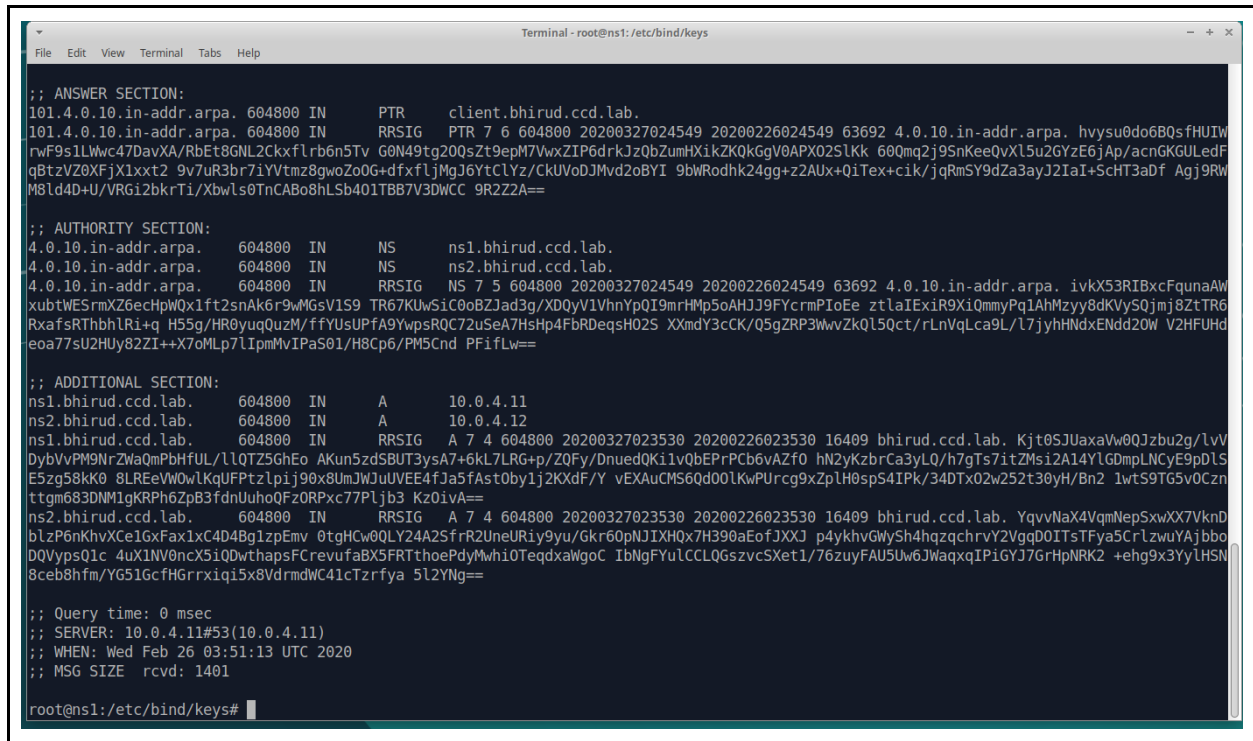


Securing Network Communications

Name	Sahil Bhirud
------	--------------

1. Upload a screenshot showing the signatures



```
Terminal - root@ns1:/etc/bind/keys
File Edit View Terminal Tabs Help

;; ANSWER SECTION:
101.4.0.10.in-addr.arpa. 604800 IN PTR client.bhirud.ccd.lab.
101.4.0.10.in-addr.arpa. 604800 IN RRSIG PTR 7 6 604800 20200327024549 20200226024549 63692 4.0.10.in-addr.arpa. hvysu0do6B0sfHUIW
rwF9s1LWwc47DavXA/RbEt8GNL2Ckxflrb6n5Tv G0N49tg200sZt9epM7VwxZIP6drkZz0bZumHXikZK0kGgV0APX025LkK 60Qmq2j9SnKeeQvXl5u2GYzE6jAp/acnGKGULedF
qBtzVZ0XfjXlxt2 9v7uR3br7iYVtmz8gwoZo0G+dfxfljMgJ6YtCLYz/CkUVo0Jmvd2oBYI 9bWRodhk24gg+z2AUx+Q1Tex+cik/jqRmSY9dZa3ayJ2IaI+ScHT3aDf Agj9RW
M8ld4D+U/VRGi2bkrTi/Xbwls0TnCABo8hLSb401TBB7V3DWCC 9R2Z2A==

;; AUTHORITY SECTION:
4.0.10.in-addr.arpa. 604800 IN NS ns1.bhirud.ccd.lab.
4.0.10.in-addr.arpa. 604800 IN NS ns2.bhirud.ccd.lab.
4.0.10.in-addr.arpa. 604800 IN RRSIG NS 7 5 604800 20200327024549 20200226024549 63692 4.0.10.in-addr.arpa. ivkX53RIBxcFqunaAW
xubtWESrmXZ6ecHpwQx1ft2snAk6r9wMGsV159 TR67KUwSiC0oBZJad3g/XDQyV1VhnYpQI9mrHMP5oAHJJ9FYcrmpIoEe ztlaIExiR9XiQmmyPq1AhMzyy8dKVySjQjmj8ZtTR6
RxafsRThbhlRi+q H55g/HR0yuqQuzM/ffYUsUPfA9YwpsRQC72uSeA7HsHp4FbRdeqsH02S XXmdY3cCK/Q5gZRP3WwvZkQ15Qct/rLnVqLca9L/L7jyhHNdxENdd2OW V2HFUhd
