

Php.ini与web安全

web安全不仅与php.ini设置有关，还与目录权限、web服务器运行权限等紧密相关

目的：就算被上传webshell，也不能执行
就算拿到了webshell，他也不能读目录或者
文件，不能执行命令

1. register_globals.

这个配置影响到php如何接收传递过来的参数，说白了register_globals的意思就是注册为全局变量，所以当该参数为值On的时候，传递过来的值会被直接的注册为全局变量直接使用，而当该参数值为Off的时候，我们需要到从特定的数组里去得到它。（php目前的最高版中此参数都是默认是Off）

- register_globals

```
<form name="hack" id="hack" action="URL">;  
<input type="text" name="user_name" id="user_name">;  
<input type="password" name="user_pass" id="user_pass">;  
<input type="submit" value="login">;  
</form>;
```

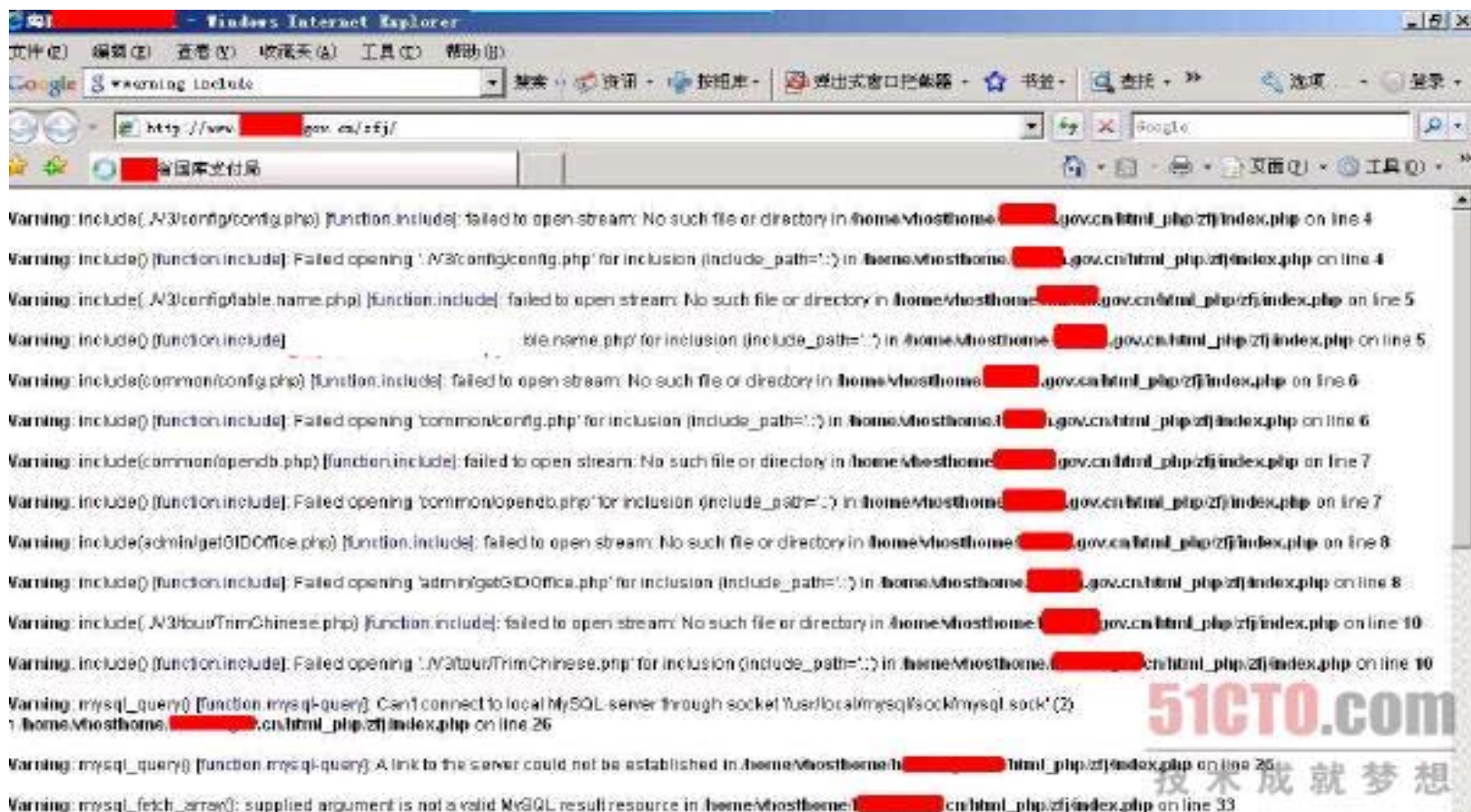
- register_globals=Off时，服务器端获取数据的时候用
\$_GET['user_name']和\$_GET['user_password']
当然当form的method的属性为post的时候用\$_POST['user_name'],
\$_POST['user_name']
- register_globals=On时，服务器端程序可以直接使用\$user_name和
\$user_pass这样的全局变量值来接受值
- php4.2版本后默认关闭

