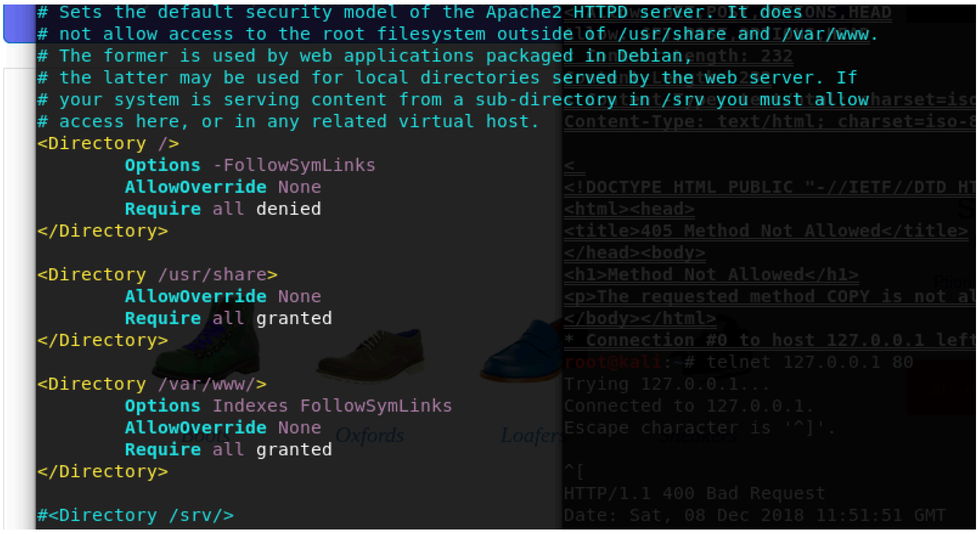
9. Disable symbolic links.

Before:



```
# access here, or in any related virtual host.
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

#<Directory /srv/>
#       Options Indexes FollowSymLinks
#       AllowOverride None
#       Require all granted
#</Directory>
```

After:



```
# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
        Options -FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

#<Directory /srv/>
```

10. Enable SSL
11. Run apache on separate user group
12. Allow only selected/required request types such as (GET/POST)

Conclusion

According to above analysis, Web Server hardening and improve the security is must for E-Commerce websites.

******************** End *********************