

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ



Návrh, správa a bezpečnost počítačových sítí
2020/2021

4. laboratorne cvičenie

1 Zadanie

Celé zadanie laboratórnej úlohy je možné nájsť v e-learningu na karte predmetu alebo na Dropboxe¹. Cieľom tejto laboratórnej úlohy bude inštalácia webového serveru Apache. Základné zoznámenie a konfigurácia

- Instalace serveru a základní seznámení s konfigurací
- Zprovoznění HTTPS.
- Vygenerujete serverové certifikáty, povolte příjem na portu 443 a otestujte (pozor na práva a umístění).
- Změňte baner služby (resp. HTTP(S) hlavičku) na pouhý Apache.
- Pro chyby 404 vytvořte vlastní chybový dokument (nejlépe vytvořit jednu stránku pro všechny chybové stránky).
- Zajistěte, aby měl každý uživatel v Debianu místo pro své webové prezentace ve svém domovském adresáři, např. ve \$HOME/www/.
- Vytvořte .htaccess v uživatelově prostoru tak aby bylo zakázáno listování souborů.
- Zapněte přesměrování na z HTTP na HTTPS (přesměrování, pouhé vypnutí naslouchání na 80 není správné viz redirect v následujícím cvičení).
- Pomocí **ab** najděte limity webového serveru.
- Vytvoření adresáře /private/, kde je nutné login a heslo atd.

2 Nastavenie pracoviska

Príklad pre pracovisko	Klient	Server
IP	192.168.17.135	192.168.17.137
MAC	00:0C:29:5C:68:C5	00:0C:29:6E:65:F1