- 2. **magic_quotes_gpc**

如果你把magic_quotes_gpc设置成了Off，那么php就不会对4种字符‘(单引号)， “ (双引号)， \ (反斜线) 和 空字符进行转义，那这样的话就会造成服务器可能会被非法注入的可能。但是如果你把Magic_quotes_gpc设置成On的话，php就会给\$_POST，\$_GET，\$_COOKIE提交的变量中如果有上面四种字符的话就会加上\反斜杠。这样就会大大地提高php的安全性

- 3. **display_errors**

对display_errors没有进行设置，导致web目录泄露。这对于黑客来说可是非常重要的信息，因为很多时候的渗透都需要知道web目录，例如webshell的写入等等



4. safe_mode

就是我们常说的安全模式。php的安全模式是个非常重要的内嵌的安全机制，能够控制一些php中的函数，比如system()等函数，同时把很多文件操作函数进行了权限控制，也不允许对某些关键文件的访问，比如/etc/passwd，但是默认的php.ini是没有打开安全模式的

5. open_basedir

使用open_basedir选项能够控制PHP脚本只能访问指定的目录，这样能够避免PHP脚本访问不应该访问的文件，一定程度上限制了webshell的危害，我们一般可以设置为只能访问网站目录（假设网站目录为E:\test）：

open_basedir = E:\test

- 如果启用，可以有效的消除本地文件或者远程文件被include()等函数的调用攻击

- **6. disable_functions**

使用**disable_functions**可以限制一些对于系统来说威胁很大的函数，建议设置为：

`disable_functions = phpinfo, passthru, exec , system, chroot, scandir, chgrp, chown, shell_exec, proc_open, proc_get_status , ini_alter, ini_alter, ini_restore, dl, pfsockopen, openlog, syslog, readlink, symlink, popepassthru, stream_socket_server`

。

7. com.allow_dcom

PHP设置即使在安全模式下(**safe_mode**)，仍旧允许攻击者使用**COM()**函数来创建系统组件来执行任意命令，如果是默认的**Apache**设置或者**Web**服务器以**Loacalsystem**权限或**Administrators**权限运行，攻击者可以使用这个漏洞来提升权限。我们需要把这个参数修改成

