# How do PyMySQL prevent user from sql injection attack?



Asked 2 years, 4 months ago Active 2 years, 4 months ago Viewed 2k times

3

Sorry for ask here but I cannot found much reference about pymysql's security guide about how do we prevent sql injection, When I do PHP develope I know use mysql preparedstatement(or called Parameterized Query or stmt),but I cannot found reference about this in pymysql

simple code use pymysql like

```
sqls="select id from tables where name=%s"
attack="jason' and 1=1"
cursor.execute(sqls,attack)
```

How do I know this will prevent sql injection attack or not?if prevent succeed,how do pymysql prevent?Is cursor.execute already use preparedstatement by default?

python sql-injection pymysql server-side-attacks

share improve this question follow

asked Aug 2 '18 at 6:55
Jason117
95 1 6

attack sql should be "jason' and 1='1" I think – Jason117 Aug 2 '18 at 6:56

To be a significant SQL injection, it should be "jason' OR 1='1". If you use AND, the result doesn't change. – Bill Karwin Aug 2 '18 at 16:33

add a comment

## 1 Answer

Active Oldest Votes

6

Python drivers do not use real query parameters. In python, the argument (the variable `attack` in your example) is interpolated into the SQL string before sending the SQL to the database server.

This is not the same as using a query parameter. In a real parameterized query, the SQL string is sent to the database server with the parameter placeholder intact.

But the Python driver does do properly escape the argument as they interpolate, which protects against SQL injection.

I can prove it when I turn on the query log:

```
mysql> SET GLOBAL general_log=ON;
```

And tail the log while I run the Python script:

```
$ tail -f /usr/local/var/mysql/bkarwin.log
...
180802  8:50:47    14 Connect   root@localhost on test
           14 Query SET @@session.autocommit = OFF
           14 Query select id from tables where name='jason\' and 1=1'
           14 Quit
```

You can see that the query has had the value interpolated into it, and the embedded quote character is preceded by a backslash, which prevents it from becoming an SQL injection vector.

I'm actually testing MySQL's Connector/Python, but pymysql does the same thing.

I disagree with this design decision for the Python connectors to avoid using real query parameters (i.e. real parameters work by sending the SQL query to the database with parameter placeholders, and sending the values for those parameters separately). The risk is that programmers will think that *any* string interpolation of parameters into the query string will work the same as it does when you let the driver do it.

Example of SQL injection vulnerability:

```
attack="jason' and '1'='1"
sqls="select id from tables where name='%s'" % attack
cursor.execute(sqls)
```

The log shows this has resulted in SQL injection:

```
180802  8:59:30    16 Connect   root@localhost on test
           16 Query SET @@session.autocommit = OFF
           16 Query select id from tables where name='jason' and '1'='1'
           16 Quit
```

share improve this answer follow edited Aug 2 '18 at 16:01

answered Aug 2 '18 at 15:53
Bill Karwin
443k 77 590 745

Isn't this why you create wrappers around low-level drivers to provide a high-level interface as well as data validation? – Jamie Ivanov Aug 2 '18 at 16:35

If the developer who writes the wrapper understands how to write safe code, then sure. – Bill Karwin Aug 2 '18 at 16:36

Thanks Karwin,This solved my confusion,Glad to receive your answer,and have a nice day!! – Jason117 Aug 3 '18 at 3:24

Glad to help. By the way, it's customary on Stack Overflow to upvote or accept an answer that helped you. – Bill Karwin Aug 3 '18 at 6:02

add a comment

## Your Answer

Sign up or log in

Sign up using Google
Sign up using Facebook
Sign up using Email and Password

Post as a guest
Name
Email
Required, but never shown

Post Your Answer

By clicking "Post Your Answer", you agree to our terms of service, privacy policy and cookie policy

Not the answer you're looking for? Browse other questions tagged python sql-injection pymysql server-side-attacks or ask your own question.

The Overflow Blog
How to write an effective developer resume: Advice from a hiring manager
Podcast 290: This computer science degree is brought to you by Big Tech

Featured on Meta
"Question closed" notifications experiment results and graduation
MAINTENANCE WARNING: Possible downtime early morning Dec 2/4/9 UTC (8:30PM…
Congratulations VonC for reaching a million reputation

Linked
3 Is this python/mysql query susceptible to SQL injection
0 Insert Data with pymysql using inputs
0 Query parameterization in PyMySQL for query with "IN" keyword
0 Python MySQL, is this a prepared statement?

Related
2773 How can I prevent SQL injection in PHP?
1156 How can I sanitize user input with PHP?
676 Are PDO prepared statements sufficient to prevent SQL injection?
1844 How to randomly select an item from a list?
1113 How does the SQL injection from the "Bobby Tables" XKCD comic work?
2714 List changes unexpectedly after assignment. How do I clone or copy it to prevent this?
678 SQL injection that gets around mysql_real_escape_string()
1994 How to remove a key from a Python dictionary?
2262 How to select rows from a DataFrame based on column values

Hot Network Questions
How does the title "Revenge of the Sith" suit the plot?
Are Van Der Waals Forces the Similar to Van der Waal Equation?
Do it while you can or "Strike while the iron is hot" in French
Construct a polyhedron from the coordinates of its vertices and calculate the area of each face
What is Qui-Gon Jinn saying to Anakin by waving his hand like this?
more hot questions
Question feed



site design / logo © 2020 Stack Exchange Inc; user contributions licensed under cc by-sa. rev 2020.11.30.38071