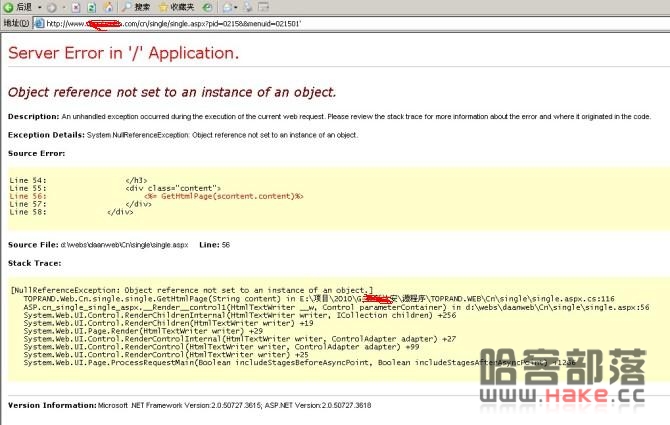
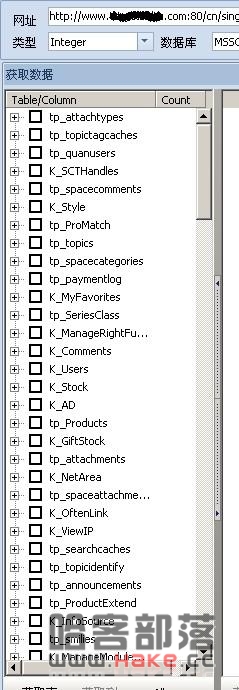
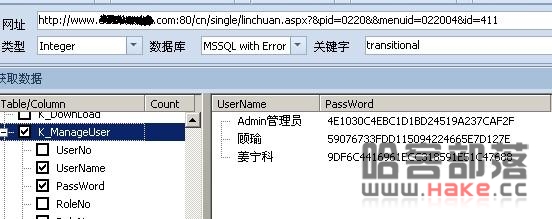
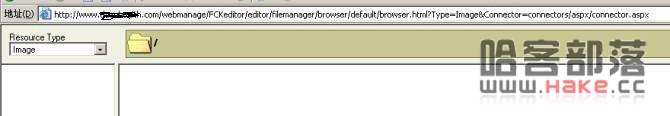
感觉异常的蛋疼,今天搞了个站,准备去博客发表的,发现不能上传图片了,貌似在博客换服务器之前从来没出现过这种情况,后来问了几位大牛,确实是服务器问题,真TM操蛋.暂时先发QQ空间,等过几天博客换服务器了再发上去,无奈.  
不扯蛋了,进入正题.  
先介绍下咱们公司:咱们公司(XX医学检验所)乃是国内外闻名的医学检验机构,内有无数专家教授,人才济济,师资力量雄厚,屹立千年不倒!  
在一个夜黑风高的夜晚,通宵没精神,无聊到蛋疼,于是乎,心血来潮,检测下咱们公司的网站.  
  
目标:[http://www.XXXX.com](http://www.xxxx.com/)  
进去看看,页面是ASPX的.  
简单的踩点:  发现服务器绑定了4个域名:  
[http://www.XXXX.com](http://www.xxxx.com/)  
[http://gz.XXXX.com](http://gz.xxxx.com/)  
[http://www.XXXXX.com](http://www.xxxxx.com/)  
[http://bbs.XXXXX.com](http://bbs.xxxxx.com/)  
其中第一个和第三个都是我们的目标站的域名.  
论坛竟然也是ASPX页面的,看起来比较像DZnt.  
gz开头的那啥是个检验结果查询系统,咱只是个外勤,自然没有帐号,猜了几个都没进去,于是忽略之.  
通过扫描器发现网站是IIS6.0,那服务器就应该是windows2003+IIS6.0,扫了下开放端口,发现开放了80,443,1521.  
当时就感觉不对劲,连21端口都不开,难道管理员不用FTP管理网站文件吗?某非是自己的服务器?  
1521是oracle数据库服务端口,这种是企业级数据库,一般一些大的不得了的网站才会用这种库,这网站怎么看都不像是用那种库的站,而且gz开头的那啥有个连接端口6006,还有9008,扫描器都没显示,初步判断有可能web服务器位于内网.并且有可能站库分离.  
  
  
先从主站入手吧,跑去目标站,随便找了个链接,顺手在参数后面加了个单引号,报错了,如图:  
  
   
  
居然连源文件物理路径都爆出来了,不知道用的啥人才网站程序,或者哪个人才程序员编写的,连提交参数都不严格过滤,当时就以为是注入漏洞,但是and 1=1  and 1=2判断了下,居然跳到百度了.无奈,换成and+1=1  and+1=2继续测试,居然不是注入漏洞,放进啊D里也提示不可注入.郁闷,从上图可以看出是single.aspx这个文件对用户提交的参数没有严格过滤,但是却不是注入漏洞,不死心,他既然一个文件能写的马虎,肯定还有其他更马虎的地方.没准能给我个惊喜,于是继续翻,搜索处sitesearch.aspx这个文件写的也有问题,在搜索框填如1提交,报错了:  
  
