

Re: Using q() to define a query

Source: <http://coding.derkeiler.com/Archive/Perl/perl.dbi.users/2008-01/msg00018.html>

- *From:* scoles@xxxxxxxxxxxx (John Scoles)
 - *Date:* Fri, 11 Jan 2008 07:00:50 -0500
-

I beleive most SQL parsers will ignore white space like that in an SQL query. Normally single quotes in parameters are the bug bear of the the SQL programmer,

ie

```
select name,rank,ser_no from sailors where name = O'Tool
```

It is always good practice to use parameterized queries instead that you prepared first

```
my $sql="select name,rank,ser_no from sailors where name =:name";
my $c=$db->prepare($sql);
$c->bind_param(":name","O'Tool");
$c->execute();
```

or

```
my $sql="select name,rank,ser_no from sailors where name =?";
my $c=$db->prepare($sql);
$c->execute("O'Tool");
```

as DBI and DBD driver will take care of the quotes for you and it prevents any SQL injection attacks on your app.

Cheers

Colin Wetherbee wrote:

Greetings.

I have a DBI (DBD::Pg) application I'm building in mod_perl. My queries tend to look something like the following.

```
my $sql = q(SELECT departure_date, eq.name AS equipment,
dp.full_city AS departure_city, ap.full_city AS arrival_city,
ca.name AS carrier_name, number
FROM jsjourneys
FULL OUTER JOIN jscarriers AS ca ON jsjourneys.carrier = ca.id
FULL OUTER JOIN jsequipment AS eq ON jsjourneys.equipment = eq.id
JOIN jsports AS dp ON jsjourneys.departure_port = dp.id
```

Re: Using q() to define a query

```
JOIN jsports AS ap ON jsjourneys.arrival_port = ap.id  
ORDER BY departure_date);
```

And, then, I execute them as follows.

```
$dbh->selectall_arrayref($sql, { Slice => {} });
```

Which works quite well.

However, I'm concerned about \$sql because when I output it to Apache's debug log, it looks like this:

```
[Fri Jan 11 03:49:09 2008] [debug] Log.pm(36): [client 192.168.171.80] [JetSet] SELECT  
departure_date, eq.name AS equipment,\n dp.full_city AS departure_city, ap.full_city AS  
arrival_city,\n ca.name AS carrier_name, number\n FROM jsjourneys\n FULL OUTER JOIN  
jscarriers AS ca ON jsjourneys.carrier = ca.id\n FULL OUTER JOIN jsequipment AS eq ON  
jsjourneys.equipment = eq.id\n JOIN jsports AS dp ON jsjourneys.departure_port = dp.id\n JOIN jsports AS ap ON jsjourneys.arrival_port = ap.id\n ORDER BY departure_date
```

Notice the newline characters in there. If those were really in the query, I can't imagine the database would run it, so I suppose they're an artifact of the combination of using q() to quote my query and using Apache's logger to output it.

All this leads up to a pretty simple question: is using q() to quote my queries a bad thing, and/or will it cause trouble in the future?

(As an aside, how do you guys quote your queries? I find that for anything longer than about 60 characters, q() and " and everything else start to look horribly inelegant.)

Thanks.

Colin