## 网站弱口令问题

弱口令看上去很弱智，但是仍旧是一个十分严峻的问题。17dz当前线上存在很多的弱口令，提醒相应测试人员提高密码的复杂度。

## 隐藏不必要的nginx信息

Nginx请求的响应头，有时候包含一行server:nginx，表明使用了nginx服务器，由于某些漏洞只存在nginx的特定版本，因此nginx响应信息一定程度可以提高安全性

|  |
| --- |
| server\_tokens off |

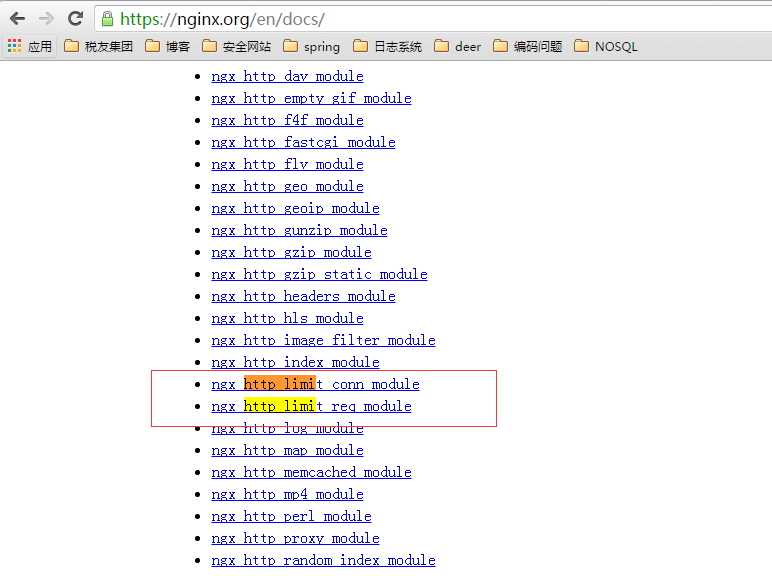
淘宝的nginx增强版 [Tengine](http://tengine.taobao.org/index_cn.html) 可以指定 server\_tag 为 off。另外，nginx 500等错误页面也需要自定义设置。

禁用一些非必要的HTTP请求方法(http、get、put、delete、trace)等。

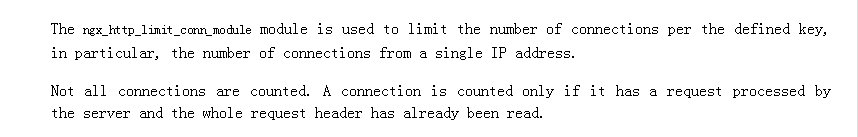
## nginx恶意扫描防御方案

Web网站攻击与扫描，供给制控制肉鸡(几百台甚至成千上万台)同时向我们的网站发送恶意请求。发送请求一部分是蓄意破坏，另一部分为了挖掘网站可能存在的漏洞，这些漏洞可通过一些漏洞扫描、目录扫描工具。

