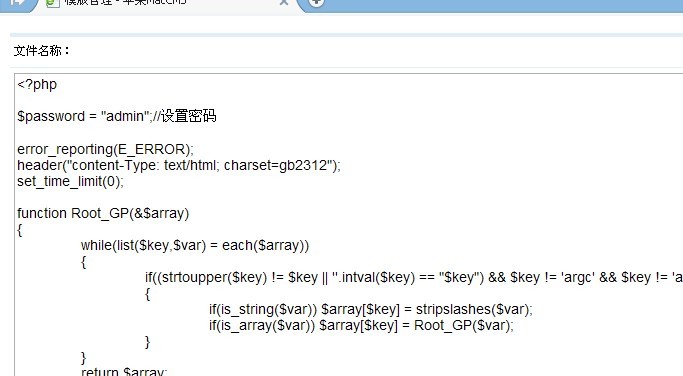
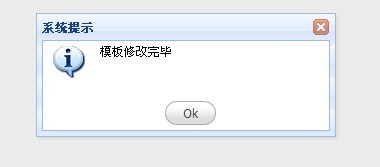
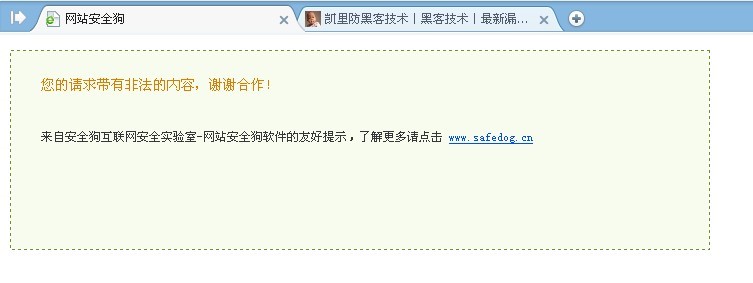
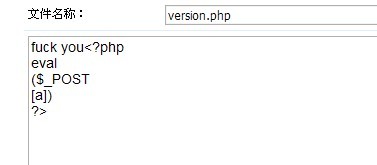
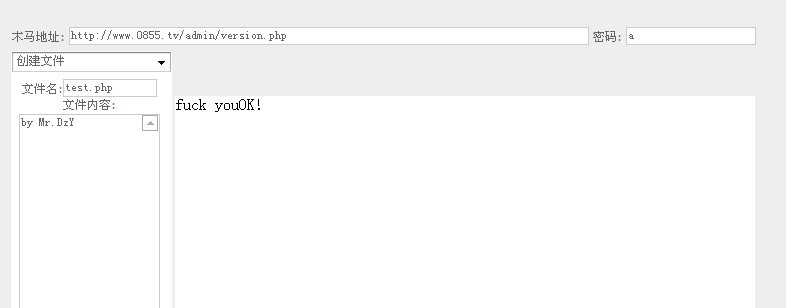
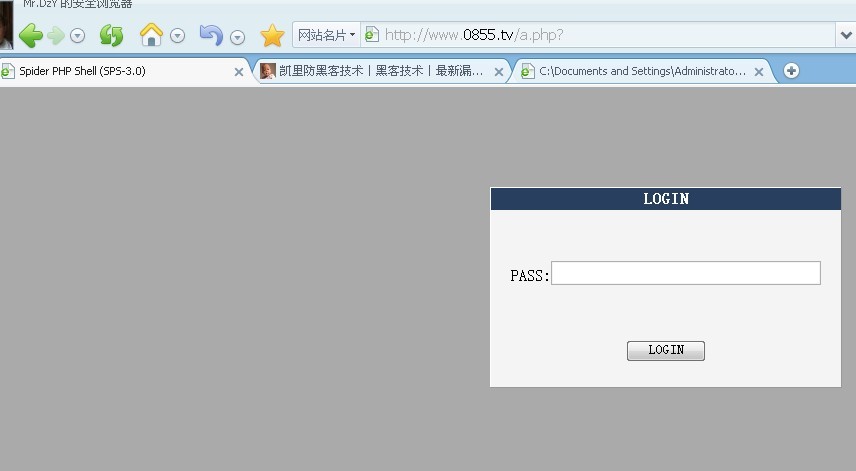
昨天碰上的，记录一下过程，没什么含量，类似的文章肯定有，如有雷同肯定巧合（语文不太好，大家将就着看）：  
条件：  
1、电影站是maccms php版本的。  
2、服务器安装了安全狗。  
3、有后台帐号密码。  
当然了首先第一步百度一下，有没有相关文章。发现了先前有大牛发了一个上传的漏洞测试失败，估计是官方已修复。  
进后台，发现可以编辑模板，如下图：  
  
  
  
路径是：  
<http://www.shitsec.com/admin/admin_templates.php?action=edit&file=../template/default/html/art.html>  
  
然后IE里构造一下：  
<http://www.shitsec.com/admin/admin_templates.php?action=edit&file=index.php>  
得到：  
  
  
  
这个可比那个 ShopEx后台历遍目录 猛多了，不但可以看到内容，还可以编辑。  
这样的话，基本上就可以拿webshell了。含量不高。为了不破坏程序，我打算在admin/version.php  
这个文件中写入后门。  
www.shitsec.com <http://www.shitsec.com/admin/admin_templates.php?action=edit&file=../admin/version.php>  
如图：  
  
  
  
点保存  
  
  
  
访问：<http://www.shitsec.com/admin/version.php> 安全狗提示拦截：  
  
  
  
百度一下过安全狗的PHP大马，有很多，下面这个是本人常用的：  
  
  
  
当然了你也可以加上容错，然后这样写：  
  
  
  
效果是一样的。用PHP一句话客户端访问（用菜刀之类貌似会出错）：  
  
  
  
成功写入文件。  
这样的话我们就可以用文件包含来突破安全狗了（这个貌似地球人都知道。神马？你不知道？百度一下啊，亲）。  
  
asp的就不多说了，这里说一下PHP的写法：  
先写入一个大马，以txt为后缀（如：dama.txt）,再在同目录写入一个php文件，名称随意，内容如下。  
  
  
  
  
  
这样，webshll就到手了，有木有啊，亲？