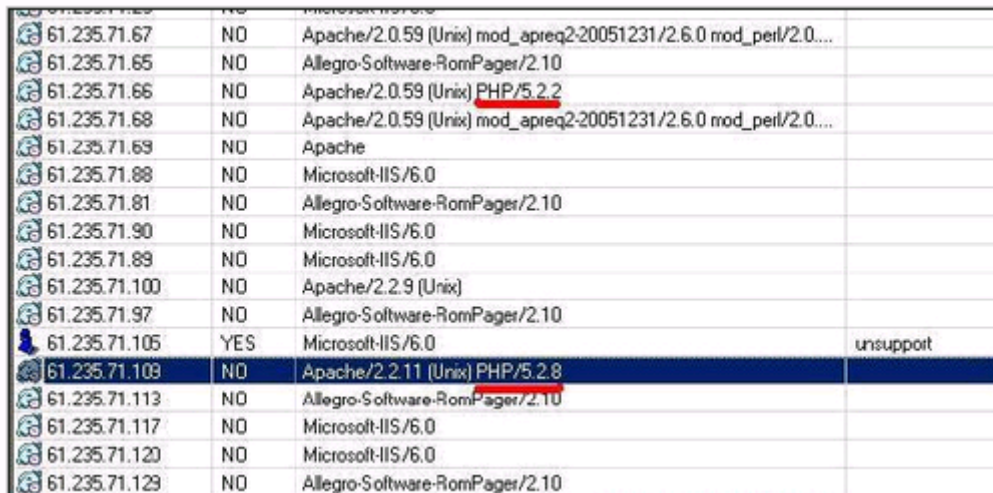
```
com.allow_dcom=false
```

8.allow_url_fopen

作用是调用远程文件的功能，如果开启就支持远程调用文件

- 9. expose_php

这个参数决定是否暴露 PHP 被安装在服务器上。如图3所示，如果这个参数设置为On的话就会把php的版本等泄露出来了。我们的推荐值是Off



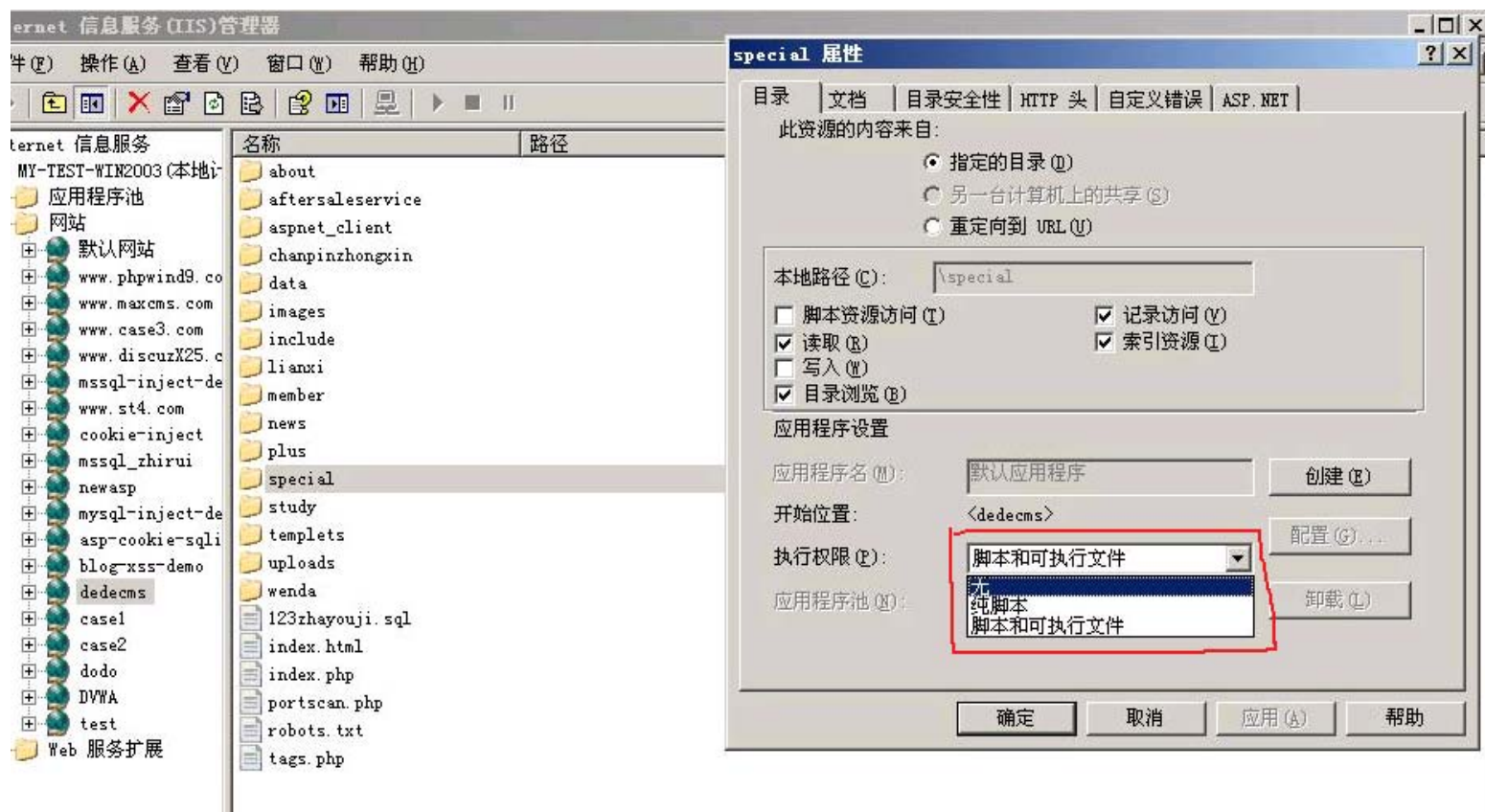
61.235.71.67	NO	Apache/2.0.59 (Unix) mod_apreq2-20051231/2.6.0 mod_perl/2.0...	
61.235.71.65	NO	Allegro-Software-RomPager/2.10	
61.235.71.66	NO	Apache/2.0.59 (Unix) <u>PHP/5.2.2</u>	
61.235.71.68	NO	Apache/2.0.59 (Unix) mod_apreq2-20051231/2.6.0 mod_perl/2.0...	
61.235.71.69	NO	Apache	
61.235.71.88	NO	Microsoft-IIS/6.0	
61.235.71.81	NO	Allegro-Software-RomPager/2.10	
61.235.71.90	NO	Microsoft-IIS/6.0	
61.235.71.89	NO	Microsoft-IIS/6.0	
61.235.71.100	NO	Apache/2.2.9 (Unix)	
61.235.71.97	NO	Allegro-Software-RomPager/2.10	
61.235.71.105	YES	Microsoft-IIS/6.0	unsupport
61.235.71.109	NO	Apache/2.2.11 (Unix) <u>PHP/5.2.8</u>	
61.235.71.113	NO	Allegro-Software-RomPager/2.10	
61.235.71.117	NO	Microsoft-IIS/6.0	
61.235.71.120	NO	Microsoft-IIS/6.0	
61.235.71.129	NO	Allegro-Software-RomPager/2.10	

