/

help with SQL injection in quick search form field to find number of items to purchase

✉ You are subscribed. Unsubscribe   ❓ UNRESOLVED   ⚙

🏷 **SQLinjectionOnQuickItemSearch** ×   + Add Tag   Sort replies by: Oldest first   Newest first   Most popular

---

🔲 Karen West · 3 hours ago 🔗   ⚙

From the bad store manual, it recommended the following SQL injection to enter in the Quick Item Search but it did not work - any further recommendations? I'm trying to find the correct number of items for purchase since I know what you can actually see on the What's New page is not correct. The bad store manual says if you enter this SQL injection in the quick item search, you should see all items for sale including the test items, but the only thing I get is an error message. Does anyone know what I'm doing wrong with my SQL Injection? It said by entering the following SQL Injection: "The ' (tick mark) character is used to delineate variables in a SQL query, and 1=1 always evaluates as True. So, what we're doing in this simple example is telling the web application to evaluate our request as valid, potentially bypassing application security controls." Any help appreciated! The SQL injection they recommended in the manual for this was:
1001' OR 1=1 OR '1002

No items matched your search criteria:

SELECT itemnum, sdesc, ldesc, price FROM itemdb WHERE '1001' OR 1=1 OR '1002' IN (itemnum,sdesc,ldesc)

⬆ 0 ⬇ · flag

Stewart Bell · 8 minutes ago ⧉

Is ' the same as ' ?

Glad you got your VM working again, it seems it wasn't quite the 11th hour after all. Good heads up by Dionysios there about applying the extra days!

⬆ 0 ⬇ · flag

Karen West · just now ⧉ ⚙

Yes - I had not known about that until yesterday so that was good news for me. ;-)

As for the SQL injection - I just made a separate post on that, since I still don't understand why '# (tick mark followed by hash symbol/pound sign) at the end of the login's or in the quick item search bypasses security. It worked but I don't know why. Would I better understand if I examined some of the source code for that web page? Or is there something else I'm missing there?

I have no idea why the VM started to work again - I went back to the first bad store VM I had installed and it was able to get an IP address and I was able to finish the assignment today. I'm glad it worked but I wish I knew why it did not work in case it happens again, I better know how to solve the problem.

Thanks for the responses!

⬆ 0 ⬇ · flag

+ Comment

New post

To ensure a positive and productive discussion, please read our forum posting policies before posting.

| **B** | *I* | ☰ | ☷ | % Link | <code> | 🖼 Pic | Math | | Edit: Rich ▾ | Preview |

☐ Resolve thread

This thread is marked as unresolved. If the problem is fixed, please check the above box and make a post to let staff know that they no longer need to monitor this thread.

☐ Make this post anonymous to other students

☑ Subscribe to this thread at the same time

Add post