ichunqiu在线挑战--网站综合渗透实验 writeup

转载

巷中人 于 2015-11-11 23:49:00 发布 150 收藏
文章标签： 数据库
原文链接：http://www.cnblogs.com/renzongxian/p/4957762.html

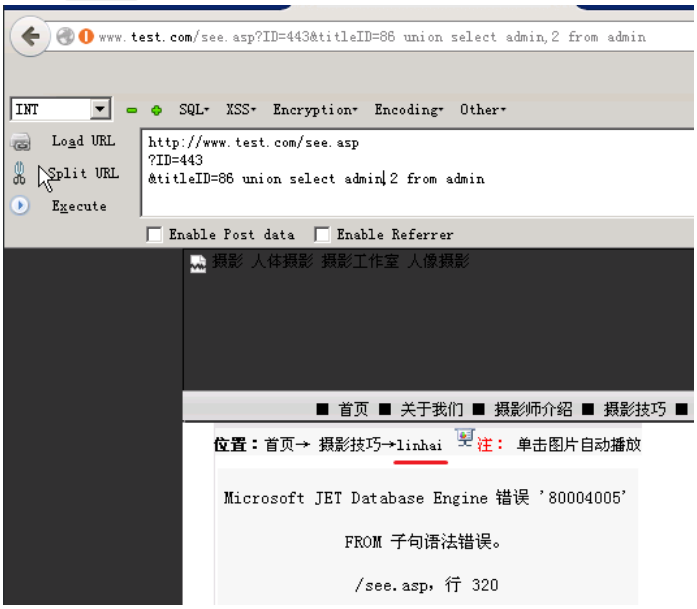
- 挑战链接：http://www.ichunqiu.com/tiaozhan/111
- 知识点：后台弱口令，md5破解，SQL Injection，写一句话木马，敏感信息泄露， 提权，登陆密码破解

这个挑战与“我很简单，请不要欺负我”相比稍难一些，但大同小异，前面的一些思路这里仍然可以用到。但是一定要注意的是，看清楚问题问的是**论坛**还是**网站**，不然就呵呵了……

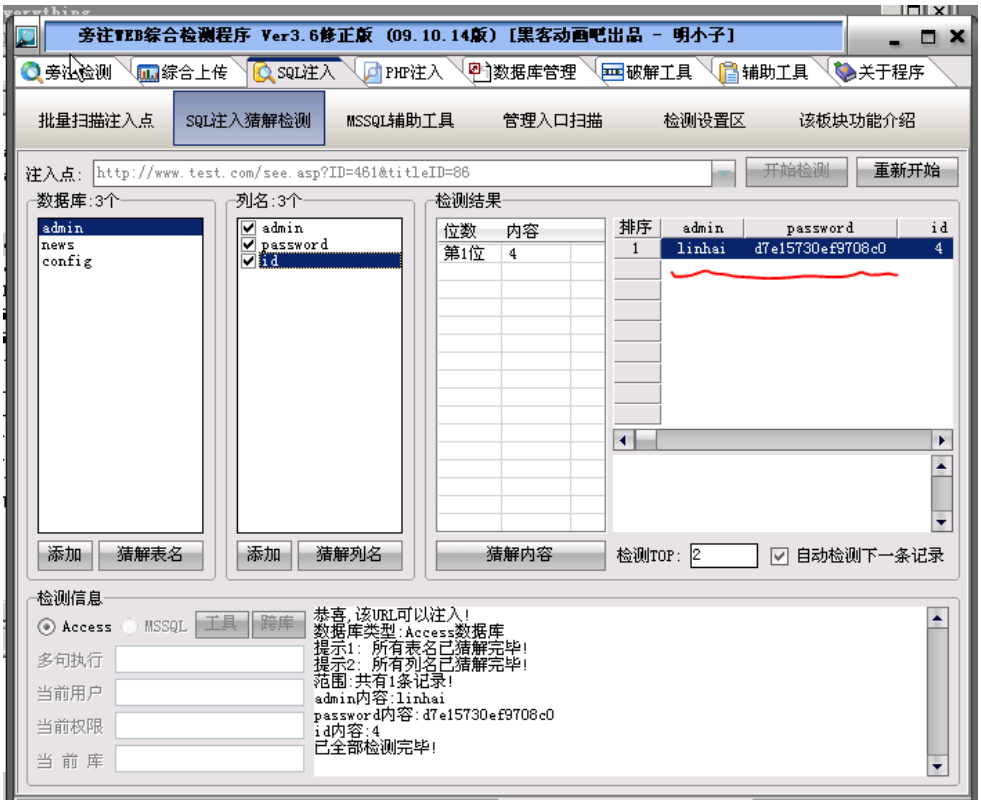
第一个问题问的是“本实验中论坛管理员`linhai`的密码是？”。首先要看到“论坛”二字，论坛管理员与网站管理员不是一回事哦。不论网站标题还是网站中都出现了“秋潮视觉工作室”的字样，感觉又是个老的CMS啊，拿出谷歌一搜，果不其然，见下图。拿linhai，123456作为账号密码登录一下后台，成功了！

