文字版的！不想再去检测一次！呵呵！  
踩点！呵呵！那个站是个asp的站！没有发现注入点！没有发现编辑器！没有发现上传！也没发现后台！没有神马能利用的！我就想起了旁站！从旁站上去了！结果发现组件全部被删掉！aspx支持！星外的系统！我找了一个目录写cmd！能set！挺高兴的！结果蛋疼了!pr提权试了！鸽子试了！烤肉试了！反正能试的都试了！就是提不上权限！纠结啊！不过突然想起tpye命令！不过没办法爆出那个主站的目录！木有办法！C:\7i24.com\iissafe\log\在这个目录跟一些其他目录！都翻了！最后在一个日志里面翻到那个主站的目录！试着tpye了一下！结果成功了！哇哈哈！rp不错！虽然注册还有一些提权的方法没有搞到服务器！但是我拿下主站就算完成任务！直接去去读那个站的登录文件！因为登录文件有连接数据的东西！避免盲目的去找数据库连接文件！浪费时间！拿到数据库！直接连接！破个md5！直接上去拿shell！呵呵！小小淫荡一把！  
  
星外常用可写目录 C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index\,C:\php\PEAR\,C:\Program Files\Zend\ZendOptimizer-3.3.0\,C:\Program Files\Common Files\,C:\7i24.com\iissafe\log\,C:\RECYCLER,C:\windows\temp\,C:\Program Files\Microsoft SQL Server\90\Shared\ErrorDumps\,e:\recycler\,f:\recycler\,C:\Program Files\Symantec AntiVirus\SAVRT\,C:\WINDOWS\7i24.com\FreeHost,C:\php\dev,C:\~1,C:\System Volume Information,C:\Program Files\Zend\ZendOptimizer-3.3.0\docs,C:\Documents and Settings\All Users\DRM\,C:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection,C:\Documents and Settings\All Users\Application Data\360safe\softmgr