Tabuľka 1: Nastavenie pracoviska

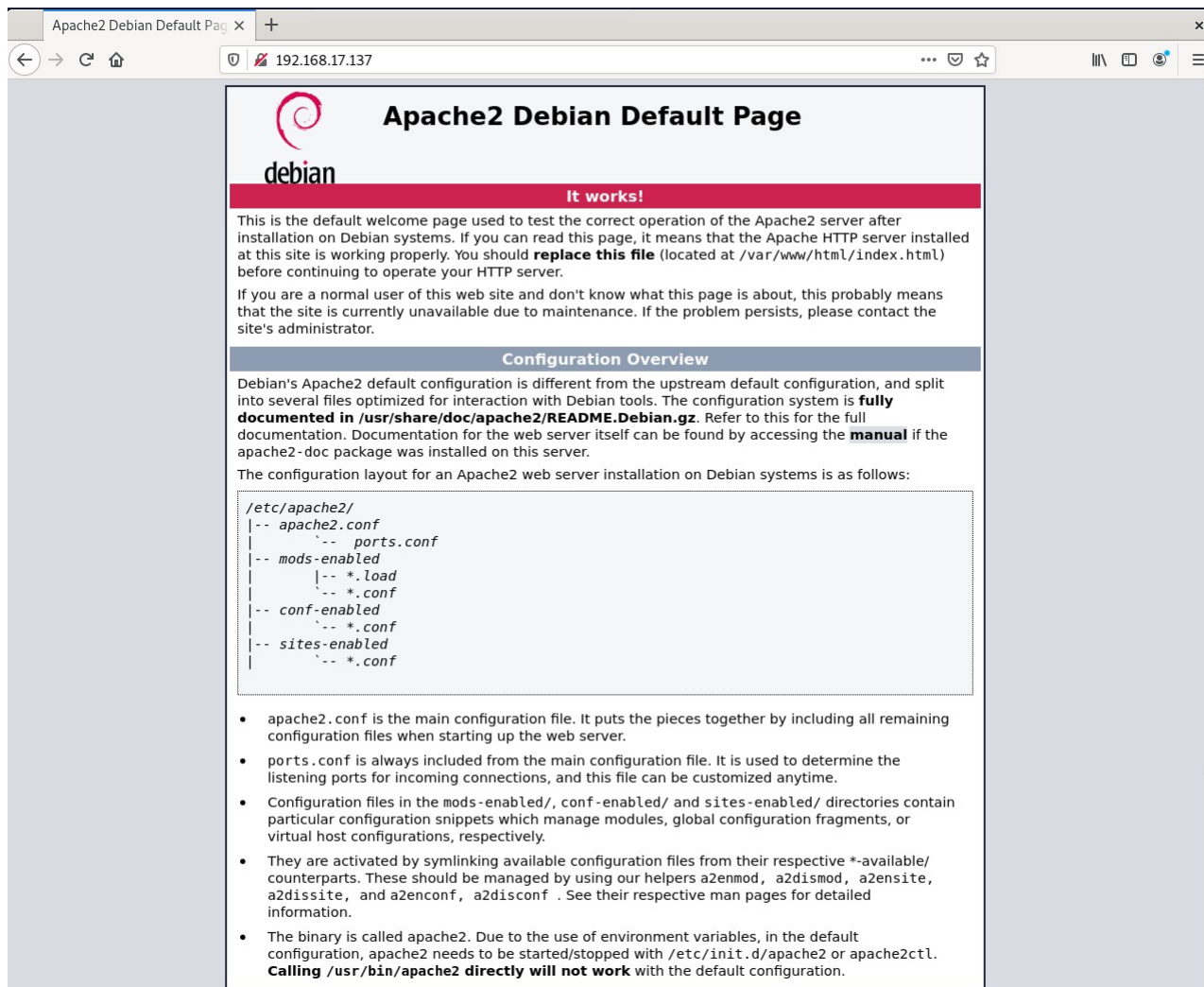
3 Riešenie

V tejto sekcii bude vyriešené laboratórna úloha číslo 4.

¹<https://paper.dropbox.com/doc/4-CV-FkqYxAiaPOtwk8dJbwtP9>

3.1 Inštalácia serveru Apache a PHP

Ako je možné vidieť na obrázku 1, tak Apache server sa nainštaloval a služba beží. Rovnako bolo nainštalované PHP a následne otvorená požadovaná stránka `192.168.17.137/testphp.php` vid'. 2



Obr. 1: Webový server bol úspešne nainštalovaný Apache



Obr. 2: PHP bolo úspešne nainštalované

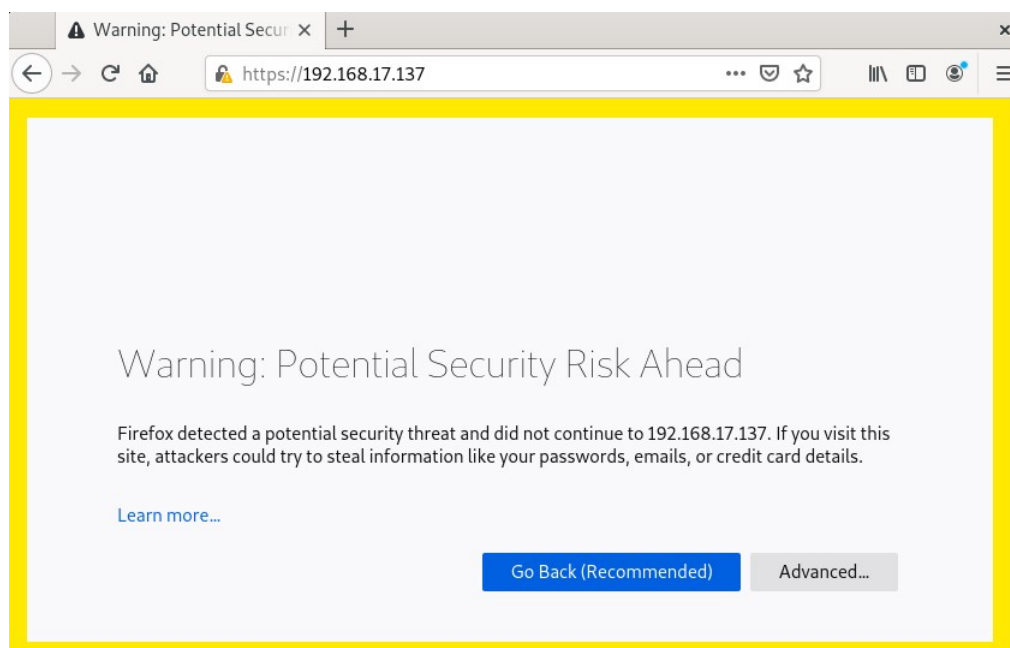
3.2 HTTPS

Službu **HTTPS** je možné spustiť pomocou príkazu `sudo a2enmod ssl`. Následne je potrebné reštartovať *Apache* pomocou príkazu `systemctl restart apache2`. Na obrázku 3, môžeme vidieť že služba HTTPS skutočne beží na serveri.

```
root@debianServer:/etc/apache2/mods-enabled# ss -ntl
State      Recv-Q    Send-Q    Local Address:Port    Peer Address:Port
LISTEN     0          128       0.0.0.0:22             0.0.0.0:*
LISTEN     0          128       *:443                  *:
LISTEN     0          128       *:80                   *:
LISTEN     0          128       [::]:22                [::]:*
```

