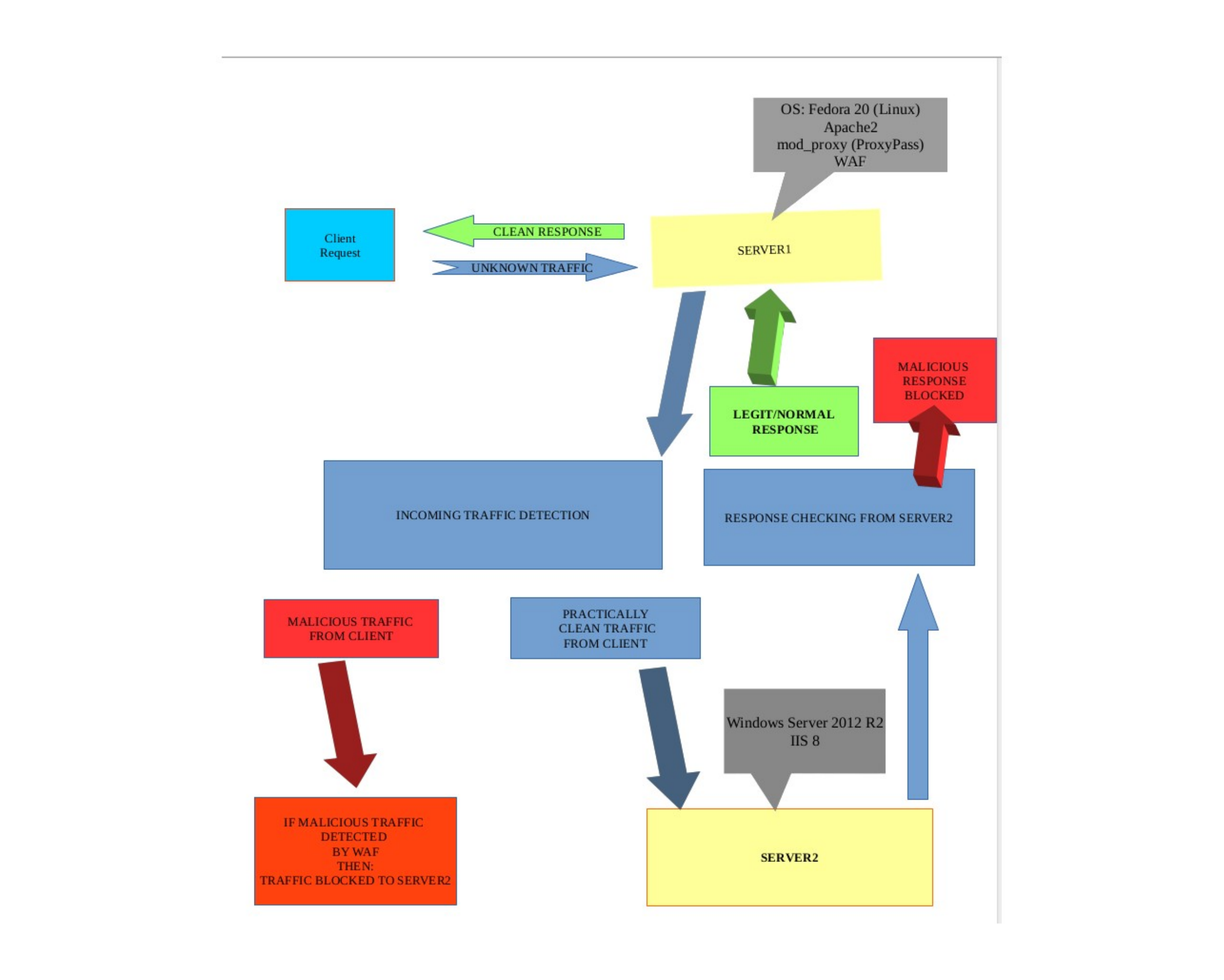


Müəllif: AkaStep

Müasir dövrümüzdə informasiya texnologiyalarının sürətli inkişafı və eyni zamanda virtual həyatımıza sıx şəkildə özünü inteqrə etməsi qaçılmaz olması ilə yanaşı ekvivalent olaraq bir sıra risklərə (haker müdaxiləsi/onun nəticəsində məlumatın oğurlanması/məhv edilməsi/bu oğurlanmış məlumatın müxtəlif məqsədlərlə istifadəsi) günümüzdə **İnformasiya Təhlükəsizliyi** məsələsini üzərindən xətt çəkilməyən bir aktual amilə çevirmişdir.

Bu məqaləni də yazmaqda səbəb məhz sistem administratorlarının bu kimi informasiya resurslarının təhlükəsizliyini lazımı dərəcədə təmin etməsini asanlaşdırmaqdan ibarətdir.
Onları məlumatlandırmaqdan ibarətdir.

Bügünkü taskımız aşağıdakı halı özündə əhatə edəcək
Hesab edək ki:

OS: **Windows Server 2012 R2** və onun üzərində qurulmuş **Web Serverimiz var (IIS 8.5)** və eyni zamanda həmin Web Server üzərində qurulmuş saytı(-ları) haker hücumlarından lazımı dərəcədə qorumaq lazımdır.

İlk ağla gələn WAF (Web Application Firewall)-dır.
Giriş üçün onu deyim ki, WAF -ın əsas rolu sayta/web serverə qarşı həyata keçirilən müxtəlif növ hücumları analiz etmək/onların qarşısını vaxtında dərhal almaqdan ibarətdir.

Ancaq bir məsələ var. IIS üzərində WAF qurmaq,onu xüsusilə .NET əsaslı sayta uyğunlaşdırmaq çox çətin məsələdir.
Məsələn deyə bilərsiniz ki, WebPI(Microsoft Web platform installer) üzərində mod_security bizə install etməyə təklif edilir.
Haqlısınız lakin onu bir daha qeyd edim ki, mod_security-nin manage edilməsi/configlərin editlənməsi/hücum vektorlarının/signaturalarının whitelist edilməsi/daha da harden edilməsi sözün əsl mənasında real problemdir.

Bundan əlavə mod_security IIS üzərində əksər hallarda səbəbi bilinmədən crash-lar/saytın fəaliyyətinin dayanması/fəaliyyətinin pozulmasına gətirir.
Bu kimi problemlər təkcə mod_security-də deyil Windows OS(IIS) üzərində qurulmaq üçün nəzərdə tutulmuş müxtəlif növ WAF-larda qeydə alınır.Bu da ola bilsin ki, IIS -in özəyinin (core) Əməliyyat sistemi ilə daha dərin inteqrəsindən qaynaqlanır.
Bunları tam əminliklə ona görə deyirəm ki, real hallarda ən azı 3 ayrı-ayrı şirkətdən müxtəlif növ WAF-lar mənim tərəfimdən IIS üzərində yoxlanılıb və bu kimi ciddi problemlərlə qarşılaşmışam.Stabilliyi heç cürə ala bilməmişəm.

Bu səbəbdən məsləhət görərdim ki, IIS-üzərində WAF install etməyəsiniz.

Alternativ çıxış yolu olaraq IIS-in qarşısında bir Linux (məsələn Fedora 20/21 sınanılıb) qurub proksifikasiya və eyni zamanda traffiki WAF -dan keçirməklə bunu həyata keçirəsiniz.
(Bu sizə daha elastik/rahat idarə edilə bilən/stabil konfiqurasiya verəcək)

Planımız aşağıdakı kimidir.

Frontend (Qarşıdakı serverimizdir(Publicə baxacaq port mappinglə)
OS: Fedora Workstation 21
[Apache 2.4 + mod_proxy modulu ilə+ WAF (Applicure DotDefender 5.13)])
IP: 192.168.1.103

Backend (Windows Server 2012 R2 + IIS 8.5)
IP: 192.168.1.105

İlk öncə Frontend qismində Fedora 21-i qururuq.(https://getfedora.org/en/workstation/)

Unutmuruq ki, sistem qalxdıqdan sonra bütün paketləri up2date (güncəl) vəziyyətə gətirməliyik.

```
yum -y update
```

Və daha sonra aşağıdakı kimi (tam prosesi terminaldan copy və paste edirəm) çünki hər bir direktivin nə üçün nəzərdə tutulmasını yazmaq məqalədən kənardır.Əsas virtualhost direktivlərinə fikir verməyinizi xahiş edirəm)

```
[root@localhost ~]# cat /etc/os-release
NAME=Fedora
VERSION="21 (Twenty One)"
ID=fedora
VERSION_ID=21
PRETTY_NAME="Fedora 21 (Twenty One)"
ANSI_COLOR="0;34"
CPE_NAME="cpe:/o:fedoraproject:fedora:21"
HOME_URL="https://fedoraproject.org/"
BUG_REPORT_URL="https://bugzilla.redhat.com/"
REDHAT_BUGZILLA_PRODUCT="Fedora"
REDHAT_BUGZILLA_PRODUCT_VERSION=21
REDHAT_SUPPORT_PRODUCT="Fedora"
REDHAT_SUPPORT_PRODUCT_VERSION=21

[root@localhost ~]# uname -a
Linux localhost.localdomain 3.18.7-200.fc21.x86_64 #1 SMP Wed Feb 11 21:53:17 UTC 2015 x86_64
x86_64 x86_64 GNU/Linux


[root@localhost ~]# ifconfig -V
net-tools 2.10-alpha
[root@localhost ~]# ifconfig
eno16777736: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.175.131  netmask 255.255.255.0  broadcast 192.168.175.255
        inet6 fe80::20c:29ff:fe18:504c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:18:50:4c  txqueuelen 1000  (Ethernet)
        RX packets 26  bytes 4328 (4.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46  bytes 6329 (6.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eno33554976: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.103  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe18:5056  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:18:50:56  txqueuelen 1000  (Ethernet)
        RX packets 108438  bytes 155998763 (148.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 70411  bytes 5287190 (5.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 605718  bytes 59560660 (56.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 605718  bytes 59560660 (56.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 36:d0:b8:d9:1c:d2  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0



[blackhat@localhost ~]$ yum info httpd.x86_64
Loaded plugins: langpacks
Installed Packages
Name        : httpd
Arch        : x86_64
Version     : 2.4.10
Release     : 9.fc21
Size        : 3.8 M
Repo        : installed
From repo   : koji-override-0
Summary     : Apache HTTP Server
URL         : http://httpd.apache.org/
License     : ASL 2.0
Description : The Apache HTTP Server is a powerful, efficient, and extensible
            : web server.



[root@localhost ~]# yum -y install httpd
Loaded plugins: langpacks
Resolving Dependencies
--> Running transaction check
---> Package httpd.x86_64 0:2.4.10-9.fc21 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                        Arch                           Version                                Repository
Size
==================================================================================
==================================================================================
Installing:
 httpd                          x86_64                         2.4.10-9.fc21                          fedora
1.2 M

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

Total download size: 1.2 M
Installed size: 3.8 M
Downloading packages:
httpd-2.4.10-9.fc21.x86_64.rpm                                                                              | 1.2
MB  00:00:03
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction (shutdown inhibited)
  Installing : httpd-2.4.10-9.fc21.x86_64
1/1
  Verifying  : httpd-2.4.10-9.fc21.x86_64
1/1

Installed:
  httpd.x86_64 0:2.4.10-9.fc21

Complete!

[root@localhost ~]# nmap localhost -p 80

Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-09 02:10 AZT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000072s latency).
rDNS record for 127.0.0.1: localhost.localdomain
PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

[root@localhost ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to
/usr/lib/systemd/system/httpd.service.
```

```
[root@localhost ~]# nmap localhost

Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-09 02:11 AZT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000033s latency).
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds

[root@localhost ~]# curl -I localhost:80
HTTP/1.1 403 Forbidden
Date: Sun, 08 Mar 2015 22:11:44 GMT
Server: Apache/2.4.10 (Fedora)
Last-Modified: Wed, 03 Sep 2014 14:45:59 GMT
ETag: "1201-5022a4b5077c0"
Accept-Ranges: bytes
Content-Length: 4609
Content-Type: text/html; charset=UTF-8




[root@localhost ~]# /usr/sbin/httpd -V
Server version: Apache/2.4.10 (Fedora)
Server built:   Sep  3 2014 14:49:30
Server's Module Magic Number: 20120211:36
Server loaded:  APR 1.5.1, APR-UTIL 1.5.4
Compiled using: APR 1.5.1, APR-UTIL 1.5.3
Architecture:   64-bit
Server MPM:     prefork
  threaded:     no
    forked:     yes (variable process count)
Server compiled with....
 -D APR_HAS_SENDFILE
 -D APR_HAS_MMAP
 -D APR_HAVE_IPV6 (IPv4-mapped addresses enabled)
 -D APR_USE_SYSVSEM_SERIALIZE
 -D APR_USE_PTHREAD_SERIALIZE
 -D SINGLE_LISTEN_UNSERIALIZED_ACCEPT
 -D APR_HAS_OTHER_CHILD
 -D AP_HAVE_RELIABLE_PIPED_LOGS
 -D DYNAMIC_MODULE_LIMIT=256
 -D HTTPD_ROOT="/etc/httpd"
 -D SUEXEC_BIN="/usr/sbin/suexec"
 -D DEFAULT_PIDLOG="/run/httpd/httpd.pid"
 -D DEFAULT_SCOREBOARD="logs/apache_runtime_status"
 -D DEFAULT_ERRORLOG="logs/error_log"
 -D AP_TYPES_CONFIG_FILE="conf/mime.types"
 -D SERVER_CONFIG_FILE="conf/httpd.conf"


[root@localhost ~]# /usr/sbin/httpd -M
Loaded Modules:
 core_module (static)
 so_module (static)
 http_module (static)
 access_compat_module (shared)
 actions_module (shared)
 alias_module (shared)
 allowmethods_module (shared)
 auth_basic_module (shared)
 auth_digest_module (shared)
 authn_anon_module (shared)
 authn_core_module (shared)
 authn_dbd_module (shared)
 authn_dbm_module (shared)
 authn_file_module (shared)
 authn_socache_module (shared)
 authz_core_module (shared)
 authz_dbd_module (shared)
 authz_dbm_module (shared)
 authz_groupfile_module (shared)
 authz_host_module (shared)
 authz_owner_module (shared)
 authz_user_module (shared)
 autoindex_module (shared)
 cache_module (shared)
 cache_disk_module (shared)
 data_module (shared)
 dbd_module (shared)
 deflate_module (shared)
 dir_module (shared)
 dumpio_module (shared)
 echo_module (shared)
 env_module (shared)
 expires_module (shared)
 ext_filter_module (shared)
 filter_module (shared)
 headers_module (shared)
 include_module (shared)
 info_module (shared)
 log_config_module (shared)
 logio_module (shared)
 macro_module (shared)
 mime_magic_module (shared)
 mime_module (shared)
 negotiation_module (shared)
 remoteip_module (shared)
 reqtimeout_module (shared)
 request_module (shared)
 rewrite_module (shared)
 setenvif_module (shared)
 slotmem_plain_module (shared)
 slotmem_shm_module (shared)
 socache_dbm_module (shared)
 socache_memcache_module (shared)
 socache_shmcb_module (shared)
 status_module (shared)
 substitute_module (shared)
 suexec_module (shared)
 unique_id_module (shared)
 unixd_module (shared)
 userdir_module (shared)
 version_module (shared)
 vhost_alias_module (shared)
 dav_module (shared)
 dav_fs_module (shared)
 dav_lock_module (shared)
 lua_module (shared)
 mpm_prefork_module (shared)
 proxy_module (shared)
 lbmethod_bybusyness_module (shared)
 lbmethod_byrequests_module (shared)
 lbmethod_bytraffic_module (shared)
 lbmethod_heartbeat_module (shared)
 proxy_ajp_module (shared)
 proxy_balancer_module (shared)
 proxy_connect_module (shared)
 proxy_express_module (shared)
 proxy_fcgi_module (shared)
 proxy_fdpass_module (shared)
 proxy_ftp_module (shared)
 proxy_http_module (shared)
 proxy_scgi_module (shared)
 systemd_module (shared)
 cgi_module (shared)
[root@localhost ~]#


[root@localhost ~]# cd /etc/httpd/
```

```
[root@localhost httpd]# pwd;ls
/etc/httpd
conf  conf.d  conf.modules.d  logs  modules  run
[root@localhost httpd]# cd conf
[root@localhost conf]# ls
httpd.conf  magic
[root@localhost conf]# nano httpd.conf
[root@localhost conf]# cd ..
[root@localhost httpd]# find ./ -name 'welcome.conf'
./conf.d/welcome.conf
[root@localhost httpd]# mv ./conf.d/welcome.conf ./conf.d/welcome_conf.disabled;chmod 600
./conf.d/welcome_conf.disabled;ls -tliash ./conf.d/
total 24K
917872 4.0K drwxr-xr-x. 2 root root 4.0K Mar  9 02:16 .
917576 4.0K drwxr-xr-x. 5 root root 4.0K Mar  9 02:10 ..
918632 4.0K -rw-r--r--. 1 root root  366 Sep  3  2014 README
917870 4.0K -rw-r--r--. 1 root root 2.9K Sep  3  2014 autoindex.conf
917871 4.0K -rw-r--r--. 1 root root 1.3K Sep  3  2014 userdir.conf
917873 4.0K -rw-------. 1 root root  516 Sep  3  2014 welcome_conf.disabled
[root@localhost httpd]# systemctl restart httpd

[root@localhost httpd]# ps aux|grep -i "http"
root      3393  0.0  0.3 227796  7876 ?        Ss   02:25   0:00 /usr/sbin/httpd -DFOREGROUND
apache    3394  0.0  0.3 230016  6368 ?        S    02:25   0:00 /usr/sbin/httpd -DFOREGROUND
apache    3395  0.0  0.3 230016  6368 ?        S    02:25   0:00 /usr/sbin/httpd -DFOREGROUND
apache    3396  0.0  0.3 230016  6368 ?        S    02:25   0:00 /usr/sbin/httpd -DFOREGROUND
apache    3397  0.0  0.3 230016  6368 ?        S    02:25   0:00 /usr/sbin/httpd -DFOREGROUND
apache    3398  0.0  0.3 229880  6368 ?        S    02:25   0:00 /usr/sbin/httpd -DFOREGROUND
apache    3399  0.0  0.3 229880  6368 ?        S    02:25   0:00 /usr/sbin/httpd -DFOREGROUND
apache    3402  0.0  0.3 229880  6368 ?        S    02:25   0:00 /usr/sbin/httpd -DFOREGROUND
root      3667  0.0  0.1 113004  2264 pts/1    S+   02:30   0:00 grep --color=auto -i http


[root@localhost httpd]# ab -n 60000 -c 300 http://localhost:80/
This is ApacheBench, Version 2.3 <$Revision: 1604373 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking localhost (be patient)
Completed 6000 requests
Completed 12000 requests
Completed 18000 requests
Completed 24000 requests
Completed 30000 requests
Completed 36000 requests
Completed 42000 requests
Completed 48000 requests
Completed 54000 requests
Completed 60000 requests
```

```
Finished 60000 requests


Server Software:        Apache
Server Hostname:        localhost
Server Port:            80

Document Path:          /
Document Length:        209 bytes

Concurrency Level:      300
Time taken for tests:   11.043 seconds
Complete requests:      60000
Failed requests:        0
Non-2xx responses:      60000
Total transferred:      22380000 bytes
HTML transferred:       12540000 bytes
Requests per second:    5433.41 [#/sec] (mean)
Time per request:       55.214 [ms] (mean)
Time per request:       0.184 [ms] (mean, across all concurrent requests)
Transfer rate:          1979.16 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0    2  29.2      1    1006
Processing:     2   38 523.0     12   11012
Waiting:        1   38 523.0     12   11012
Total:          8   40 524.5     13   11026

Percentage of the requests served within a certain time (ms)
  50%     13
  66%     14
  75%     14
  80%     14
  90%     15
  95%     16
  98%     16
  99%     17
 100%  11026 (longest request)
```

```
[root@localhost httpd]# cat conf/httpd.conf
#
# This is the main Apache HTTP server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
# for a discussion of each configuration directive.
#
# Do NOT simply read the instructions in here without understanding
# what they do.  They're here only as hints or reminders.  If you are unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path.  If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# server as '/www/log/access_log', where as '/log/access_log' will be
# interpreted as '/log/access_log'.

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path.  If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used.  If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
NameVirtualHost :80

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO) Support
```

```
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding `LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf

#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User apache
Group apache
ServerTokens Prod

# 'Main' server configuration
#
# The directives in this section set up the values used by the 'main'
# server, which responds to any requests that aren't handled by a
# <VirtualHost> definition.  These values also provide defaults for
# any <VirtualHost> containers you may define later in the file.
#
# All of these directives may appear inside <VirtualHost> containers,
# in which case these default settings will be overridden for the
# virtual host being defined.
#


LoadModule deflate_module modules/mod_deflate.so
<Location />
AddOutputFilterByType DEFLATE text/html text/plain text/css text/xml
</Location>



<VirtualHost 192.168.1.103:80>



ServerName saytim.remote
```

```
ServerAlias www.saytim.remote
DocumentRoot /var/www/html/remote/
#Header unset Content-Type



setenv proxy-initial-not-pooled 1
Header set X-UA-Compatible: IE=EmulateIE9
Header set X-FRAME-OPTIONS: SAMEORIGIN


ProxyBadHeader Ignore
ProxyPreserveHost On
ProxyPass /dotdefender !
ProxyPass / http://192.168.1.105:8083/ retry=10 acquire=3000 timeout=5000 Keepalive=On
ErrorLog logs/saytim.remote.error_log
CustomLog logs/saytim.remote-access_log combined
</VirtualHost>






#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed.  This address appears on some server-generated pages, such
# as error documents.  e.g. admin@your-domain.com
#
ServerAdmin root@localhost

#
# 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.example.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>
```

```
#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"

#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options -Indexes -FollowSymLinks

    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    AllowOverride None

    #
    # Controls who can get stuff from this server.
    #
    Require all granted
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
<IfModule dir_module>
    DirectoryIndex index.html
</IfModule>

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<Files ".ht*">
    Require all denied
</Files>

#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "logs/error_log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O"
combinedio
    </IfModule>
    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    #CustomLog "logs/access_log" common

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    CustomLog "logs/access_log" combined
</IfModule>

<IfModule alias_module>
    #
    # Redirect: Allows you to tell clients about documents that used to
    # exist in your server's namespace, but do not anymore. The client
    # will make a new request for the document at its new location.
    # Example:
    # Redirect permanent /foo http://www.example.com/bar

    #
    # Alias: Maps web paths into filesystem paths and is used to
    # access content that does not live under the DocumentRoot.
    # Example:
    # Alias /webpath /full/filesystem/path
    #
    # If you include a trailing / on /webpath then the server will
    # require it to be present in the URL.  You will also likely
    # need to provide a <Directory> section to allow access to
    # the filesystem path.

    #
    # ScriptAlias: This controls which directories contain server scripts.
    # ScriptAliases are essentially the same as Aliases, except that
    # documents in the target directory are treated as applications and
    # run by the server when requested rather than as documents sent to the
    # client.  The same rules about trailing "/" apply to ScriptAlias
    # directives as to Alias.
    #
    ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"

</IfModule>

#
```

```
# "/var/www/cgi-bin" should be changed to whatever your ScriptAliased
# CGI directory exists, if you have that configured.
#
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>

<IfModule mime_module>
    #
    # TypesConfig points to the file containing the list of mappings from
    # filename extension to MIME-type.
    #
    TypesConfig /etc/mime.types

    #
    # AddType allows you to add to or override the MIME configuration
    # file specified in TypesConfig for specific file types.
    #
    #AddType application/x-gzip .tgz
    #
    # AddEncoding allows you to have certain browsers uncompress
    # information on the fly. Note: Not all browsers support this.
    #
    #AddEncoding x-compress .Z
    #AddEncoding x-gzip .gz .tgz
    #
    # If the AddEncoding directives above are commented-out, then you
    # probably should define those extensions to indicate media types:
    #
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz

    #
    # AddHandler allows you to map certain file extensions to "handlers":
    # actions unrelated to filetype. These can be either built into the server
    # or added with the Action directive (see below)
    #
    # To use CGI scripts outside of ScriptAliased directories:
    # (You will also need to add "ExecCGI" to the "Options" directive.)
    #
    #AddHandler cgi-script .cgi

    # For type maps (negotiated resources):
    #AddHandler type-map var

    #
    # Filters allow you to process content before it is sent to the client.
    #
    # To parse .shtml files for server-side includes (SSI):
    # (You will also need to add "Includes" to the "Options" directive.)
    #
    AddType text/html .shtml
    AddOutputFilter INCLUDES .shtml
</IfModule>

#
# Specify a default charset for all content served; this enables
# interpretation of all content as UTF-8 by default.  To use the
# default browser choice (ISO-8859-1), or to allow the META tags
# in HTML content to override this choice, comment out this
# directive:
#
AddDefaultCharset UTF-8

DefaultType None


AddType application/javascript .axd .js
#AddType text/html .html .htm
#AddType text/plain .txt
#AddType text/richtext .rtx
#AddType text/tab-separated-values .tsv
#AddType text/x-setext .etx
#AddType text/x-server-parsed-html .shtml .sht
#AddType application/macbinhex-40 .hqx
#AddType application/netalivelink .nel
#AddType application/netalive .net
#AddType application/news-message-id
#AddType application/news-transmission
#AddType application/octet-stream .bin .exe
#AddType application/oda .oda
#AddType application/pdf .pdf
#AddType application/postscript .ai .eps .ps
#AddType application/remote-printing
#AddType application/rtf .rtf
#AddType application/slate
#AddType application/zip .zip
#AddType application/x-mif .mif
#AddType application/wita
#AddType application/wordperfect5.1
#AddType application/x-csh .csh
#AddType application/x-dvi .dvi
#AddType application/x-hdf .hdf
#AddType application/x-latex .latex
#AddType application/x-netcdf .nc .cdf
#AddType application/x-sh .sh
```

```
#AddType application/x-tcl .tcl
#AddType application/x-tex .tex
#AddType application/x-texinfo .texinfo .texi
#AddType application/x-troff .t .tr .roff
#AddType application/x-troff-man .man
#AddType application/x-troff-me .me
#AddType application/x-troff-ms .ms
#AddType application/x-wais-source .src
#AddType application/x-bcpio .bcpio
#Type image/ief .ief
#AddType image/jpeg .jpeg .jpg .jpe .JPG
#AddType image/tiff .tiff .tif
#AddType image/x-cmu-raster .ras
#AddType image/x-portable-anymap .pnm
#AddType image/x-portable-bitmap .pbm
#AddType image/x-portable-graygmap .pgm
```

```
#<IfModule mime_magic_module>
    #
    # The mod_mime_magic module allows the server to use various hints from the
    # contents of the file itself to determine its type.  The MIMEMagicFile
    # directive tells the module where the hint definitions are located.
    #
#   MIMEMagicFile conf/magic
#</IfModule>

#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#

#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files.  This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
```