eoa77sU2Huy82ZI++X7oMLp7LlpmMvIPaS01/H8Cp6/PM5Cnd PFifLw==

;; ADDITIONAL SECTION:
ns1.bhirud.ccd.lab. 604800 IN A 10.0.4.11
ns2.bhirud.ccd.lab. 604800 IN A 10.0.4.12
ns1.bhirud.ccd.lab. 604800 IN RRSIG A 7 4 604800 20200327023530 20200226023530 16409 bhirud.ccd.lab. Kjt0SJUaxaVw0QJzbu2g/lvV
DybVvPM9NrZwaQmPbHfUL/llQTZ5GhEo AKun5zdSBUT3ysA7+6kL7LRG+p/ZQFy/DnuedQK1lvQbEPfPCb6vAZf0 hN2yKzbrCa3yLQ/h7gTs7itZMs12A14YlG0mpLNCyE9pDLS
E5zg58kK0 8LREeVw0wLkqUFPTzlpj90x8UmJWJuUVEE4fJa5fAst0by1j2KXd/Y vEXAuCMS6Qd00LkWPURcg9xZpLH0spS4IPk/340Tx02w252t30yH/Bn2 1wtS9TG5v0Czn
ttgm683DMM1gKRPh6ZpB3fdnUuhoQFzORPxc77Pljb3 Kz0ivA==
ns2.bhirud.ccd.lab. 604800 IN RRSIG A 7 4 604800 20200327023530 20200226023530 16409 bhirud.ccd.lab. YqvvMaX4VqmNepSxwXX7VknD
blzP6nKhvXcElGxFaxlxc4D4BglzpEmv 0tgHCw0QLY24A2SfrR2UneURiy9yu/Gkr60pNJIHX0x7H390aEofJXXJ p4ykhvGWySh4hqzqchrVY2VgqD0ITsTFya5CrLzWuYAjbb0
DQVypsQ1c 4uX1NV0ncX5iQDwthapsFCrevufaBX5FRTthoePdyMwhi0TeqdxawGoc IbNgFYuLCCLQGsZvcSxet1/76zuyFAU5Uw6JWaqxqIPiGYJ7GrHpNRK2 +ehg9x3YyLHSN
8ceb8hfm/YG51GcfHGrrxiqi5x8VdrmdWC41cTzrfya 5L2YNg==

;; Query time: 0 msec
;; SERVER: 10.0.4.11#53(10.0.4.11)
;; WHEN: Wed Feb 26 03:51:13 UTC 2020
;; MSG SIZE rcvd: 1401

root@ns1:/etc/bind/keys#
```

