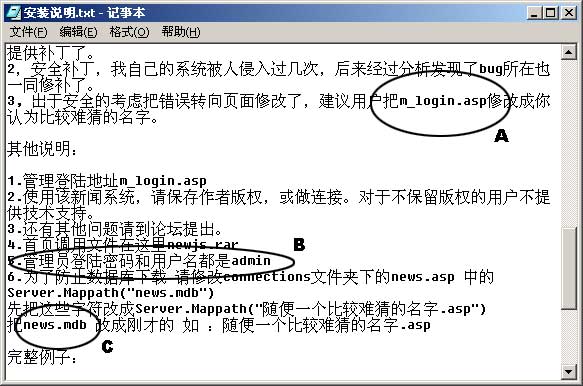
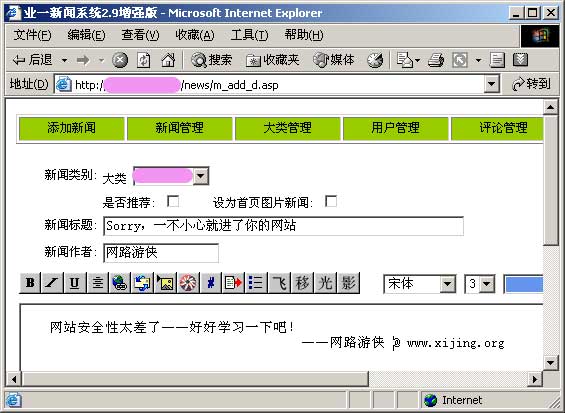
看到这个题目可能很多人感到奇怪:黑客不是都在埋头学Perl、溢出、SQL注入……?怎么又来了一个社会工程学?  
  
下面我们就来聊一下社会工程学入侵:  
  
当然，社会工程学的原本意思我就不详细解释了，因为我看了很久都没有看出是什么意思来，枯燥的厉害，是架着眼镜的老先生研究的问题，我们不去考虑。我们说的是社会工程学在信息安全方面的实现。  
  
基本的意思就是:利用一切途径、手段，搜集攻击目标的资料，然后利用已知资料攻陷对方。比如某某网站的站长在他那里发表了很多不利于我的言论，要是他在我面前，我立刻会扑上去咬死他(好在不在我面前，呵呵)，但是我却是一个技术菜鸟，什么注入、溢出、脚本之类的一点也不懂，怎么办?就此罢休?——当然不!下面就看我是如何搞定一个网站的。OK，Let’s go!  
  
首先……打开我要攻击的网站，首先看看各个页面，浏览一下。就好比小偷在下手之前要先查看一下身边的地形、人群一样，就是“踩点”了。首页做的不怎么样，有个新闻系统，点一条新闻之后弹出页面，看了就很熟悉。在[www.target.com/news](http://www.target.com/news) 后面添加admin进入管理目录看看，因为很多管理系统这个都是默认的管理目录。结果无法显示，又用admin.asp和login.asp这两个使用频率很高的文件，也无法显示。结果一看浏览器的标题栏，赫然写着“业一新闻系统2.9增强版”!好像网上比较多哦。下载一个看看!  
  
立刻上[www.baidu.com](http://www.baidu.com/)搜索一下“业一新闻系统2.9增强版”。找到了用这个做新闻系统的，但是没有找到这个的下载，但是找到了他们的官方网站，于是下载了一个“业一新闻系统2.9专业版”，应该都差不多吧。  
  
有个“安装说明”，打开看看(图1):  
  
http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

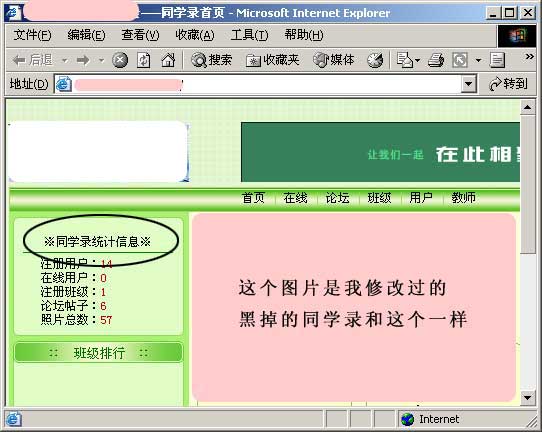
http://forum.chinesehonker.org/images/attachicons/image.gif[h1.jpg](http://forum.chinesehonker.org/attachment.php?aid=37&nothumb=yes) (51.36 KB)

2009-5-8 13:15

上面的三处地方:  
  
A、我们知道了后台管理的文件是m\_login.asp，为进入后台奠定第一步，否则即时有管理员权限也没有地方管理 J  
  
B、默认的用户名和密码，这年头真的有人不修改就直接用的，我以前曾经用默认用户名和密码黑过不少留言本和其它类似的系统。  
  
C、默认的数据库名称news.mdb，是Access的数据库，在浏览器可以直接下载的。  
  
现在我们开始第一步，进入[www.target.com/news/m\_login.asp](http://www.target.com/news/m_login.asp)，显示出要管理员登陆的界面。用默认的用户名admin、密码admin看看，提示错误。然后呢?在浏览器写上[www.target.com/news/news.mcb](http://www.target.com/news/news.mcb)就是默认的数据库路径了，回车。  
  
天啊——居然提示文件下载!幸福ing……保存。用Office组件中的Access打开，终于看到了数据库里面的文件。本想还要再下载一个破解Access数据库的东东来者，结果数据库没有加密。嘿嘿，用户名target、密码target。用这个登陆m\_login.asp成功(图2):   
  
http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[h2.jpg](http://forum.chinesehonker.org/attachment.php?aid=38&nothumb=yes) (40.19 KB)