Obr. 3: Služba HTTPS je v prevádzke

Po načítaní webovej stránky `https://192.168.17.137/` sa zobrazí chybová hláška **Secure Connection failed**, ktorá značí, že je potrebné vygenerovať si vlastný SSL certifikát. Tento certifikát je možné si vygenerovať pomocou príkazu `sudo a2ensite default-ssl.conf` a následne službu *Apache* reštartovať. Warning na obrázku 4 značí, že server si sám podpísal certifikát a nepatrí medzi dôveryhodné certifikáty



Obr. 4: Self signed certifikát

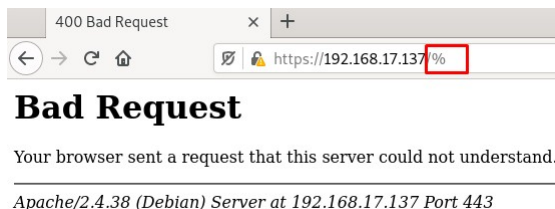
Na obrázku 5 môžeme vidieť že HTTPS naozaj funguje.



Obr. 5: Webová stránku, sprístupnená cez HTTPS

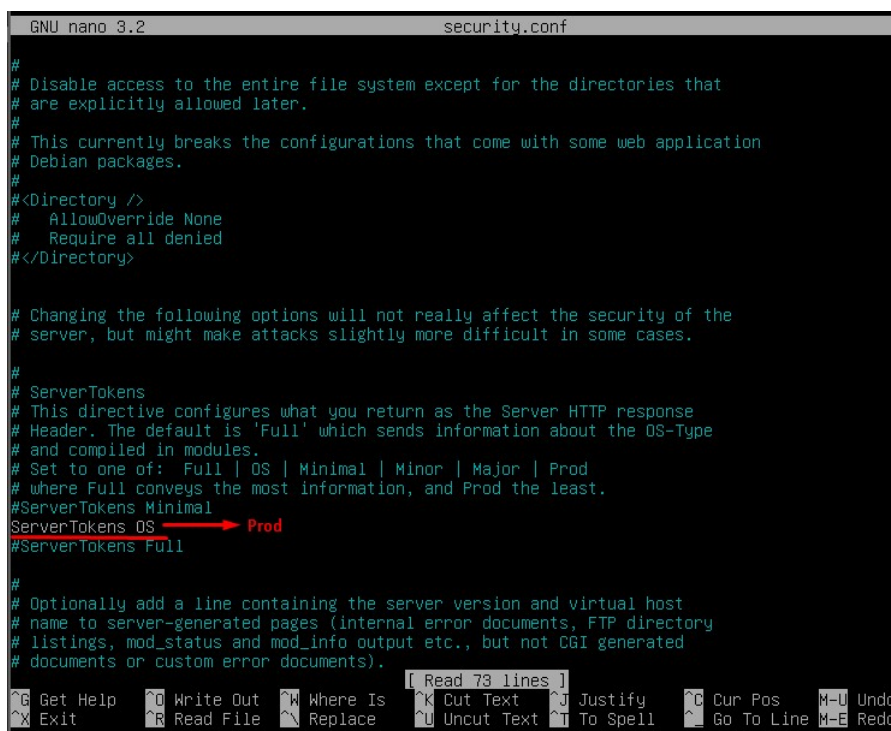
3.3 Token (baner) v hlavičke HTTP(S)

Na obrázku 6 je možné vidieť, že server o sebe prezrádza príliš mnoho informácií. Tieto informácie by potenciálne mohli byť zneužitie prípadným útočníkom. Je potrebné tieto citlivé údaje zneprístupniť.



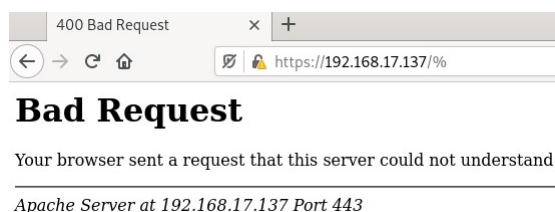
Obr. 6: Citlivé údaje

Je potrebné v adresári `/etc/apache2/conf-enabled/security` modifikovať súbor `security.conf`. Konkrétne sa jedná o záznam `ServerTokens OS`, ktorý je potrebné zmeniť na záznam `ServerTokens Prod` vid' 7 a následne službu pomocou príkazu `/etc/init.d/apache2 restart` reštartovať.



