目录

[Nginx 安全 2](#_Toc1281137457)

[一、 优化Nginx服务的安全配置 2](#_Toc1322218508)

[1) 删除不需要的模块 2](#_Toc1751674104)

[2) 修改版本信息,并隐藏具体版本号 2](#_Toc1397296471)

[3) 限制并发量 3](#_Toc1685843339)

[4) 拒绝非法请求 4](#_Toc1762849711)

[5) 防止buffer溢出 5](#_Toc712960068)

[附:Nginx模块详解 6](#_Toc1470878367)

[一、 Nginx 核心模块 6](#_Toc1065709385)

[二、 标准HTTP模块 6](#_Toc1655387527)

[三、 可选 HTTP 模块 9](#_Toc1469583204)

[四、 邮件模块 11](#_Toc640252093)

# Nginx 安全

Nginx安全优化包括：删除不要的模块、修改版本信息、限制并发、拒绝非法请求、防止buffer溢出。

1. 优化Nginx服务的安全配置
2. 删除不需要的模块

Nginx是模块化设计,需要(禁用)什么功能,可以在编译安装时自定义.

--with可以开启某些模块

--without可以禁用某些模块

(最小化安装永远是正确的)

Eg: # ./configure \

>--without-http\_autoindex\_module \    //禁用自动索引文件目录模块

>--without-http\_ssi\_module //支持服务器端的include

1. 修改版本信息,并隐藏具体版本号

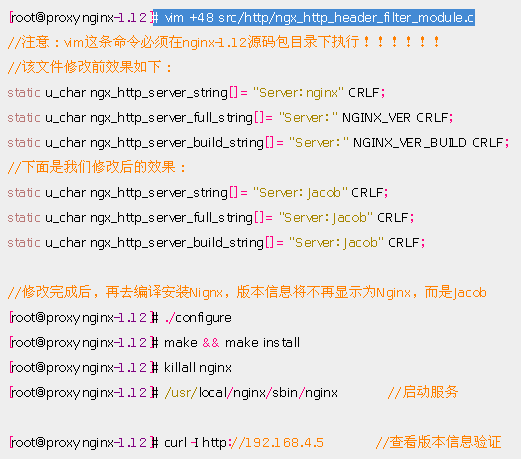
# vim /usr/local/nginx/conf/nginx.conf

在http下面手动添加 server\_tokens off; 重启nginx

测试:# curl -I http://192.168.x.x //查看服务器响应的头部信息

直接修改版本信息

配置文件:# vim +48 src/http/ngx\_http\_header\_filter\_module.c



1. 限制并发量

DDOS攻击者会发送大量的并发连接，占用服务器资源（包括连接数、带宽等），这样会导致正常用户处于等待或无法访问服务器的状态。

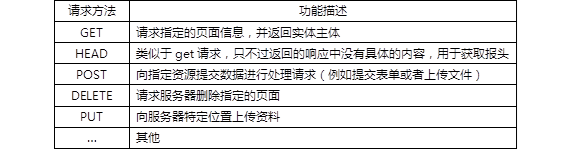
Nginx提供了一个ngx\_http\_limit\_req\_module模块，可以有效降低DDOS攻击的风险.



Ab测试软件测试结果# ab -c 100 -n 100 http://192.168.4.5/

1. 拒绝非法请求

网站使用的是HTTP协议，该协议中定义了很多方法，可以让用户连接服务器，获得需要的资源。但实际应用中一般仅需要get和post。



未修改前 # curl -i -X GET http://192.168.4.5

-i选项:访问服务器页面时,显示HTTP的头部信息

-x选项:指定请求服务器的方法

设置让Nginx拒绝非法的请求方法

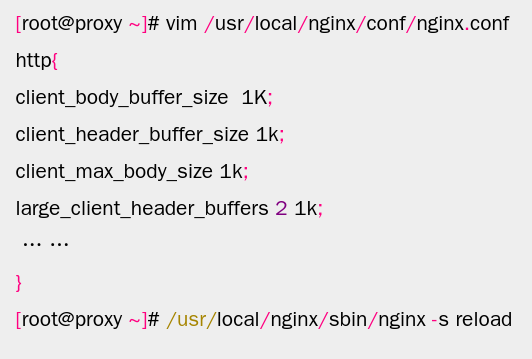


1. 防止buffer溢出

当客户端连接服务器时，服务器会启用各种缓存，用来存放连接的状态信息。

如果攻击者发送大量的连接请求，而服务器不对缓存做限制的话，内存数据就有可能溢出（空间不足）。

修改Nginx配置文件，调整各种buffer参数，可以有效降低溢出风险



附:Nginx模块详解

Nginx 模块必须在编译时就进行选择，目前不支持在运行时进行模块选择。在编译时，可以通过命令 ./configure --help 运行所提供的配置脚本来查看所有支持的编译选项列表（包含可选模块）。

