

i春秋在线挑战详细攻略-《你是会员吗》

原创

[i春秋论坛](#) 于 2017-03-15 09:47:53 发布 4709 收藏

分类专栏: [网络渗透技术](#) [网站安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/wodafa/article/details/62215759>

版权



[网络渗透技术](#) 同时被 2 个专栏收录

12 篇文章 2 订阅

订阅专栏



[网站安全](#)

28 篇文章 0 订阅

订阅专栏



试验地址: <http://www.ichunqiu.com/racing/54399>

实验平台: i春秋

Step 0

实验环境

操作机: Windows XP [172.16.11.2]

目标网址: [www.test.ichunqiu](http://www.test.ichunqiu.com) [172.16.12.2]

实验工具: 中国菜刀

实验目标: 获取[www.test.ichunqiu](http://www.test.ichunqiu.com)网站的FLAG信息, 学习一些简单的提权方式。

小提示:

在本次实验中, 请注意实验工具、实验文件存放路径, 不同的文件路径可能会出现不一样的实验结果。

在实验环境中无法连接互联网, 请使用您本地的网络环境。

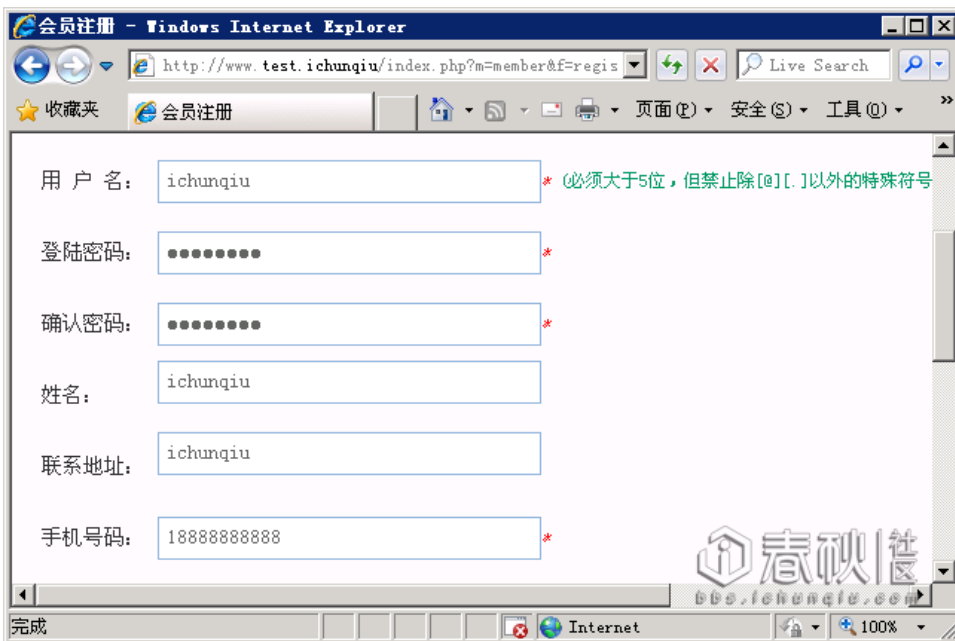
Step 1

XDCMS

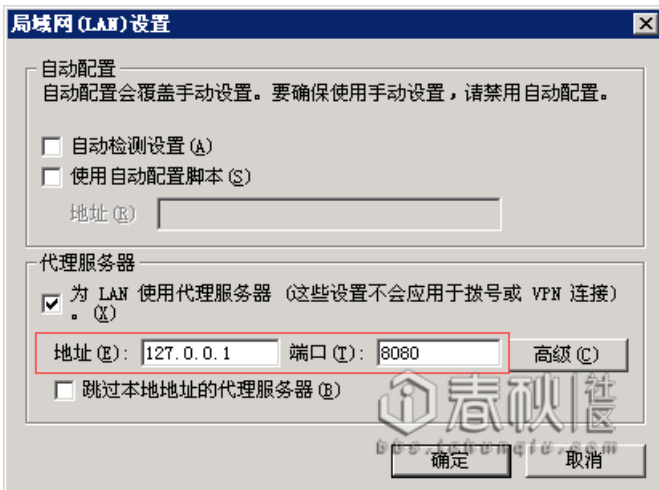
首先利用注入漏洞获取用户名和密码; 打开浏览器, 输入网址, 打开网站首页, 点击页面上方的 [免费注册];