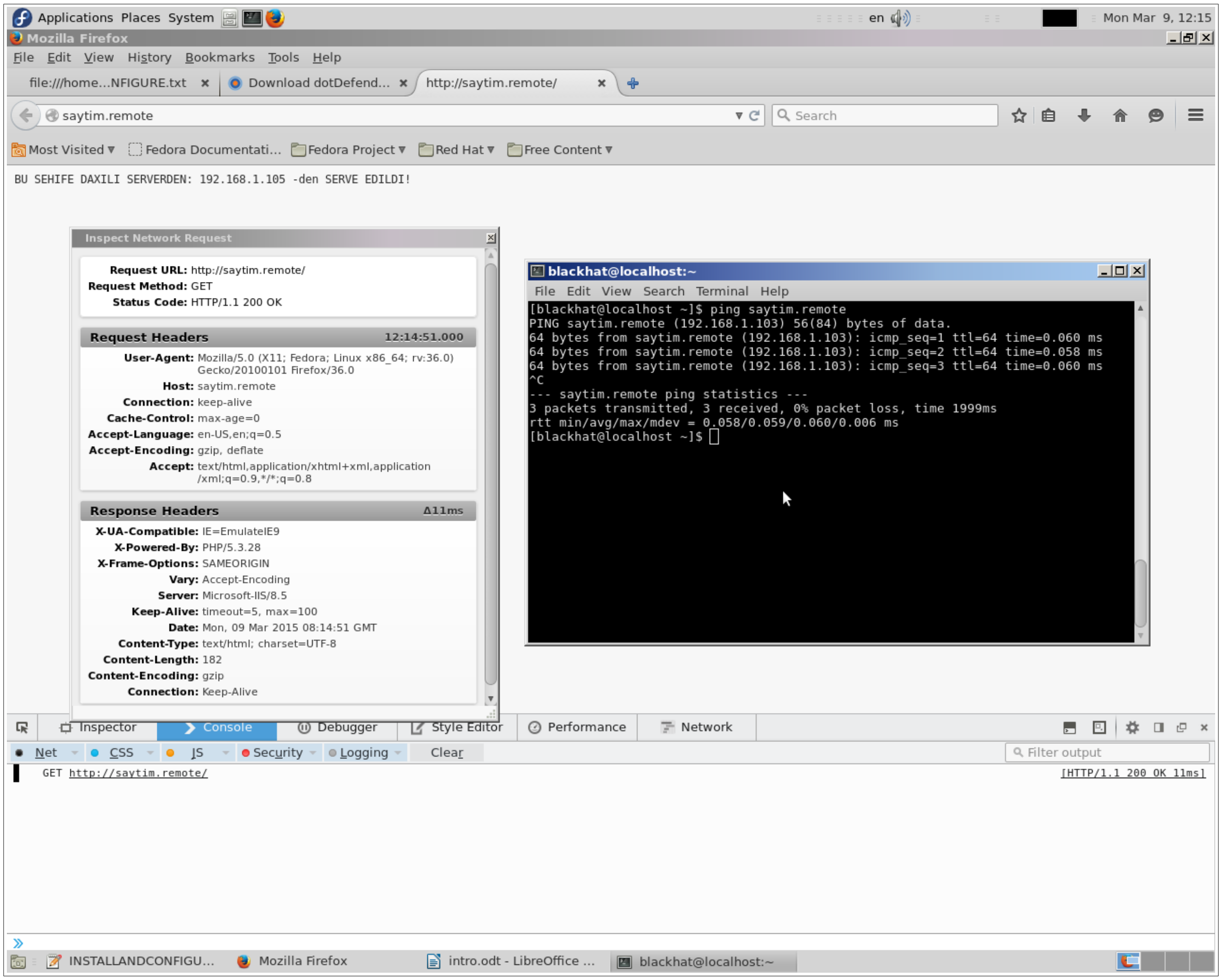
```
#EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf




[root@localhost httpd]# cat /etc/hosts
127.0.0.1               localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6




192.168.1.103   saytim.remote
192.168.1.103   www.saytim.remote


[root@localhost httpd]# mkdir /var/www/html/remote/

[root@localhost httpd]# cd /var/www/html/

[root@localhost html]# ls -tliash
total 12K
535945 4.0K drwxr-xr-x. 3 root root 4.0K Mar  9 02:51 .
526049 4.0K drwxr-xr-x. 2 root root 4.0K Mar  9 02:51 remote
535787 4.0K drwxr-xr-x. 4 root root 4.0K Dec  4 00:43 ..

[root@localhost html]# systemctl restart httpd

[root@localhost ~]# curl -I localhost:80
HTTP/1.1 403 Forbidden
Date: Sun, 08 Mar 2015 23:01:08 GMT
Server: Apache
Content-Type: text/html; charset=iso-8859-1



[root@localhost html]# while true;do netstat -tulpan|grep -i ":8083" && sleep 3;done;
tcp        0      1 192.168.1.103:32956     192.168.1.105:8083      SYN_SENT    4017/httpd
tcp        0      1 192.168.1.103:32958     192.168.1.105:8083      SYN_SENT    4018/httpd
tcp        0      1 192.168.1.103:32960     192.168.1.105:8083      SYN_SENT    4019/httpd
```

```
[root@localhost ~]# ls /etc/httpd/logs/
access_log  error_log  saytim.remote-access_log  saytim.remote.error_log

[root@localhost ~]# ls -tliash /etc/httpd/logs/
total 20M
437572 5.2M -rw-r--r--.  1 root root 5.2M Mar  9 03:01 access_log
437571  15M -rw-r--r--.  1 root root  15M Mar  9 03:01 error_log
437351 4.0K -rw-r--r--.  1 root root 1.6K Mar  9 02:54 saytim.remote-access_log
437350 8.0K -rw-r--r--.  1 root root 4.5K Mar  9 02:54 saytim.remote.error_log
426525 4.0K drwx------.  2 root root 4.0K Mar  9 02:46 .
425883 4.0K drwxr-xr-x. 16 root root 4.0K Mar  9 01:55 ..

[root@localhost ~]# cd /etc/httpd/logs/

[root@localhost logs]# ls -tliash
total 20M
437572 5.2M -rw-r--r--.  1 root root 5.2M Mar  9 03:01 access_log
437571  15M -rw-r--r--.  1 root root  15M Mar  9 03:01 error_log
437351 4.0K -rw-r--r--.  1 root root 1.6K Mar  9 02:54 saytim.remote-access_log
437350 8.0K -rw-r--r--.  1 root root 4.5K Mar  9 02:54 saytim.remote.error_log
426525 4.0K drwx------.  2 root root 4.0K Mar  9 02:46 .
425883 4.0K drwxr-xr-x. 16 root root 4.0K Mar  9 01:55 ..

[root@localhost logs]# head -n 30 saytim.remote-access_log
192.168.1.103 - - [09/Mar/2015:02:46:47 +0400] "GET / HTTP/1.1" 503 299 "-" "Mozilla/5.0 (X11;
Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0"
192.168.1.103 - - [09/Mar/2015:02:46:52 +0400] "GET / HTTP/1.1" 503 299 "-" "Mozilla/5.0 (X11;
Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0"
192.168.1.103 - - [09/Mar/2015:02:46:52 +0400] "GET /favicon.ico HTTP/1.1" 503 299 "-"
"Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0"
192.168.1.103 - - [09/Mar/2015:02:46:52 +0400] "GET /favicon.ico HTTP/1.1" 503 299 "-"
"Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0"
192.168.1.103 - - [09/Mar/2015:02:47:59 +0400] "GET / HTTP/1.1" 503 299 "-" "Mozilla/5.0 (X11;
Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0"
192.168.1.103 - - [09/Mar/2015:02:52:32 +0400] "GET / HTTP/1.1" 503 299 "-" "Mozilla/5.0 (X11;
Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0"
192.168.1.103 - - [09/Mar/2015:02:53:30 +0400] "GET / HTTP/1.1" 503 299 "-" "Mozilla/5.0 (X11;
Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0"
192.168.1.103 - - [09/Mar/2015:02:53:37 +0400] "GET / HTTP/1.1" 503 299 "-" "Mozilla/5.0 (X11;
Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0"
192.168.1.103 - - [09/Mar/2015:02:53:52 +0400] "GET / HTTP/1.1" 503 299 "-" "Mozilla/5.0 (X11;
Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0"
192.168.1.103 - - [09/Mar/2015:02:54:32 +0400] "GET / HTTP/1.1" 503 299 "-" "Mozilla/5.0 (X11;
Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0"

[root@localhost logs]# tail -n 10 saytim.remote.error_log
[Mon Mar 09 02:53:33.238321 2015] [proxy_http:error] [pid 4017] [client 192.168.1.103:54255]
```

```
AH01114: HTTP: failed to make connection to backend: 192.168.1.105
[Mon Mar 09 02:53:40.642203 2015] [proxy:error] [pid 4018] (113)No route to host: AH00957: HTTP:
attempt to connect to 192.168.1.105:8083 (192.168.1.105) failed
[Mon Mar 09 02:53:40.642271 2015] [proxy:error] [pid 4018] AH00959: ap_proxy_connect_backend
disabling worker for (192.168.1.105) for 10s
[Mon Mar 09 02:53:40.642285 2015] [proxy_http:error] [pid 4018] [client 192.168.1.103:54257]
AH01114: HTTP: failed to make connection to backend: 192.168.1.105
[Mon Mar 09 02:53:55.206157 2015] [proxy:error] [pid 4019] (113)No route to host: AH00957: HTTP:
attempt to connect to 192.168.1.105:8083 (192.168.1.105) failed
[Mon Mar 09 02:53:55.206215 2015] [proxy:error] [pid 4019] AH00959: ap_proxy_connect_backend
disabling worker for (192.168.1.105) for 10s
[Mon Mar 09 02:53:55.206227 2015] [proxy_http:error] [pid 4019] [client 192.168.1.103:54259]
AH01114: HTTP: failed to make connection to backend: 192.168.1.105
[Mon Mar 09 02:54:35.218191 2015] [proxy:error] [pid 8550] (113)No route to host: AH00957: HTTP:
attempt to connect to 192.168.1.105:8083 (192.168.1.105) failed
[Mon Mar 09 02:54:35.218256 2015] [proxy:error] [pid 8550] AH00959: ap_proxy_connect_backend
disabling worker for (192.168.1.105) for 10s
[Mon Mar 09 02:54:35.218275 2015] [proxy_http:error] [pid 8550] [client 192.168.1.103:54261]
AH01114: HTTP: failed to make connection to backend: 192.168.1.105

# Backend-de neymiz var baxaq #
[blackhat@localhost ~]$ su -c "nmap -sS -sV -PN 192.168.1.105"
Password:

Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-09 12:05 AZT

Nmap scan report for 192.168.1.105
Host is up (0.00043s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Microsoft IIS httpd 8.5
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
8083/tcp  open  http        Microsoft IIS httpd 8.5
49155/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 00:0C:29:F1:0B:C7 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.44 seconds


# Frontendde- neyimiz var baxaq #
# Fikir verin proksifikasiya hesabina Apacheni IIS olaraq gosterir. #

[blackhat@localhost ~]$ su -c "nmap -sS -sV -PN 192.168.1.103"
Password:
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-09 12:07 AZT
Nmap scan report for saytim.remote (192.168.1.103)
Host is up (0.000017s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 8.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.19 seconds
[blackhat@localhost ~]$ curl -I 192.168.1.103:80
HTTP/1.1 200 OK
Date: Mon, 09 Mar 2015 08:09:08 GMT
Server: Microsoft-IIS/8.5
Content-Type: text/html; charset=UTF-8
X-Powered-By: PHP/5.3.28
X-UA-Compatible: IE=EmulateIE9
X-FRAME-OPTIONS: SAMEORIGIN

[blackhat@localhost ~]$ curl -I 192.168.1.103:80/lolllllll
HTTP/1.1 404 Not Found
Date: Mon, 09 Mar 2015 08:09:15 GMT
Server: Microsoft-IIS/8.5
Content-Length: 1245
Content-Type: text/html; charset=UTF-8
X-UA-Compatible: IE=EmulateIE9
X-FRAME-OPTIONS: SAMEORIGIN

[blackhat@localhost ~]$ curl -I 192.168.1.103:80/dotdefender/
HTTP/1.1 404 Not Found
Date: Mon, 09 Mar 2015 08:09:26 GMT
Server: Apache
Content-Type: text/html; charset=iso-8859-1
```

Proksifikasiyanın işlədiyinə əmin olmaq üçün bir neçə sadə yoxlanış edirik:



```
BU SEHIFE DAXILI SERVERDEN: 192.168.1.105 -den SERVE EDILDI!
```

Inspect Network Request

Request URL: http://saytim.remote/
Request Method: GET
Status Code: HTTP/1.1 200 OK

Request Headers 12:14:51.000

User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0
Host: saytim.remote
Connection: keep-alive
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

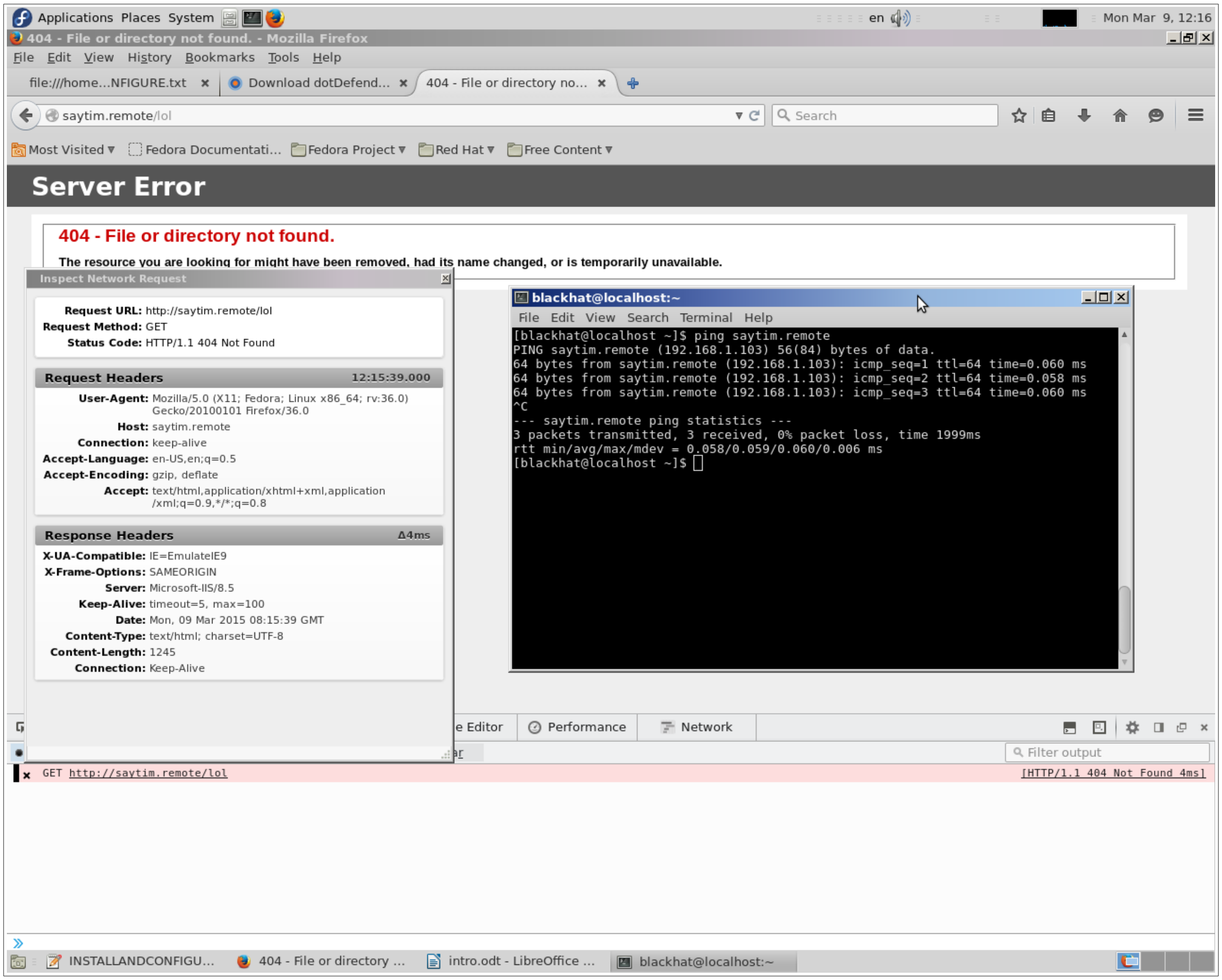
Response Headers Δ11ms

X-UA-Compatible: IE=EmulateIE9
X-Powered-By: PHP/5.3.28
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
Keep-Alive: timeout=5, max=100
Date: Mon, 09 Mar 2015 08:14:51 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 182
Content-Encoding: gzip
Connection: Keep-Alive

blackhat@localhost:~

```
[blackhat@localhost ~]$ ping saytim.remote
PING saytim.remote (192.168.1.103) 56(84) bytes of data.
64 bytes from saytim.remote (192.168.1.103): icmp_seq=1 ttl=64 time=0.060 ms
64 bytes from saytim.remote (192.168.1.103): icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from saytim.remote (192.168.1.103): icmp_seq=3 ttl=64 time=0.060 ms
^C
--- saytim.remote ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.058/0.059/0.060/0.006 ms
[blackhat@localhost ~]$ 
```

```
GET http://saytim.remote/                                    [HTTP/1.1 200 OK 11ms]
```


Applications Places System
en
Mon Mar 9, 12:16
404 - File or directory not found. - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home...NFIGURE.txt
Download dotDefend...
404 - File or directory no...
saytim.remote/lol
Search
Most Visited ▾
Fedora Documentati...
Fedora Project ▾
Red Hat ▾
Free Content ▾

Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Request URL: http://saytim.remote/lol
Request Method: GET
Status Code: HTTP/1.1 404 Not Found

