linux配置防盗链及访问控制介绍

[原创](javascript:;)[Gary\_加油涛](http://blog.51cto.com/taoxie)[2017-12-25 19:09:20](javascript:;)[评论(0)](http://blog.51cto.com/taoxie/2054502#comment)[173人阅读](javascript:;)

**配置防盗链**

防盗链，就是不让别人盗用你网站上的资源，这个资源，通常指的是图片、视频、歌曲、文档等。

**referer的概念**

你通过A网站的一个页面http://a.com/a.html 里面的链接去访问B网站的一个页面http：//b.com/b.html ，那么这个B网站页面的referer就是http://a.com/a.html。 也就是说，一个referer其实就是一个网址。

1. 配置防盗链

[root@gary-tao 111.com]*# vim /usr/local/apache2.4/conf/extra/httpd-vhosts.conf*

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl -t*

Syntax OK

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl graceful*

**参考配置文件内容如下：**

**<Directory /data/wwwroot/111.com>**

SetEnvIfNoCase Referer "http://111.com" local\_ref

SetEnvIfNoCase Referer "http://111.com" local\_ref

SetEnvIfNoCase Referer "^$" local\_ref

**<filesmatch "\.(txt|doc|mp3|zip|rar|jpg|gif｜png)">**

Order Allow,Deny

Allow from env=local\_ref

**</filesmatch>**

**</Directory>**

**解释说明：**

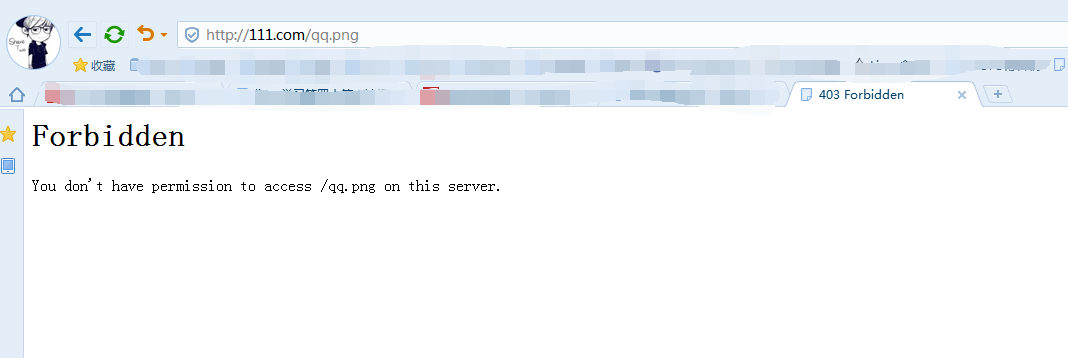
首先定义允许访问链接的referer，其中^$为空referer，当直接在浏览器里输入图片地址去访问它时，它的referer就为空。然后又使用filesmatch来定义需要保护的文件类型，访问txt、doc、mp3、zip、rar、jpg、gif、png格式的文件，当访问这样的类型文件时就会被限制。

**修改后示例如下图：**

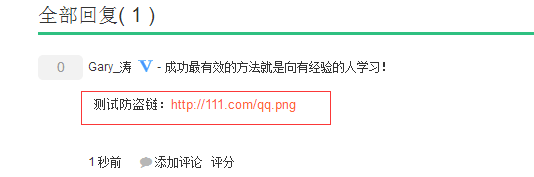
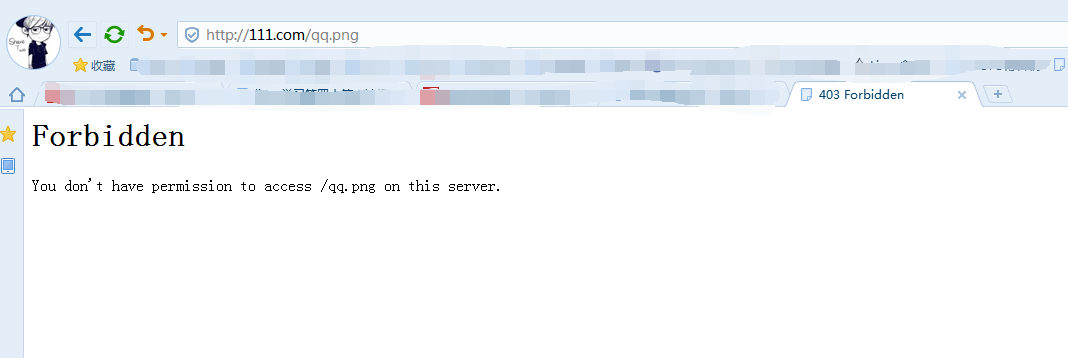