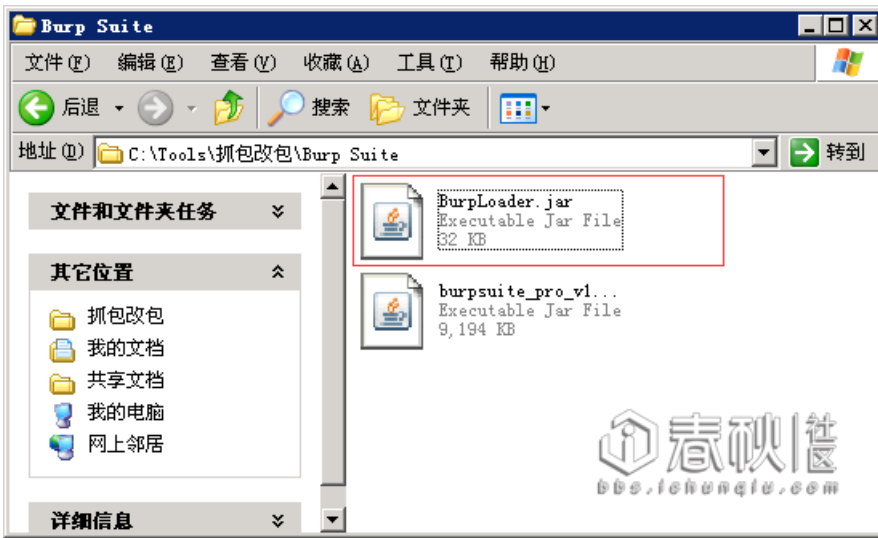
进入注册页面后，依次填入表单内容；



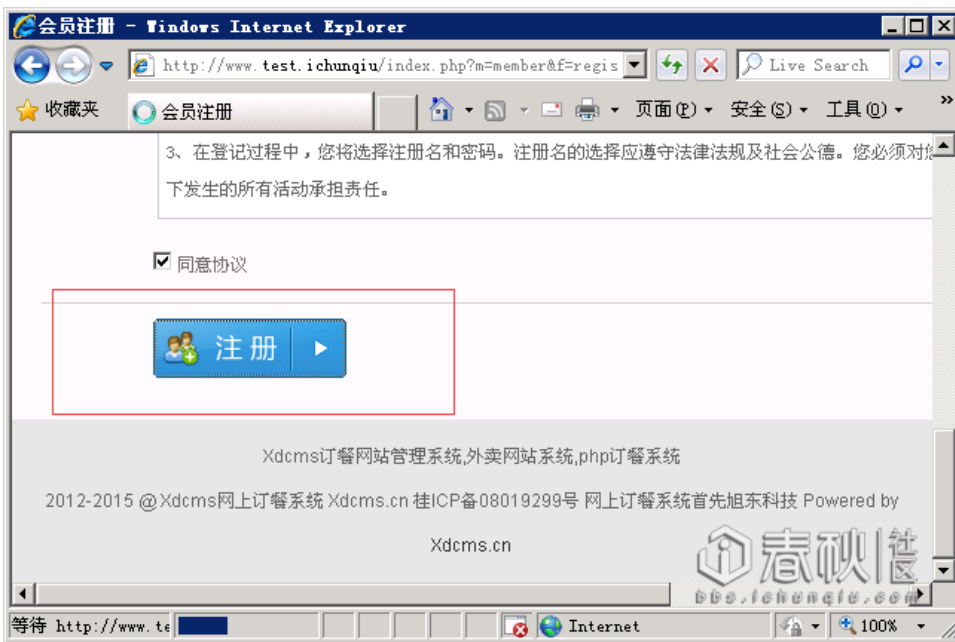
在提交之前，配置浏览器代理，操作步骤：[工具]-->[Internet选项]-->[连接]-->[局域网设置]；



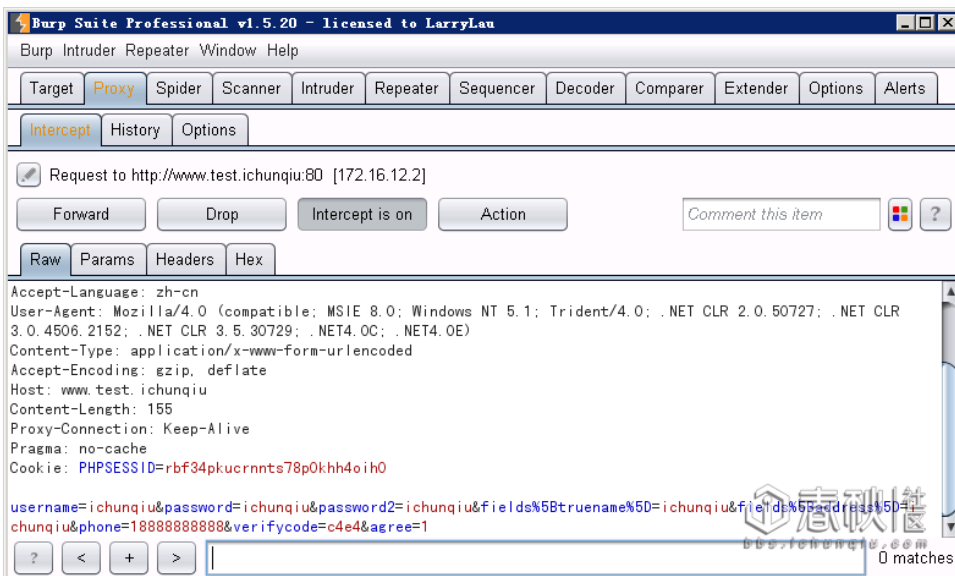
打开神器进行抓包改包；工具路径：C:\Tools\抓包改包\Burp Suite\