2. Upload a screenshot of the following commands to show that OpenLDAP is correctly configured to use TLS

```
Terminal - root@ldap:~
File Edit View Terminal Tabs Help
root@ldap:~# ldapsearch -H ldap:// -x -b "dc=bhirud,dc=ccd,dc=lab" -LLL dn
Confidentiality required (13)
Additional information: TLS confidentiality required
root@ldap:~# ldapsearch -H ldap:// -x -b "dc=bhirud,dc=ccd,dc=lab" -LLL -ZZ dn
dn: dc=bhirud,dc=ccd,dc=lab

dn: cn=admin,dc=bhirud,dc=ccd,dc=lab
dn: ou=Users,dc=bhirud,dc=ccd,dc=lab
dn: ou=Groups,dc=bhirud,dc=ccd,dc=lab
dn: cn=sbhirud2,ou=Groups,dc=bhirud,dc=ccd,dc=lab
dn: uid=sbhirud2,ou=Users,dc=bhirud,dc=ccd,dc=lab
dn: cn=krbContainer,dc=bhirud,dc=ccd,dc=lab
dn: cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab
dn: krbPrincipalName=K/M@BHIRUD.CCD.LAB,cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab
dn: krbPrincipalName=krbtgt/BHIRUD.CCD.LAB@BHIRUD.CCD.LAB,cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab
dn: krbPrincipalName=kadmin/admin@BHIRUD.CCD.LAB,cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab
dn: krbPrincipalName=kadmin/krb.bhirud.ccd.lab@BHIRUD.CCD.LAB,cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab
dn: krbPrincipalName=kiprop/krb.bhirud.ccd.lab@BHIRUD.CCD.LAB,cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab

dn: krbPrincipalName=kiprop/krb.bhirud.ccd.lab@BHIRUD.CCD.LAB,cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab

dn: krbPrincipalName=kadmin/changepw@BHIRUD.CCD.LAB,cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab
dn: krbPrincipalName=kadmin/history@BHIRUD.CCD.LAB,cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab
dn: krbPrincipalName=sbhirud2/admin@BHIRUD.CCD.LAB,cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab
dn: krbPrincipalName=host/ssh.bhirud.ccd.lab@BHIRUD.CCD.LAB,cn=BHIRUD.CCD.LAB,cn=krbContainer,dc=bhirud,dc=ccd,dc=lab

root@ldap:~# netstat -plnt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN      3450/slapd
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      3450/slapd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      160/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      240/sshd
tcp        0      0 0.0.0.0:88              0.0.0.0:*               LISTEN      3376/krb5kdc
tcp        1      0 10.0.4.16:57050         10.0.4.16:389          CLOSE_WAIT  203/systemd-logind
tcp        0      0 127.0.0.1:54770         127.0.0.1:389          TIME_WAIT   -
tcp        0      0 127.0.0.1:54772         127.0.0.1:389          TIME_WAIT   -
tcp        0      0 127.0.0.1:54768         127.0.0.1:389          TIME_WAIT   -
tcp        0      0 127.0.0.1:54766         127.0.0.1:389          TIME_WAIT   -
tcp        0      0 127.0.0.1:54764         127.0.0.1:389          TIME_WAIT   -
tcp6       0      0 :::636                  :::*                   LISTEN      3450/slapd
tcp6       0      0 :::389                  :::*                   LISTEN      3450/slapd
tcp6       0      0 :::22                   :::*                   LISTEN      240/sshd
tcp6       0      0 :::88                   :::*                   LISTEN      3376/krb5kdc
root@ldap:~# ldapsearch -H ldap:// -x -b "dc=bhirud,dc=ccd,dc=lab" -LLL dn
```

3. Upload a screenshot showing that you can still successfully login after editing the configuration

```
sahilbhirud@ubuntu:~$ lxc exec ssh -- /bin/bash
root@ssh:~# su - sbhirud2
sbhirud2@ssh:~$
sbhirud2@ssh:~$
```

```
sahilbhirud@ubuntu:~$ lxc exec ns2 -- /bin/bash
root@ns2:~# su - sbhirud2
sbhirud2@ns2:~$
```

```
root@ns1:~# su - sbhirud2
sbhirud2@ns1:~$
sbhirud2@ns1:~$
```

```
sahilbhirud@ubuntu:~$ lxc exec krb -- /bin/bash
root@krb:~# su - sbhirud2
sbhirud2@krb:~$
```

```
sahilbhirud@ubuntu:~$ lxc exec client -- /bin/bash
root@client:~# su - sbhirud2
sbhirud2@client:~$
```

```
root@ldap:~# su - sbhirud2
sbhirud2@ldap:~$
```

