Forums / Assignments Help

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 · 2 days 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 · 2 days 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 · 2 days ago

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

Stewart Bell · 9 hours ago

Hi Karen, top marks for your tenacity, sleuthly decipherings, and seemingly maniacal dedication :) I imagine that, despite the frustrations, it's also been a week finely rewarded with increased knowledge, and a better score to boot!

I'm pretty much new to SQL myself so I'm afraid I'm barely beyond understanding anything but the basic concept of mangling the parsing of the query in some way. Still one of many things on my list of things to suss.

From my limited understanding, I doubt the source code of the page would help in figuring out what query to enter as the SQL-related code resides server-side. However, in the case of the poorly sanitised BadStore, a malformed query, such as the one you mention above, may return some information about the format of the query that the server expects. This, in turn, may help an attacker refine the structure of their input.

With regard to the initial SQLi you tried, example 2 here - https://www.owasp.org/index.php/SQL_Injection - may serve to shed a little more light on it. This page is worth bookmarking too I reckon: http://www.w3schools.com/sql/sql_injection.asp. I've not got round to looking at the '# just yet.

I mentioned the tick ('), in contrast to the backquote character (`) as the query 1001' OR 1=1 OR '1002 worked for me. (Remember the gdb -p `pgrep wisdom-alt` command from the first project where backquotes had to be used rather than single-quote ticks. I was thinking such specificity is also required here, namely that the SQLi has to use the tick character, and that maybe you'd entered backquotes instead which is why it proved ineffective.)

Speaking of ticks, I can hear the clock a-tick-tocking. All too loudly! Week 5 material beckons, and from what I've seen of it so far... Oh boy, I might well be applying some late days myself this time round! :/

May the Gods of Comprehension smile upon us. At least the project uses the same VM as the first week's, so hopefully no major woes for you on that front this time round. I'm sure your son will be happy about it too - he can have his laptop back now! :)

↑ 0 ↓ · flag

Kevin Tam Signature Track · 9 hours ago

Karen, for your education, try putting in something like
'foobar

and it will probably complain with something like "Invalid SQL" and print out the SQL string. From that, you can guess what the query looks like with '#

To answer your question anyway, it looks like that # is the comment symbol in use for whatever database this is.

↑ 0 ↓ · flag

Karen West · 4 minutes ago

Stewart Bell:
I laughed when I saw your post first thing this Thanksgiving day holiday morning for the US (my entire house still sleeping, so I can do a bit of work for a short time!) Yes - I'm unemployed right now, and when my 9 and 11 year old kids and overworked husband are not interrupting, I'm almost "maniacal" in my dedication to solve problems I may be having in an online course! When I first lost my job, a friend suggested that I "expand" my skill set outside my Electrical Engineering and Embedded C programming I had done for 18 years, since the market was not hiring for that as much at that time, and I find sometimes when I take these CS or IT classes, I'm at a definite disadvantage to those who may have been better exposed to these tricks that I am trying to learn for fun while stuck at home! ;-) My next thought with your humorous comment was that you might be British - since my husband is from England and their culture and comments revolve around joking approaches to life's challenges, but then again anyone who deals with life in a joking manor would say it that way, but with me being from the US, I have observed a definite cultural difference in the amount of joking his country does verses mine.

I've been unemployed 5+ years in the Boston,MA area, and never planned life this way, so I do work hard at everything I do, even it's an online course where I never know if it will be helpful in what ever job I get in life! "top marks for your tenacity, sleuthly decipherings, and seemingly maniacal dedication :) I imagine that, despite the frustrations, it's also been a week finely rewarded with increased knowledge, and a better score to boot!" The sleuthly decipherings were tougher in this case since it was beyond just knowing any syntax of a new language well, but also in knowing how to trick the system. I was honest though in that although I'm very happy when I get a good grade online, it's all about the learning that is important to me. In some online classes I've taken I've gotten a bad grade on something where I learned so much from the experience that I did not care! I've even posted some projects like that online in my shared projects section on Linked In, to demonstrate the complicated solution, even if I got it wrong, to demonstrate having learned from the experience. In terms of being a sleuth--I could never be a sleuth like Sherlock Holmes but if someone goes a bit slower in their explanation pace such as Watson, perhaps I can. ;-)

I will bookmark those pages on SQL injection that you shared. Not only did I book mark all the things I've discovered in this class (and others that were brand new areas of expertise to me that I've done in the free online space) but I often print an entire discussion forum comment chain to a pdf file to save it for future reference in the class directory, in the event I lose the book mark! I've done that for some of the interesting "humanity" type conversations I've had too, in case I ever want to reference it, since I'm not one of those that if I don't reference something for awhile, it stays in my head - have to look it up!

I also recall the back quote verses tick mark thing from the first assignment, and now I'm not sure if the first time I attempted the SQL injection, if I used the back quote or the tick mark! I know that the time that it worked when I used the tick mark follwed by # character, it did not work when I did the tick mark followed by --[space char], yet that was the example that worked in the class video. And not having been exposed to what some may have seen in their database or other IT and-or security classes, I had no idea and wasted a ton of time trying to figure that out!