## Nginx 核心模块

这些模块是必须的。

|  |  |
| --- | --- |
| **名称** | **说明** |
| [Main](http://wiki.nginx.org/CoreModuleChs" \o "CoreModuleChs) | 配置错误日志、进程、权限等。 |
| [Events](http://wiki.nginx.org/EventsModuleChs" \o "EventsModuleChs) | 配置epoll、kqueue、select、poll等。 |

1. 标准HTTP模块

这些模块是默认均被编译进去的，除非通过configure明确地禁用它们。

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 说明 | 版本 | 禁用选项 |
| [Core](http://wiki.nginx.org/HttpCoreModuleChs" \o "HttpCoreModuleChs) | 控制端口、location、错误页、别名和其他必要配置。 |  | --without-http |
| [Access](http://wiki.nginx.org/HttpAccessModuleChs" \o "HttpAccessModuleChs) | 基于客户端IP地址允许/拒绝Http请求。 |  | --without-http\_access\_module |
| [Auth Basic](http://wiki.nginx.org/HttpAuthBasicModuleChs" \o "HttpAuthBasicModuleChs) | Basic HTTP 认证。 |  | --without-http\_auth\_basic\_module |
| [Auto Index](http://wiki.nginx.org/HttpAutoindexModuleChs" \o "HttpAutoindexModuleChs) | 自动为没有索引页面的目录生成文件列表。 |  | --without-http\_autoindex\_module |
| [Browser](http://wiki.nginx.org/index.php?title=HttpBrowserModuleChs&action=edit&redlink=1" \o "HttpBrowserModuleChs (page does not exist)) | 翻译"User-Agent" 字符串。 | 0.4.3 | --without-http\_browser\_module |
| [Charset](http://wiki.nginx.org/index.php?title=HttpCharsetModuleChs&action=edit&redlink=1" \o "HttpCharsetModuleChs (page does not exist)) | 对Web页面重新编码。 |  | --without-http\_charset\_module |
| [Empty GIF](http://wiki.nginx.org/HttpEmptyGifModuleChs" \o "HttpEmptyGifModuleChs) | 在内存中生成一个高1像素、宽1像素的GIF图片，并对外提供服务。 | 0.3.10 | --without-http\_empty\_gif\_module |
| [FastCGI](http://wiki.nginx.org/HttpFastcgiModuleChs" \o "HttpFastcgiModuleChs) | 提供对FastCGI的支持。 |  | --without-http\_fastcgi\_module |
| [Geo](http://wiki.nginx.org/HttpGeoModuleChs" \o "HttpGeoModuleChs) | 通过IP地址的键值对来设置配置参数。 | 0.1.17 | --without-http\_geo\_module |
| [Gzip](http://wiki.nginx.org/HttpGzipModuleChs" \o "HttpGzipModuleChs) | 支持使用Gzip压缩响应内容。 |  | --without-http\_gzip\_module |
| [Headers](http://wiki.nginx.org/HttpHeadersModuleChs" \o "HttpHeadersModuleChs) | 可以设定任意的HTTP响应头。 |  |  |
| [Index](http://wiki.nginx.org/HttpIndexModuleChs" \o "HttpIndexModuleChs) | 控制将哪些文件作为索引页面。 |  |  |
| [Limit Requests](http://wiki.nginx.org/index.php?title=HttpLimitReqModuleChs&action=edit&redlink=1" \o "HttpLimitReqModuleChs (page does not exist)) | 限定客户端创建连接的频率。 | 0.7.20 | --without-http\_limit\_req\_module |
| [Limit Zone](http://wiki.nginx.org/HttpLimitZoneModuleChs" \o "HttpLimitZoneModuleChs) | 限定客户端同时建立连接的最大数。从1.1.8起不再推荐使用，建议使用 Limit Conn。 | 0.5.6 | --without-http\_limit\_zone\_module |
