Contents

[Bước 1: Cài đặt thư viện 1](#_Toc77911746)

[Bước 2: Thêm config ở trong nginx.conf 2](#_Toc77911747)

[Bước 3 : Thêm vào Block location/ 2](#_Toc77911748)

[Bước 5: Test: 3](#_Toc77911749)

[6. Custom NAXSI log 4](#_Toc77911750)

<https://www.nixdevsoft.com/community/t/how-to-install-naxsi-as-a-dynamic-module-in-nginx-centos-ubuntu-rhel/211>

<https://github.com/nbs-system/naxsi/wiki/naxsi-compile>

# Bước 1: Cài đặt thư viện

yum install gcc gcc-c++ cmake ncurses ncurses-devel libxml2 libxml2-devel zlib zlib-devel gd gd-devel openssl openssl-devel curl curl-devel libtool pcre pcre-devel wget unzip

mkdir -p /setup ; cd /setup

wget <http://nginx.org/download/nginx-1.20.1.tar.gz>

wget <https://github.com/nbs-system/naxsi/archive/master.zip>

tar -xvzf nginx-1.20.0.tar.gz

unzip master.zip

cd nginx-1.20.0

./configure --sbin-path=/usr/bin/nginx --prefix=/opt/nginx --conf-path=/opt/nginx/nginx.conf --error-log-path=/opt/nginx/logs/error.log --http-log-path=/opt/nginx/logs/access.log --with-pcre --pid-path=/var/run/nginx.pid --with-http\_ssl\_module --with-http\_realip\_module --with-http\_stub\_status\_module --add-module=/opt/nginx/modules\_extend/ngx\_http\_geoip2\_module-master --add-dynamic-module=/setup/naxsi-master/naxsi\_src

make

make install

# Bước 2: Thêm config ở trong nginx.conf

user nginx;

pid /run/nginx.pid;

worker\_processes auto;

worker\_rlimit\_nofile 65535;

load\_module /opt/nginx/modules/ngx\_http\_naxsi\_module.so;

http {

...

include /setup/naxsi-master/naxsi\_config/naxsi\_core.rules;

...

}

...

# Bước 3 : Thêm vào Block location/

server {

...

location / { # naxsi is enabled, and in learning mode

SecRulesEnabled; #enable naxsi

LearningMode; #enable learning mode

LibInjectionSql; #enable libinjection support for SQLI

LibInjectionXss; #enable libinjection support for XSS

DeniedUrl "/RequestDenied"; #the location where naxsi will redirect the request when it is blocked

CheckRule "$SQL >= 8" BLOCK; #the action to take when the $SQL score is superior or equal to 8

CheckRule "$RFI >= 8" BLOCK;

CheckRule "$TRAVERSAL >= 5" BLOCK;

CheckRule "$UPLOAD >= 5" BLOCK;

CheckRule "$XSS >= 8" BLOCK;

proxy\_pass http://127.0.0.1;

....

}

location /admin { # naxsi is disabled

SecRulesDisabled; #optional, naxsi is disabled by default

allow 1.2.3.4;

deny all;

proxy\_pass http://127.0.0.1;

....

}

location /vuln\_page.php { # naxsi is enabled, and is \*not\* in learning mode

SecRulesEnabled;

proxy\_pass http://127.0.0.1;

}

**#phải có phần này vì NAXSI lái sang.**

location /RequestDenied {

internal;

return 403;

}

...

}

Log sẽ lưu ở error log.

# Bước 5: Test:

curl -v -H 'Host: my.vnpt.com.vn' "http://localhost/?q='1 OR 1=1"

\* About to connect() to localhost port 80 (#0)

\* Trying 127.0.0.1...

\* Connected to localhost (127.0.0.1) port 80 (#0)

> GET /?q='1 OR 1=1 HTTP/1.1

> User-Agent: curl/7.29.0

> Accept: \*/\*

> Host: my.vnpt.com.vn

>

< HTTP/1.1 403 Forbidden

< Server: nginx

< Date: Fri, 14 May 2021 15:38:50 GMT

< Content-Type: text/html; charset=utf-8

< Content-Length: 146

< Connection: keep-alive

<

<html>

<head><title>403 Forbidden</title></head>

<body>

<center><h1>403 Forbidden</h1></center>

<hr><center>nginx</center>

</body>

</html>

\* Connection #0 to host localhost left intact

<https://my.vnpt.com.vn/tinh-nang/ung-dung?q=1%20UNION%20ALL%22>

# 6. Custom NAXSI log

Cấu hình ngoài location, dưới listen

#set $naxsi\_extensive\_log 1;

set $naxsi\_json\_log 1;

Ở trong location để như sau:

location /xxxx

#Add NAXSI

include /opt/nginx/conf.d/naxi/\*.conf;

set $naxsi\_json\_log 1;

sd