Request Headers 12:15:39.000

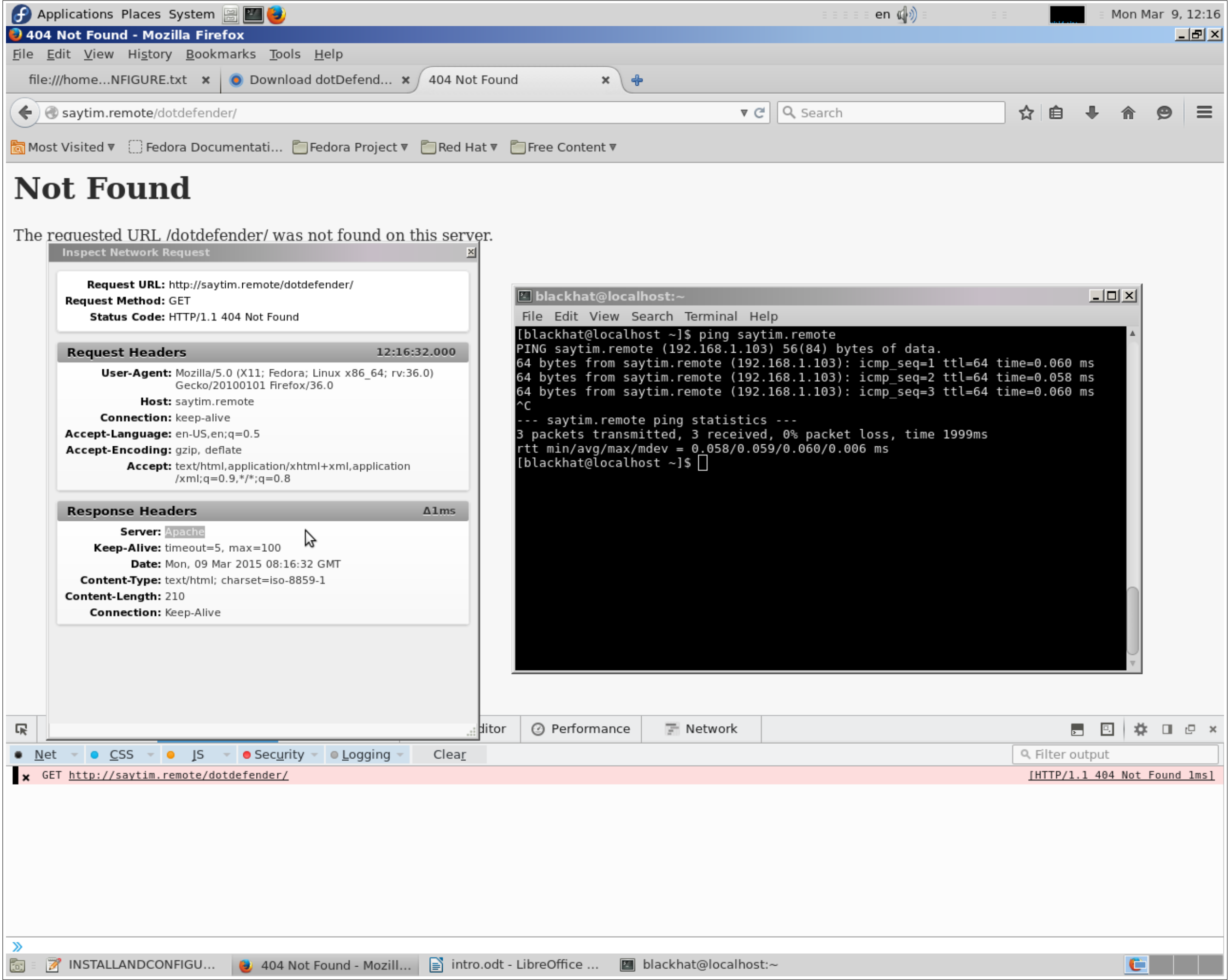
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0
Host: saytim.remote
Connection: keep-alive
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Response Headers Δ4ms

X-UA-Compatible: IE=EmulateIE9
X-Frame-Options: SAMEORIGIN
Server: Microsoft-IIS/8.5
Keep-Alive: timeout=5, max=100
Date: Mon, 09 Mar 2015 08:15:39 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1245
Connection: Keep-Alive

```
[blackhat@localhost ~]$ ping saytim.remote
PING saytim.remote (192.168.1.103) 56(84) bytes of data.
64 bytes from saytim.remote (192.168.1.103): icmp_seq=1 ttl=64 time=0.060 ms
64 bytes from saytim.remote (192.168.1.103): icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from saytim.remote (192.168.1.103): icmp_seq=3 ttl=64 time=0.060 ms
^C
--- saytim.remote ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.058/0.059/0.060/0.006 ms
[blackhat@localhost ~]$
```

```
GET http://saytim.remote/lol                                    [HTTP/1.1 404 Not Found 4ms]
```



Not Found

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

Inspect Network Request

Request URL: http://saytim.remote/dotdefender/
Request Method: GET
Status Code: HTTP/1.1 404 Not Found

Request Headers 12:16:32.000

User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0
Host: saytim.remote
Connection: keep-alive
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Response Headers Δ1ms

Server: Apache
Keep-Alive: timeout=5, max=100
Date: Mon, 09 Mar 2015 08:16:32 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 210
Connection: Keep-Alive

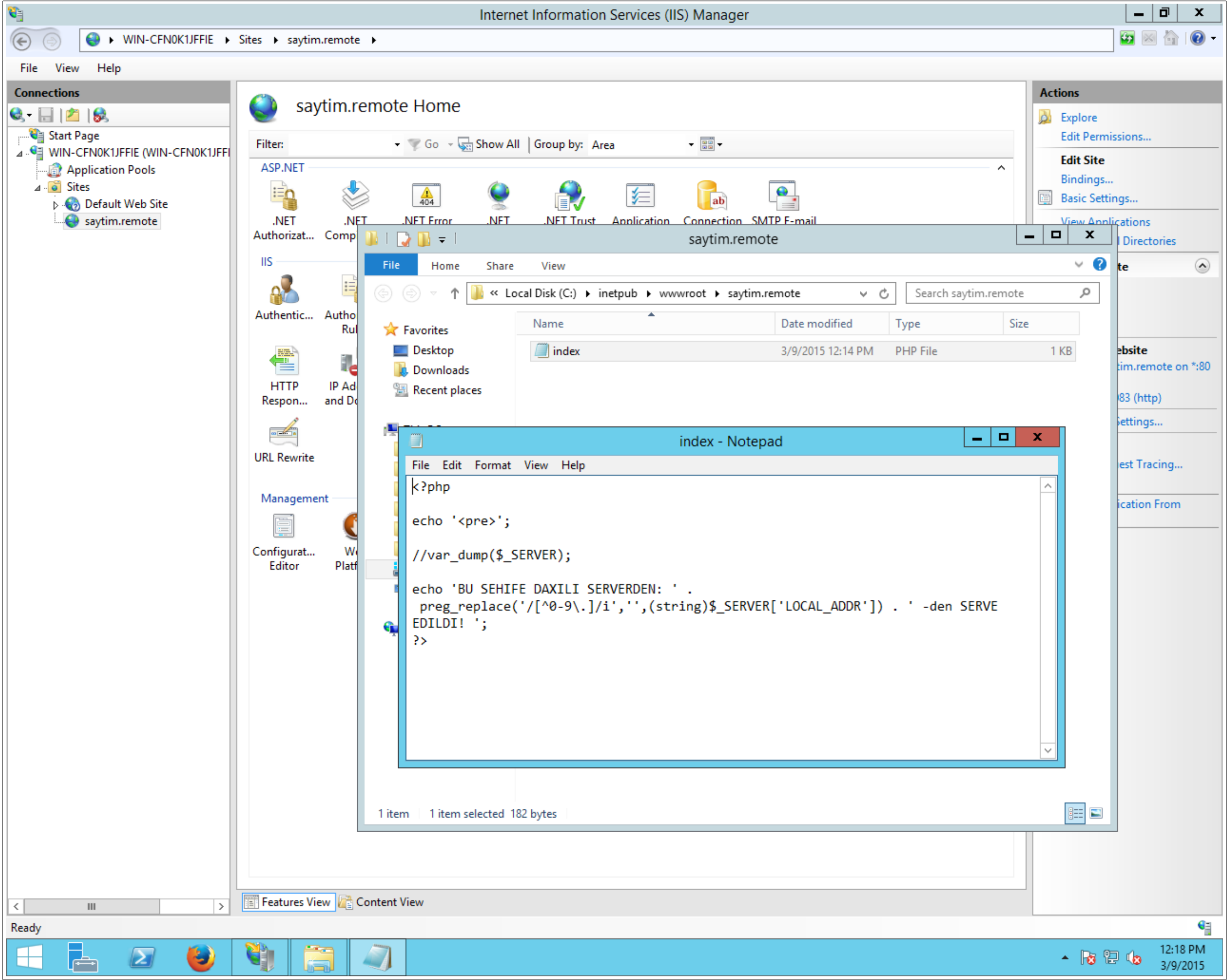
blackhat@localhost:~

File Edit View Search Terminal Help

```
[blackhat@localhost ~]$ ping saytim.remote
PING saytim.remote (192.168.1.103) 56(84) bytes of data.
64 bytes from saytim.remote (192.168.1.103): icmp_seq=1 ttl=64 time=0.060 ms
64 bytes from saytim.remote (192.168.1.103): icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from saytim.remote (192.168.1.103): icmp_seq=3 ttl=64 time=0.060 ms
^C
--- saytim.remote ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.058/0.059/0.060/0.006 ms
[blackhat@localhost ~]$
```

```
GET http://saytim.remote/dotdefender/                    [HTTP/1.1 404 Not Found 1ms]
```

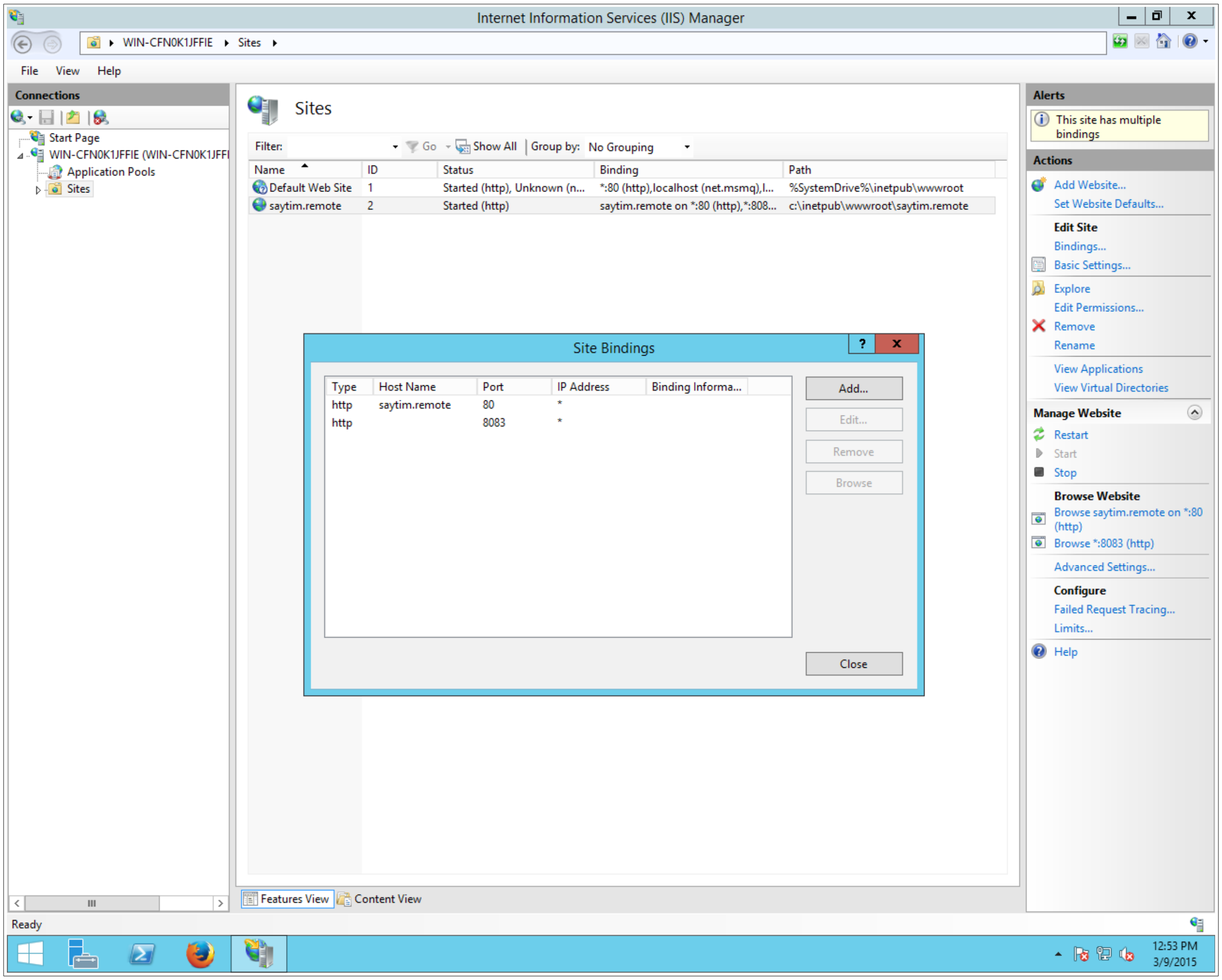
**Aşağıdakı şəkildə isə gördüyünüz Backend-dir (IIS 8.5).
Yazılan skript isə oxucuya informasiyanı daha aydın şəkildə çatdırmaq üçün nəzərdə tutulub.Onu yerinə sizdə Backend-dəki web application olacaq.**


Internet Information Services (IIS) Manager
WIN-CFN0K1JFFIE ▸ Sites ▸ saytim.remote
saytim.remote Home
saytim.remote
Local Disk (C:) ▸ inetpub ▸ wwwroot ▸ saytim.remote
index - Notepad

Name	Date modified	Type	Size
index	3/9/2015 12:14 PM	PHP File	1 KB

```
<?php

echo '<pre>';

//var_dump($_SERVER);

echo 'BU SEHIFE DAXILI SERVERDEN: ' .
 preg_replace('/[^0-9\.]/i','',(string)$_SERVER['LOCAL_ADDR']) . ' -den SERVE
EDILDI! ';
?>
```

Növbəti aşağıdakı şəkildə isə Backend-də aşağıdakı PORT bindingləri vermişəm. Məhz 8083 portuna Frontend-dən sorğular gələcək.



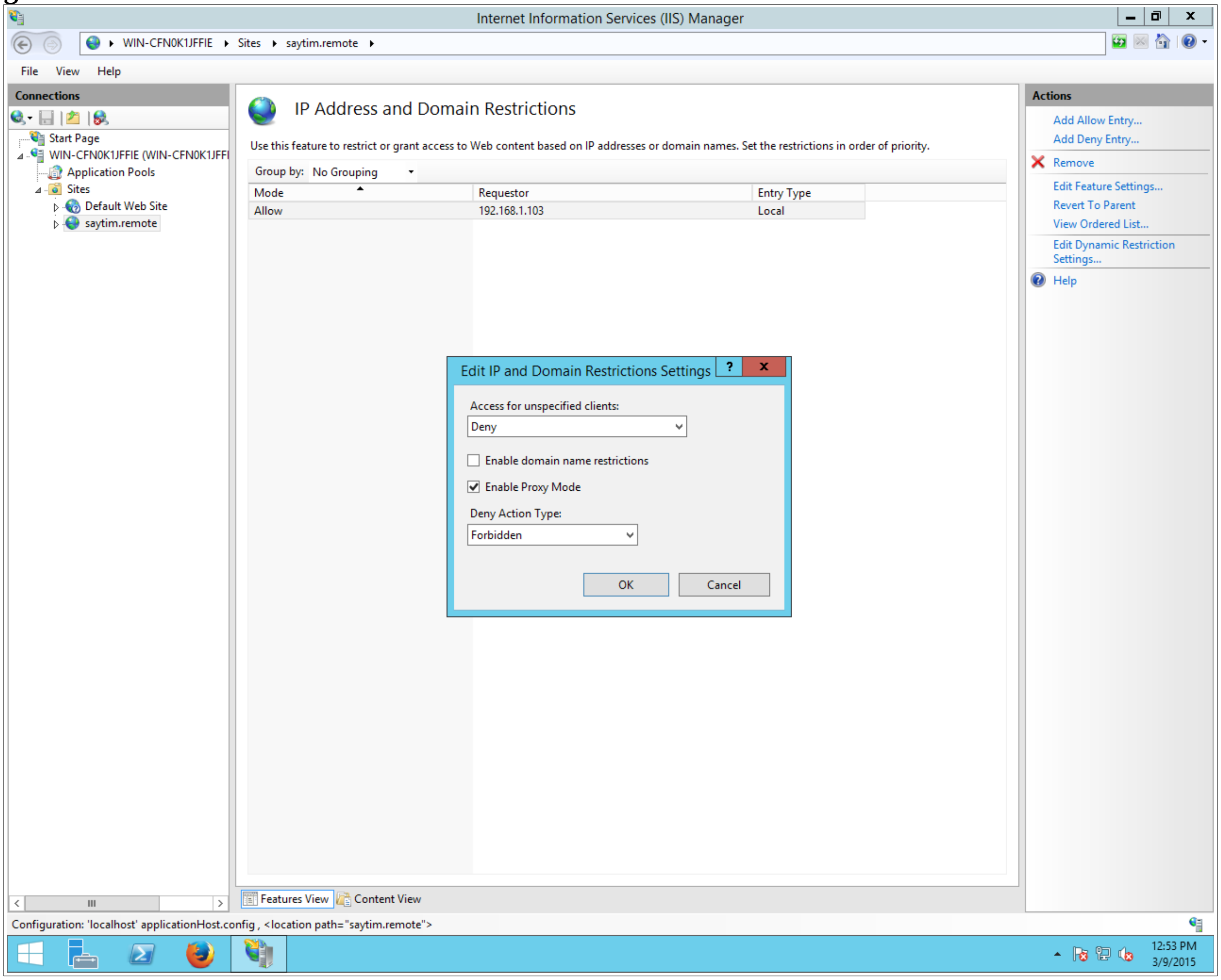
This site has multiple bindings

Name	ID	Status	Binding	Path
Default Web Site	1	Started (http), Unknown (n...	*:80 (http),localhost (net.msmq),l...	%SystemDrive%\inetpub\wwwroot
saytim.remote	2	Started (http)	saytim.remote on *:80 (http),*:808...	c:\inetpub\wwwroot\saytim.remote

Type	Host Name	Port	IP Address	Binding Informa...
http	saytim.remote	80	*	
http		8083	*	

Növbəti aşağıdakı şəkildə isə bir qədər də preventativ tədbirlər görərək IIS 8.5 üzərində **IP Address And Domain Restrictions** modulunun köməkliyi ilə Backend-ə yalnız sorğuların Frontend-

dən daxil olmasını təmin edirik.
İşdir sizdə **IP Address And Domain Restrictions** **modulu yoxdursa onu install etməyi məsləhət görürəm.**



IP Address and Domain Restrictions

Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.

Group by: No Grouping

Mode	Requestor	Entry Type
Allow	192.168.1.103	Local

Edit IP and Domain Restrictions Settings

Access for unspecified clients: Deny

□ Enable domain name restrictions

☑ Enable Proxy Mode

Deny Action Type: Forbidden

OK Cancel

Configuration: 'localhost' applicationHost.config , <location path="saytim.remote">

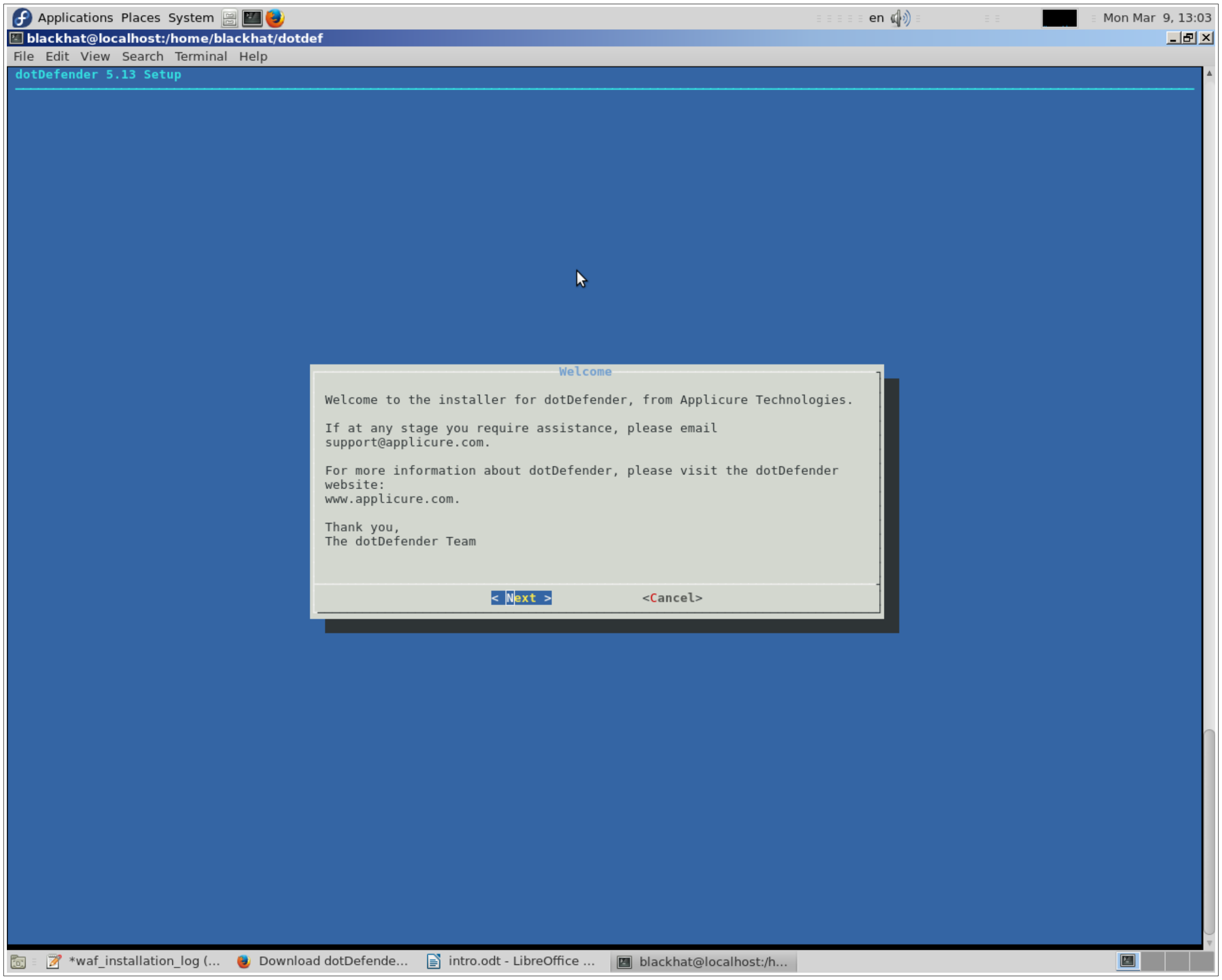
Bir daha proksifikasiyanın normal getdiyinə yuxarıdakı bir sıra testlərdən sonra əmin olduqdan sonra artıq Dotdefenderin Frontend-də install əməliyyatına başlamaq olar.

http://www.applicure.com/download-latest
Daxil oluruq və **dotDefender for Linux RPM 64bit** versiyasını yükləyirik.

