

Re: SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-06/0059.html>

From: Kevin Spett (kspett@spidynamics.com)

Date: 06/11/02

From: "Kevin Spett" <kspett@spidynamics.com>
To: "Qyves" <zqyves@netscape.net>, <pen-test@securityfocus.com>
Date: Tue, 11 Jun 2002 16:57:57 -0400

> I am currently pen-testing a web app and I am stuck in trying to execute two queries sequentially in Oracle.
> To my knowledge I can do this in SQL by separating the two queries with ; however this is not happening in my case in two circumstances...

You won't have luck with this in Oracle. Their ODBC driver prevents multiple statements from reaching the server. I don't know of any way to circumvent this. You may want to try the -- comment character though. It will work on occasion, depending on how the ODBC stuff is configured. No clue what it needs to look like from the sysadmin's perspective, but I have seen web apps that use Oracle backends that it will work on.

> *Case 1:*

> I have discovered an injectable sql query that is fed its data from a web form, the end query build by a cgi-script being
> something along those lines:
> (insert into tab_nam values ('a','b','c','d','e')); -- a-e values from the web form- with me being able to inject through
> concatenation and subqueries between any of those fields a SELECT query.
> e.g.
> e='||select password from users where username='adm'||'
> query=(insert into tab_nam values ('a','b','c','d',''||select password from users where username='adm'||')));
> I tried an INSERT to no avail, fair enough since I don't think that INSERTs are allowed in nested queries... (or are they??)
> The last characters added by the cgi script are the));

You are correct. An INSERT in a subquery is bad syntax.

> *Case 2:*

> I have also found a second query I can insert to and parts of it are actually shown raw in the URL as an input to a servlet
> script e.g. /stupid.cgi?A=123%20AND%20%ID=101
> This query appears to be something in the form of:
> SELECT foo from bar where [URL] ;
> I can inject an OR 1=1 in the above Url and get all the rows... However

SecurityFocus Penetration: Re: SQL Injection

when I try the sequential queries again I fail

- > miserably url=/stupid.cgi?A=123%20AND%20%ID=101%20OR%20I=1
- > original url=/stupidservlet?A=123%20AND%20%ID=101
- > modified url=/stupidservlet?A=123%20AND%20%ID=101; insert into powerusers values ('test', 'pwd')
- > I have full control over the url however I get just a "Server Error" back.
- > Any clues on how to make any of these methods work anyone??

Just do a plain old vanilla UNION SELECT. Try something like this

(remember to convert the spaces to + or %20):

/stupidservlet?A=123 AND 1=0 UNION SELECT name FROM cat WHERE 1=1

(that'll give you table names)

I'm going to be updating my SQL Injection paper

(<http://www.spidynamics.com/whitepapers.html> I think) in the next two weeks with my findings in Oracle.

I hope that helped.

Kevin Spett
SPI Dynamics, Inc.

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- **Previous message:** [Oliver Petruzel: "Testing other prot's and layers."](#)
- **In reply to:** [Qyves: "SQL Injection"](#)
- **Next in thread:** [Breidenbach, Beth: "RE: SQL Injection"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)