2.测试网页访问：

* 浏览器访问：<http://111.com/qq.png>

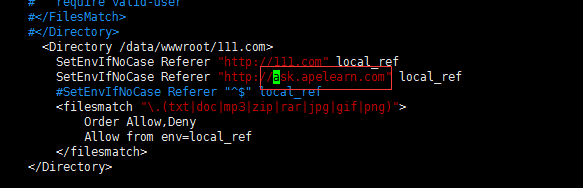


* 在其它网站上链接这个网址，还是打不开。

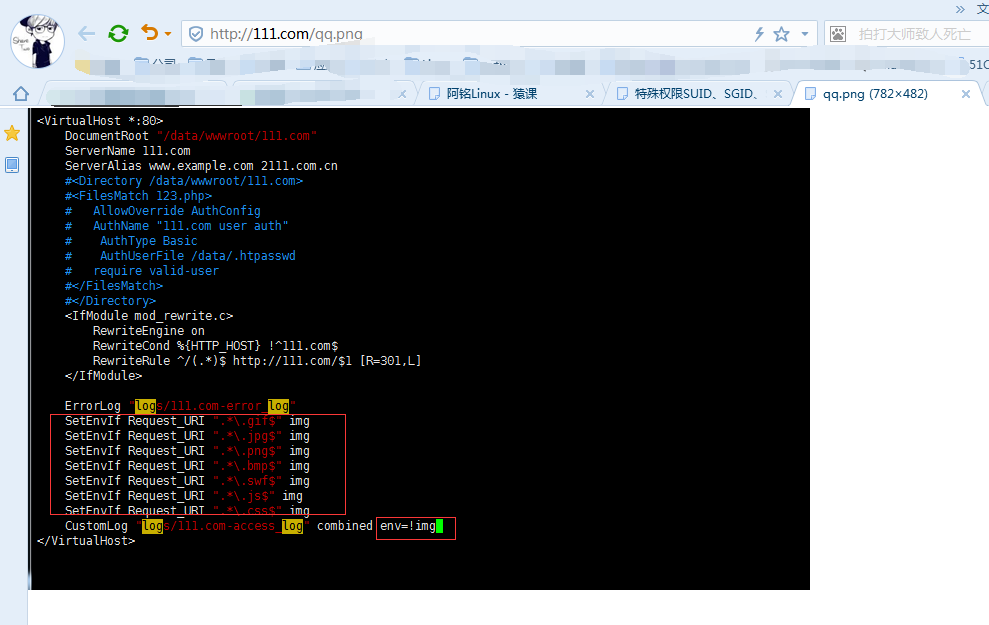
  


* 然后在虚拟主机配置文件里把第三方站点加入到白名单

[root@gary-tao 111.com]*# vim /usr/local/apache2.4/conf/extra/httpd-vhosts.conf*

* 在下面图片上把第三方站点网址加入到白名单，然后保存退出重新加载配置。  
  

在点击链接http://111.com/qq.png 访问就可以了，这就是referer，如下图



3.使用curl测试

[root@gary-tao 111.com]*# curl -x127.0.0.1:80 111.com/qq.png -I*

HTTP/1.1 200 OK

**Date: Thu, 21 Dec 2017 13:41:38 GMT**

**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**Last-Modified: Thu, 21 Dec 2017 06:18:31 GMT**

**ETag: "91ab-560d3ab3fbbc0"**

**Accept-Ranges: bytes**

**Content-Length: 37291**

**Cache-Control: max-age=86400**

**Expires: Fri, 22 Dec 2017 13:41:38 GMT**

**Content-Type: image/png**

[root@gary-tao 111.com]*# curl -e "http://wwww.qq.com/123.txt" -x127.0.0.1:80 111.com/qq.png -I //使用-e来定义referer，这个referer一定要以http://开头，否则不管用。*

HTTP/1.1 403 Forbidden

**Date: Thu, 21 Dec 2017 13:42:17 GMT**

**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**Content-Type: text/html; charset=iso-8859-1**

[root@gary-tao 111.com]*# curl -e "http://111.com/123.txt" -x127.0.0.1:80 111.com/qq.png -I*

HTTP/1.1 200 OK

**Date: Thu, 21 Dec 2017 13:42:34 GMT**

**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**Last-Modified: Thu, 21 Dec 2017 06:18:31 GMT**

**ETag: "91ab-560d3ab3fbbc0"**

**Accept-Ranges: bytes**

**Content-Length: 37291**

**Cache-Control: max-age=86400**

**Expires: Fri, 22 Dec 2017 13:42:34 GMT**

**Content-Type: image/png**

**访问控制Directory**

对于一些比较重要的网站内容,除了可以使用用户认证限制访问之外,还可以通过其他一些方法做到限制,比如可以限制IP,也可以限制user\_agent,限制IP指的是限制访问网站的来源IP,而限制user\_agent,通常用来限制恶意或者不正常的请求。

