

## R: [Full-Disclosure] sql injection question

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-10/0942.html>

---

**From:** Manuel [ekerazha] ([ekerazha\\_at\\_yahoo.it](mailto:ekerazha_at_yahoo.it))

**Date:** 10/15/03

To: <[full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)>

Date: Wed, 15 Oct 2003 18:48:00 +0200

Yeah... you are vulnerable to sql-injection.

You have to replace the single quotes with two quotes in the postdata received from the search form.

ASP Ex: `Replace(Request.QueryString("SOMETHING"), "'", "' '")`

Byeee ;-)

P.S.

Excuse me for my english :S

-----Messaggio originale-----

Da: [full-disclosure-admin@lists.netsys.com](mailto:full-disclosure-admin@lists.netsys.com)

[<mailto:full-disclosure-admin@lists.netsys.com>] Per conto di Richard Stevens

Inviato: mercoledì 15 ottobre 2003 17.58

A: [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)

Cc: David Rees

Oggetto: [Full-Disclosure] sql injection question

Quick question for the list, if I may,

We have a third party application that we are piloting for using as web store front end.

I have no idea on programming sql at all, but have read of some of the sql injection techniques on this list.

In the search box on the app, by inserting ' followed by a space, the following message is generated:

---

-----  
Technical Information (for support personnel)  
Error Type:  
Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)  
[Microsoft][ODBC SQL Server Driver][SQL Server]Line 1: Incorrect syntax near  
' insert into @promptable select a.ItemCode, a.SysNumber, a.TechDescription,  
a.InvoiceDescription, a.Classification, a.ProductGrou'.

R: [Full-Disclosure] sql injection question

## Full-Disclosure: R: [Full-Disclosure] sql injection question

/eshop/search.asp, line 265

Browser Type:

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)

Page:

GET

/eshop/search.asp?SessionId=PR10006210200315411635Q3TLJ310ELW679PQ7Y&QuickSearch=%27+

Time:

Wednesday, October 15, 2003, 4:45:30 PM

Also, the password for SA is stored in clear text in the site in a text config file. This would not strike me as being sensible.

These are both ringing alarm bells !

From this info, would you assume it would be easy for someone skilled in sql injection to get unauthorised access to the database?.. or is it not that simple?

The input seems to be filtered correctly on the logon.asp, as entering these characters has no apparent effect.

TIA

Richard

---

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

---

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>