**不知道大家那是不是这样的，一中和二中很多时候在小县城里都是最好的两所高中。作为这两所学校里的人，很多时候也就带上了敌意，恨不得让彼此出丑！**

**接触网络安全（暂且这样称呼）一来，心里一直想拿下对方学校的网站。以前也翻过几次学校的网页，纯静态！都放弃了。外面下大雨，闲来无事又想去搞下那个网站，这次再搞不下，真的就准备放弃一段时间了。**

**开始翻页面，都是静态的，想从主站进行注入看来是没有戏了**

****

     没办法了，只能旁注了。打开114best.com，查询了一下，运气还不错，同服务器的有十多个网站，都是我们那的政府等等的

开始一个一个的检测了

出现以下的提示，心里凉了，恐怕也注入不了了，难道真的要杯具么



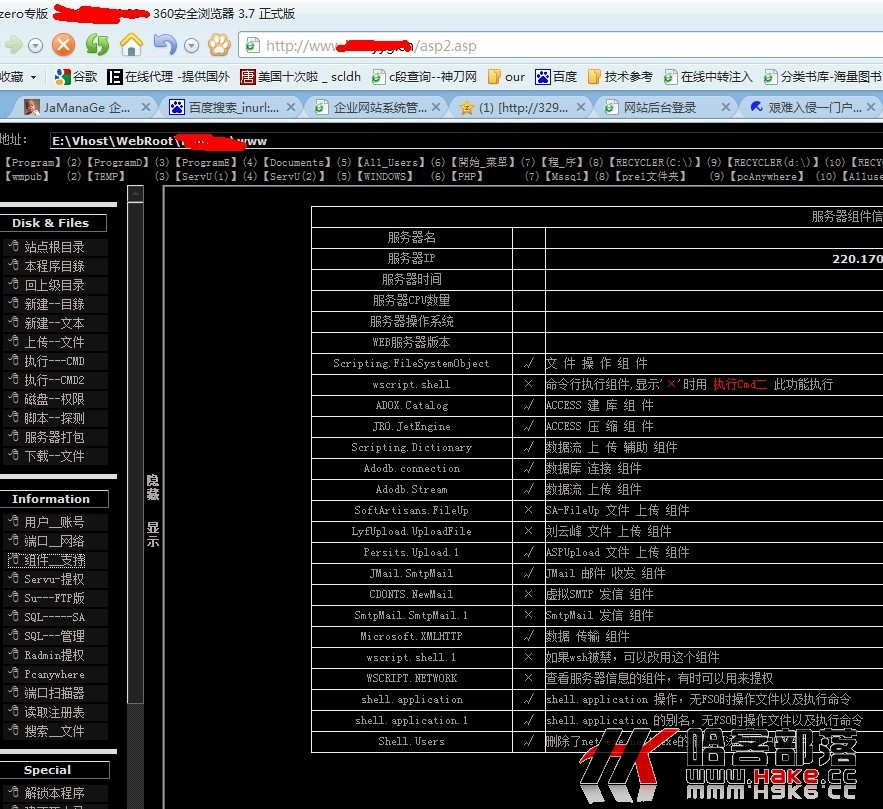
   换了好几个站，都是这样，若无其事的

在一个网站的后面加了个login.asp，跳转到管理员页面，怀着碰运气的态度

输入admin，admin成功进入，



有备份，而且备份功能完好，拿shell就不成问题了。上传图片马，备份拿到shell



Wscript组建被删除，提权路径就少了许多了

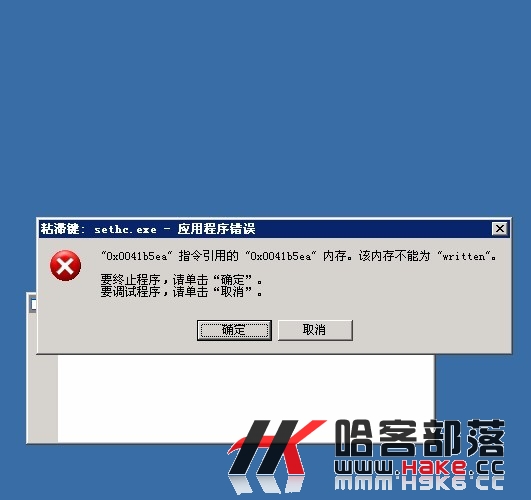
扫描了下端口，发现有seru服务，开放了3389，随手点击了su提权

然后在账号那里惊喜得的看到admin$

立即远程连接，成功登陆



不久前在某人的博客上看到过一个T00ls Lpk Sethc 后门，感觉相当的好用，配置好后，执行，却出现了以下提示



     这次入侵完全是运气使然加上一点点的侥幸，无技术含量，希望大家不要见笑

不知道该怎么解决了，希望大家可以给出意见。。。。