1. 修改虚拟主机配置：

[root@gary-tao 111.com]*# vim /usr/local/apache2.4/conf/extra/httpd-vhosts.conf*

核心配置文件内容如下：

<Directory /data/wwwroot/www.123.com/admin/>

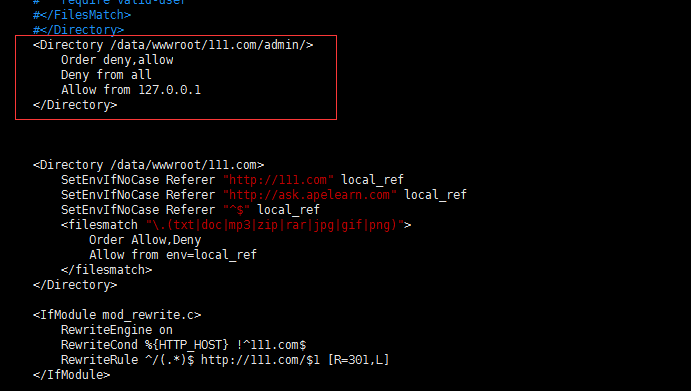
Order deny,allow

Deny **from** all

Allow **from** 127.0.0.1

</Directory>

**配置示例图：**



**解释说明：**

使用<Directory>来指定要限制访问的目录，order定义控制顺序，哪个在前面就先匹配哪个规则，在本例中deny在前面，所以要先匹配Deny from all,这样所有的来源IP都会被限制，然后匹配Allow from 127.0.0.1,这样又允许了127.0.0.1这个IP。最终的效果是，只允许来源IP为127.0.0.1的访问。

**验证如下：**

[root@gary-tao 111.com]*# mkdir /data/wwwroot/111.com/admin/ //创建admin目录，模拟网站后台*

[root@gary-tao 111.com]*# ls*

123.php admin index.php qq.png

[root@gary-tao 111.com]*# touch /data/wwwroot/111.com/admin/index.php //在后台目录下面创建文件*

[root@gary-tao 111.com]*# ls admin/*

index.php

[root@gary-tao 111.com]*# vim admin/index.php //并写入内容*

[root@gary-tao 111.com]*# cat admin/index.php*

123456789

[root@gary-tao 111.com]*# curl -x127.0.01:80 111.com/admin/index.php -I*

HTTP/1.1 200 OK

**Date: Mon, 25 Dec 2017 02:34:14 GMT**

**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**X-Powered-By: PHP/7.1.6**

**Cache-Control: max-age=0**

**Expires: Mon, 25 Dec 2017 02:34:14 GMT**

**Content-Type: text/html; charset=UTF-8**

[root@gary-tao 111.com]*# curl -x127.0.01:80 111.com/admin/index.php*

123456789

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl graceful //加载配置*

[root@gary-tao 111.com]*# curl -x172.16.111.100:80 111.com/admin/index.php*

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

<html><head>

<title>403 Forbidden</title>

</head><body>

<h1>Forbidden</h1>

<p>You don't have permission to access /admin/index.php

on this server.<br />

</p>

</body></html>

[root@gary-tao 111.com]*# curl -x127.0.01:80 111.com/admin/index.php*

123456789

[root@gary-tao 111.com]*# tail /usr/local/apache2.4/logs/111.com-access\_20171225.log //查看日志*

127.0.0.1 - - [25/Dec/2017:10:34:14 +0800] "HEAD HTTP://111.com/admin/index.php HTTP/1.1" 200 - "-" "curl/7.29.0"

127.0.0.1 - - [25/Dec/2017:10:34:30 +0800] "GET HTTP://111.com/admin/index.php HTTP/1.1" 200 10 "-" "curl/7.29.0"

172.16.111.100 - - [25/Dec/2017:10:36:54 +0800] "GET HTTP://111.com/admin/index.php HTTP/1.1" 403 224 "-" "curl/7.29.0"

127.0.0.1 - - [25/Dec/2017:10:37:33 +0800] "GET HTTP://111.com/admin/index.php HTTP/1.1" 200 10 "-" "curl/7.29.0"

[root@gary-tao 111.com]*# curl -x127.0.0.1:80 http://111.com/admin/adfafdafdas -I*

HTTP/1.1 404 Not Found

**Date: Mon, 25 Dec 2017 02:54:48 GMT**

**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**Content-Type: text/html; charset=iso-8859-1**

[root@gary-tao 111.com]*# curl -x172.16.111.100:80 http://111.com/admin/adfafdafdas -I*