Obr. 7: security.conf

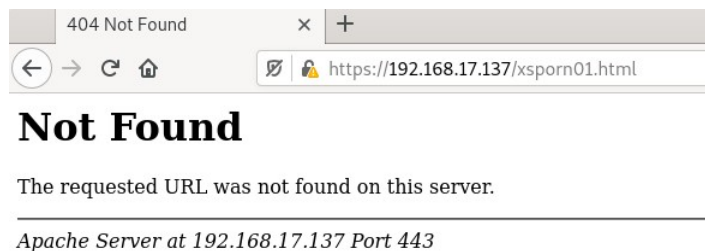
Následne je možné si znovu otestovať chybovú hlášku ale tentokrát bez citlivých informácií vid' 8.



Obr. 8: redukované citlivé údaje

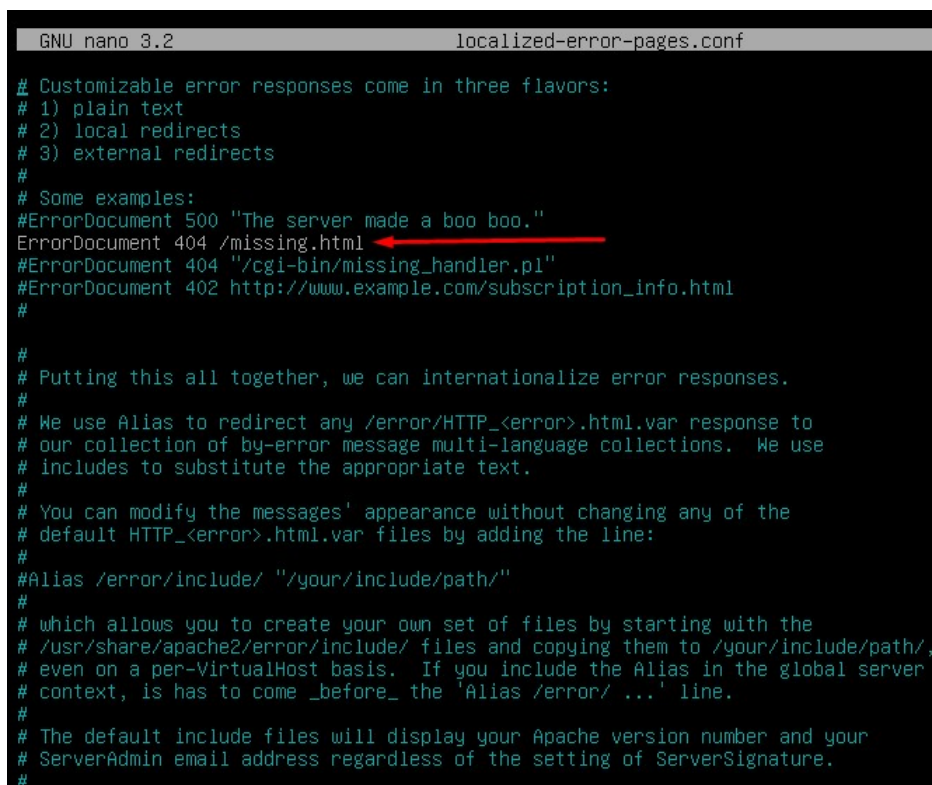
3.4 Vlastná chybová stránka 404

Vyvoláme si chybovú stránku 404 vid'. 9. Následne v adresári `/etc/apache2/conf-enabled/` bude



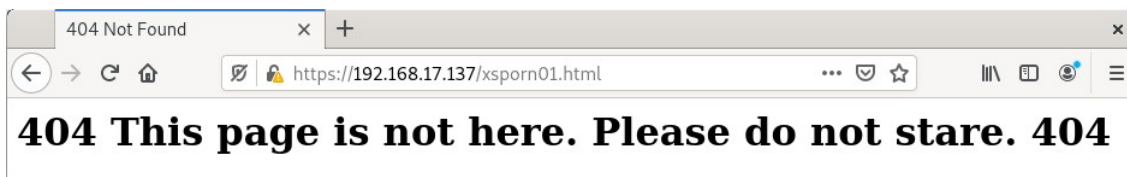
Obr. 9: Chybová stránka

modifikovaný súbor `localized-error-pages.conf`, konkrétne záznam *ErrorDocument 404*, ktorý odkomentujeme vid'. 10.