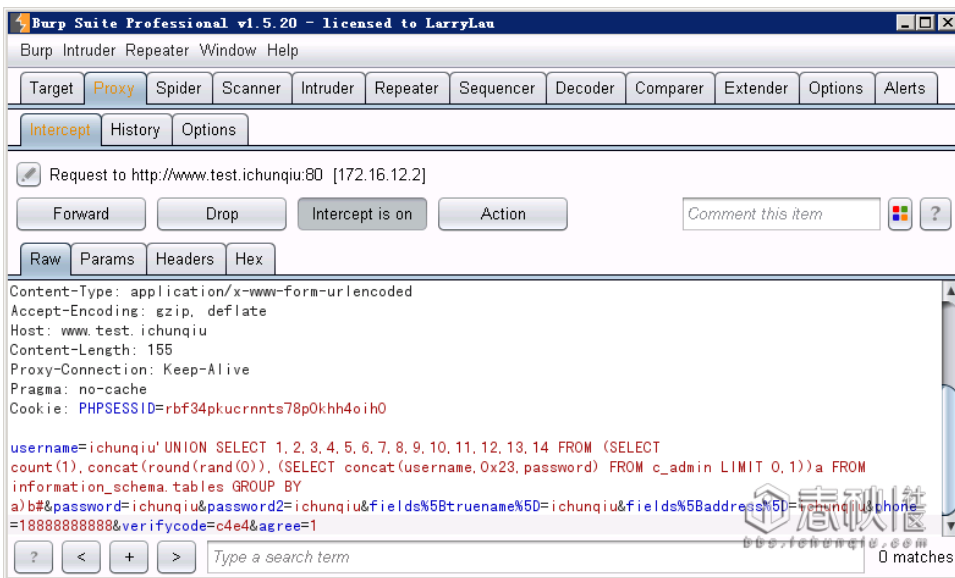
打开神器后，回到浏览器页面，点击 [注册]；



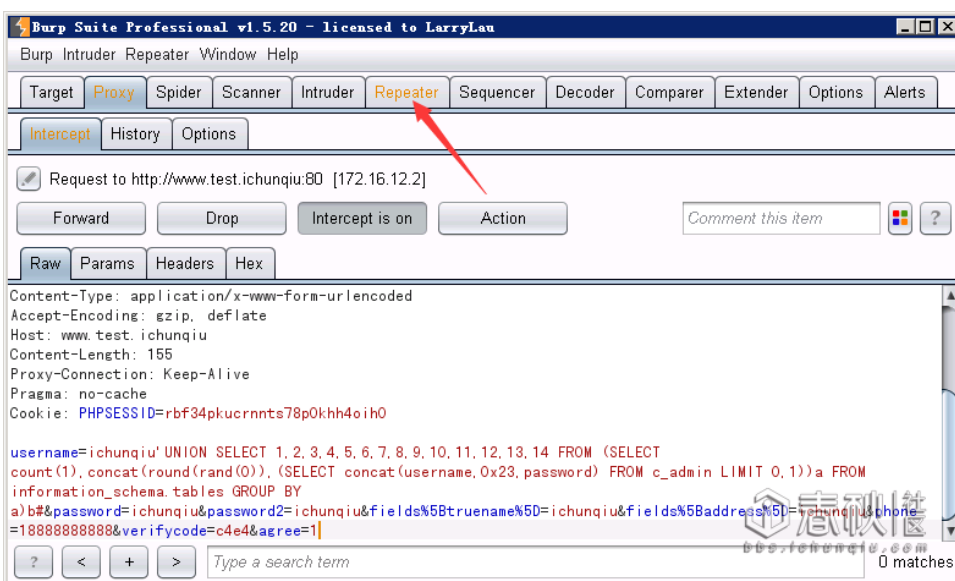
此时，BP抓包成功：



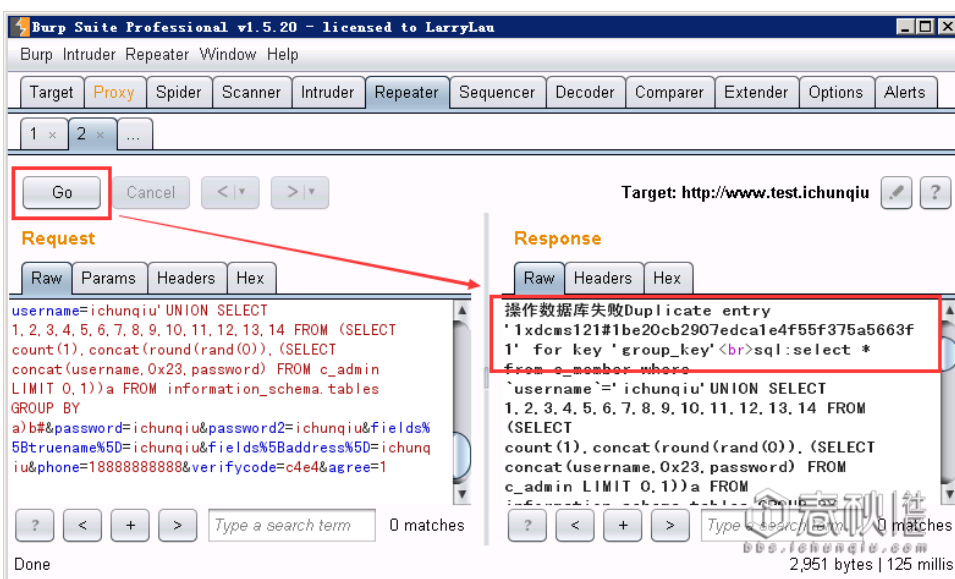
注意POST参数中的username值，在该值后面加入exp:



然后点击 [Action] 或者右键，在弹出的菜单中选择 [Send to Repeater]:



待 [Repeater] 标签变色后，选择该选项卡，点击左侧请求页面的 [GO]，右侧响应页面会爆出用户名和密码MD5值:



把MD5值 [1be20cb2907edca1e4f55f375a5663f1] 扔到解密网站上，得到结果，顺便看到了加密方式:

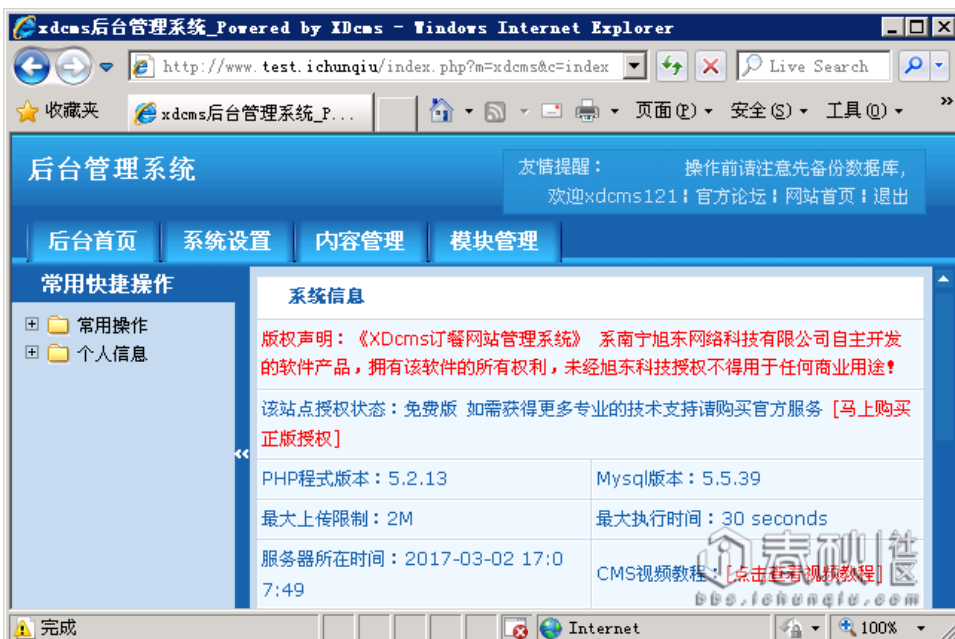


Step 2

打开后台登录界面，准备挂马，后台用路径扫描工具一扫就出来了，这里就不截图了；
后台路径：www.test.ichunqiu/admin



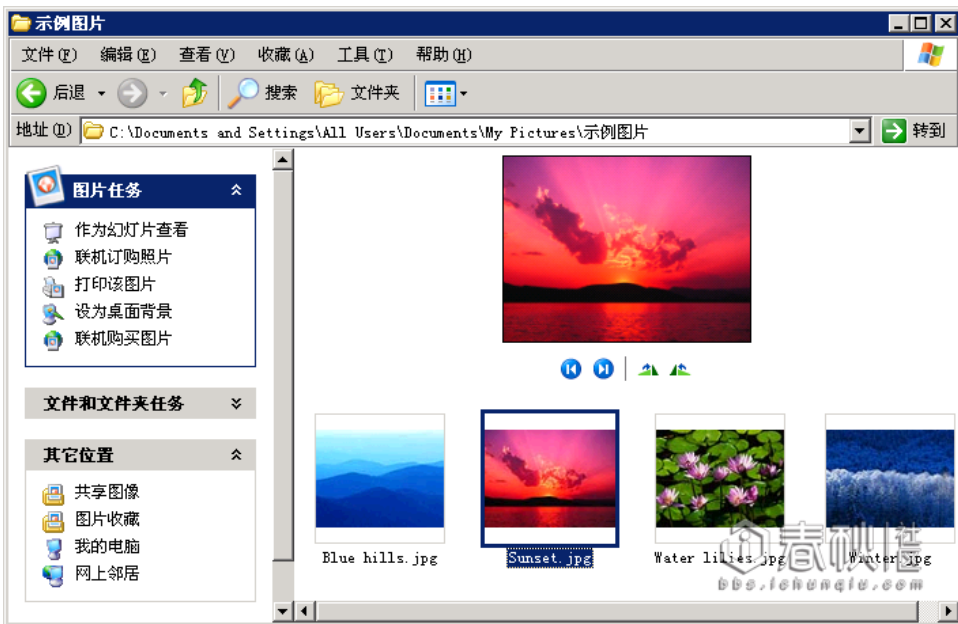
输入得到的用户名和密码 [xdcms121/xdcms212]，成功登录后台：



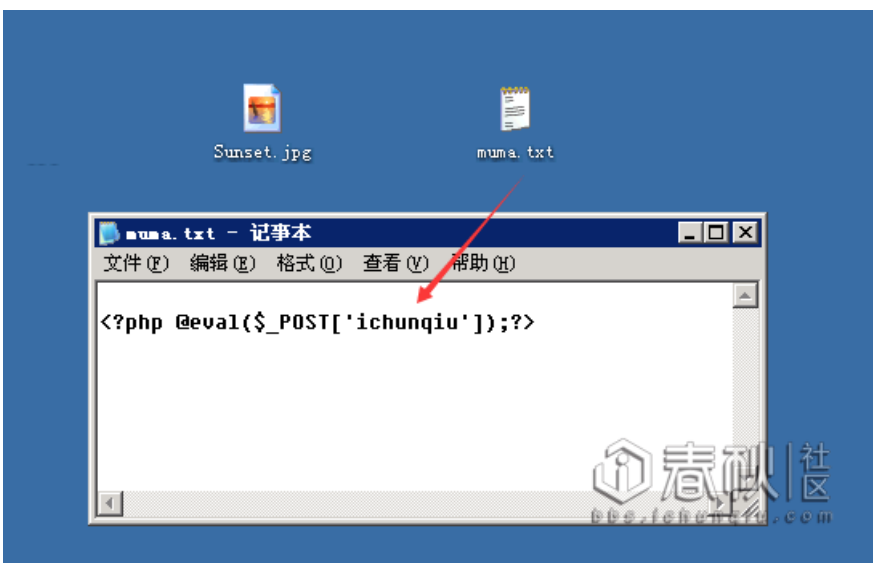