HTTP/1.1 403 Forbidden

**Date: Mon, 25 Dec 2017 02:54:59 GMT**

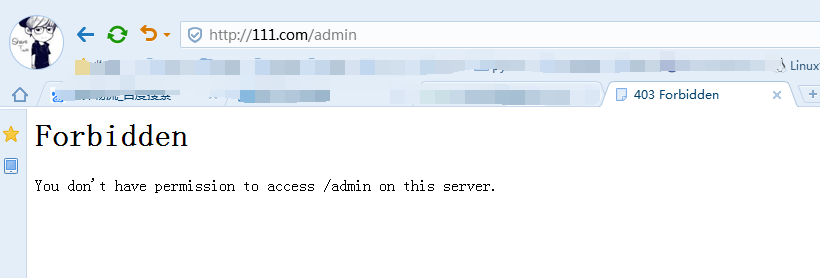
**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**Content-Type: text/html; charset=iso-8859-1**

**解释说明:**

本机有两个IP,一个是172.16.111.100,一个是127.0.0.1,通过这两个IP都可以访问到站点.而来源分别为172.16.111.110和127.0.0.1,其实和本机IP是一样的,curl测试状态码为403则被限制访问了。

**使用windowo浏览器访问示例图**



[root@gary-tao 111.com]*# tail /usr/local/apache2.4/logs/111.com-access\_20171225.log //windows浏览器访问日志*

172.16.111.1 - - [25/Dec/2017:11:00:37 +0800] "GET /admin HTTP/1.1" 403 214 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0"

172.16.111.1 - - [25/Dec/2017:11:00:39 +0800] "GET /admin HTTP/1.1" 403 214 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0"

172.16.111.1 - - [25/Dec/2017:11:00:39 +0800] "GET /admin HTTP/1.1" 403 214 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0"

172.16.111.1 - - [25/Dec/2017:11:00:40 +0800] "GET /admin HTTP/1.1" 403 214 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0"

**解释说明：**

浏览器访问提示Forbidden，其实就是403,再来看日志，可以查看到对应的来源IP为172.16.111.1，希望不要把来源IP和本机IP搞混了，前面实验中之所以本机IP和来源IP一样，就是因为它相当于自己访问自己，而后面用浏览器访问，相当于拿windows

**访问控制FilesMatch**

1. 针对某个文件来做限制。

[root@gary-tao 111.com]*# vim /usr/local/apache2.4/conf/extra/httpd-vhosts.conf*

核心配置文件内容

<Directory /data/wwwroot/www.123.com>

<FilesMatch "admin.php(.\*)">

Order deny,allow

Deny **from** all

Allow **from** 127.0.0.1

</FilesMatch>

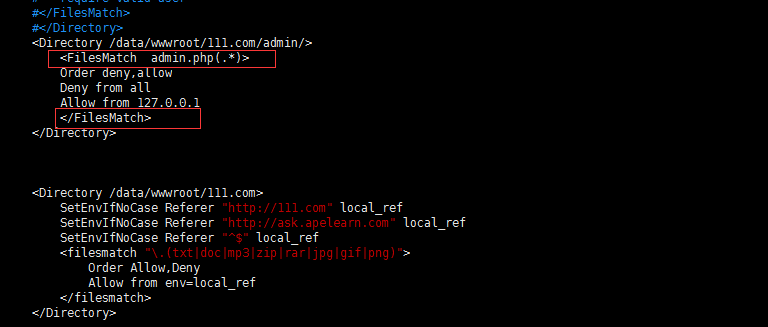
</Directory>

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl -t //检测语法*

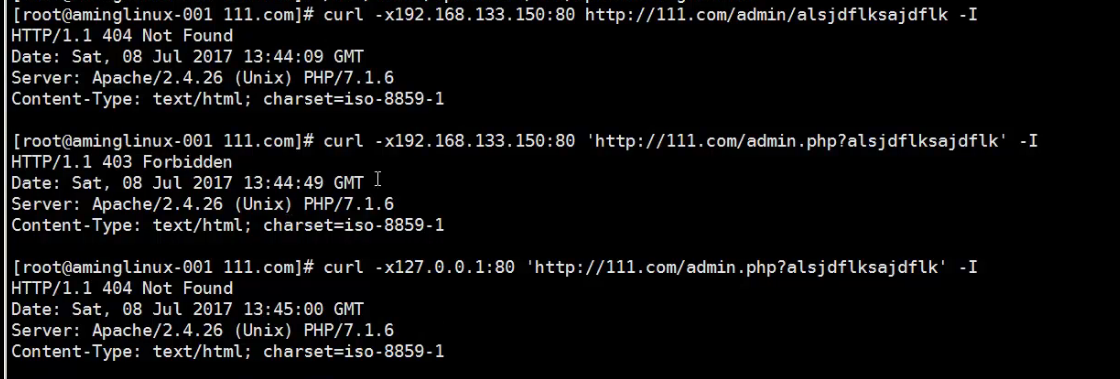
Syntax OK

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl graceful //加载配置*

**配置示例图：**



**实验结果如下：**



版权声明：原创作品，如需转载，请与作者联系。否则将追究法律责任