4. Upload a screenshot of the above commands showing your new TGT

```
Terminal - root@krb:~  
File Edit View Terminal Tabs Help  
root@krb:~# systemctl restart krb5-kdc  
root@krb:~# systemctl status krb5-kdc  
● krb5-kdc.service - Kerberos 5 Key Distribution Center  
   Loaded: loaded (/lib/systemd/system/krb5-kdc.service; enabled; vendor preset: enabled)  
   Drop-In: /lib/systemd/system/krb5-kdc.service.d  
            └─slapd-before-kdc.conf  
   Active: active (running) since Wed 2020-02-26 06:32:08 UTC; 8s ago  
     Process: 3038 ExecStart=/usr/sbin/krb5kdc -P /var/run/krb5-kdc.pid $DAEMON_ARGS (code=exited, status=0/SUCCESS)  
    Main PID: 3039 (krb5kdc)  
       Tasks: 1 (limit: 4633)  
      CGroup: /system.slice/krb5-kdc.service  
              └─3039 /usr/sbin/krb5kdc -P /var/run/krb5-kdc.pid  
  
Feb 26 06:32:08 krb krb5kdc[3038]: Setting pktinfo on socket 0.0.0.0.88  
Feb 26 06:32:08 krb krb5kdc[3038]: Setting up UDP socket for address ::.88  
Feb 26 06:32:08 krb krb5kdc[3038]: setsockopt(15,IPV6_V6ONLY,1) worked  
Feb 26 06:32:08 krb krb5kdc[3038]: Setting pktinfo on socket ::.88  
Feb 26 06:32:08 krb krb5kdc[3038]: Setting up TCP socket for address 0.0.0.0.88  
Feb 26 06:32:08 krb krb5kdc[3038]: Setting up TCP socket for address ::.88  
Feb 26 06:32:08 krb krb5kdc[3038]: setsockopt(17,IPV6_V6ONLY,1) worked  
Feb 26 06:32:08 krb krb5kdc[3038]: set up 6 sockets  
Feb 26 06:32:08 krb krb5kdc[3039]: commencing operation  
Feb 26 06:32:08 krb systemd[1]: Started Kerberos 5 Key Distribution Center.  
root@krb:~# systemctl restart krb5-admin-server  
root@krb:~# systemctl status krb5-admin-server  
● krb5-admin-server.service - Kerberos 5 Admin Server  
   Loaded: loaded (/lib/systemd/system/krb5-admin-server.service; enabled; vendor preset: enabled)  
   Drop-In: /lib/systemd/system/krb5-admin-server.service.d  
            └─slapd-before-kdc.conf  
   Active: active (running) since Wed 2020-02-26 06:32:22 UTC; 6s ago  
     Main PID: 3044 (kadmind)  
       Tasks: 1 (limit: 4633)  
      CGroup: /system.slice/krb5-admin-server.service  
              └─3044 /usr/sbin/kadmind -nofork  
  
Feb 26 06:32:08 krb krb5kdc[3039]: commencing operation  
Feb 26 06:32:08 krb systemd[1]: Started Kerberos 5 Key Distribution Center.  
root@krb:~# systemctl restart krb5-admin-server  
root@krb:~# systemctl status krb5-admin-server  
● krb5-admin-server.service - Kerberos 5 Admin Server  
   Loaded: loaded (/lib/systemd/system/krb5-admin-server.service; enabled; vendor preset: enabled)  
   Drop-In: /lib/systemd/system/krb5-admin-server.service.d  
            └─slapd-before-kdc.conf  
   Active: active (running) since Wed 2020-02-26 06:32:22 UTC; 6s ago  
     Main PID: 3044 (kadmind)  
       Tasks: 1 (limit: 4633)  
      CGroup: /system.slice/krb5-admin-server.service  
              └─3044 /usr/sbin/kadmind -nofork  
  
Feb 26 06:32:23 krb kadmind[3044]: Setting up TCP socket for address 0.0.0.0.464  
Feb 26 06:32:23 krb kadmind[3044]: Setting up TCP socket for address ::.464  
Feb 26 06:32:23 krb kadmind[3044]: setsockopt(15,IPV6_V6ONLY,1) worked  
Feb 26 06:32:23 krb kadmind[3044]: Setting up RPC socket for address 0.0.0.0.749  
Feb 26 06:32:23 krb kadmind[3044]: Setting up RPC socket for address ::.749  
Feb 26 06:32:23 krb kadmind[3044]: setsockopt(17,IPV6_V6ONLY,1) worked  
Feb 26 06:32:23 krb kadmind[3044]: set up 6 sockets  
Feb 26 06:32:23 krb kadmind[3044]: Seeding random number generator  
Feb 26 06:32:23 krb kadmind[3044]: kadmind: starting...  
Feb 26 06:32:23 krb kadmind[3044]: starting  
root@krb:~# kinit sbhirud2  
Password for sbhirud2@BHIRUD.CCD.LAB:  
root@krb:~# klist  
Ticket cache: FILE:/tmp/krb5cc_0  
Default principal: sbhirud2@BHIRUD.CCD.LAB  
  
Valid starting Expires Service principal  
02/26/20 06:32:40 02/26/20 16:32:40 krbtgt/BHIRUD.CCD.LAB@BHIRUD.CCD.LAB  
renew until 02/27/20 06:32:38  
root@krb:~#
```