(**dotDefender V5.13 for Linux - supports Apache 2.4**) çünki Fronteddəki **Apache 2.4**-dür.

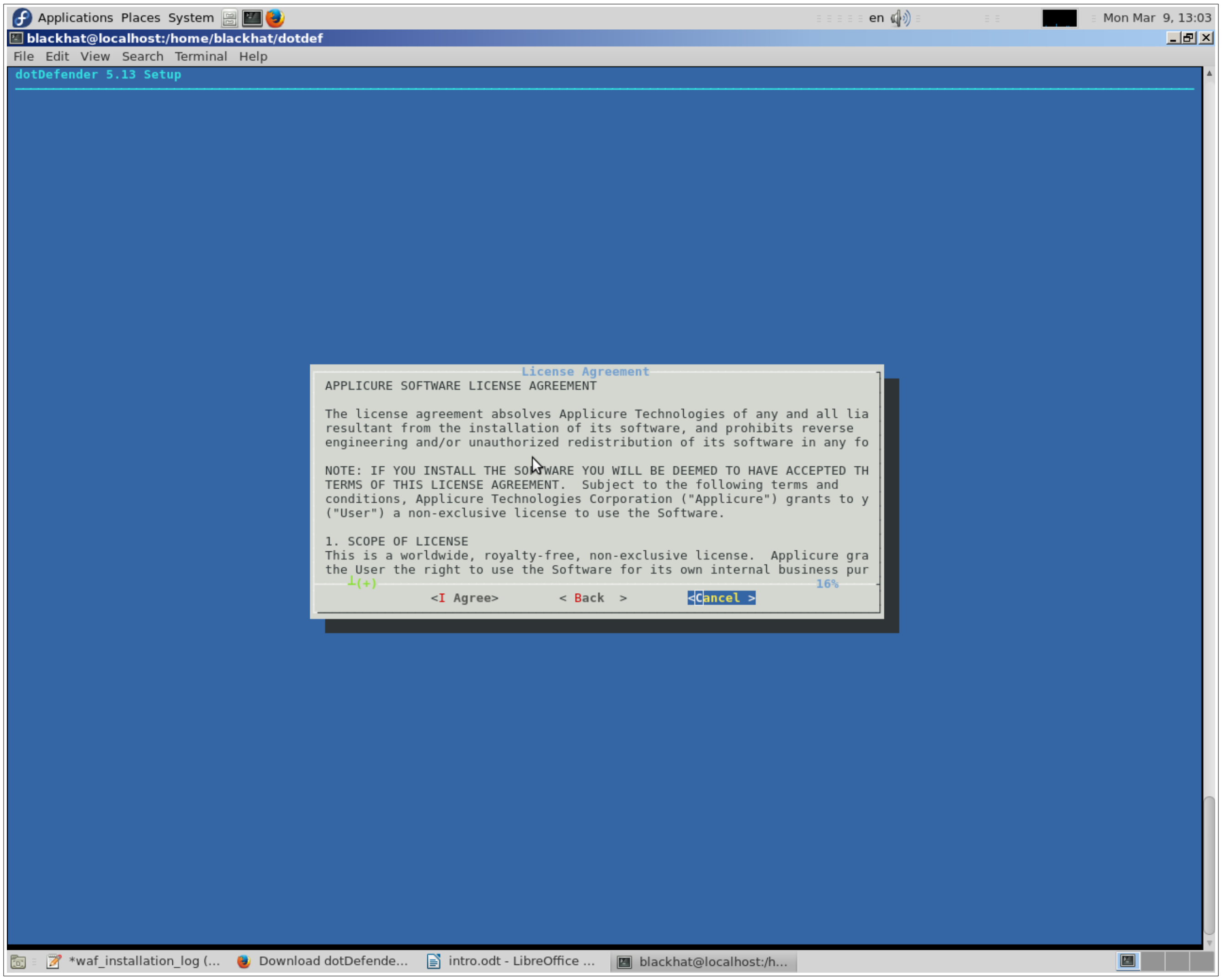
```
[blackhat@localhost ~]$ cd
[blackhat@localhost ~]$ mkdir dotdef
[blackhat@localhost ~]$ cd dotdef/
[blackhat@localhost dotdef]$ wget --user-agent="MSIE GECKO 11"
www.applicure.com/downloads/5.13/Linux/x86_64/dotDefender-5.13.Linux.x86_64.rpm.bin.gz
--2015-03-09 12:59:16--  http://www.applicure.com/downloads/5.13/Linux/x86_64/dotDefender-
5.13.Linux.x86_64.rpm.bin.gz
Resolving www.applicure.com (www.applicure.com)... 98.158.178.76
Connecting to www.applicure.com (www.applicure.com)|98.158.178.76|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17360312 (17M) [application/x-gzip]
Saving to: ‘dotDefender-5.13.Linux.x86_64.rpm.bin.gz’

dotDefender-5.13.Linux.x86_64.rpm.bin.g 100%
[================================================================
======>]  16.56M   530KB/s   in 46s

2015-03-09 13:00:03 (365 KB/s) - ‘dotDefender-5.13.Linux.x86_64.rpm.bin.gz’ saved
[17360312/17360312]

[blackhat@localhost dotdef]$ ls -tliash
total 17M
786435 4.0K drwx------. 17 blackhat blackhat 4.0K Mar  9 13:00 ..
788370 4.0K drwxrwxr-x   2 blackhat blackhat 4.0K Mar  9 12:59 .
786641  17M -rw-rw-r--   1 blackhat blackhat  17M Aug 30  2011 dotDefender-
5.13.Linux.x86_64.rpm.bin.gz
[blackhat@localhost dotdef]$ gzip -d dotDefender-5.13.Linux.x86_64.rpm.bin.gz
[blackhat@localhost dotdef]$ ls -tliash
total 18M
788370 4.0K drwxrwxr-x   2 blackhat blackhat 4.0K Mar  9 13:02 .
786435 4.0K drwx------. 17 blackhat blackhat 4.0K Mar  9 13:00 ..
787417  18M -rw-rw-r--   1 blackhat blackhat  18M Aug 30  2011 dotDefender-
5.13.Linux.x86_64.rpm.bin
[blackhat@localhost dotdef]$ chmod +x dotDefender-5.13.Linux.x86_64.rpm.bin
[blackhat@localhost dotdef]$ ls -tliash
total 18M
788370 4.0K drwxrwxr-x   2 blackhat blackhat 4.0K Mar  9 13:02 .
786435 4.0K drwx------. 17 blackhat blackhat 4.0K Mar  9 13:00 ..
787417  18M -rwxrwxr-x   1 blackhat blackhat  18M Aug 30  2011 dotDefender-
5.13.Linux.x86_64.rpm.bin
[blackhat@localhost dotdef]$ su
Password:
[root@localhost dotdef]# id
uid=0(root) gid=0(root) groups=0(root)
```

```
[root@localhost dotdef]# ./dotDefender-5.13.Linux.x86_64.rpm.bin
```

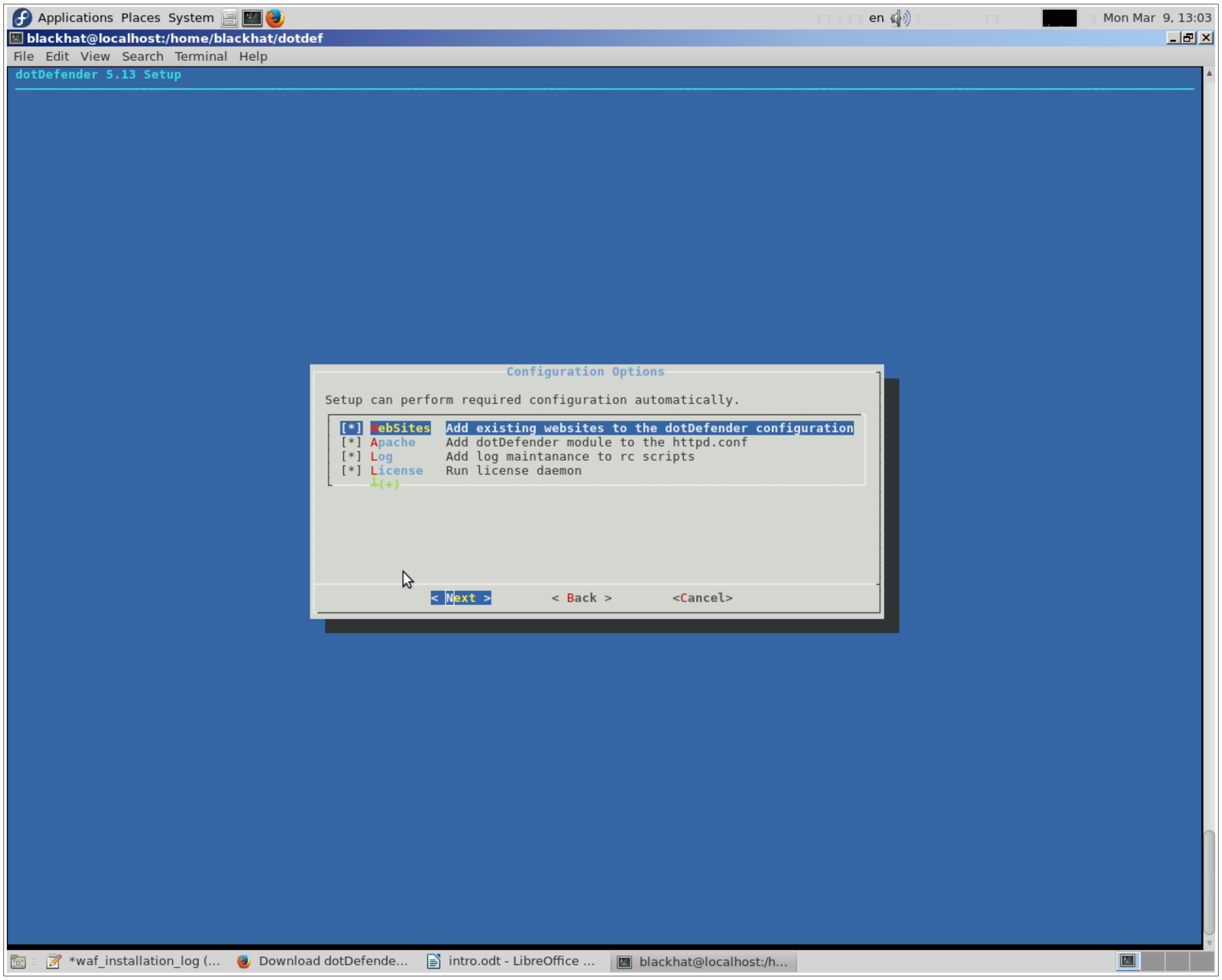


Applications Places System
en
Mon Mar 9, 13:03
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Help
*waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

Welcome

Welcome to the installer for dotDefender, from Applicure Technologies.

If at any stage you require assistance, please email
support@applicure.com.

For more information about dotDefender, please visit the dotDefender
website:
www.applicure.com.

Thank you,
The dotDefender Team

< Next >            <Cancel>
```


Applications Places System
en
Mon Mar 9, 13:03
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Help
*waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

                     License Agreement
APPLICURE SOFTWARE LICENSE AGREEMENT

The license agreement absolves Applicure Technologies of any and all lia
resultant from the installation of its software, and prohibits reverse
engineering and/or unauthorized redistribution of its software in any fo

NOTE: IF YOU INSTALL THE SOFTWARE YOU WILL BE DEEMED TO HAVE ACCEPTED TH
TERMS OF THIS LICENSE AGREEMENT.  Subject to the following terms and
conditions, Applicure Technologies Corporation ("Applicure") grants to y
("User") a non-exclusive license to use the Software.

1. SCOPE OF LICENSE
This is a worldwide, royalty-free, non-exclusive license.  Applicure gra
the User the right to use the Software for its own internal business pur
   (+)                                                        16%
          <I Agree>        < Back  >        <Cancel >
```



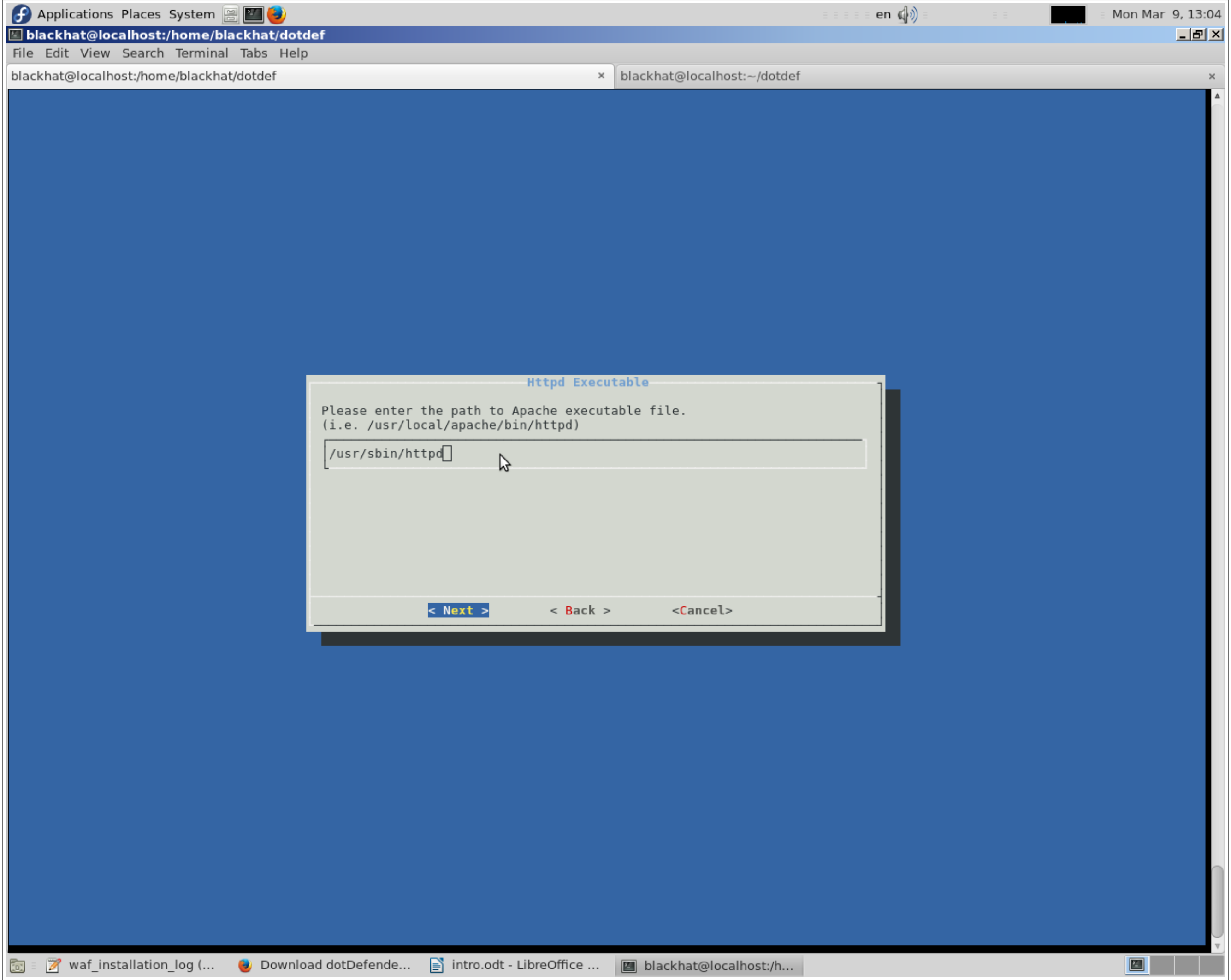
Applications Places System
en
Mon Mar 9, 13:03
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Help
*waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

Configuration Options

Setup can perform required configuration automatically.

[*] WebSites   Add existing websites to the dotDefender configuration
[*] Apache     Add dotDefender module to the httpd.conf
[*] Log        Add log maintanance to rc scripts
[*] License    Run license daemon
   (+)

< Next >      < Back >      <Cancel>
```

WAF bizdən soruşur httpd executable path-i daxil etməyi:

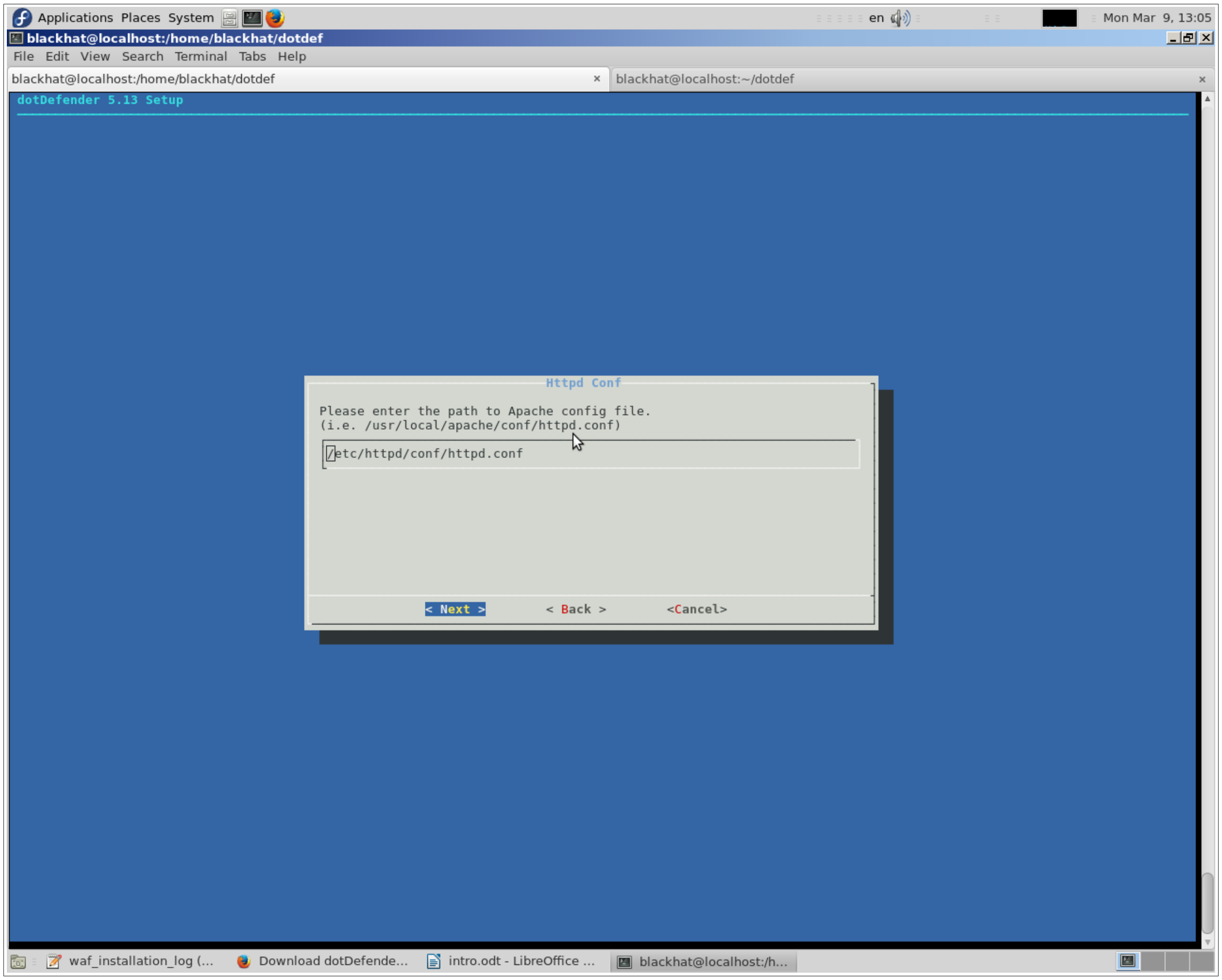
```
[blackhat@localhost dotdef]$ ps aux|grep -i "httpd"
root       1185  0.0  0.3 227792  7916 ?       Ss   03:29   0:01 /usr/sbin/httpd -DFOREGROUND
apache     1206  0.0  0.3 230008  6568 ?       S    03:29   0:00 /usr/sbin/httpd -DFOREGROUND
apache     1207  0.0  0.3 230008  6568 ?       S    03:29   0:00 /usr/sbin/httpd -DFOREGROUND
apache     1208  0.0  0.3 230008  6568 ?       S    03:29   0:00 /usr/sbin/httpd -DFOREGROUND
apache     1209  0.0  0.3 230008  6568 ?       S    03:29   0:00 /usr/sbin/httpd -DFOREGROUND
apache     1210  0.0  0.3 230008  6568 ?       S    03:29   0:00 /usr/sbin/httpd -DFOREGROUND
apache     2201  0.0  0.3 230008  6568 ?       S    03:31   0:00 /usr/sbin/httpd -DFOREGROUND
apache     2430  0.0  0.3 230008  6572 ?       S    04:40   0:00 /usr/sbin/httpd -DFOREGROUND
root       4805  0.0  0.1 111884  2568 pts/0    S+   13:03   0:00 /tmp/dotDefender/dialog --stdout
--backtitle dotDefender 5.13 Setup --title Httpd Executable --inputbox  Please enter the path to Apache
executable file. (i.e. /usr/local/apache/bin/httpd)  18 76
blackhat   4836  0.0  0.1 113004  2276 pts/1    S+   13:04   0:00 grep --color=auto -i httpd
```