第二个问题是“本实验中论坛可否获得Webshell？”。登录到论坛后台后，尝试寻找能写一句话的地方。图片上传限制的非常严格，不仅限制后缀还会完全改写文件名。也没有能改写网站文件的地方。从目前来看，论坛应该是不能获得Webshell了。

第三个问题是“本实验中SQL Server数据库sa账号的密码是？”。说实话从第二题到第三题感觉跳跃性有点大……从网站的底部可以看见有一个网站后台入口，试了几次弱口令没成功，想想应该不会又是弱口令（否则这挑战邮电无聊……），那看看有没有SQL注入吧。由于网站后台上已经表明了“Asp+Access”，知道是Access数据库，在论坛这边找诸如点（用`and 1=1`和`and 1=2`测），毛也没找到……在网站上找，感觉好多地方应该有，然而并没有这么理想……终于，找到了一个注入点，手工瞎猜试试，表名，列名倒是挺好猜的，如下图获得登录名`linhai`，不过有点碰运气的感觉……

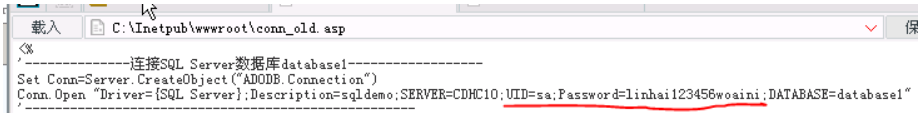


还是用工具爆一下比较靠谱，请出Domain3.6，很快出结果了，见下图，把password解md5得`linhai19760812`，我是用在线md5解密得到的，如果离线破解的话，可能就要用到社会工程学字典生成器，结合linhai出生在唐山大地震时期（1976年），还有他的邮箱头（torrow0812）来生成字典，然后用MD5Crack2加载字典破解，不过生成字典也是个巧活……



有了账号密码可以登录网站后台了，看看后台都有什么功能。“系统管理”，“数据管理”这两个应该是很重要的功能，“系统管理”中的功能应该会更改网站的文件，而“数据管理”提供了数据库文件的路径（开始我以为数据库文件里会保存sa账号密码呢，结果一看乱码一堆……），猜测这个数据库文件应该也会保存“系统管理”中的配置，于是我们在“系统管理”下的“友情链接管理”功能中写入一句话，见下图。

路径是http://www.test.com/db/bear.asp，密码为1，菜刀连接！现在我们可以看到该网站的所有文件了，那么问题就来了，怎么找到数据库中sa账户的密码呢？由于自己以前也动手做过简单的网站，通常为了省事就把数据库的口令直接写连接数据库的语句中，这个网站会不会也是这样呢？我们查找网站目录下的文件，发现了conn.asp与conn_old.asp两个可能跟数据库连接相关的文件，分别打开看看，在conn_old.asp中发现了端倪，如下图所示，sa的密码出现了！



```
Set rs=conn.Execute("SELECT * FROM table2") '返回数据表table2中的所有记录
```

接下来便是最后一个问题了，“获取管理目标服务器密码”。已经有菜刀获取的Webshell了，接下来的工作就跟ichunqiu在线挑战—我很简单，请不要欺负我 writeup一样了，提权，获取Administrator用户的密码HASH，然后解密，就能得到密码`88hvpebv`，提交，OK！

转载于:https://www.cnblogs.com/renzongxian/p/4957762.html