依次进入 [模块管理]-->[幻灯片管理]-->[管理幻灯]-->[编辑]；



进入编辑页面后，准备上传木马；在系统自带的图片中，随便选一张：

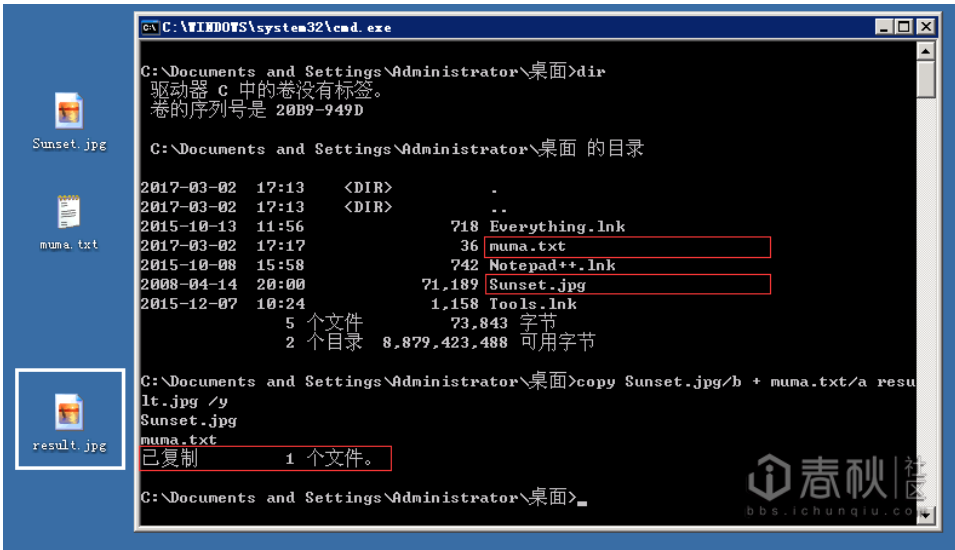


选一张图片复制到桌面上，然后新建一个文本文档，里面写入一句话木马：

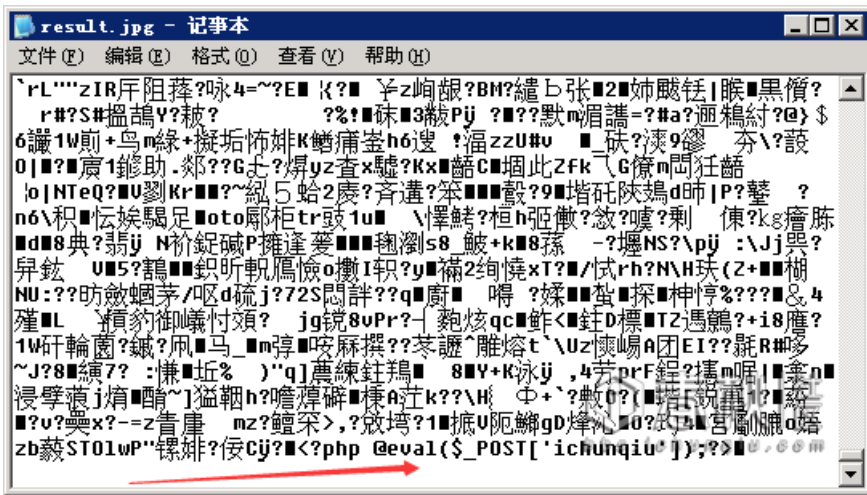


(注意：一句话之前加空行)