```
[root@localhost dotdef]# service httpd restart
Redirecting to /bin/systemctl restart  httpd.service
```



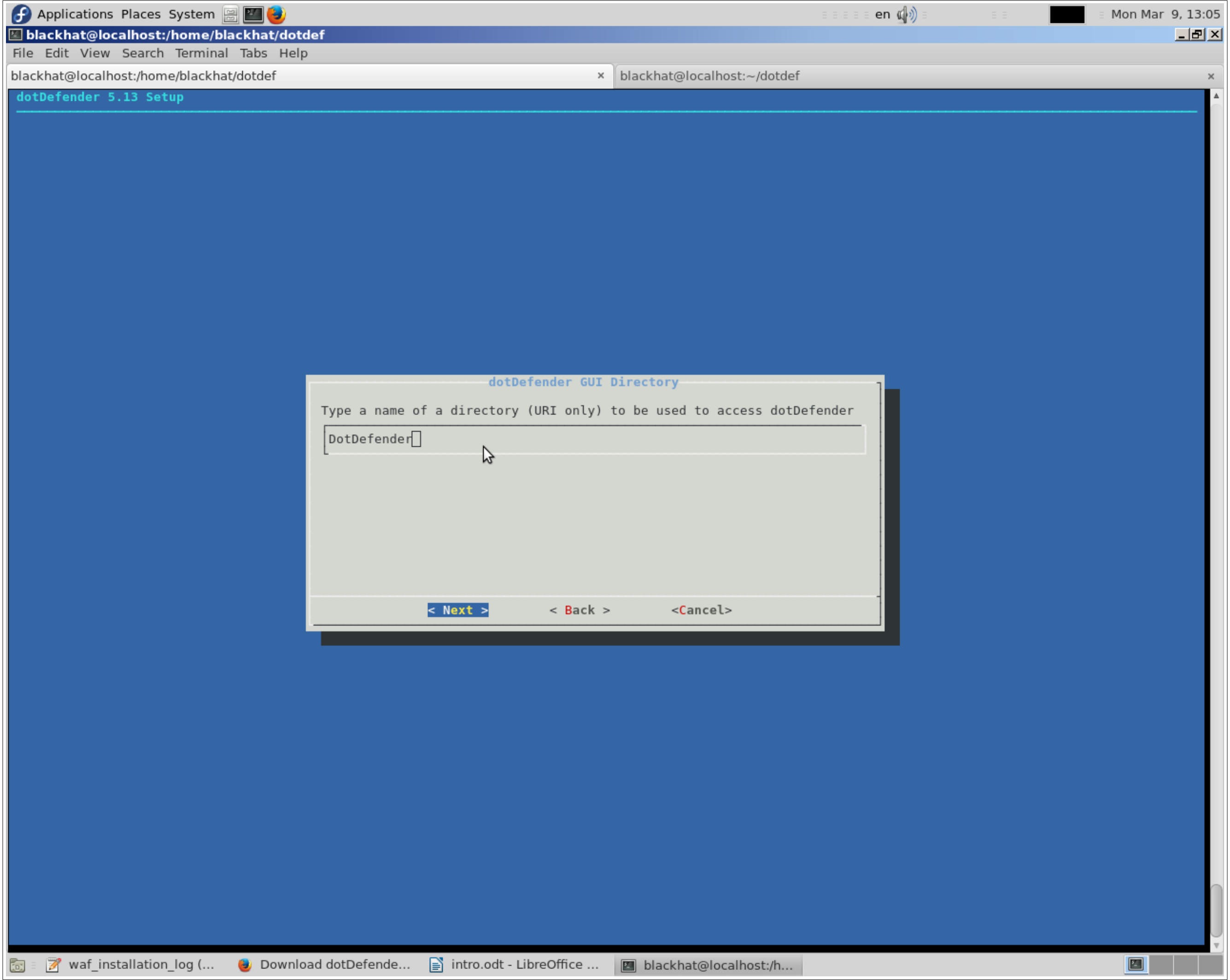
Applications Places System
en
Mon Mar 9, 13:04
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
Httpd Executable

Please enter the path to Apache executable file.
(i.e. /usr/local/apache/bin/httpd)

/usr/sbin/httpd
```



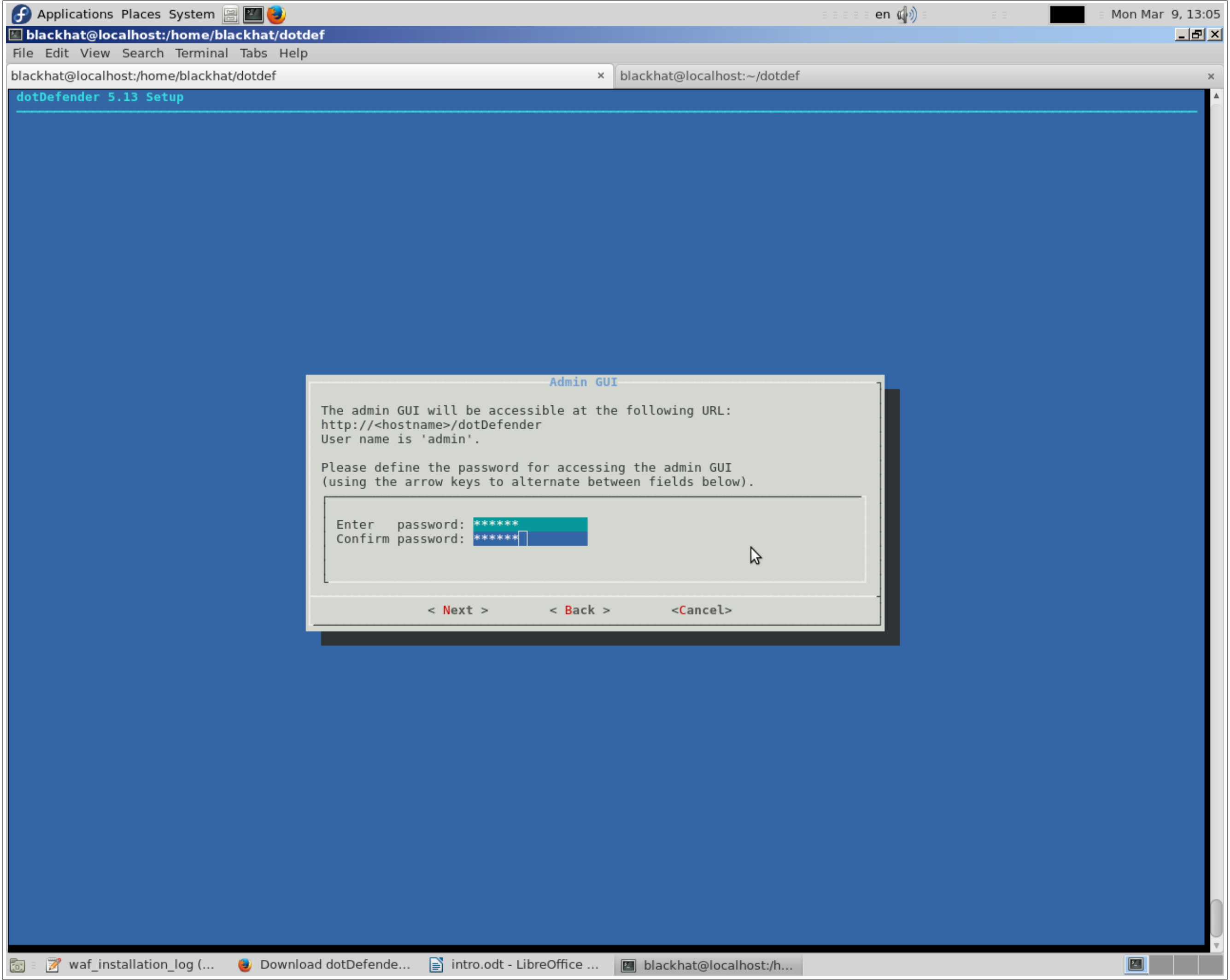
Applications Places System
en
Mon Mar 9, 13:05
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

                              Httpd Conf
  Please enter the path to Apache config file.
  (i.e. /usr/local/apache/conf/httpd.conf)

  /etc/httpd/conf/httpd.conf

         < Next >          < Back >          <Cancel>
```



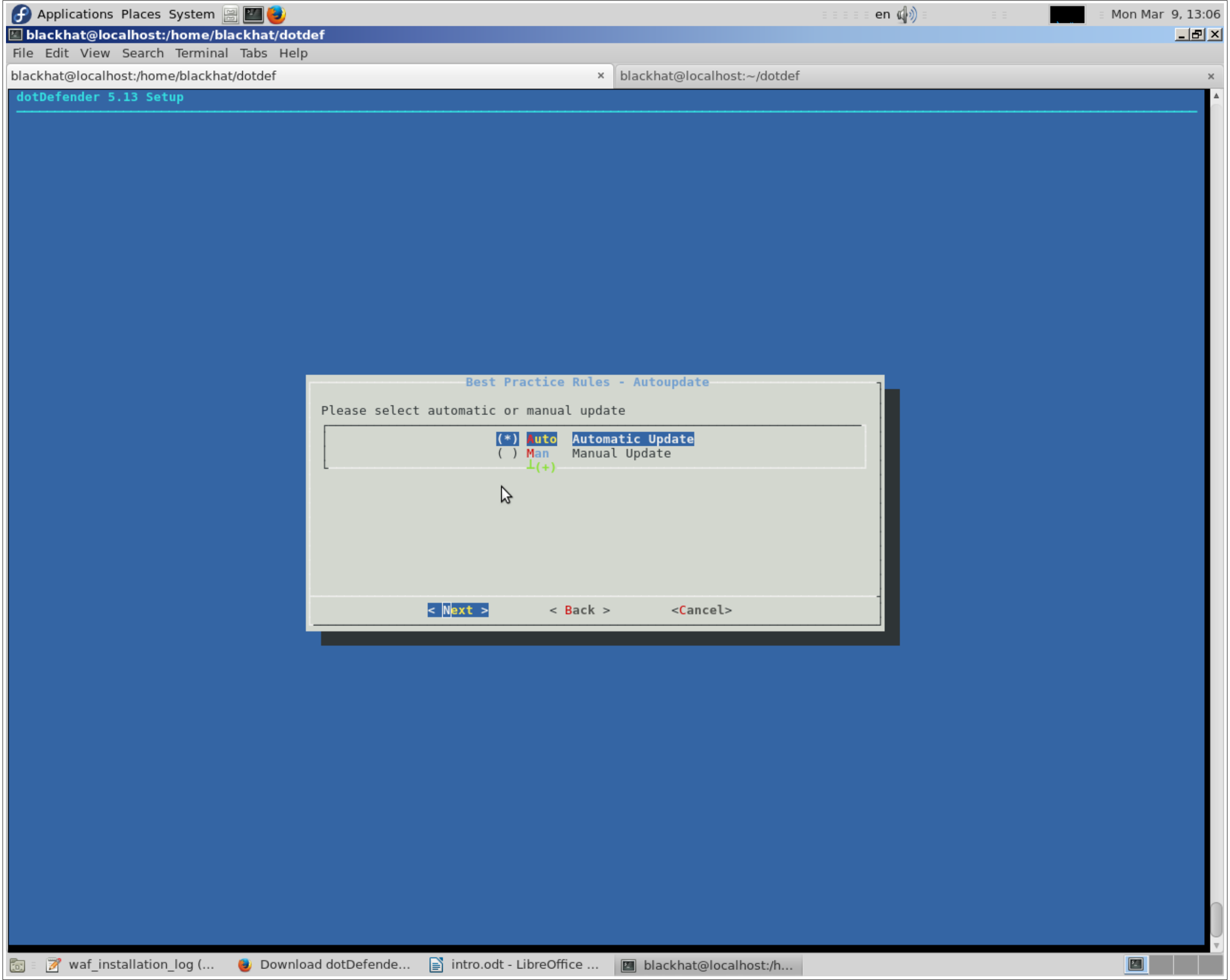
Applications Places System
en
Mon Mar 9, 13:05
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

dotDefender GUI Directory
Type a name of a directory (URI only) to be used to access dotDefender
DotDefender

< Next >        < Back >        <Cancel>
```



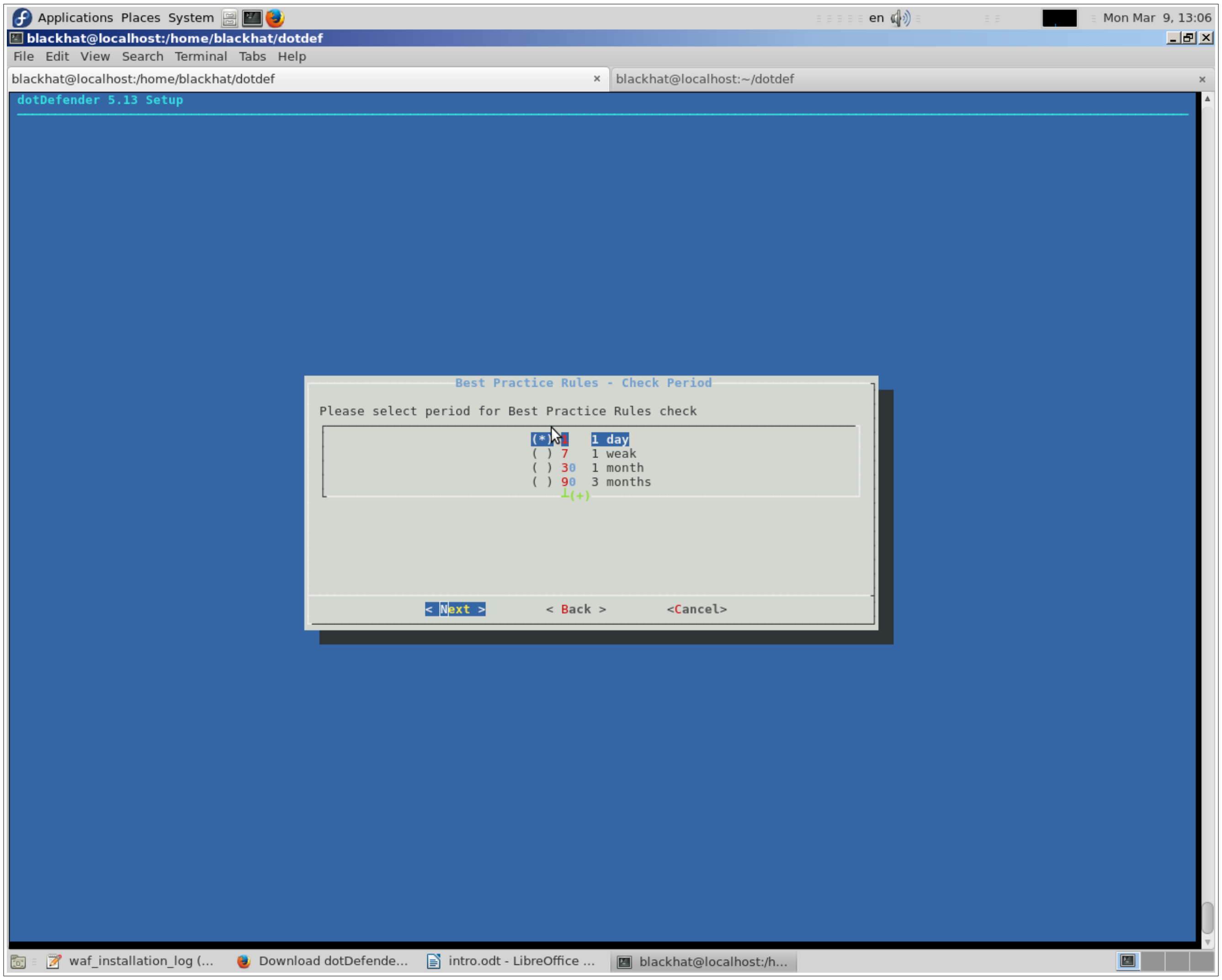
Applications Places System
en
Mon Mar 9, 13:05
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

                              Admin GUI
The admin GUI will be accessible at the following URL:
http://<hostname>/dotDefender
User name is 'admin'.

Please define the password for accessing the admin GUI
(using the arrow keys to alternate between fields below).

  Enter   password: ******
  Confirm password: ******

          < Next >        < Back >        <Cancel>
```

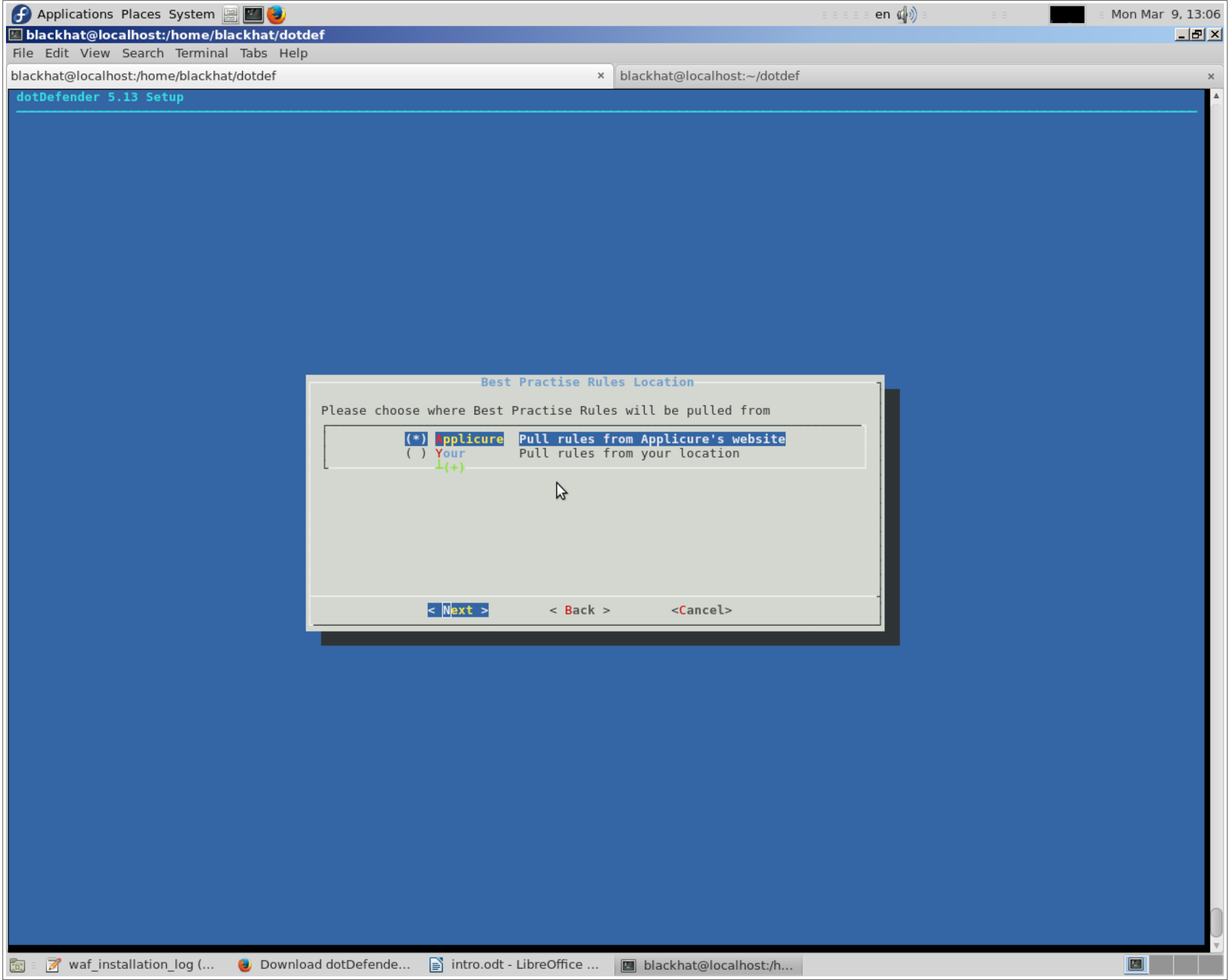


Applications Places System
en
Mon Mar 9, 13:06
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

                    Best Practice Rules - Autoupdate
Please select automatic or manual update

                (*) Auto   Automatic Update
                ( ) Man    Manual Update
                      (+)

        < Next >        < Back >        <Cancel>
```

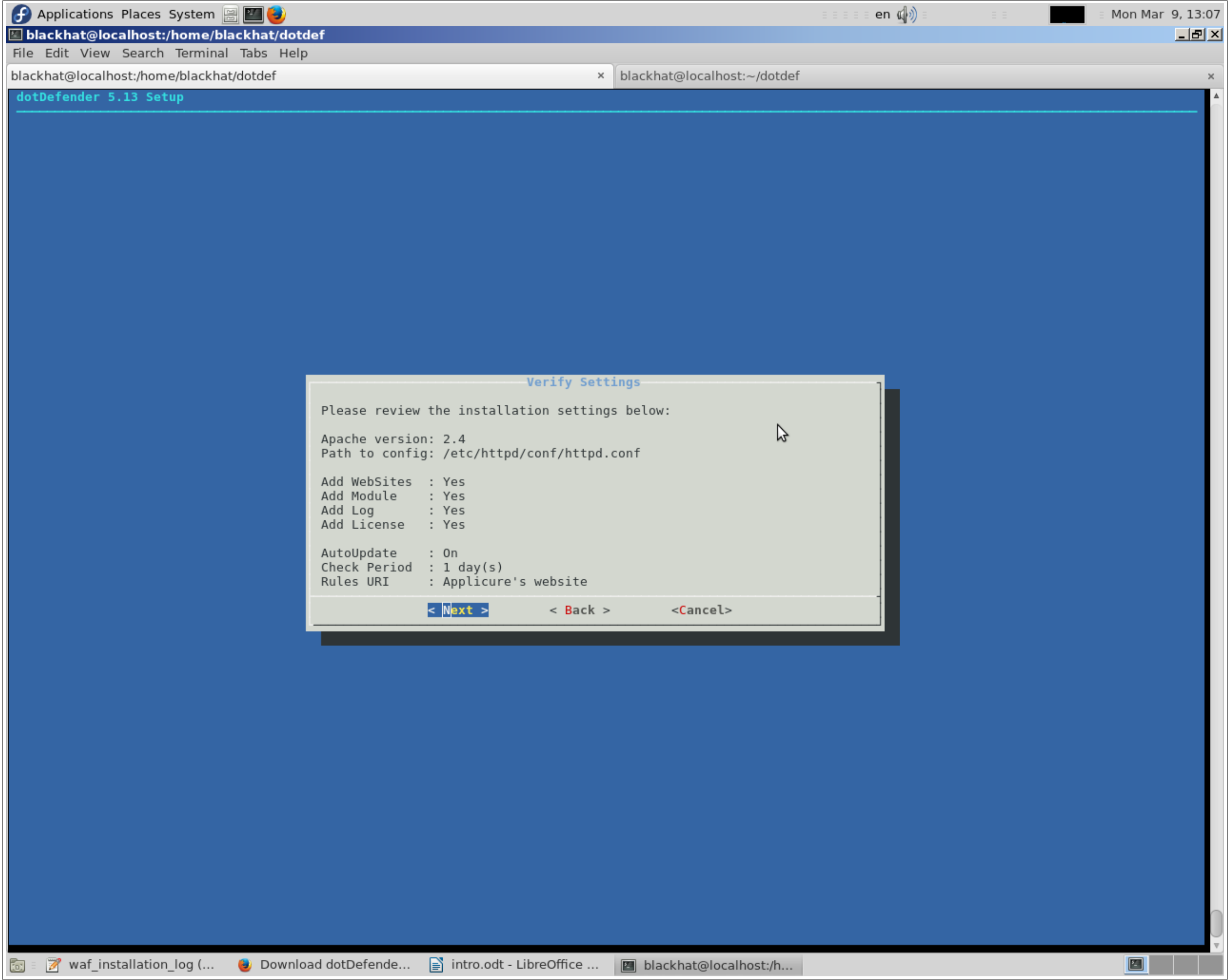

Applications Places System
en
Mon Mar 9, 13:06
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