我们可以利用nginx的某些限制某个IP在一个时间段的访问次数，Nginx有两大模块用于访问控制。



**ngx\_http\_limit\_conn\_module**:该模块主要限制每个IP同时并发访问的数量

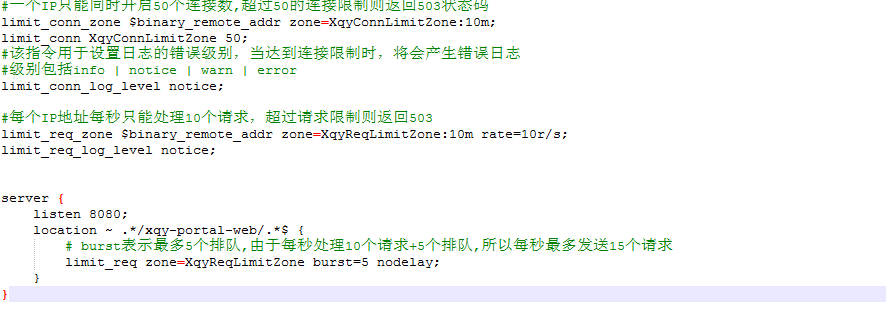


**ngx\_http\_limit\_req\_module**:限制访问数据，每秒内最多几个请求

limit\_conn\_zone和limit\_req\_module这两个模块的区别前一个是对一段时间内的连接数限制，后者是对同一时刻的连接数限制。

### 简单配置

Nginx最简单的安全配置



|  |
| --- |
| #一个IP只能同时开启50个连接数,超过50的连接限制则返回503状态码  limit\_conn\_zone $binary\_remote\_addr zone=XqyConnLimitZone:10m;  limit\_conn XqyConnLimitZone 50;  #该指令用于设置日志的错误级别，当达到连接限制时，将会产生错误日志  #级别包括info | notice | warn | error  limit\_conn\_log\_level notice;  #每个IP地址每秒只能处理10个请求，超过请求限制则返回503  limit\_req\_zone $binary\_remote\_addr zone=XqyReqLimitZone:10m rate=10r/s;  limit\_req\_log\_level notice;  server {  listen 8080;  location ~ .\*/xqy-portal-web/.\*$ {  # burst表示最多5个排队,由于每秒处理10个请求+5个排队,所以每秒最多发送15个请求  limit\_req zone=XqyReqLimitZone burst=5 nodelay;  }  } |

### 网站是否经过多层CDN代理

用户------🡪 360CDN加速----------------------🡪阿里云盾CDN加速------------🡪我们的服务器。

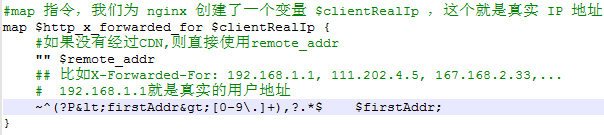
用户在到达正式网站之前，经过了好几层的CDN代理加速或者安全处理。这时候我们就不能实用**简单配置**了。因为，上面基于源IP的配置会把360CDN或者阿里云盾给限制，上面配置得到的源IP不是来自客户端IP，而是CDN服务器的IP地址。我们防御恶意扫描的目的是为了防止真是用户的扫描，因此我们必须要获得最前面用户的IP。

解决方案:

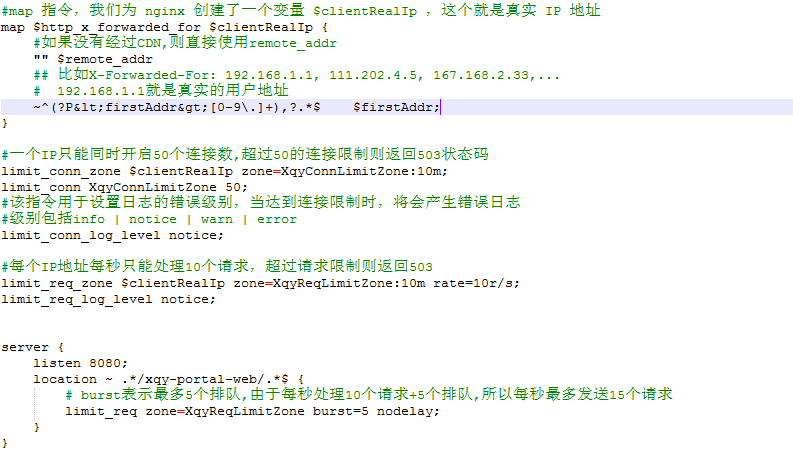
CDN将请求转发到后面的服务器时，会在请求头X-Forwarded-For加入一条自己的IP地址。

X-Forwarded-For : 用户IP，CDN1-IP，CDN2-IP。。。。

用户IP一般处在第一个位置

通过nginx的map指令提取出第一个位置  


|  |
| --- |
| #map 指令，我们为 nginx 创建了一个变量 $clientRealIp ，这个就是真实 IP 地址  map $http\_x\_forwarded\_for $clientRealIp {  #如果没有经过CDN,则直接使用remote\_addr  "" $remote\_addr  ## 比如X-Forwarded-For: 192.168.1.1, 111.202.4.5, 167.168.2.33,...  # 192.168.1.1就是真实的用户地址  ~^(?P&lt;firstAddr&gt;[0-9\.]+),?.\*$ $firstAddr;  } |



通过上面的配置，可以比较好的处理存在CDN加速代理服务器的情况。

**limit\_conn\_status可用于修改默认返回的状态码，**

默认值: limit\_conn\_status 503;

使用环境: http, server, location

该指令在 1.3.15版本后新增，当超出最大同时连接数的时候，对于新增连接返回的错误代码，默认503.

## X-Forwarded-For

<https://en.wikipedia.org/wiki/X-Forwarded-For>

## java中如何获得通过nginx代理真实用户的IP

|  |
| --- |
| proxy\_set\_header        Host            $host;  proxy\_set\_header        X-Real-IP       $remote\_addr;  proxy\_set\_header        X-Forwarded-For $proxy\_add\_x\_forwarded\_for; |