5. Explain what the two server blocks in the above configuration file do. Also explain what each location block does. You will likely have to read the nginx documentation to figure all of this out

The configuration file may include several server blocks distinguished by ports on which they listen to and by server names. The nginx first decides which server should process the request.

The first block redirects requests to HTTPS (443) and the return code 301 indicates permanent URL redirection.

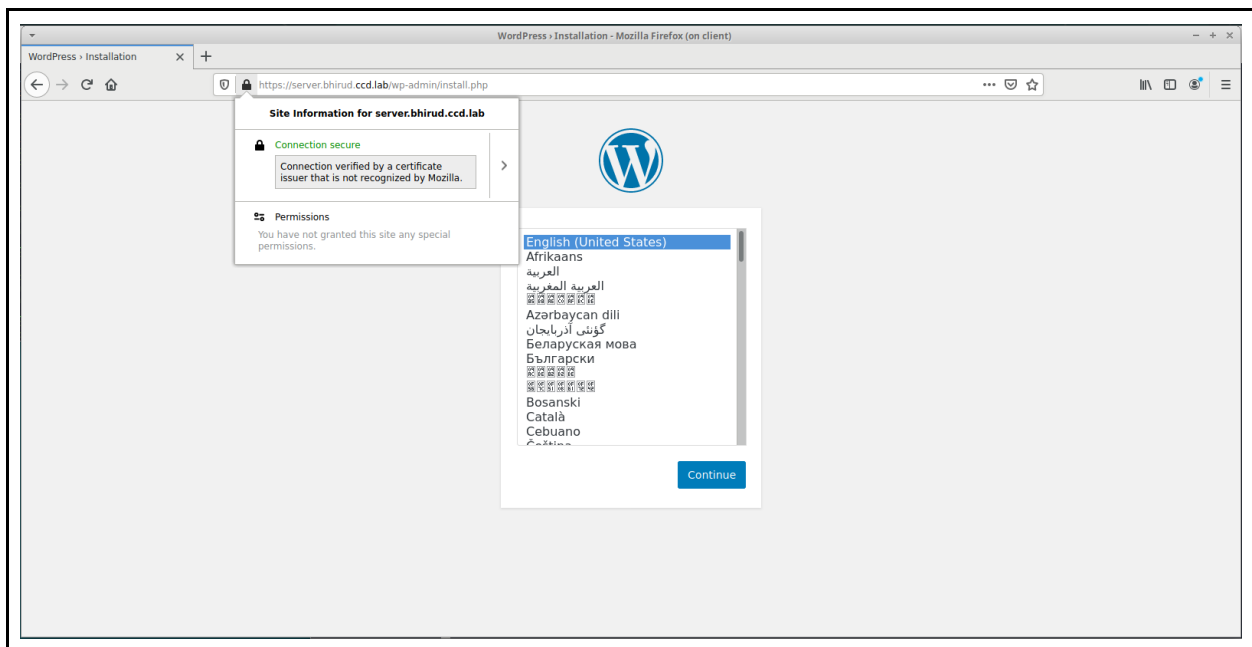
In the second server block, first 4 lines define SSL parameters like the SSL certificate and SSL Certificate Key. Next, the location for the WordPress html file is mentioned.

