

nginx给网站开启图片防盗链

大家在查看分析网站访问日志的时候,很可能发现自己网站里面的很多图片被外部网站引用 , 这样给我们自己的博客带来了最少两点的不好:

- (1)、如果别的网站引用我们网站图片的次数非常多的话,会给咱们网站服务器带来很大的负载压力;
- (2)、被其他网站引用图片会消耗我们网站的流量,如果我们的网站服务器对流量有限制的话,这样对我们网站影响很大。

针对这几点问题,我将在本文介绍如果通过nginx服务器来限制其他网站对我们网站图片的引用。

nginx服务器中的ngx_http_referer_module模块允许拦截"Referer"请求头中含有非法值的请求,阻止它们访问站点。

我们只需要在网站的配置文件里面加入以下的配置即可:

```
location ~ ₩.(gif|jpg|png|bmp)$ {
   valid_referers none blocked www.iteblog.com server_names ~\psi_google\psi. ~\psi.baidu\psi.
   if ($invalid referer) {
     return 403;
   }
}
   上面valid referers的语法如下:
   语法:valid_referers none | blocked | server_names | string ...;
   默认值: —
   上下文: server, location
   "Referer"请求头为指定值时,内嵌变量$invalid_referer被设置为空字符串,
否则这个变量会被置成"1"。查找匹配时不区分大小写。
该指令的参数可以为下面的内容:
   none
   缺少"Referer"请求头;
   blocked
   "Referer"请求头存在,但是它的值被防火墙或者代理服务器删除; 这些值都不以"http://"
或者 "https://"字符串作为开头;
   server names
   "Referer" 请求头包含某个虚拟主机名;
   string
   定义一个服务器名和可选的URI前缀。服务器名允许在开头或结尾使用"*"符号。
当nginx检查时, "Referer"请求头里的服务器端口将被忽略。
   正则表达式
   必须以"~"符号作为开头。
```



需要注意的是表达式会从"http://"或者"https://"之后的文本开始匹配。

通过上面的配置,只要访问我们网站图片的Referer不是来自www.iteblog.com、Google、null或者百度等请求全部被nginx返回403错误,也就是无法访问。

需要注意的是用户伪造一个有效的"Referer"请求头是相当容易的,因此这个模块的预期目的不在于彻底地阻止这些非法请求,而是为了阻止由正常浏览器发出的大规模此类请求。还有一点需要注意,即使正常浏览器发送的合法请求,也可能没有"Referer"请求头。

不过如果你网站流量多的去的话,其实还可以通过这个设置所有的外部图片请求都返回一张 指定的图片,你可以在这张图片做广告什么的都行,可以通过rewrite设置如下:

```
location ~ ₩.(gif|jpg|png|bmp)$ {
	valid_referers none blocked www.iteblog.com server_names ~₩.google₩. ~₩.baidu₩.
	if ($invalid_referer) {
		rewrite ^/ http://iteblog.qiniudn.com/pic/iteblog.png;
	}
}
```

修改完之后,重启nginx服务器即可。

本博客文章除特别声明,全部都是原创! 原创文章版权归过往记忆大数据(<u>过往记忆</u>)所有,未经许可不得转载。 本文链接:【】()