Obr. 10: `localized-error-pages.conf`

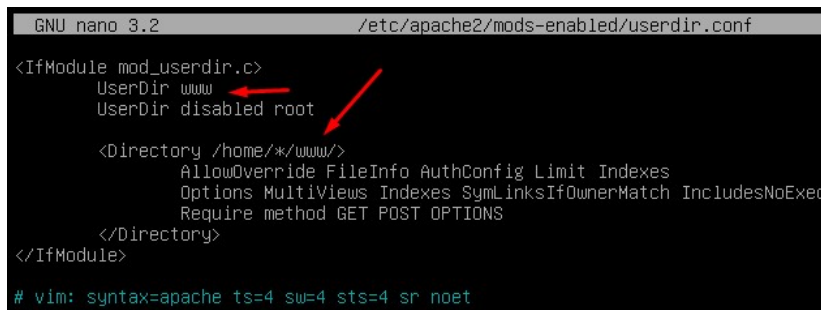
Následne v adresári `/var/www/html` vytvoríme súbor `missing.html`, ktorý je možné ľubovoľne editovať vid'. 11.



Obr. 11: Vlastná chybová hláška

3.5 Vlastná zložka užívateľov pre webové prezentácie

Najprv je potrebné aktivovať modul userdir pomocou príkazu `sudo a2enmod userdir`. Následne je potrebné modifikovať konfiguračný súbor `userdir.conf`, ktorý sa nachádza v `/etc/apache2/mods-enabled`. Následne je potrebné si vytvoriť zložku v užívateľskom adresári s názvom `www`. To je to zložky je



```
GNU nano 3.2 /etc/apache2/mods-enabled/userdir.conf

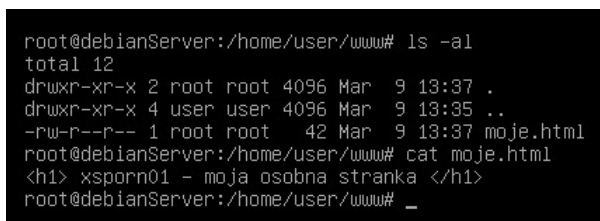
<IfModule mod_userdir.c>
  UserDir www
  UserDir disabled root

  <Directory /home/*/www/>
    AllowOverride FileInfo AuthConfig Limit Indexes
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    Require method GET POST OPTIONS
  </Directory>
</IfModule>

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

Obr. 12: `userdir.conf`

potrebné si vytvoriť súbor `moje.html` a následne ho ľubovoľne editovať viď. 13.



```
root@debianServer:/home/user/www# ls -al
total 12
drwxr-xr-x 2 root root 4096 Mar  9 13:37 .
drwxr-xr-x 4 user user 4096 Mar  9 13:35 ..
-rw-r--r-- 1 root root  42 Mar  9 13:37 moje.html
root@debianServer:/home/user/www# cat moje.html
<h1> xsporn01 - moja osobna stranka </h1>
root@debianServer:/home/user/www# _
```

Obr. 13: Obsah adresára a súboru

Po návšteve stránky `https://192.168.17.137/~user/moje.html` sa zobrazí 14



192.168.17.137/~user/moje.html x +

https://192.168.17.137/~user/moje.html

xsporn01 - moja osobna stranka

Obr. 14: `moje.html`

Vzniká bezpečnostné riziko pri ktorom je možné si zobrazíť obsah celého adresára viď. 15.



Index of /~user x +

https://192.168.17.137/~user/ ...

Index of /~user

Name	Last modified	Size	Description
Parent Directory	-	-	-
moje.html	2021-03-09 13:51	62	-

Apache Server at 192.168.17.137 Port 443

Obr. 15: Obsah adresára užívateľa `user`

Riešením je vytvoriť súbor s názvom `.htaccess`, do ktorého je potrebné pridať parameter `Options -Indexes`, ktorý zakáže listovanie v adresáry `user` vid'. 16.

