This repository Search Explore Gist Blog Help itpp16 +

nbs-system / **naxsi** Watch 75 Star 507 Fork 77

basicsetup

Edit New Page

nodecode edited this page on Dec 23, 2014 · 20 revisions

Initial setup

Let's take the first step to use : setting up learning mode for your website ! This page assumes you already know how to properly configure nginx without naxsi and make it work. /etc/nginx/nginx.conf :

```
user                www-data;
worker_processes    1;
worker_rlimit_core  500M;
working_directory   /tmp/;
error_log           /var/log/nginx/error.log;
pid                 /var/run/nginx.pid;
events {
    worker_connections 1024;
    use epoll;
    # multi_accept on;
}
http {
    include                        /etc/nginx/naxsi_core.rules;
    include                        /etc/nginx/mime.types;
    server_names_hash_bucket_size  128;
    access_log                     /var/log/nginx/access.log;
    sendfile                       on;
    keepalive_timeout              65;
```

Pages 24

Find a Page…

A fail2ban profile for Naxsi
basicsetup
compatibility
configuration
deniedurl
dynamicmodifiers
faq
Home
How to create an Apparmor profile for Naxsi
installation
Knownbugs
libinjection
Naxsi on Windows with nginx
naxsilogs

```
    tcp_nodelay                     on;
    gzip                            on;
    gzip_disable                    "MSIE [1-6]\.(?!.*SV1)";
    include                         /etc/nginx/sites-enabled/*;
}
```

Notice the /etc/nginx/naxsi_core.rules include. This is the only thing you need to add to your existing `http {}` section if you already have a configuration. naxsi_core.rules is provided in the project (naxsi_config/), and contains naxsi rules. As you might notice, these are not signatures, in the classic WAF sense, but simple "score rules", ie :

```
MainRule "str:\"" "msg:double quote" "mz:BODY|URL|ARGS|$HEADERS_VAR:Cookie" "s:$SQL:
```

You can see more about rules syntax at rulessyntax Now, let's have a look at my /etc/nginx/site-enabled/default :

```
server {
    proxy_set_header  Proxy-Connection "";
    listen            *:80;
    access_log        /tmp/nginx_access.log;
    error_log         /tmp/nginx_error.log debug;
    location / {
         include          /etc/nginx/naxsi.rules;
         proxy_pass       http://x.x.x.x/;
         proxy_set_header  Host www.mysite.com;
    }
    location /RequestDenied {
        return 418;
    }
}
```

The naxsi's configuration itself is in the file /etc/nginx/naxsi.rules :

naxsivsappscan

Show 9 more pages...

Clone this wiki locally

https://github.com/nbs-system/naxsi

Clone in Desktop

```
LearningMode; #Enables learning mode
SecRulesEnabled;
#SecRulesDisabled;
DeniedUrl "/RequestDenied";
## check rules
CheckRule "$SQL >= 8" BLOCK;
CheckRule "$RFI >= 8" BLOCK;
CheckRule "$TRAVERSAL >= 4" BLOCK;
CheckRule "$EVADE >= 4" BLOCK;
CheckRule "$XSS >= 8" BLOCK;
```

With the following setup :

- Naxsi will be enabled
- Naxsi will not block any requests (while LearningMode is active)
- To-be-blocked requests will generate event logs in your location's error.log file

Exception do look like (let's request http://127.0.0.1/?a=%3C)

```
2013/05/30 20:09:43 [error] 8404#0:*3 NAXSI_FMT: ip=127.0.0.1&server=127.0.0.1&uri=/
```

Once you get this kind of lines in your error log, you have naxsi running in [LearningMode], congrats ! You can now move to Generating Whitelists and/or Generating Reporting :)