2009-5-8 13:15

还是添加一条新闻警告一下吧，谁叫他这么大意的!^\_^  
  
搞定了这里，事情当然还没有完，网站是由几个网上下载的整站程序组成的。我们看看动画欣赏的版面，感觉还凑合。在浏览器写上<http://donghua.target.com/admin.asp>，无法显示，把admin.asp改成login.asp，跳出了超级管理登陆的界面。  
  
用户名和密码用admin，失败。换成新闻系统的，因为很多人都用一个密码的。使用target登陆成功!好的，现在动画站的控制权又到了小菜鸟我的手中。^\_^  
  
太简单了吧，一点挑战的意思都没有。随手打开网站的一个文章子站，用的是“动力文章”管理系统。页面最下面有“管理登陆”。方便，不用费心找管理文件了，呵呵。尝试了一下上面的几个密码，没有成功。  
  
怎么办?还是和搞定新闻系统的一样，从网上down一个动力文章管理系统。发现默认的数据库文件是.asp结尾的。相信站长必然不会改成.mdb了，这样就没办法下载了。难道就没有办法了?不行，不能这么放弃。继续猜解密码!  
  
尝试了几个比较无聊的数字，像123、123456、abc、iloveyou之类的之后，我敲上了target520，结果——成功了!嘿嘿，又一只羊落入狼口了。^\_^  
  
还有什么好玩的?还有校友录。恩，打开看看，界面还是很不错的哦。看站长的水平一定不是自己做的，好像找人做的可能性也不大。那就只有一条路，就是从网上下载的校友录整站程序。哪一种呢?不清楚。  
  
尝试admin目录、admin.asp和login.asp文件，不成功。  
  
看看同学录首页，仔细观察一下，页面是这个样子的http://forum.chinesehonker.org/images/smilies/default/sad.gif图3)  
  
http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[h3.jpg](http://forum.chinesehonker.org/attachment.php?aid=39&nothumb=yes) (34.28 KB)

2009-5-8 13:15

看到图片中我圈中的部分了没有?选中这些字符，包括前后的两个“※”，因为包含“同学录统计信息”的页面可能很多，但是前后同时包含两个“※”的就少了。这是为了提高搜索的准确率。^\_^  
  
当然，这一下子搜出很多的。看看基本都是这个模样的。这证明了我刚才的猜想——同学录是下载的。  
  
上百度搜一下，到有asp同学录的地方看看。发现下载最高的无非是两个:红雨同学录和风月同学录。都down一个下来，放到iis目录下面。运行之后看看界面。这下子就知道了，是用的风月同学录。看一下iis目录中的文件，最像管理员登陆文件的时候sysadm\_index.asp，在浏览器写上<http://tongxuelu.target.com/sysadm_index.asp>，眼前出现了登陆的界面。   
  
尝试用上面的几种方法，均失败。难道没有别的方法了?当然不是(要不我怎么写下面的部分，怎么骗取老编的稿费?^\_^)。  
  
先注册一个用户，随便注册一个就可以。为什么?因为我们要搞到管理员的密码，而未注册用户是无法查看用户信息的。注册进入之后就可以看所有用户的详细资料了。  
  
黑了人家这么多子站，当然明白站长是哪个了吧?找到他的资料，什么电话、QQ、ICQ、生日之类的都记下，猜解密码的时候可能用上哦。看好了这些东西我回头继续猜密码，连续猜了几次不中，考虑可能这条路不对。于是回到同学录首页，突然看到了“我忘记密码了”这个按钮，相信大家都很熟悉吧?电子信箱、论坛上面都有这么个东东的。  
  
点击之后要我输入用户名，这个简单，输入刚才找到的管理员的用户名就可以了，下一步之后出现提示，要输入问题的答案。他的问题是“Q+T”，怪怪的哦，我想可能是QQ+telephone，然后输入QQ和电话的号码，连续的号码，错误，第二次中间有“+”，成功!到此把胜利的旗帜插到了同学录的山顶。^\_^  
  
本想到此结束的，但是登陆<http://tongxuelu.target.com/sysadm_index.asp>之后，发现了一个让我很吃惊的结果(图4):  
  
http://forum.chinesehonker.org/images/lzdesign/attachimg.gif

http://forum.chinesehonker.org/images/attachicons/image.gif[h4.jpg](http://forum.chinesehonker.org/attachment.php?aid=40&nothumb=yes) (41.07 KB)

2009-5-8 13:15

看到了?好恐怖哦，所有的个人资料尽显管理员眼底，包括密码等。以后再遇到这样的同学录我是打死也不敢注册了，万一管理员有点什么念头……再想想自己的QQ、信箱、论坛……用的都是一个密码……恐怖……也提醒各位读者，以后注册之前先考虑清楚:我为什么要在这里注册?注册了有没有风险?在这里注册的n多会员，密码就都在我控制之下了。我尝试了一下，很多都是信箱和QQ共用一个密码的!  
  
好了，写到这里，这次入侵也算完成了。不知道你看过之后有什么收获?  
  
其实入侵一个网站往往不像我们想象的那么难，只要你心足够细，很多网站都可以被入侵的，特别是一些个人网站。我在学校网页制作大赛的时候，就在获奖的作品里面找到了两个网站黑了，思路和这个一样，确切的说只要下载数据库就可以了。更何况，现在一些搜索引擎都可以搜索.mdb的数据库，这样以来入侵就更加简单。  
  
其实还有很多更高深的社会工程学手段。比如你想黑掉某个网站，你可以伪造邮件，获得相关人员的信任，然后练习一回口技，捏鼻子打电话之类……总之，社会工程学入侵涉及到方方面面。