```
root@debianServer:/home/user/www# ls -all
total 16
drwxr-xr-x 2 root root 4096 Mar  9 14:03 .
drwxr-xr-x 4 user user 4096 Mar  9 13:35 ..
-rw-r--r-- 1 root root  17 Mar  9 14:03 .htaccess
-rw-r--r-- 1 root root  62 Mar  9 13:51 moje.html
root@debianServer:/home/user/www# cat .htaccess
Options -Indexes
root@debianServer:/home/user/www# _
```

Obr. 16: Obsah `.htaccess`

Aby sa vykonaná zmena dokončila, je potrebné ešte v nastaveniach domovskej zložky povoliť prepísanie vid'. 17.

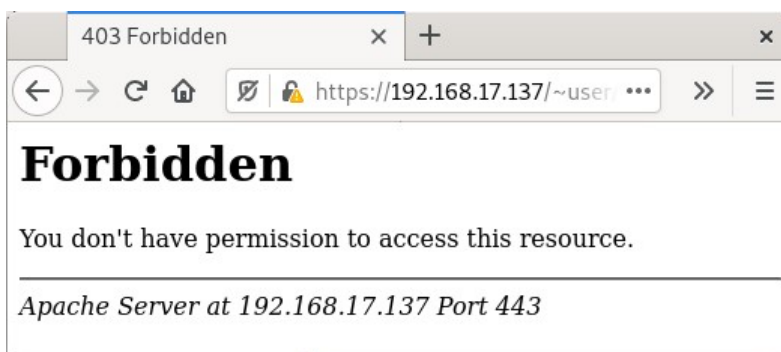
```
root@debianServer:/home/user/www# cat /etc/apache2/mods-enabled/userdir.conf
<IfModule mod_userdir.c>
    UserDir www
    UserDir disabled root

    <Directory /home/*/www/>
        AllowOverride all
        Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
        Require method GET POST OPTIONS
    </Directory>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
root@debianServer:/home/user/www#
```

Obr. 17: `userdir.conf`

Na ukážke 18 je možné vidieť, že obsah adresára `user` už nie je možné vylistovať.



Obr. 18: Obsah adresára `user` je zakázaný

3.6 Presmerovanie HTTP provozu na HTTPS

Cielom je presmerovať provoz na HTTPS vid'. 19.

Následne ak si otvoríme stránku `192.168.17.137`, tak sa automaticky presmeruje na `https://192.168.17.137/` vid'. 20.


```

root@debianServer:/home/user# cat /etc/apache2/sites-available/000-default.conf
<VirtualHost *: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 www.example.com

    ServerName 192.168.17.137
    Redirect / https://192.168.17.137

    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

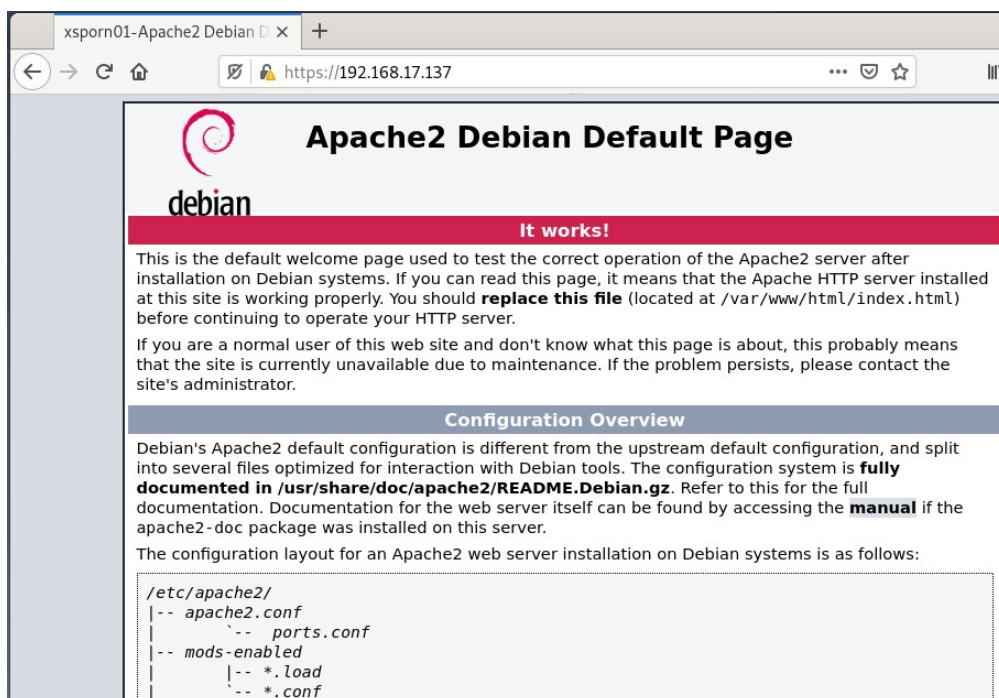
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # 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
root@debianServer:/home/user# systemctl restart apache2
root@debianServer:/home/user# _

```

Obr. 19: Nastavenie presmerovania



Obr. 20: Nastavené presmerovanie