IIS安全配置

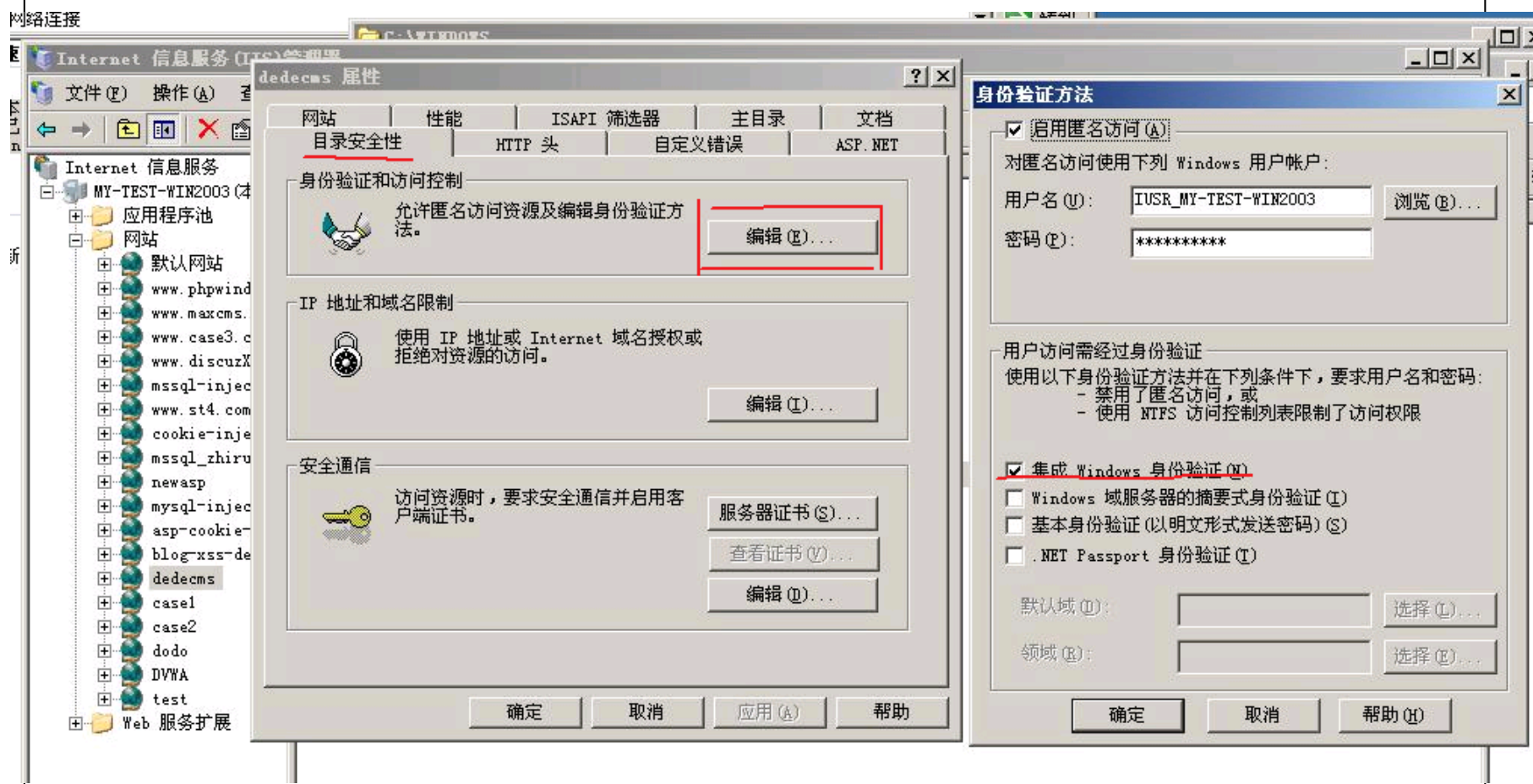
1.设置目录属性不能运行脚本文件

这里有三个选项，分别是无，纯脚本，还有一个是脚本和可执行文件。

这里我们选择无



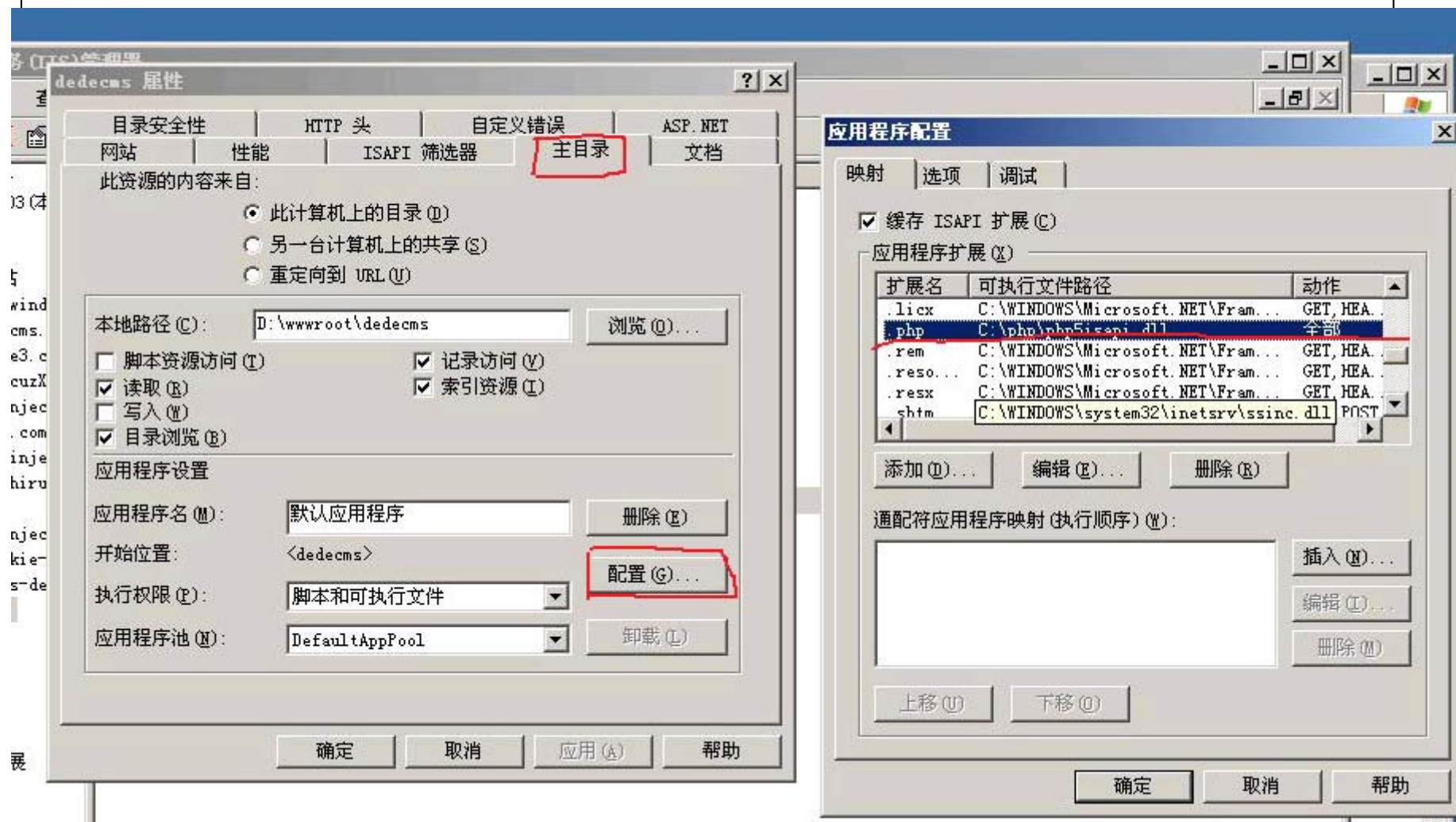
- 2.给特定的目录上集成Windows 2003的身份验证功能，例如后台的设置。



访问的时候就会另外要求输入操作系统的登陆密码



- 3.服务器只支持php其他任何脚本都不支持



• 4.对网站用户的权限设置

将网站目录对匿名网站用户访问设置为不可写，但对图片目录等需要可写的目录设置为可写。