   
多次测试以后,发现提交的数据小于三个字符就会报错,测试中未发现XSS漏洞.  
哥接着翻......  
来回翻了近一个小时,老鼠洞都让我给翻遍了,中途还注册了个用户找上传...在快绝望的时候,终于看到了个好东西:  
  
   
看出来与第一个有什么不同没?这个提示的是未闭合,当时我就激动了,立马and+1=1    
   
页面正常显示,接着,颤抖着,and+1=2  
   
看到没?神马都木有,天哪,这叫啥?传说中的注入点终于出现鸟!!!  
立马拿去穿山甲里跑:  
  
   
证实我我之前的判断,这网站确实不是用oracle库的,使用的乃是传说中的MSSQL,也就是SQL server.  
而且注入点权限非常高,居然是SA连接数据库的.人才啊,貌似在我印象中棒子国的站最喜欢用SA用户连接数据库,一个不小心有个注入点,整台服务器沦陷,不过棒子在中国黑客们的磨练下终于学乖了,现在基本上很少见到网站用SA权限连接数据库的了.居然让我在咱们公司的站遇到个,真不知道是该庆幸还是该悲哀.  
二话不说,拿着注入点就去执行命令,执行命令的时候却蛋疼了,不管我怎么整,一执行就卡死,存储过程死活恢复不了,就算执行了他死活不回显,真是日了,居然遇到个如此蛋疼的注入点.  
算了,老老实实的去跑数据库里的表吧.  
等了将近半小时,终于列出了所有表,不得不感叹下SA权限的牛X,  
貌似把服务器上所有网站的库都列出来了  
  
   
看着那么多表,头晕啊,唉,慢慢找哪个是管理员表吧.  
从上面翻到下面,终于让我翻到个比较可疑的表名:  
   
密码是经过MD5加密的,于是就找了个CMD5高级会员的哥们帮我解密.  
然后用爬虫爬出管理员登录页面.  
解密了去登录,发现不对,无奈,继续翻,既然K\_前缀的不对,我就找其他前缀的,结果又让我找到个可疑表名  
   
这次像真的了,又麻烦了那位兄弟帮我去解密,无奈,咱穷人买不起CMD5高级会员.  
OK,这次成功登陆.  
  
   
翻了翻后台,功能并不算强大,添加文章,找上传,结果弹出的上传界面让我一愣  
   
这TMD不就是传说中的FCKeditor吗,俗称FUCKeditor.  
直接利用FCK编辑器漏洞,找到上传页面  
   
测试了下,上传功能完好,没有被阉割.  
文章开始我已经判断出服务器是Windows2003+IIS6.0  
于是乎,利用IIS6.0解析漏洞  
找个牛X大马,改名1.asp;x.jpg上传,找到上传后的大马访问  
  
   
成功拿到webshell.  
先看下服务器配置:  
   
8H,8G内存的独立服务器,并不是虚拟主机,有钱淫http://ctc.qzs.qq.com/qzone/em/e154.gif  
补丁打的不是很全.  
再看组件支持.于是又震惊了:  
   
wscript.shell  
wscript.shell.1  
shell.application  
shell.application.1  
Shell.Users  
这几个危险的组件居然全部没删,不得不说那服务器管理员水平真可以.  
而且可以跨目录浏览服务器上所有网站,并且可读可写,就代表整个服务器上的网站全部沦陷.  
我可以在服务器上任何网站的网页上挂马,或者随意弄到网站管理员帐号,也就是说之前的那个报告单查询站,只要我想进去,随时能进,同样.心情不爽的话甚至可以把服务器上所有网站连同备份一起删除.但是咱良民,胆小年轻.更是不可能做出那等事.  
并且ASP大马权限极大.  
C盘若干个目录可写,虽然没SU,但这样的服务器提权已经毫无悬念了.  
如果是恶意入侵的,服务器硬件配置再好又有什么用?还是给别人做了嫁衣.  
直接net user添加用户失败,看来是服务器组策略做了限制,看来管理员还是有那么一点点安全意识的.  
上传CMD+PR,成功添加管理员帐号:  
16.jpg   
3389连接的时候发现操蛋了,连接不上,于是ipconfig看了下,与我踩点时的判断完全相符,服务器在内网.  
本来想本地开个端口监听,服务器上反弹个shell到本地连接的,但是我在网吧,也是内网,手头上也没有服务器给我中转,借也没借到.于是就作罢.  
在服务器上的三个站每个站上挂个页面走人.  
   
  
   
  
   
  
回头再通知公司的服务器和网站管理员吧,那管理员估计最低也是个大学本科毕业,啥啥砖家,啥啥工程师之类的,维护的服务器和网站居然存在如此低级而又严重的漏洞,真是人才啊,叹服...  
渗透至此就告一段落了,其实完全可以等回家了控制这台服务器,进一步渗透整个局域网的服务器的.但本人精力实在有限就算整个网段的服务器全拿下了貌似意义也不大,毕竟又不能自己用,我眼前的这台既然配置的漏洞百出,想来别的也好不到哪去,希望这次渗透测试能给服务器管理员敲响警钟,网络安全,最主要在于自身的安全意识.  
  
最后,感谢混蛋帮我解密MD5,感谢Azusr提供FCKeditor上传后的路径,你们的支持是小弟成功的关键.