In your comment about " I doubt the source code of the page would help in figuring out what query to enter as the SQL-related code resides server-side. However, in the case of the poorly sanitised BadStore, a malformed query, such as the one you mention above, may return some information about the format of the query that the server expects. This, in turn, may help an attacker refine the structure of their input." -- someone else in these many discussion forums commented that in the case of gaining "admin privilege" - that I could have modified the web page source code, so on this comment, I still do have a question--this person meant the client browser side web page code, the web page source code that I saw when I examined the login-register web page's source with the FireFox developer tools? I am new to the web world so I'm a bit confused here, since you said modifying web page code would not get me anywhere. So another thing I did to waste a ton of time was to attempt to use the FireFox Developer Tools to modify the web source page that I examined for the Login-Register link. I saw the hidden field "role" and though - well if I know how to use this web page editor, I can just change the "U" for common user to "A" for admin level privilege, changing the Value field of the hidden role field. So someone responded that I could have done that (if I did not use SQL injection to gain access instead), that if I had "double clicked" the Value field I could have used the "Inspector" tool to modify the value of the registered login from U to A level privilege by default. I never went back to try it though - so far behind already as you noticed! I'm just starting the week 5 videos this morning, and that quiz is due Monday, and with the Thanksgiving holiday today, what they call "Black Friday" tomorrow in the US (Big sale-shopping day for Christmas and a day off from school for the kids), it's going to be a challenge to get it done - but as you observed - in my maniacal fashion, it will get done - it's just a quiz, not a project that has the potential to stump me where I have to ask questions online to get through it! So I did not go back to try this--and I've been finishing up other online classes as well as applying for jobs, updated my resume(CV) to submit since my goal is to work ASAP, not take online classes, so I just did not have time to back and double check this person's comment yet. But now with your comment that you don't think you can modify web page source code because most of the code is on the server side? If you or someone else has any time left to clear up this last bit of learning confusion, that would actually be helpful!

I do understand that the client's code resides on my local machine in the browser, where I was examining the source with the tools and thought I could modify to gain admin privilege had I figured out how to make that value change with that tool before someone else helped me get there with SQL injection instead. However - did you say that this would not work? I know the server is the web store code that the VM was running (albeit on my local machine, not in another machine location) and it would respond back to my web browser with responses to my bad store web page running in the browser as the client on my machine. That's about as far as I get with this though - any further clarification on why this would or would not work would actually be furthering my education here! I know the browser client is sending HTTP requests to the badstore server VM who responds back to my client browser--but I'm not clear on why I can't modify the web page source code I saw when I "examined source" and saw the hidden role field, and why I could not just change the U to an A there and gain admin access that way too. I took an introductory web apps class about 1.5 years ago, and it used Ruby on Rails, and I started to learn about their MVC (model/view/controller) architecture of web apps, but I got so lost in the Ruby language combined with new web app structuring, that I just made it through, passed with a certificate at an introductory level, but never got beyond that, and I know there are gaps to be filled there! I was taking other demanding classes at the same time and had not expected to find it challenging but I did. When I first did client-server programming in 1993, before the world of the web began, and it is actually how I met my husband as my project partner way back when at our first grad.

school, we simply wrote C code as the client and server, socket communications all done in C (which I can see is easy to break into in this class, at least at the app level, rather than OS level where you really need it to be C for performance reasons), TCP/IP connections with RSA encrypted/decrypted packet keys, maintained a file database using C, and followed some Commitment protocol, where we had to undo the log files (not using any relational database-regular files) if the transaction did not complete successfully, etc. There was no HTTP web protocol to follow or web app structure, and life was simple. So this is all fairly new to me although I have learned it a bit at an introductory level, and apologize in advance for stupid questions! I am curious to know if that person who said I could modify the U to an A in the web page source I examined was correct.

As for project 3, I saw they are using the VM from project 1, so I may be able to again use my SUSE Linux machine that I did the first project on, rather than negotiating time on my son's Win7 lap top or confiscating it when he is at school to use and get the project done then. ;-) However, I had to use KVM QEMU to make the first project's VM work on my SUSE Linux machine, since Oracle's Virtual Box would not cooperate for me no matter how I tried for project 1! I got that project done the night before it was due too, since I started so late with trying to get my VM to work! My husband who gave me this SUSE Linux machine to use when I lost my job said it should work without issue, but I have no idea where I went wrong with getting VB to work on this machine, and he is too busy to help! So I borrowed my son's Win7 machine and some automation in that installation process must have gotten it right, since it did work there. I got KVM QEMU to work for project 1 with LOTS of help from even more kind people on the discussion forum. So I cannot predict which will work for me on project 3, but my guess is that if it uses the VM from project 1, then I can use SUSE Linux rather than negotiate time on my son's lap top. ;-)

Thank you for your help if you have time to read this long response! Happy Thanksgiving if you celebrate that holiday! ;-)

↑ ↓ · flag

Karen West · in a minute

Kevin Tam: from your comment:
for your education, try putting in something like
'foobar

and it will probably complain with something like "Invalid SQL" and print out the SQL string. From that, you can guess what the query looks like with '#

To answer your question anyway, it looks like that # is the comment symbol in use for whatever database this is.

Someone sent me a link in a discussion forum post that what you say is correct, that the '# is the same as '-- that we covered in lecture for SQL injection. So those who knew to look at the MySQL link that someone shared with me (have to look that up if you would like it) said that tick-mark-#-space is a format that many databases except since # is a comment just as --space was in the SQL injection we used in lecture.

I did try just what you said many times, enter something in the Quick Item Search that resulted in it giving me an error message of my invalid SQL, but nothing I tried worked until some people on the discussion forum clued me in on how to trick it. I took a class on introductory databases once almost 2 years ago, and we did have to format SQL statements, but I could not get this one to work.

Thanks for your help and Happy Thanksgiving if you celebrate it! ;-)

↑ ↓ · 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