然后用cmd下的copy命令，将这两个文件合并成一个图片文件：

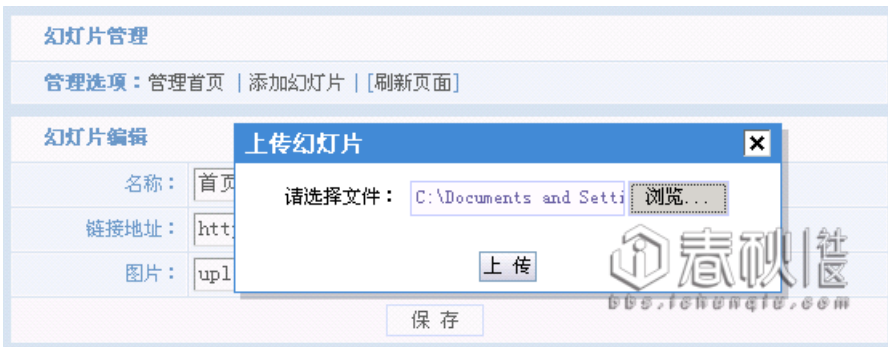
Copy Sunset.jpg/b + muma.txt/a result.jpg /y



用记事本打开合成的图片文件，拉到最下面，可以看到木马已经加进去了；



回到页面，点击上传幻灯片图片，将制作的木马图片上传上去：



把图片路径复制下来，点击 [保存]；

幻灯片管理

管理选项：管理首页 | 添加幻灯片 | [刷新页面]