                        Best Practice Rules - Check Period

   Please select period for Best Practice Rules check

                             (*) 1    1 day
                             ( ) 7    1 weak
                             ( ) 30   1 month
                             ( ) 90   3 months
                                  (+)

                < Next >       < Back >        <Cancel>
```



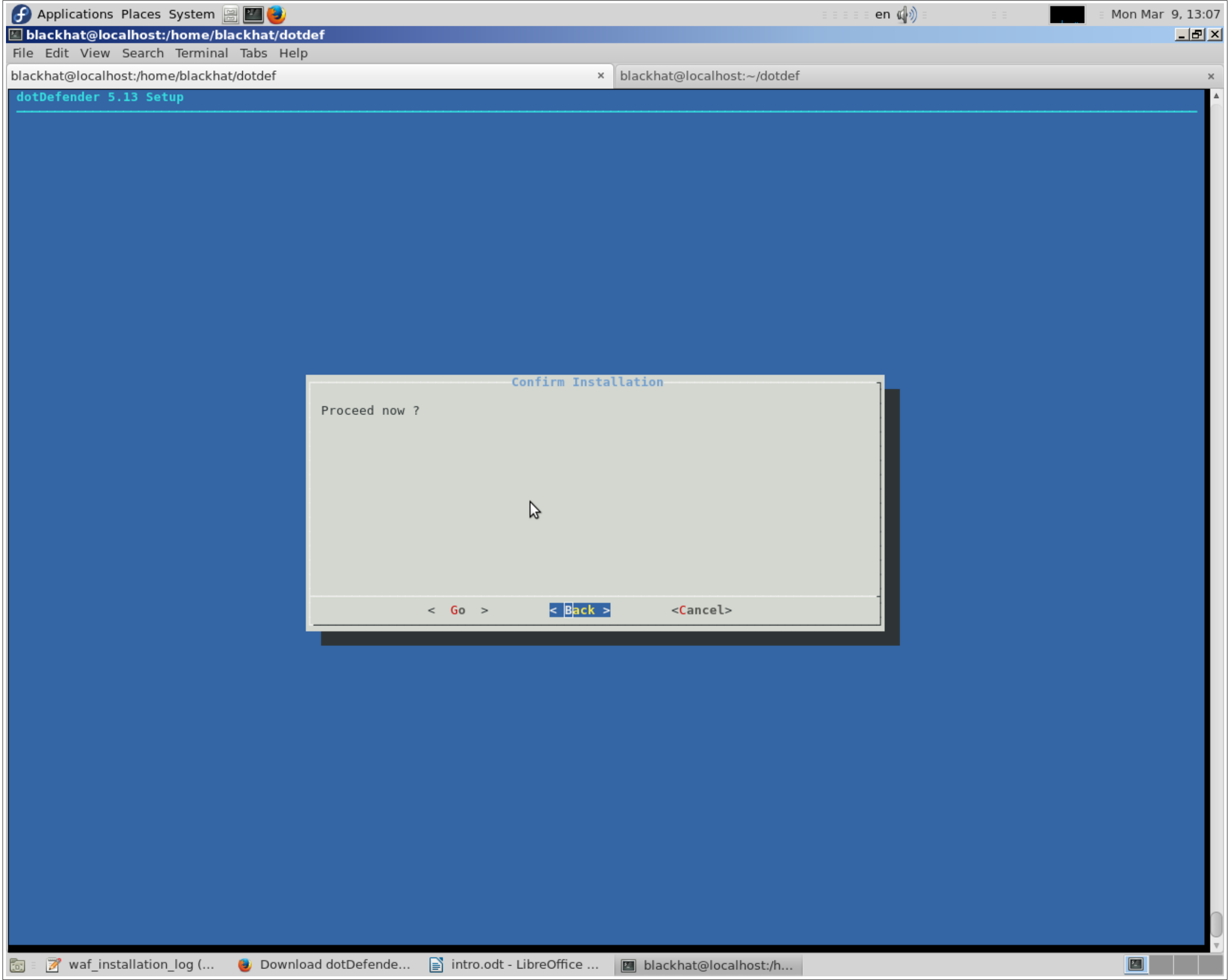
Applications Places System
en
Mon Mar 9, 13:06
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

                 Best Practise Rules Location

 Please choose where Best Practise Rules will be pulled from

           (*) Applicure   Pull rules from Applicure's website
           ( ) Your        Pull rules from your location
               ┴(+)

             < Next >        < Back >        <Cancel>
```



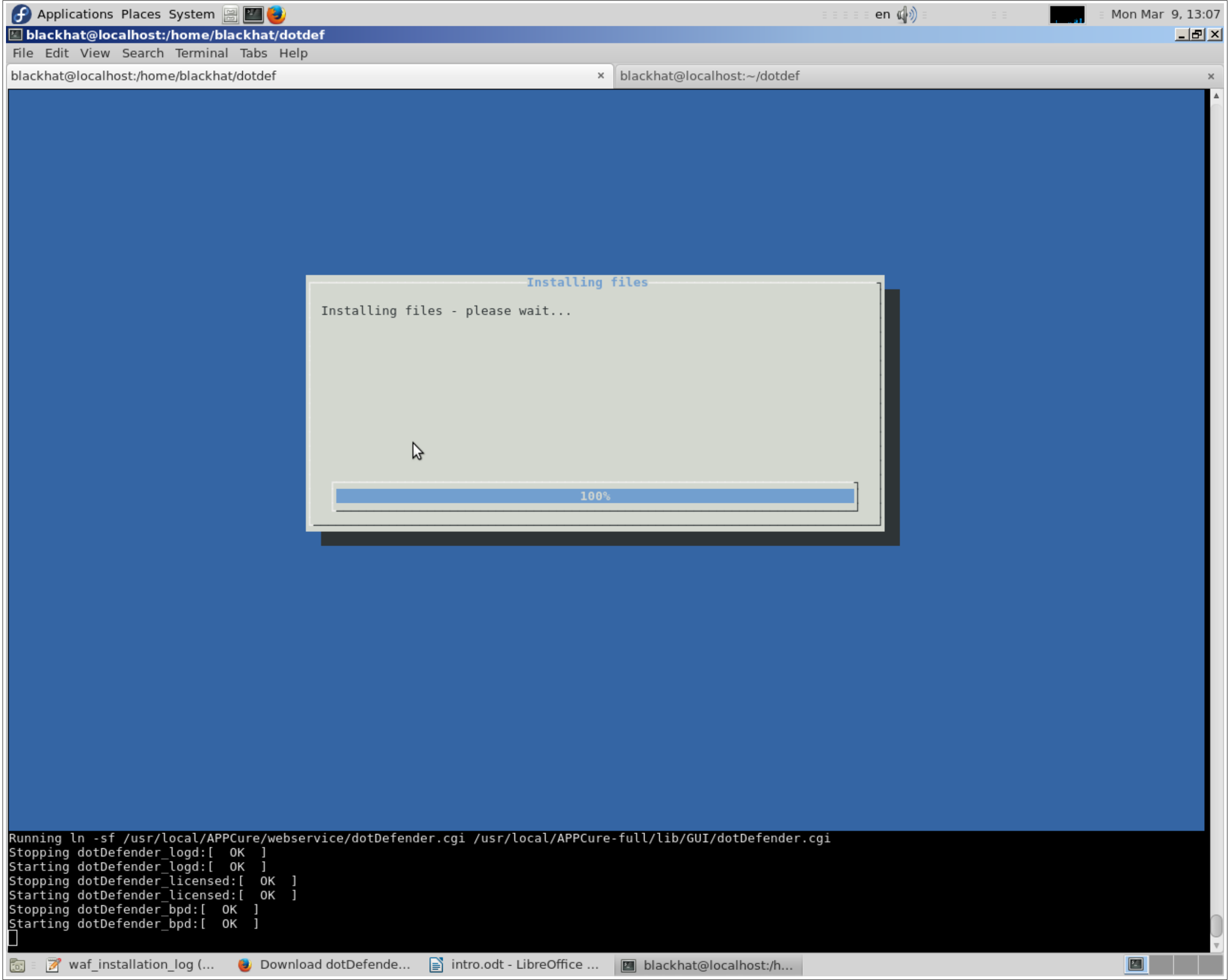
Applications Places System
en
Mon Mar 9, 13:07
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

                         Verify Settings
Please review the installation settings below:

Apache version: 2.4
Path to config: /etc/httpd/conf/httpd.conf

Add WebSites  : Yes
Add Module    : Yes
Add Log       : Yes
Add License   : Yes

AutoUpdate    : On
Check Period  : 1 day(s)
Rules URI     : Applicure's website

              < Next >       < Back >       <Cancel>
```



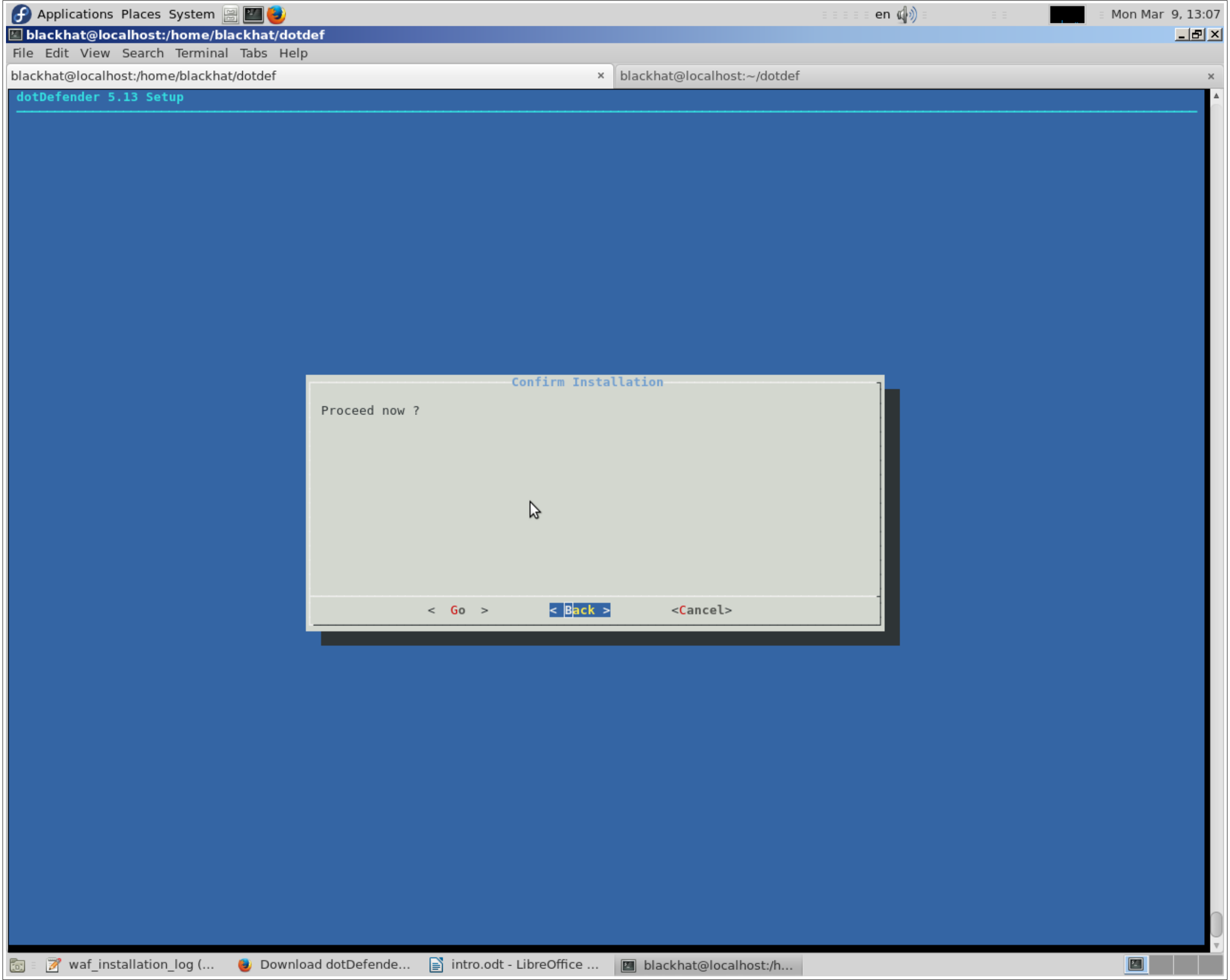
Applications Places System
en
Mon Mar 9, 13:07
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

Confirm Installation

Proceed now ?

<  Go  >    < Back >    <Cancel>
```


Applications Places System
en
Mon Mar 9, 13:07
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
Installing files

Installing files - please wait...

100%
```

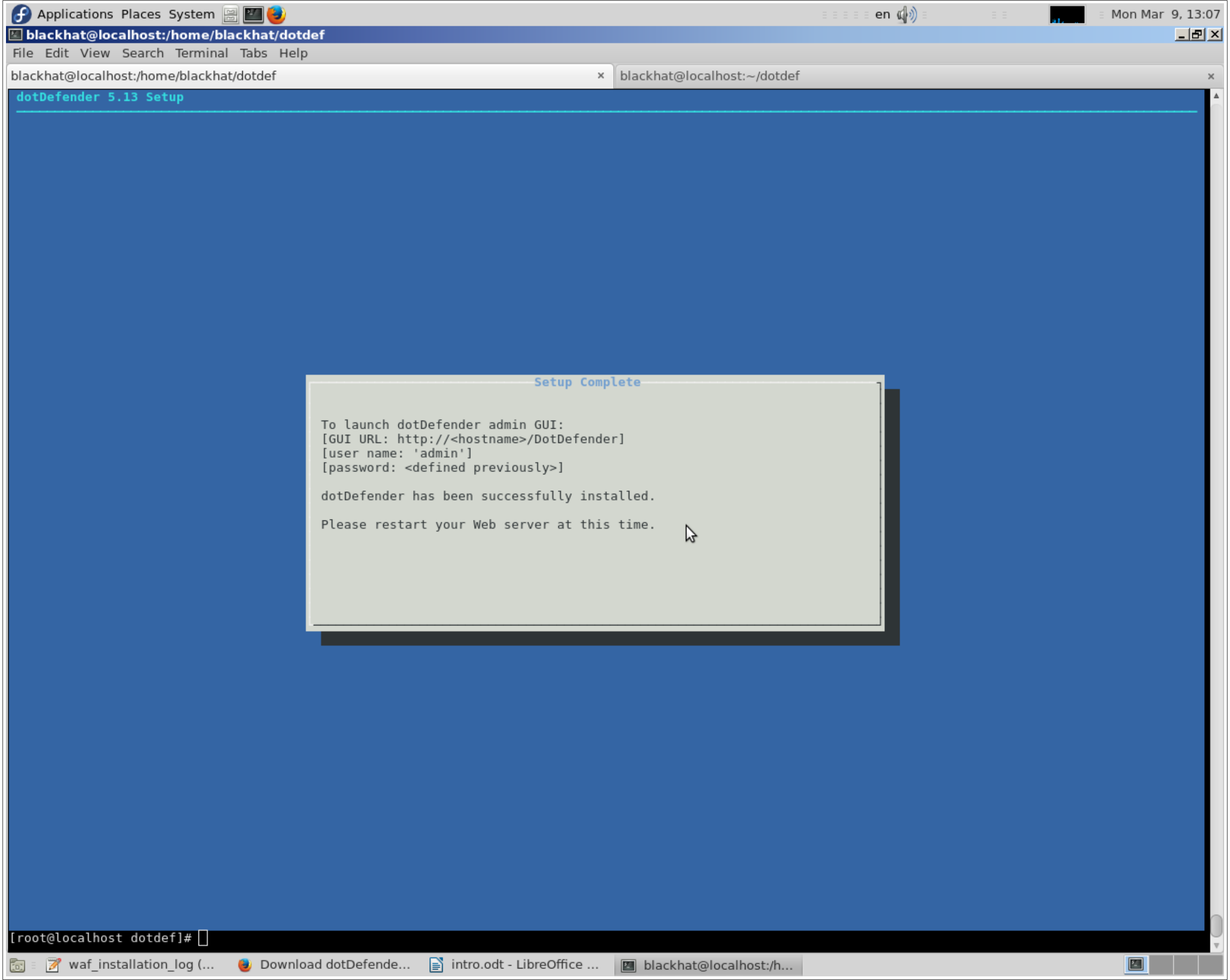
```
Running ln -sf /usr/local/APPCure/webservice/dotDefender.cgi /usr/local/APPCure-full/lib/GUI/dotDefender.cgi
Stopping dotDefender_logd:[  OK  ]
Starting dotDefender_logd:[  OK  ]
Stopping dotDefender_licensed:[  OK  ]
Starting dotDefender_licensed:[  OK  ]
Stopping dotDefender_bpd:[  OK  ]
Starting dotDefender_bpd:[  OK  ]
```



Applications Places System
en
Mon Mar 9, 13:07
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef

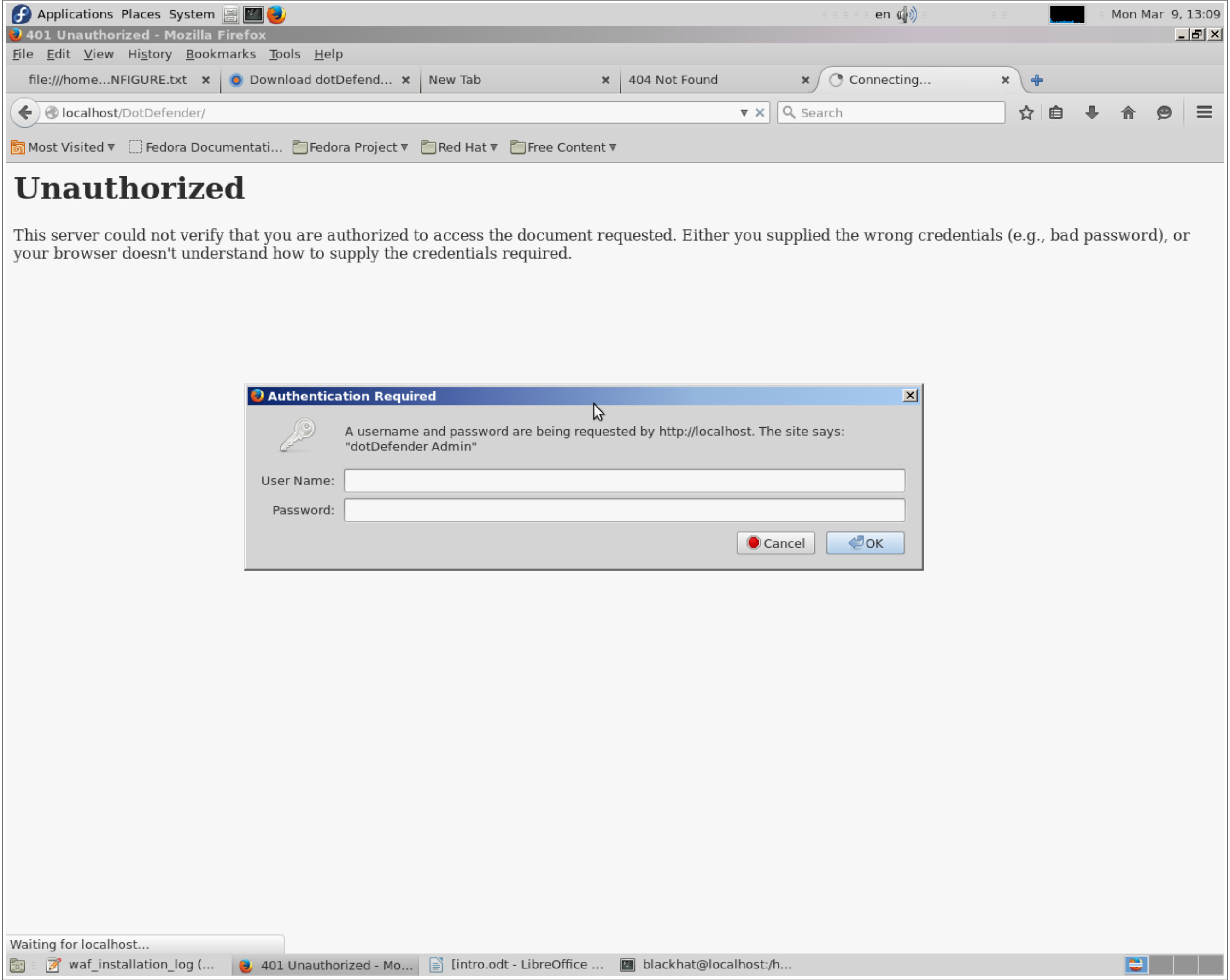
```
dotDefender 5.13 Setup

Confirm Installation

Proceed now ?

<  Go  >    < Back >    <Cancel>
```

waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...



Applications Places System
en
Mon Mar 9, 13:07
blackhat@localhost:/home/blackhat/dotdef
File Edit View Search Terminal Tabs Help
blackhat@localhost:/home/blackhat/dotdef
blackhat@localhost:~/dotdef
waf_installation_log (...
Download dotDefende...
intro.odt - LibreOffice ...
blackhat@localhost:/h...

```
dotDefender 5.13 Setup

                              Setup Complete

To launch dotDefender admin GUI:
[GUI URL: http://<hostname>/DotDefender]
[user name: 'admin']
[password: <defined previously>]

dotDefender has been successfully installed.

Please restart your Web server at this time.

