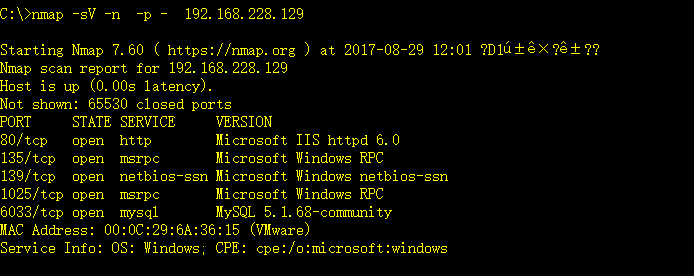


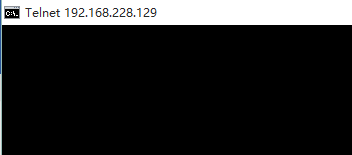
首先使用对主机进行了端口扫描

端口扫描

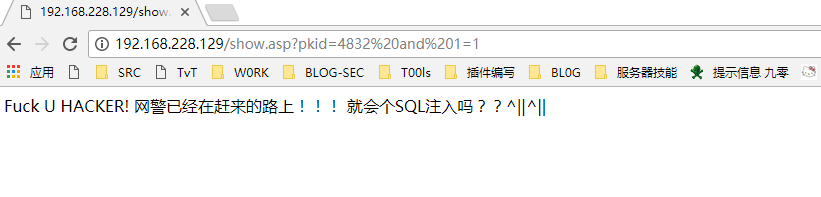


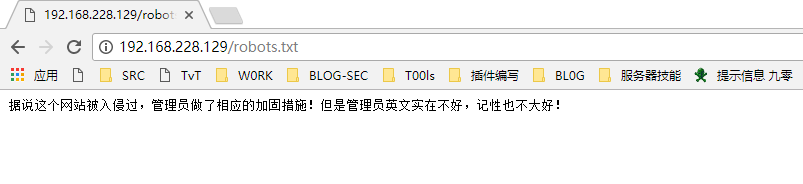
通过扫描可以知道

开通了80 及 6033 可以看出是mysql 测试发现允许外链，可以进行爆破获取flag



通过扫描web站点可知道有网站有防护





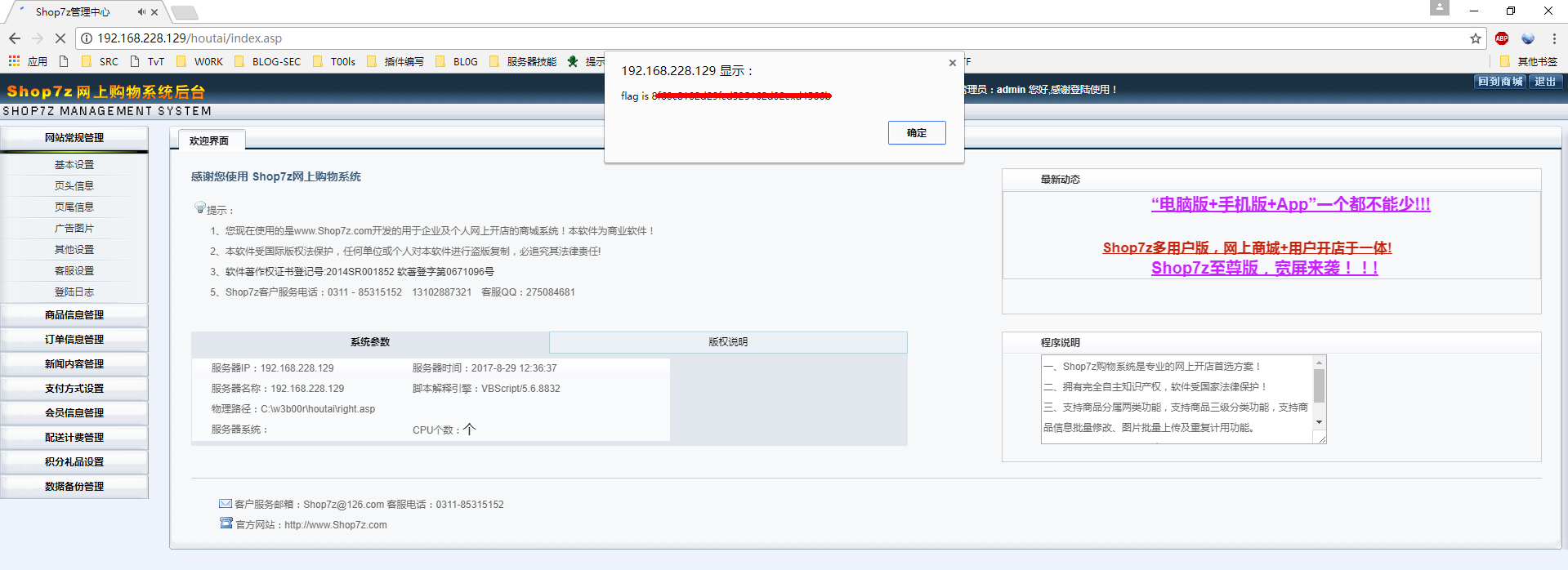
扫描或猜测出后台

<http://192.168.228.129/houtai/login.asp>



测试验证码无效

登陆后台

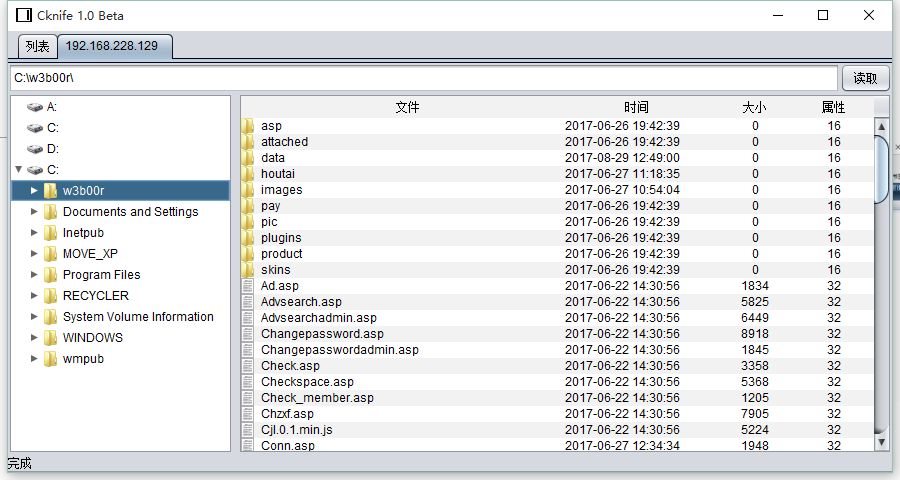


登陆后台

上传cer文件图片马



<http://192.168.228.129/product/uploadimages/178291247331.cer>



上传CMD、上传3389、上传开启远程bat文件3389.bat进行提权即可。