A location block defines how nginx should handle requests for different resources and URIs for the parent server.

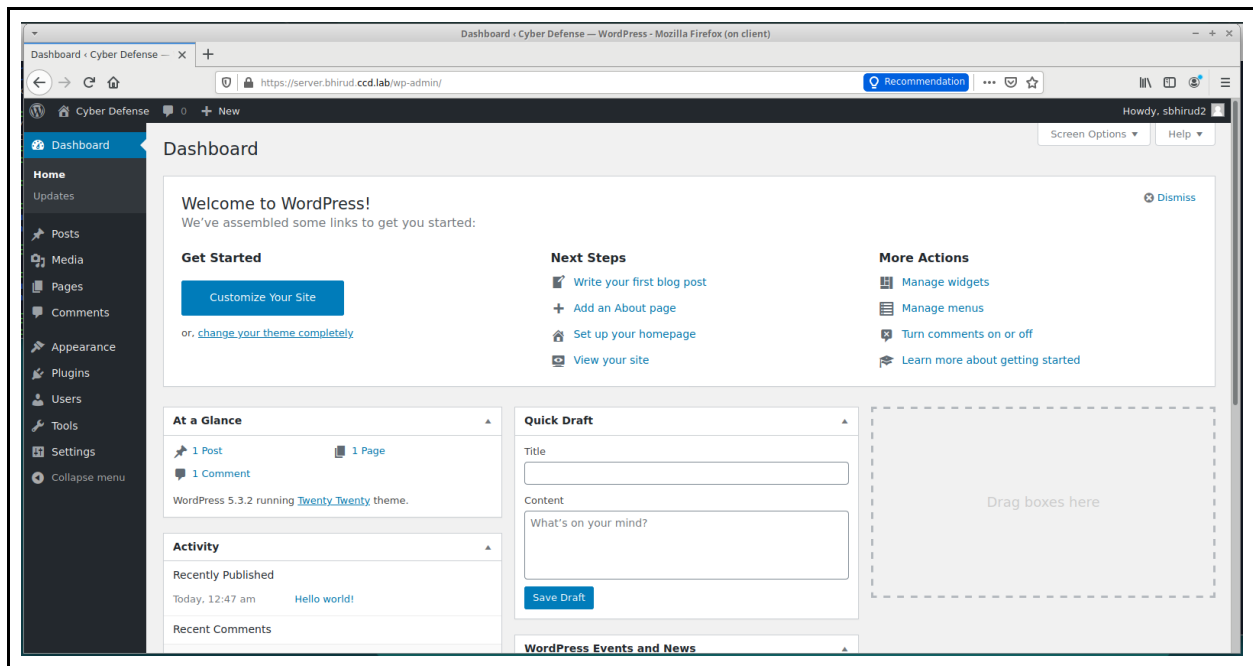
In the first location block, `try_files` command checks the existence and if found, processes the file `index.php`.

In the second location block, the `fastcgi` configuration file is included and nginx is instructed to proxy requests to it via `FCGI` protocol.

6. Upload a screenshot of your Firefox window showing the green padlock icon and the WordPress setup screen



7. Finish the setup of Wordpress and upload a screenshot of the dashboard after you have successfully logged in. Use your Ninernet username here so that we can later link it to your LDAP user that was created in the previous lab



8. Upload a screenshot of this