[root@localhost dotdef]#
```



Unauthorized

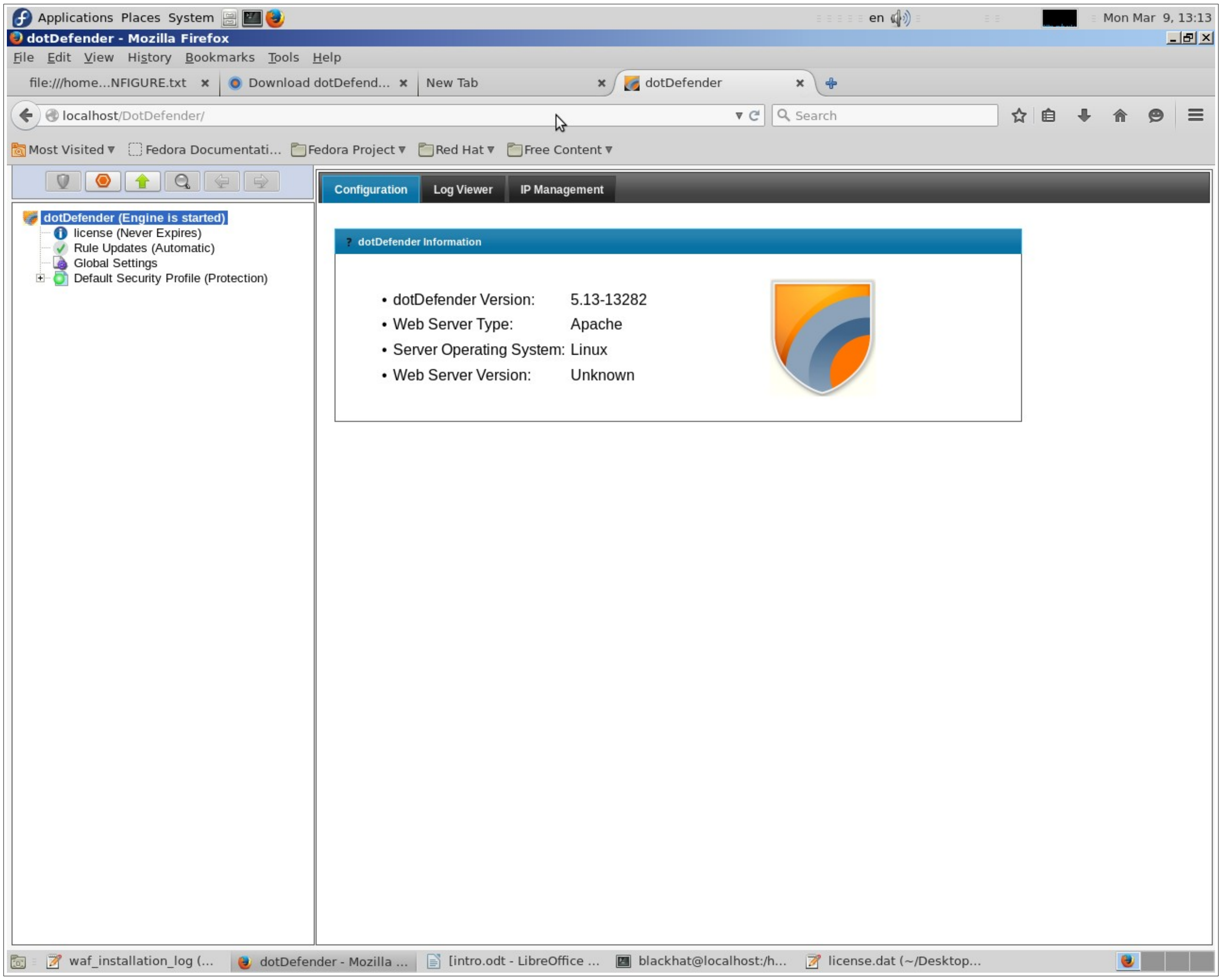
This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

Authentication Required

A username and password are being requested by http://localhost. The site says: "dotDefender Admin"

User Name:

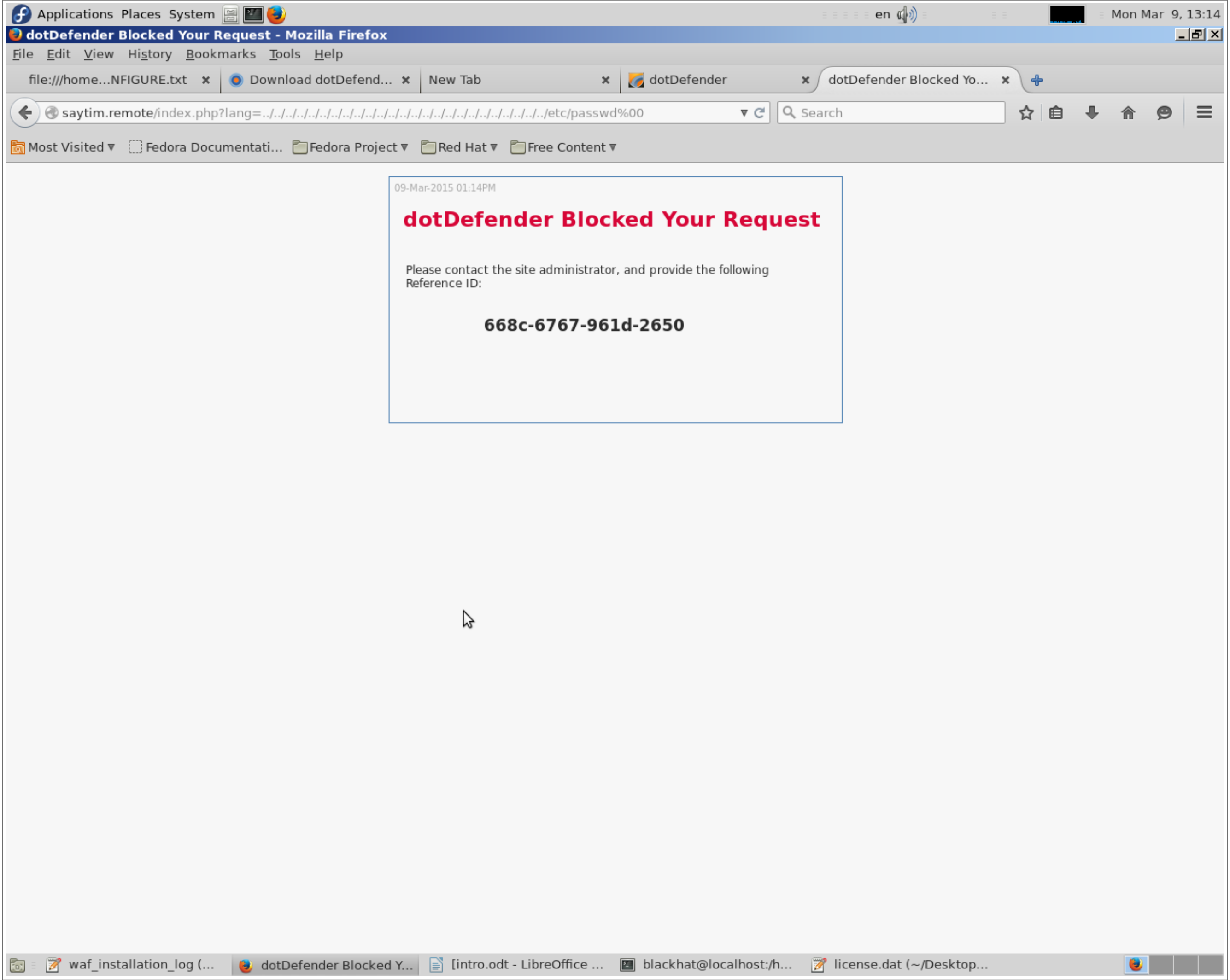
Password:


Applications Places System
en
Mon Mar 9, 13:13
dotDefender - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home...NFIGURE.txt
Download dotDefend...
New Tab
dotDefender
localhost/DotDefender/
Search
Most Visited
Fedora Documentati...
Fedora Project
Red Hat
Free Content
Configuration
Log Viewer
IP Management
waf_installation_log (...
dotDefender - Mozilla ...
[intro.odt - LibreOffice ...
blackhat@localhost:/h...
license.dat (~/Desktop...

dotDefender (Engine is started)
license (Never Expires)
Rule Updates (Automatic)
Global Settings
Default Security Profile (Protection)

dotDefender Information

dotDefender Version:	5.13-13282
Web Server Type:	Apache
Server Operating System:	Linux
Web Server Version:	Unknown



Applications Places System
en
Mon Mar 9, 13:14
dotDefender Blocked Your Request - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home...NFIGURE.txt
Download dotDefend...
New Tab
dotDefender
dotDefender Blocked Yo...
Search
Most Visited
Fedora Documentati...
Fedora Project
Red Hat
Free Content
waf_installation_log (...
dotDefender Blocked Y...
[intro.odt - LibreOffice ...
blackhat@localhost:/h...
license.dat (~/Desktop...

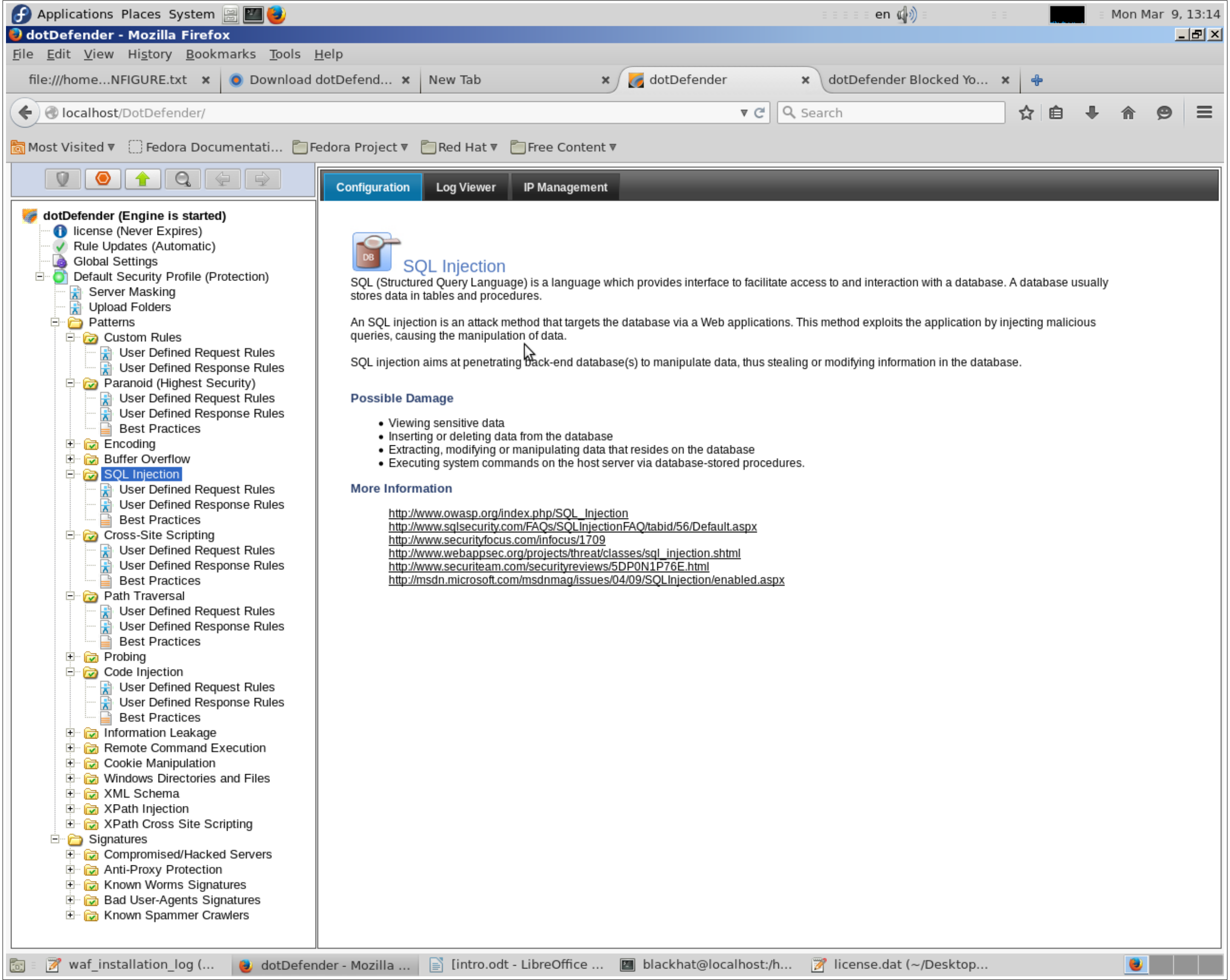
```
saytim.remote/index.php?lang=../../../../../../../../../../../../../../../../../../../../../etc/passwd%00
```

09-Mar-2015 01:14PM

dotDefender Blocked Your Request

Please contact the site administrator, and provide the following Reference ID:

668c-6767-961d-2650



Applications Places System
en
[redacted]
Mon Mar 9, 13:14
dotDefender - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home...NFIGURE.txt
Download dotDefend...
New Tab
dotDefender
dotDefender Blocked Yo...
localhost/DotDefender/
Search
Most Visited
Fedora Documentati...
Fedora Project
Red Hat
Free Content
Configuration
Log Viewer
IP Management
dotDefender (Engine is started)
license (Never Expires)
Rule Updates (Automatic)
Global Settings
Default Security Profile (Protection)
Server Masking
Upload Folders
Patterns
Custom Rules
User Defined Request Rules
User Defined Response Rules
Paranoid (Highest Security)
User Defined Request Rules
User Defined Response Rules
Best Practices
Encoding
Buffer Overflow
SQL Injection
User Defined Request Rules
User Defined Response Rules
Best Practices
Cross-Site Scripting
User Defined Request Rules
User Defined Response Rules
Best Practices
Path Traversal
User Defined Request Rules
User Defined Response Rules
Best Practices
Probing
Code Injection
User Defined Request Rules
User Defined Response Rules
Best Practices
Information Leakage
Remote Command Execution
Cookie Manipulation
Windows Directories and Files
XML Schema
XPath Injection
XPath Cross Site Scripting
Signatures
Compromised/Hacked Servers
Anti-Proxy Protection
Known Worms Signatures
Bad User-Agents Signatures
Known Spammer Crawlers
DB
waf_installation_log (...
dotDefender - Mozilla ...
[intro.odt - LibreOffice ...
blackhat@localhost:/h...
license.dat (~/Desktop...

SQL Injection

SQL (Structured Query Language) is a language which provides interface to facilitate access to and interaction with a database. A database usually stores data in tables and procedures.

An SQL injection is an attack method that targets the database via a Web applications. This method exploits the application by injecting malicious queries, causing the manipulation of data.

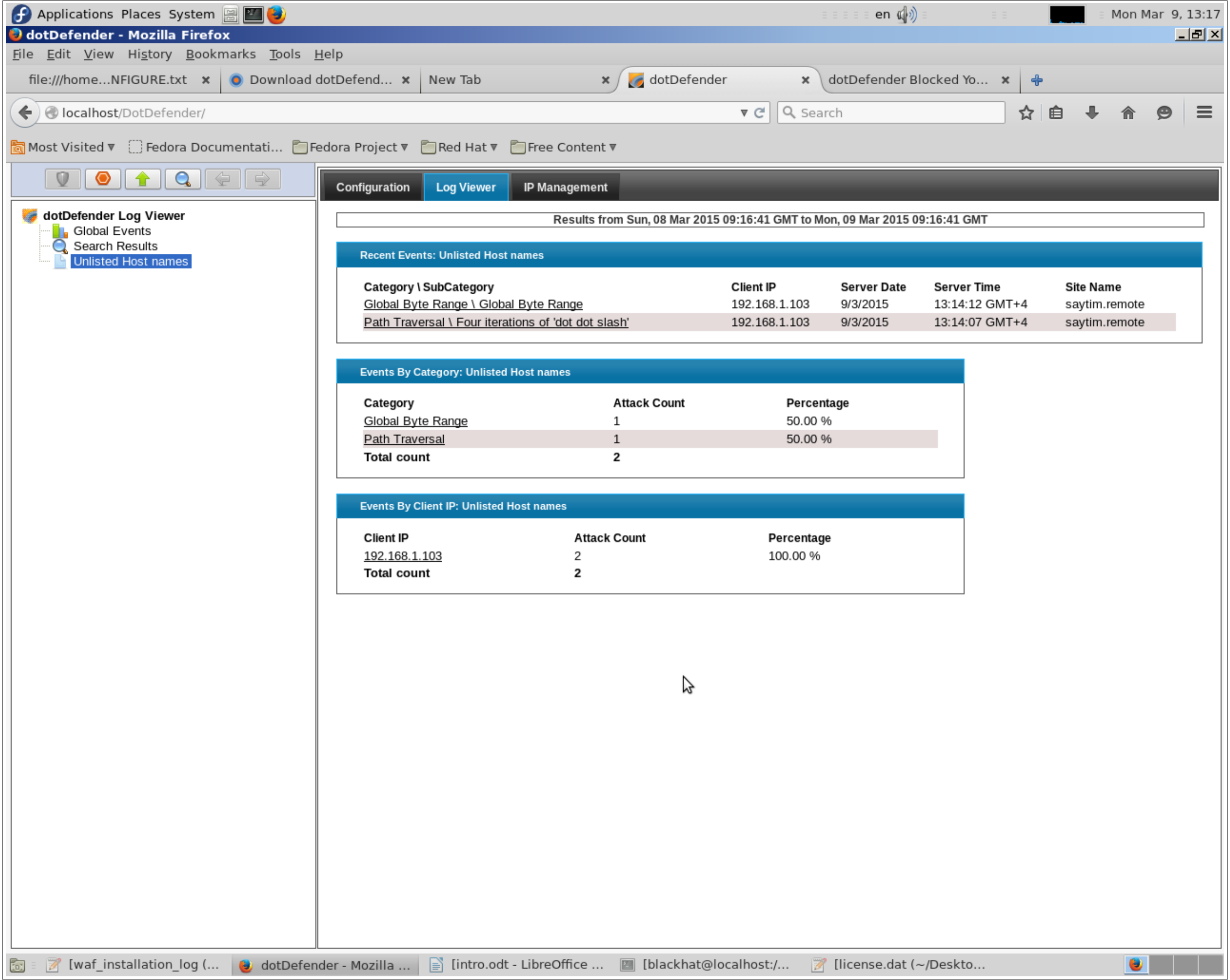
SQL injection aims at penetrating back-end database(s) to manipulate data, thus stealing or modifying information in the database.

Possible Damage

- Viewing sensitive data
- Inserting or deleting data from the database
- Extracting, modifying or manipulating data that resides on the database
- Executing system commands on the host server via database-stored procedures.

More Information

http://www.owasp.org/index.php/SQL_Injection
http://www.sqlsecurity.com/FAQs/SQLInjectionFAQ/tabid/56/Default.aspx
http://www.securityfocus.com/infocus/1709
http://www.webappsec.org/projects/threat/classes/sql_injection.shtml
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://msdn.microsoft.com/msdnmag/issues/04/09/SQLInjection/enabled.aspx



Results from Sun, 08 Mar 2015 09:16:41 GMT to Mon, 09 Mar 2015 09:16:41 GMT

Recent Events: Unlisted Host names

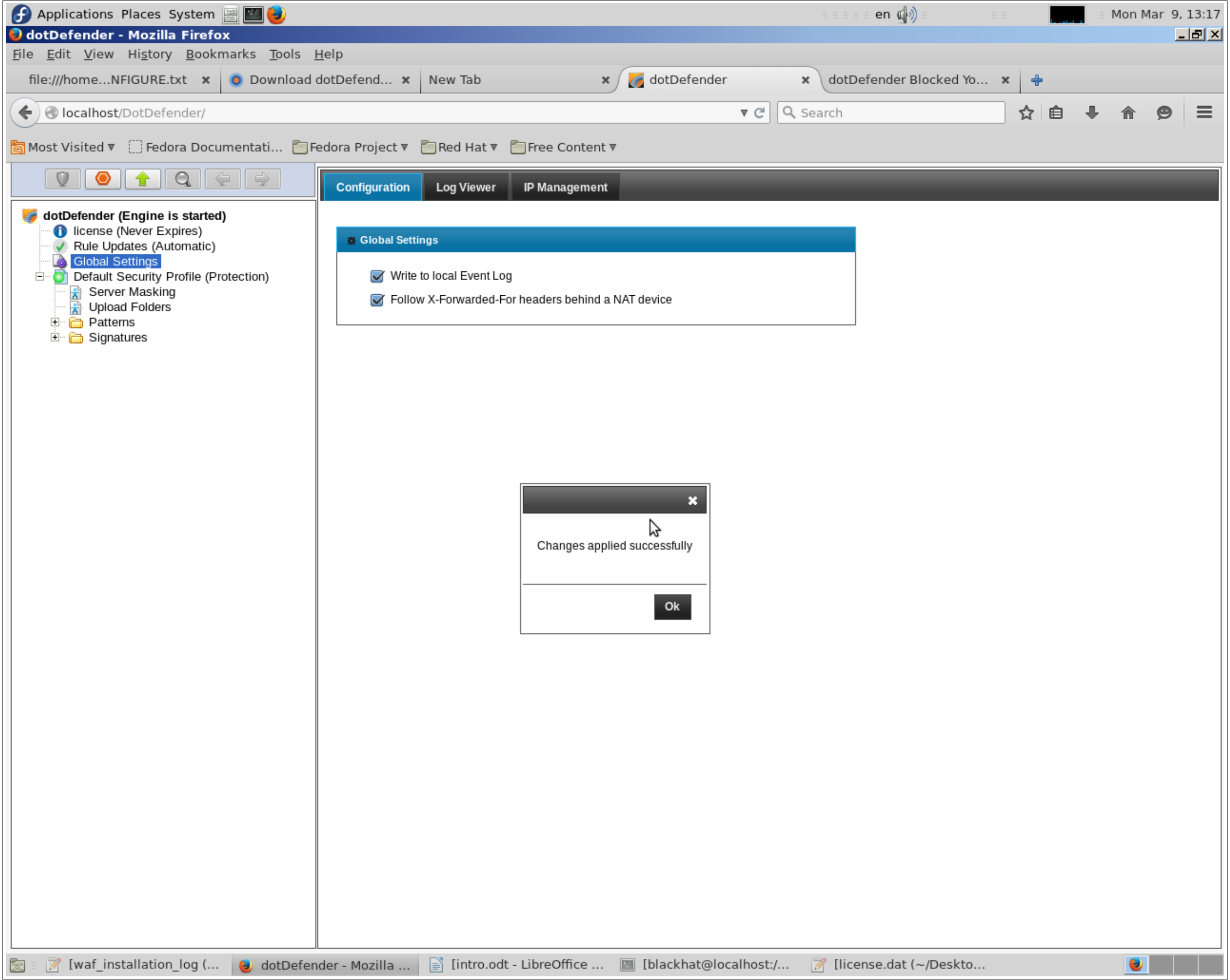
Category \ SubCategory	Client IP	Server Date	Server Time	Site Name
Global Byte Range \ Global Byte Range	192.168.1.103	9/3/2015	13:14:12 GMT+4	saytim.remote
Path Traversal \ Four iterations of 'dot dot slash'	192.168.1.103	9/3/2015	13:14:07 GMT+4	saytim.remote

Events By Category: Unlisted Host names

Category	Attack Count	Percentage
Global Byte Range	1	50.00 %
Path Traversal	1	50.00 %
Total count	**2**	

Events By Client IP: Unlisted Host names

Client IP	Attack Count	Percentage
192.168.1.103	2	100.00 %
Total count	**2**	



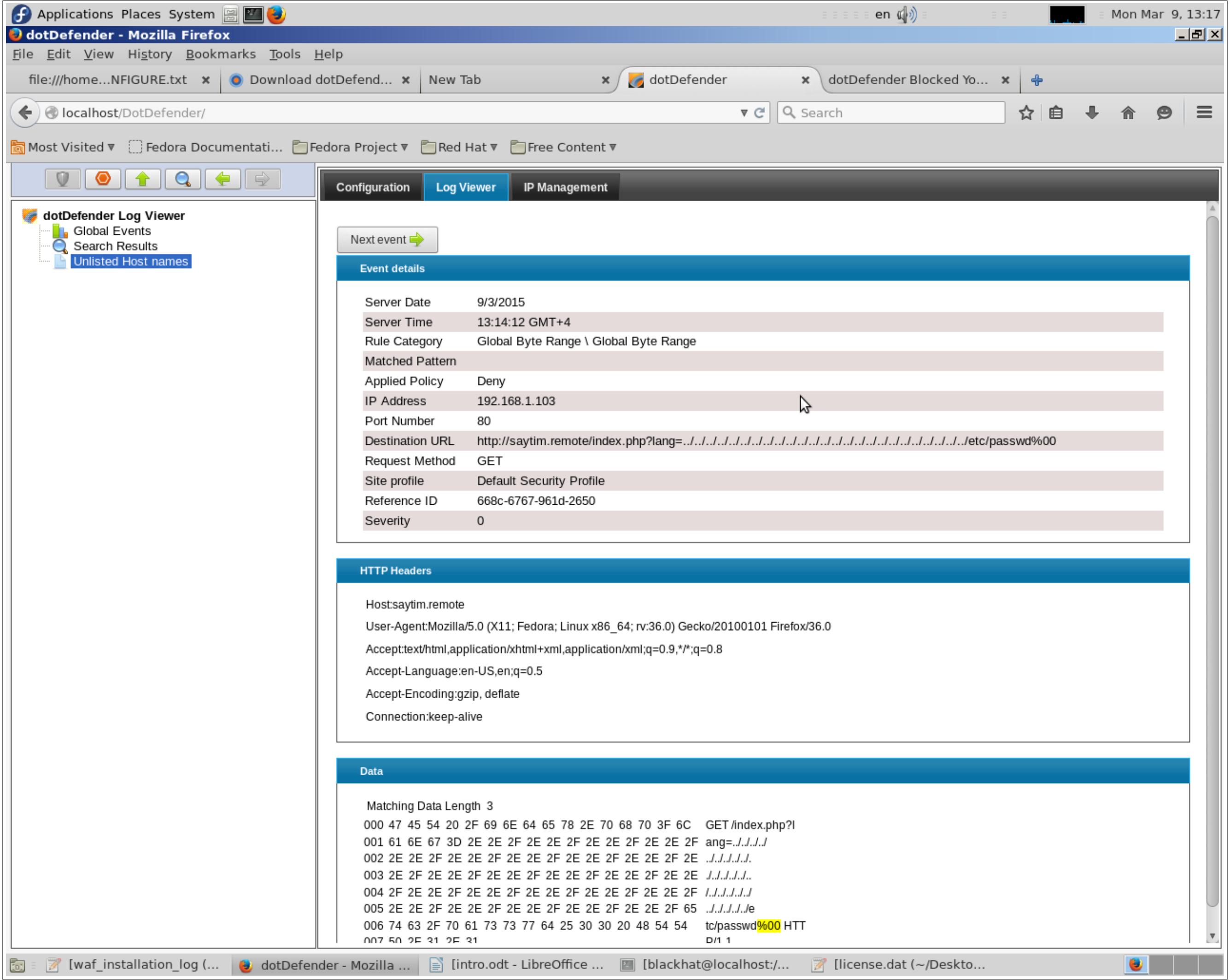
Applications Places System
en
Mon Mar 9, 13:17
dotDefender - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home...NFIGURE.txt
Download dotDefend...
New Tab
dotDefender
dotDefender Blocked Yo...
localhost/DotDefender/
Search
Most Visited
Fedora Documentati...
Fedora Project
Red Hat
Free Content
dotDefender (Engine is started)
license (Never Expires)
Rule Updates (Automatic)
Global Settings
Default Security Profile (Protection)
Server Masking
Upload Folders
Patterns
Signatures
Configuration
Log Viewer
IP Management
Ok
[waf_installation_log (...
dotDefender - Mozilla ...
[intro.odt - LibreOffice ...
[blackhat@localhost:/...
[license.dat (~/Deskto...

Global Settings

☑ Write to local Event Log

☑ Follow X-Forwarded-For headers behind a NAT device

Changes applied successfully



Event details

Server Date	9/3/2015
Server Time	13:14:12 GMT+4
Rule Category	Global Byte Range \ Global Byte Range
Matched Pattern	
Applied Policy	Deny
IP Address	192.168.1.103
Port Number	80
Destination URL	http://saytim.remote/index.php?lang=../etc/passwd%00
Request Method	GET
Site profile	Default Security Profile
Reference ID	668c-6767-961d-2650
Severity	0

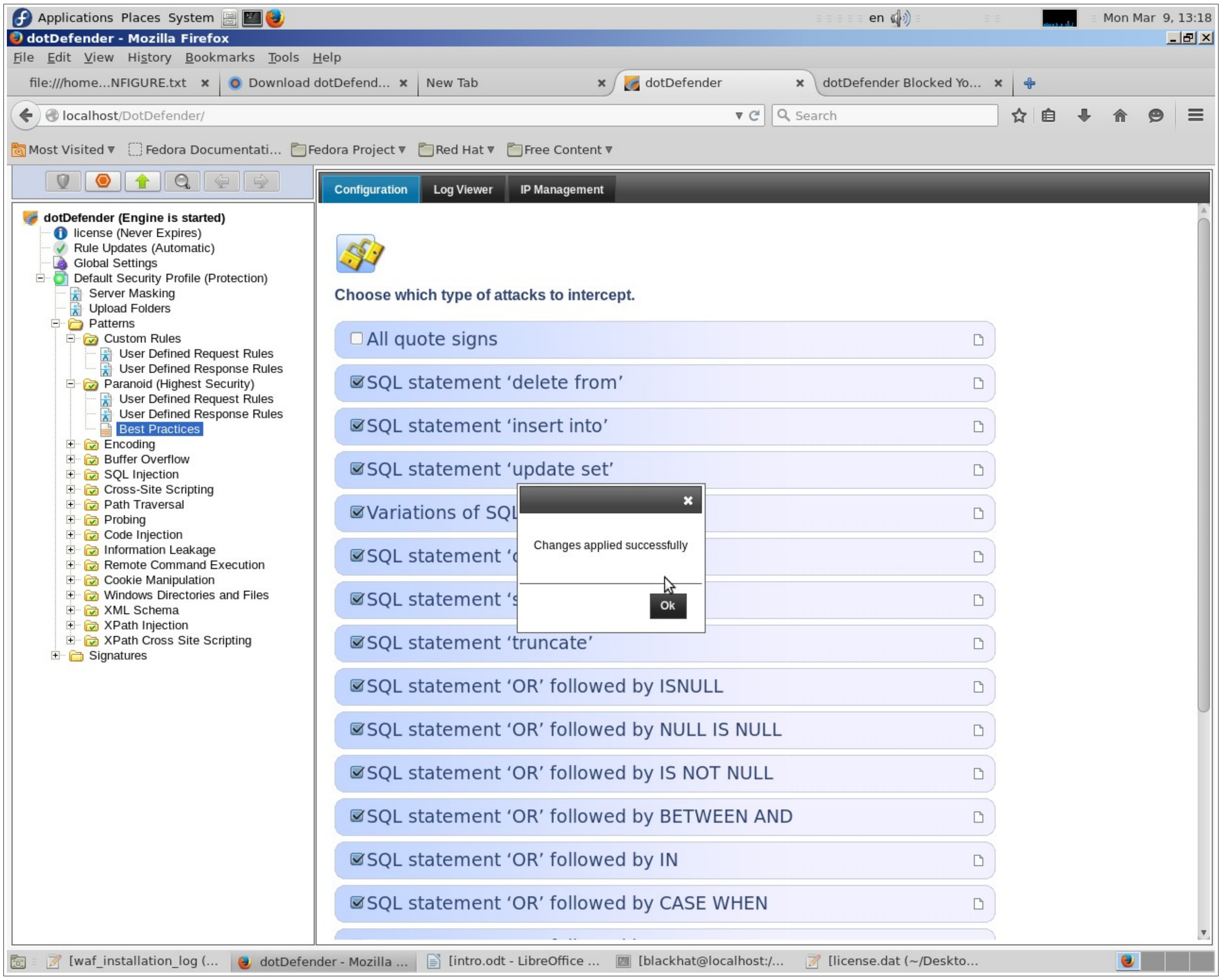
HTTP Headers

