

RE: SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-06/0073.html>

From: Breidenbach, Beth (Beth.Breidenbach@getronics.com)

Date: 06/12/02

Date: Wed, 12 Jun 2002 13:40:44 -0700

From: "Breidenbach, Beth" <Beth.Breidenbach@getronics.com>

To: "Sverre H. Huseby" <shh@thathost.com>

My apologies -- I live in the SQLServer world and regularly take advantage of multiple statement batches as well.

Agreed that the word "hole" is misapplied -- better to have said something along the lines of "feature that could be misused if the application coder is sloppy." :-)

Anyway, there was no intent to imply any of the db engines is superior to the rest (it's just not a religious issue for me) -- each has different features and the developer should know the particulars of the database s/he is coding against.

Beth

-----Original Message-----

From: Sverre H. Huseby [<mailto:shh@thathost.com>]

Sent: Wednesday, June 12, 2002 1:35 PM

To: Breidenbach, Beth

Cc: Qyves; pen-test@securityfocus.com

Subject: Re: SQL Injection

[Breidenbach, Beth]

| Oracle doesn't support sending multiple, semi-colon delimited
| statements such as you are describing. That particular hole is
| generally only seen with Postres and SQLServer (and a few MySQL
| modules).

I may misunderstand your statement, but here it goes anyway:

As a die hard fan of PostgreSQL, I must object when you call the support for multiple statements a "hole". The hole is not in what the RDBMS supports. It is in how the caller passes data to the RDBMS.

Even if Oracle and others does not support multiple statements in a single request, attackers may gain access to information that is not for their eyes using other constructs if the application programmer is sloppy when it comes to input validation and meta character handling.

SecurityFocus Penetration: RE: SQL Injection

Would you call that a "hole" in Oracle? Probably not.

With support for multiple statements an attacker may more easily do more harm, but it is still the application programmer that is to blame, not the database.

Just my two cents, or whatever you say over there.

Sverre.

--

shh@thathost.com

Computer Geek? Try my Nerd Quiz

<http://shh.thathost.com/http://nerdquiz.thathost.com/>

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:* [Sverre H. Huseby: "Re: SQL Injection"](#)
- *Maybe in reply to:* [Qyves: "SQL Injection"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)