幻灯片编辑

名称：

链接地址：

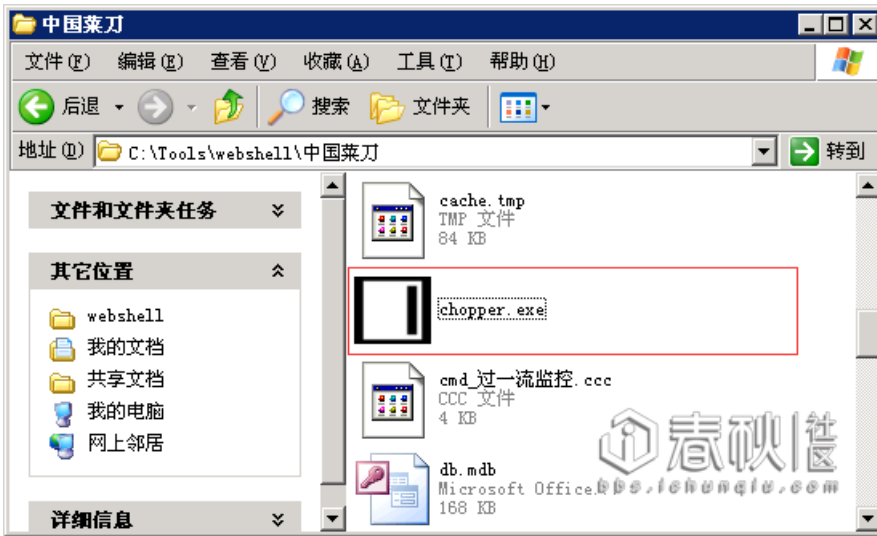
图片： 上传 


bbs.ichunqiu.com

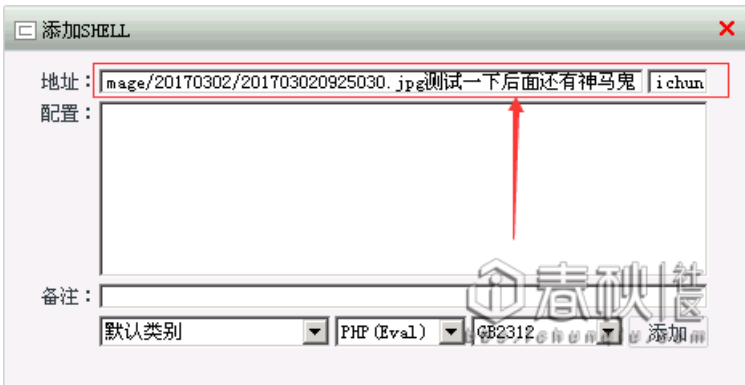
Step 3

利用文件包含连接菜刀；

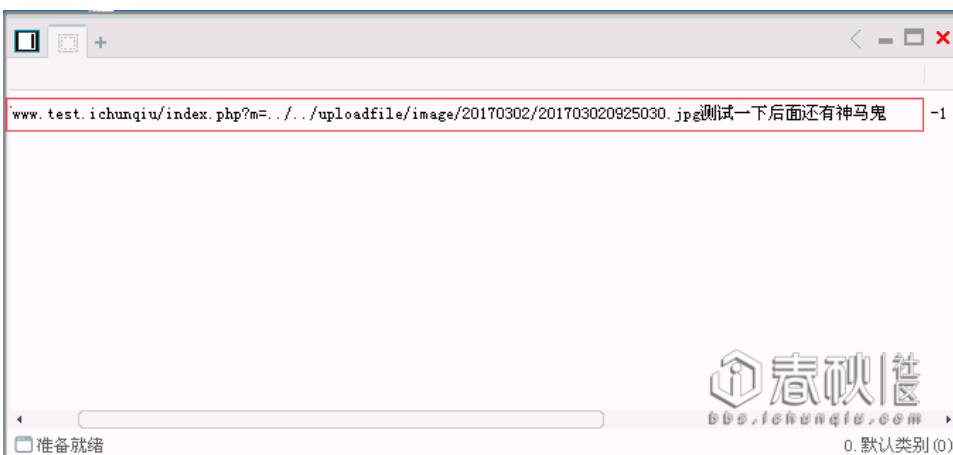
工具：中国菜刀，路径：C:\Tools\webshell\中国菜刀



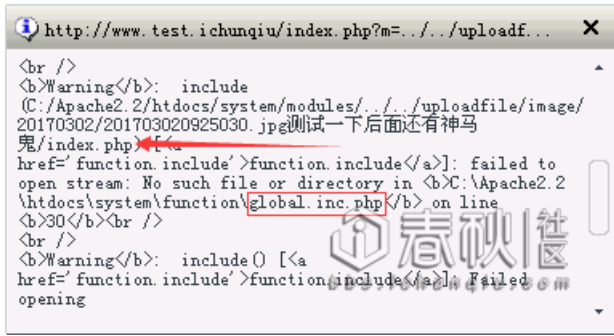
点击右键，选择 [添加]，首先我们在地址栏中输入错误的路径，看看会出现什么结果：



