

## RE: SQL

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-11/0083.html>

---

*From:* Holmes, Ben ([Ben.Holmes@getronics.com](mailto:Ben.Holmes@getronics.com))

*Date:* 11/20/01

Message-ID: <0C5EECDCFE105C4BB8FC618DD243ED700196DD97@excausy103.australia.unity>

From: "Holmes, Ben" <[Ben.Holmes@getronics.com](mailto:Ben.Holmes@getronics.com)>

To: "'[garyo@sec-1.com](mailto:garyo@sec-1.com)'" <[garyo@sec-1.com](mailto:garyo@sec-1.com)>, "'[pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)'" <[pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)>

Subject: RE: SQL

Date: Tue, 20 Nov 2001 19:55:52 +1100

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

I'm not all that knowledgeable about SQL testing.. I usually get help from people who know a lot about SQL to help with the actual code syntax, but, here is a thing about the parsing of unquoted code to an SQL server (and that is what it sounds like you have). I am flying on my own here...

You may have a hole there.

Try (as a username): aa'; CREATE USER hack WITH SYSID 0 PASSWORD 'hacked' \\*

The "\\*" is the "Quote start" character in SQL and will quote the rest of the command out.

You may have to make the password something like: \*\; SET foo TO 'bar

Or something to that effect.

This should pass the command like this to the SQL server:

```
<stuff the programmer thought would go there> USER to 'aa'; CREATE USER hack  
WITH SYSID 0 PASSWORD 'hacked' \*<more stuff that is now commented out>*\;  
SET foo TO 'bar'
```

The extra quote on the end is the one that has caused you grief.

Just a thought. It certainly warrants trying some SQL commands.

Here are some references to look at:

List of SQL commands:

<http://www.postgresql.org/docs/index.php/sql-commands.html>

RE: SQL

SecurityFocus Penetration: RE: SQL

A quick search brings up a good article about hacking SQL through bad perl at: <http://www.attrition.org/security/advisory/rfp/rfp2k01>

You may be able to find even more stuff at "<http://www.wiretrip.net/rfp>"

--- Benjamin Holmes  
Getronics, Brisbane, Queensland, AUSTRALIA

> -----Original Message-----

> From: Gary O'leary-Steele [mailto:[GaryO@sec-1.com](mailto:GaryO@sec-1.com)]

> Sent: Tuesday, 20 November 2001 2:24 AM

> To: [PEN-TEST@securityfocus.com](mailto:PEN-TEST@securityfocus.com)

> Subject: SQL

>

>

> Hello all,

>

>

> I am doing a pen test against a IIS 5 web server. The web

> server requires a

> user name and password via a logon form. if a single quote

> character is

> entered (username)the following error is produced

>

> [Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark

> before the character string " and password=".

>

> I remember reading somewhere that this can be used to gain

> further access?

> but i cant find the info.

>

> Can any one help?

>

> Thanks in advance.

>

> Gary

>

>

> -----

> -----

> 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/>

>

-----BEGIN PGP SIGNATURE-----

Version: PGPfreeware 7.0.3 for non-commercial use <<http://www.pgp.com>>

Comment: Pee Gee Peeeee!

RE: SQL

SecurityFocus Penetration: RE: SQL

iQA/AwUBO/oamHLvuelW5gCIEQJyfACfaYYUwKXZyBgYToNYJMxmDZluqZgAoM7G  
ReMm/fhHDz1AHrbxpWku/OB6  
=0sjP  
-----END PGP SIGNATURE-----

---

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:*** Alla Bezroutchko: "Re: One Big Review, One Small Script?"
- ***Maybe in reply to:*** Gary O'leary-Steele: "SQL"
- ***Next in thread:*** Kevin Spett: "Re: SQL"
- ***Messages sorted by:*** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]