| [Limit Conn](http://wiki.nginx.org/index.php?title=HttpLimitConnModuleChs&action=edit&redlink=1" \o "HttpLimitConnModuleChs (page does not exist)) | 通过配置参数限定客户端的最大并发连接数。 |  | --without-http\_limit\_conn\_module |
| [Log](http://wiki.nginx.org/HttpLogModuleChs" \o "HttpLogModuleChs) | 可以定制访问日志。 |  |  |
| [Map](http://wiki.nginx.org/index.php?title=HttpMapModuleChs&action=edit&redlink=1" \o "HttpMapModuleChs (page does not exist)) | 以键值对的方式设定任意配置参数。 | 0.3.16 | --without-http\_map\_module |
| [Memcached](http://wiki.nginx.org/HttpMemcachedModuleChs" \o "HttpMemcachedModuleChs) | 支持Memcached。 |  | --without-http\_memcached\_module |
| [Proxy](http://wiki.nginx.org/HttpProxyModuleChs" \o "HttpProxyModuleChs) | 代理上级服务器。 |  | --without-http\_proxy\_module |
| [Referer](http://wiki.nginx.org/index.php?title=HttpRefererModuleChs&action=edit&redlink=1" \o "HttpRefererModuleChs (page does not exist)) | 基于RefererHTTP请求头对请求进行过滤。 |  | --without-http\_referer\_module |
| [Rewrite](http://wiki.nginx.org/HttpRewriteModuleChs" \o "HttpRewriteModuleChs) | 使用正则表达式对请求进行重写。 |  | --without-http\_rewrite\_module |
| [SCGI](http://wiki.nginx.org/index.php?title=HttpScgiModuleChs&action=edit&redlink=1" \o "HttpScgiModuleChs (page does not exist)) | 支持SCGI协议。 | 0.8.42 | --without-http\_scgi\_module |
| [Split Clients](http://wiki.nginx.org/index.php?title=HttpSplitClientsModuleChs&action=edit&redlink=1" \o "HttpSplitClientsModuleChs (page does not exist)) | 基于某些条件将客户端分类。 | 0.8.37 | --without-http\_split\_clients\_module |
| [SSI](http://wiki.nginx.org/HttpSsiModuleChs" \o "HttpSsiModuleChs) | 支持服务器端的include。 |  | --without-http\_ssi\_module |
| [Upstream](http://wiki.nginx.org/HttpUpstreamModuleChs" \o "HttpUpstreamModuleChs) | 支持负载均衡。 |  | --without-http\_upstream\_ip\_hash\_module (ip\_hash directive only) |
| [User ID](http://wiki.nginx.org/index.php?title=HttpUseridModuleChs&action=edit&redlink=1" \o "HttpUseridModuleChs (page does not exist)) | 发行用户身份标识cookie。 |  | --without-http\_userid\_module |
| [uWSGI](http://wiki.nginx.org/index.php?title=HttpUwsgiModuleChs&action=edit&redlink=1" \o "HttpUwsgiModuleChs (page does not exist)) | 支持uWSGI协议。 | 0.8.40 | --without-http\_uwsgi\_module |
| [X-Accel](http://wiki.nginx.org/index.php?title=X-accelChs&action=edit&redlink=1" \o "X-accelChs (page does not exist)) | 类X-Sendfile模块。 |  |  |