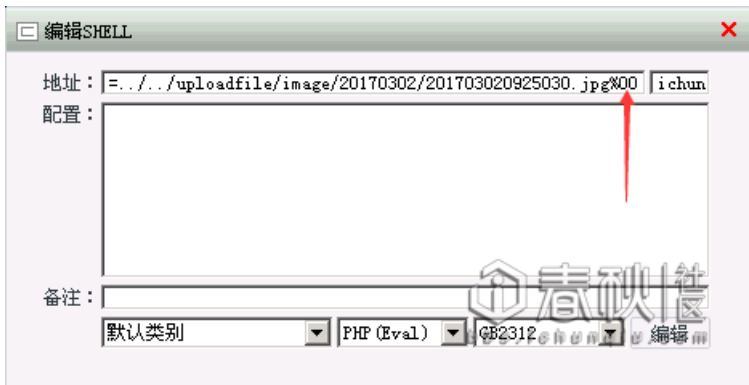
输入完成后，点击 [添加]；



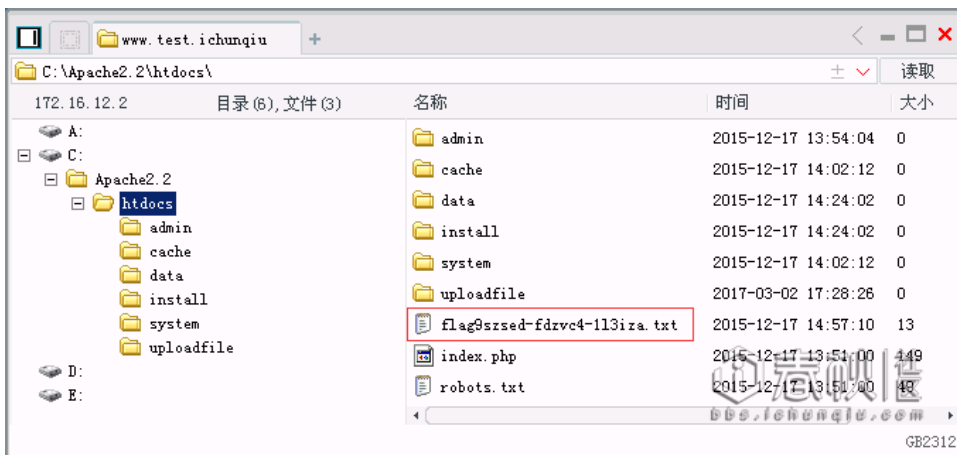
双击后，显示如下结果，注意图示：



我们发现，后面自动添加了/index.php，这样路径肯定是错的，用%00截断后面的附加值即可；在原路径的基础上，尾部添加%00即可；



这次成功进入，得到旗标。



最后说一下菜刀路径中的几个注意点：

```
[url]http://www.test.ichunqiu/index.php?m=../../uploadfile/image/2017.....5030.jpg%00[/url]
```

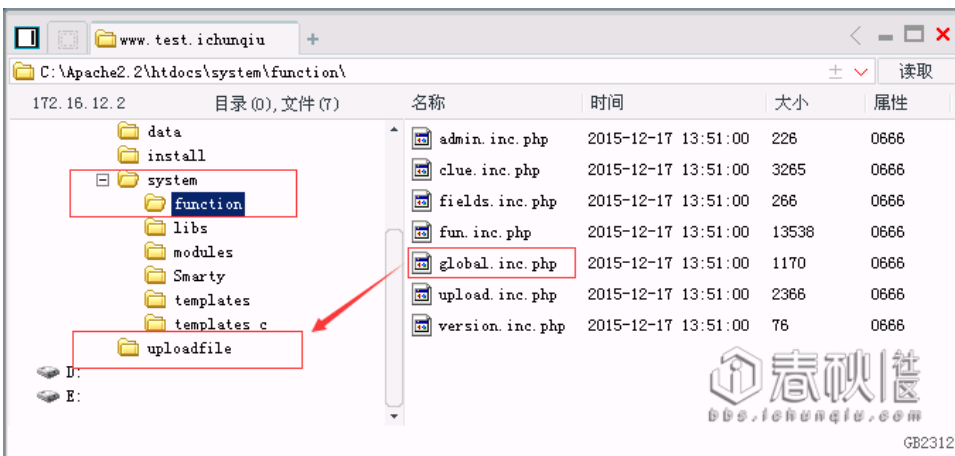
路径中的 m=? c=? f=? 这三个参数分别表示：模块，类，方法；具体位置在/system/function/global.inc.php文件中：

```

//接收参数
$m=safe_replace(safe_html(isset($_GET["m"]))) ? safe_replace(safe_html($_GET["m"])) : "content";
$c=safe_replace(safe_html(isset($_GET["c"]))) ? safe_replace(safe_html($_GET["c"])) : "index";
$f=safe_replace(safe_html(isset($_GET["f"]))) ? safe_replace(safe_html($_GET["f"])) : "init";
//判断模块是否存在
if(!file_exists(MOD_PATH.$m)){
    showmsg(C('module_not_exist'),'');
}
//判断类文件是否存在
if(!file_exists(MOD_PATH.$m."/".$c.".php")){
    showmsg(C('class_not_exist'),'');
}
include MOD_PATH.$m."/".$c.".php"; //调用类
//判断类是否存在
if(!class_exists($c)){
    showmsg(C('class_not_exist'),'');
}
$p=new $c(); //实例化
$p->$f(); //调用方法

```

global.inc.php 文件位置在根目录/system/function下，uploadfile直接在根目录下，所以得向上翻两级，也就是../



--END--

ps：部分知识点的内容转自网络；路漫漫其修远兮，感谢小盆友们的帮助；
Dare and the world always yields.