

27 Nginx 的防盗链

更新时间：2020-03-12 10:23:19



“衡量一个人的真正品格，是看他在知道没人看见的时候干些什么。——孟德斯鸠”

前言

上一篇文章中，我们介绍了如何安装 LNMP 是如何一步一步的安装的，不知道大家是否亲自安装成功了呢？这一篇文章，我们介绍一个非常实用的功能，那就是 **图片盗链** 问题。

盗链

我们首先有必要介绍一下什么是 **盗链**。

有一些资源是一些网站独有的，有人通过技术手段在其它网站上访问或者下载，这就是 **盗链**。比如图片，百度或者腾讯上面有狠毒图片，但是有些图片我们只能在百度或者腾讯的服务上面才能访问，我们单独把网址拿出来放到自己的服务器上面就无法访问了，这就是因为他们做了防盗链的机制。

防盗链

防盗链的方法有很多，我们这里介绍最常用的一种。

这种方式是和 **HTTP** 协议相关的，**HTTP** 协议的请求头部有一个字段叫做 **Referer**，这个字段表示了当前我们访问的页面的前一个页面是从哪里来的。

讲到这里大家是不是就有一种茅塞顿开的感觉？是的，我们可以根据这个字段来进行防盗链。

实战

我们可以通过 **Web** 浏览器的方式通过 **html** 页面来测试盗链。

Nginx 配置

在这里我们要了解两个一个配置指令，这是 **Nginx** 专门为防盗链准备的。

```
valid_referers 指令  
$invalid_referer 变量
```

顾名思义，**valid_referers** 就是设置一些符合要求的 **Referer**。如果遇到我们符合我们设置的 **Referer**，那么 **\$invalid_referer** 变量的值就是 **0**，否则就是 **1**。

所以我们可以 **Nginx** 的配置文件中增加下面的代码段：

```
location ~* \.(jpeg|png|gif|jpg)$ {  
    valid_referers none www.test.com;  
    if ($invalid_referer){  
        return 200 "don't steal my pic";  
    }  
}
```

这段代码的作用是这样：

如果请求的 **Referer** 为空，或者为 **www.test.com**，那么 **\$invalid_referer** 的值是 **0**，否则是 **1**。

当 **\$invalid_referer** 的值是 **1** 的时候，会返回一个固定的字符串 **don't steal my pic**。当然了，真实的线上环境中，应该返回 **404**，或者一张其他固定的图片。我们这里是为了测试才这样做的。

使用 **curl** 进行测试

启动 **Nginx** 并进行测试.....

首先看一下我们的图片大小：

```
[root@793ef45fcbc7 html]# ll  
total 196  
-rw-r--r-- 1 root root 187700 Mar  4 21:35 1.jpeg  
-rw-r--r-- 1 root root  494 Mar  8 04:02 50x.html  
-rw-r--r-- 1 root root  658 Mar  8 11:41 index.html  
-rw-r--r-- 1 root root  715 Mar  8 11:42 stealpic.html  
[root@793ef45fcbc7 html]#  
[root@793ef45fcbc7 html]#
```

不带 **Referer** 的请求

```
[root@793ef45fcbc7 html]#  
[root@793ef45fcbc7 html]# curl -I http://www.test.com/1.jpeg  
HTTP/1.1 200 OK  
Server: nginx/1.16.1  
Date: Sun, 08 Mar 2020 12:29:32 GMT  
Content-Type: image/jpeg  
Content-Length: 187700  
Last-Modified: Wed, 04 Mar 2020 21:35:04 GMT  
Connection: keep-alive  
ETag: "5e601f08-2dd34"  
Accept-Ranges: bytes
```

图片大小

带 Referer 的请求

这里我们测试两种情况，Referer 分别是 `www.test.com` 和其他值的情况。

```
[root@793ef45fcbc7 html]#  
[root@793ef45fcbc7 html]# curl -I -H 'Referer: http://www.test.com' http://www.test.com/1.jpeg  
HTTP/1.1 200 OK  
Server: nginx/1.16.1  
Date: Sun, 08 Mar 2020 12:31:09 GMT  
Content-Type: image/jpeg  
Content-Length: 187700  
Last-Modified: Wed, 04 Mar 2020 21:35:04 GMT  
Connection: keep-alive  
ETag: "5e601f08-2dd34"  
Accept-Ranges: bytes
```

referer=www.test.com

图片大小

这里说明当 Referer 是 `www.test.com` 的时候是可以正常访问图片的。

```
[root@793ef45fcbc7 html]#  
[root@793ef45fcbc7 html]#  
[root@793ef45fcbc7 html]# curl -i -H 'Referer: http://www.test1234.com' http://www.test.com/1.jpeg  
HTTP/1.1 200 OK  
Server: nginx/1.16.1  
Date: Sun, 08 Mar 2020 12:32:58 GMT  
Content-Type: image/jpeg  
Content-Length: 18  
Connection: keep-alive  
  
don't steal my pic [root@793ef45fcbc7 html]#  
[root@793ef45fcbc7 html]#  
[root@793ef45fcbc7 html]#  
[root@793ef45fcbc7 html]#
```

其他 referer 值

不要盗图 ~~~~

这里可以看到当 Referer 为其他值的时候，图片不能正常的访问。

不过 HTTP Referer 可以通过程序来伪装生成的，所以通过 Referer 信息防盗链并非 100% 可靠，但是，它能够限制大部分的盗链。

}