1. 可选 HTTP 模块

下面的模块必须在编译时为 configure 明确地设定相应的启用选项

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 说明 | 版本 | 启用选项 |
| [Addition](http://wiki.nginx.org/index.php?title=HttpAdditionModuleChs&action=edit&redlink=1" \o "HttpAdditionModuleChs (page does not exist)) | 可以为页面追加文本。 |  | --with-http\_addition\_module |
| [Degradation](http://wiki.nginx.org/index.php?title=HttpDegradationModuleChs&action=edit&redlink=1" \o "HttpDegradationModuleChs (page does not exist)) | 允许当剩余内存较低时对某些位置的请求返回 204 或 404 状态码。 | 0.8.25 | --with-http\_degradation\_module |
| [Embedded Perl](http://wiki.nginx.org/index.php?title=HttpPerlModuleChs&action=edit&redlink=1" \o "HttpPerlModuleChs (page does not exist)) | 允许在配置文件中使用 Perl。 | 0.3.21 | --with-http\_perl\_module |
| [FLV](http://wiki.nginx.org/index.php?title=HttpFlvModuleChs&action=edit&redlink=1" \o "HttpFlvModuleChs (page does not exist)) | 支持 Flash视频(Flash Streaming Video)。 | 0.4.7 | --with-http\_flv\_module |
| [GeoIP](http://wiki.nginx.org/index.php?title=HttpGeoipModuleChs&action=edit&redlink=1" \o "HttpGeoipModuleChs (page does not exist)) | 根据来自 [MaxMind](http://www.maxmind.com/) 的 GeoIP 二进制文件中的信息创建变量。 | 0.8.6, 0.7.63 | --with-http\_geoip\_module |
| [Google Perftools](http://wiki.nginx.org/index.php?title=GooglePerftoolsModuleChs&action=edit&redlink=1" \o "GooglePerftoolsModuleChs (page does not exist)) | 支持 Google 性能工具。 | 0.6.29 | --with-google\_perftools\_module |
| [Gzip Precompression](http://wiki.nginx.org/index.php?title=HttpGzipStaticModuleChs&action=edit&redlink=1" \o "HttpGzipStaticModuleChs (page does not exist)) | 提供预压缩的静态文件。 | 0.6.23 | --with-http\_gzip\_static\_module |
| [Image Filter](http://wiki.nginx.org/index.php?title=HttpImageFilterModuleChs&action=edit&redlink=1" \o "HttpImageFilterModuleChs (page does not exist)) | 支持使用 Libgd 对图片进行变换。 | 0.7.54 | --with-http\_image\_filter\_module |
| [MP4](http://wiki.nginx.org/index.php?title=HttpMp4ModuleChs&action=edit&redlink=1" \o "HttpMp4ModuleChs (page does not exist)) | 允许对 mp4 流进行寻址。 | 1.1.3, 1.0.7 | --with-http\_mp4\_module |
| [Random Index](http://wiki.nginx.org/index.php?title=HttpRandomIndexModuleChs&action=edit&redlink=1" \o "HttpRandomIndexModuleChs (page does not exist)) | 允许使目录索引随机化。 | 0.7.15 | --with-http\_random\_index\_module |
| [Real IP](http://wiki.nginx.org/HttpRealipModuleChs" \o "HttpRealipModuleChs) | 允许将 nginx 作为后端服务器。 | 0.3.8 | --with-http\_realip\_module |
| [Secure Link](http://wiki.nginx.org/HttpSecureLinkModuleChs" \o "HttpSecureLinkModuleChs) | 允许通过密钥保护指定的文件。 | 0.7.18 | --with-http\_secure\_link\_module |
| [SSL](http://wiki.nginx.org/index.php?title=HttpSslModuleChs&action=edit&redlink=1" \o "HttpSslModuleChs (page does not exist)) | 支持 HTTPS/SSL。 |  | --with-http\_ssl\_module |
| [Stub Status](http://wiki.nginx.org/HttpStubStatusModuleChs" \o "HttpStubStatusModuleChs) | 提供查看服务器统计信息的能力。 | 0.1.18 | --with-http\_stub\_status\_module |
| [Substitution](http://wiki.nginx.org/index.php?title=HttpSubModuleChs&action=edit&redlink=1" \o "HttpSubModuleChs (page does not exist)) | 可以替换页面中的文本。 |  | --with-http\_sub\_module |
| [WebDAV](http://wiki.nginx.org/HttpDavModuleChs" \o "HttpDavModuleChs) | 支持 WebDAV 穿透。 | 0.3.38 | --with-http\_dav\_module |
| [XSLT](http://wiki.nginx.org/index.php?title=HttpXsltModuleChs&action=edit&redlink=1" \o "HttpXsltModuleChs (page does not exist)) | 允许对页面使用 XSLT 进行后处理。 | 0.7.8 | --with-http\_xslt\_module |

1. 邮件模块

|  |  |  |
| --- | --- | --- |
| 名称 | 说明 | 配置参数 |
| [Core](http://wiki.nginx.org/index.php?title=MailCoreModuleChs&action=edit&redlink=1" \o "MailCoreModuleChs (page does not exist)) | 使 Nginx 能够处理/代理 IMAP、POP3、SMTP协议。 | --with-mail --without-mail\_pop3\_module --without-mail\_imap\_module --without-mail\_smtp\_module |
| [Auth](http://wiki.nginx.org/index.php?title=MailAuthModuleChs&action=edit&redlink=1" \o "MailAuthModuleChs (page does not exist)) | 使用 Nginx 为邮件服务进行认证。 |  |
| [Proxy](http://wiki.nginx.org/index.php?title=MailProxyModuleChs&action=edit&redlink=1" \o "MailProxyModuleChs (page does not exist)) | 使 Nginx 能够代理 IMAP、POP3、SMTP协议。 |  |
| [SSL](http://wiki.nginx.org/index.php?title=MailSslModuleChs&action=edit&redlink=1" \o "MailSslModuleChs (page does not exist)) | 该模块可以让 POP3/IMAP/SMTP 使用 SSL/TLS。 | --with-mail\_ssl\_module |