```
Host:saytim.remote
User-Agent:Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:en-US,en;q=0.5
Accept-Encoding:gzip, deflate
Connection:keep-alive
```

Data

```
Matching Data Length  3
000 47 45 54 20 2F 69 6E 64 65 78 2E 70 68 70 3F 6C  GET /index.php?l
001 61 6E 67 3D 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F  ang=../../../../
002 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E  ../../../../../.
003 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E  ./../../../../..
004 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F  /../../../../../
005 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 65  ../../../../../e
006 74 63 2F 70 61 73 73 77 64 25 30 30 20 48 54 54  tc/passwd%00 HTT
007 50 2F 31 2F 31                                   P/1 1
```

DotDefender-in WEB interfeysində Best practice rulelara da fikir verməyi məsləhət görürəm. (aşağıdakı şəkildə)

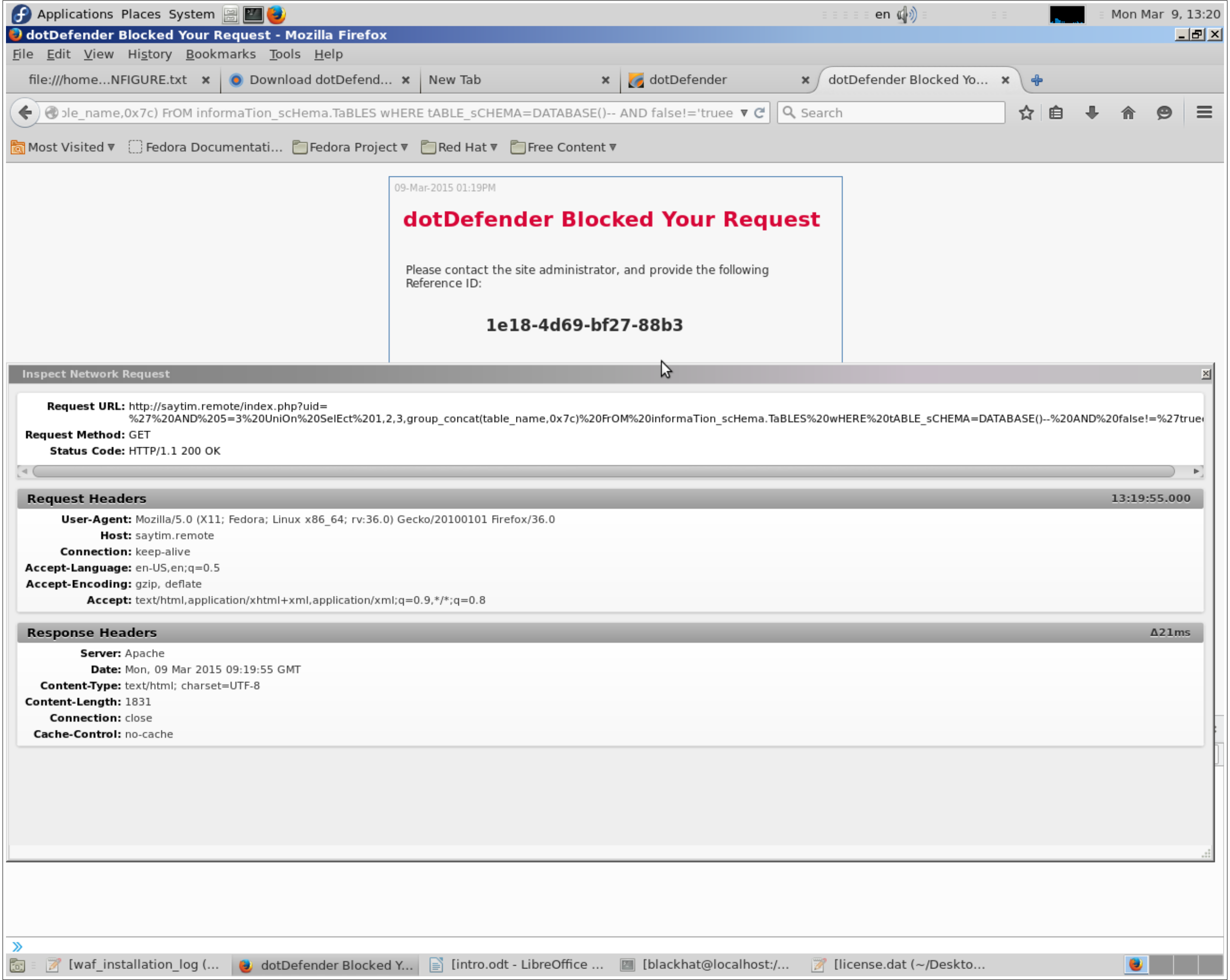


Choose which type of attacks to intercept.

- ☐ All quote signs
- ☑ SQL statement ‘delete from’
- ☑ SQL statement ‘insert into’
- ☑ SQL statement ‘update set’
- ☑ Variations of SQL
- ☑ SQL statement ‘
- ☑ SQL statement ‘s
- ☑ SQL statement ‘truncate’
- ☑ SQL statement ‘OR’ followed by ISNULL
- ☑ SQL statement ‘OR’ followed by NULL IS NULL
- ☑ SQL statement ‘OR’ followed by IS NOT NULL
- ☑ SQL statement ‘OR’ followed by BETWEEN AND
- ☑ SQL statement ‘OR’ followed by IN
- ☑ SQL statement ‘OR’ followed by CASE WHEN

Changes applied successfully

Frontend-ə hücum (simulyasiya) edərək WAF-ın işləkliyini yoxlamaq vaxtıdır:


Applications Places System
en
Mon Mar 9, 13:20
dotDefender Blocked Your Request - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home...NFIGURE.txt
Download dotDefend...
New Tab
dotDefender
dotDefender Blocked Yo...
ɔle_name,0x7c) FrOM informaTion_scHema.TaBLES wHERE tABLE_sCHEMA=DATABASE()-- AND false!='truee
Search
Most Visited
Fedora Documentati...
Fedora Project
Red Hat
Free Content
[waf_installation_log (...
dotDefender Blocked Y...
[intro.odt - LibreOffice ...
[blackhat@localhost:/...
[license.dat (~/Deskto...

09-Mar-2015 01:19PM

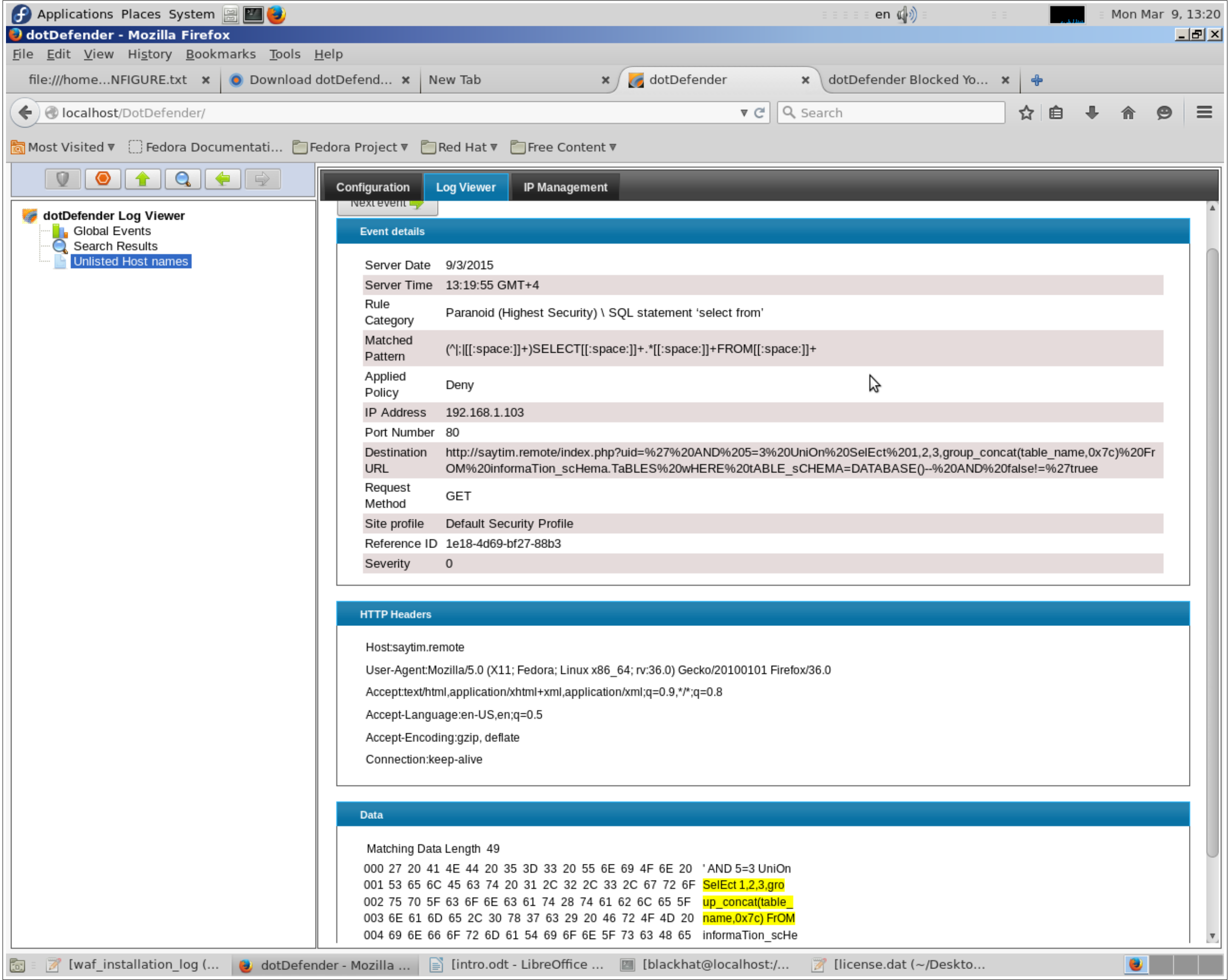
dotDefender Blocked Your Request

Please contact the site administrator, and provide the following Reference ID:

1e18-4d69-bf27-88b3

```
Inspect Network Request

     Request URL: http://saytim.remote/index.php?uid=
                  %27%20AND%205=3%20UniOn%20SelEct%201,2,3,group_concat(table_name,0x7c)%20FrOM%20informaTion_scHema.TaBLES%20wHERE%20tABLE_sCHEMA=DATABASE()--%20AND%20false!=%27true
  Request Method: GET
     Status Code: HTTP/1.1 200 OK

Request Headers                                                                 13:19:55.000
      User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0
            Host: saytim.remote
      Connection: keep-alive
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate
          Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Response Headers                                                                Δ21ms
          Server: Apache
            Date: Mon, 09 Mar 2015 09:19:55 GMT
    Content-Type: text/html; charset=UTF-8
  Content-Length: 1831
      Connection: close
   Cache-Control: no-cache
```

gördüyümüz kimi normaldır hər şey.Və edilən hücum cəhdi müvəffəqiyyətlə Log-a qeyd edilib.



Event details

Server Date	9/3/2015
Server Time	13:19:55 GMT+4
Rule Category	Paranoid (Highest Security) \ SQL statement 'select from'
Matched Pattern	(^|;|[[:space:]]+)SELECT[[:space:]]+.*[[:space:]]+FROM[[:space:]]+
Applied Policy	Deny
IP Address	192.168.1.103
Port Number	80
Destination URL	http://saytim.remote/index.php?uid=%27%20AND%205=3%20UniOn%20SelEct%201,2,3,group_concat(table_name,0x7c)%20FrOM%20informaTion_scHema.TaBLES%20wHERE%20tABLE_sCHEMA=DATABASE()--%20AND%20false!=%27truee
Request Method	GET
Site profile	Default Security Profile
Reference ID	1e18-4d69-bf27-88b3
Severity	0

HTTP Headers

```
Host:saytim.remote
User-Agent:Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:en-US,en;q=0.5
Accept-Encoding:gzip, deflate
Connection:keep-alive
```

Data

```
Matching Data Length  49
000 27 20 41 4E 44 20 35 3D 33 20 55 6E 69 4F 6E 20  ' AND 5=3 UniOn
001 53 65 6C 45 63 74 20 31 2C 32 2C 33 2C 67 72 6F  SelEct 1,2,3,gro
002 75 70 5F 63 6F 6E 63 61 74 28 74 61 62 6C 65 5F  up_concat(table_
003 6E 61 6D 65 2C 30 78 37 63 29 20 46 72 4F 4D 20  name,0x7c) FrOM
004 69 6E 66 6F 72 6D 61 54 69 6F 6E 5F 73 63 48 65  informaTion_scHe
```

Məqaləyə əlavələr:

http://httpd.apache.org/docs/current/mod/mod_proxy.html	Apache 2.4 mod_proxy
https://fedoraproject.org/wiki/Overview	Fedora
http://www.iis.net/learn/get-started/getting-started-with-iis	IIS 8.5
http://blogs.msdn.com/b/benjaminperkins/archive/2013/06/25/what-s-new-in-iis-8-5.aspx	IIS 8.5
http://www.microsoft.com/en-us/server-cloud/products/windows-server-2012-r2/ http://applicure.com	Windows Server 2012 R2 Applicure DotDefender WAF

Beləliklə çox da çətin olmayan əməliyyatlar vasitəsilə Windows Server üzərində qurulan web serveri Frontendə qorumağa nail olduq.
Ümüdvaram çox adamın işinə yarayacaq.

QEYD: Məqaləni yazdığım dövrdə Dotdefender WAF <=5.13 XSS təhlükəsizlik boşluğu tapmışam.
İşdir bu məqaləni oxuyarkən DotDefender-in rəsmi saytında daha yeni və fixlənmiş versiyanı endirin.
Tapdığım boşluq barədə bu günlərdə elə məlumat verəcəyəm PUBLIC-ə.

YARATDIM Kİ, İZİM QALA:)
/AkaStep   15 Mart 2015