

# [NT] Hacking Sybase/MS-SQL for the NT Administrator

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0065.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 05/14/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Tue, 14 May 2002 08:29:11 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Hacking Sybase/MS-SQL for the NT Administrator

---

## SUMMARY

The following is a short explanation on how to "hack" into a Sybase/MS-SQL without having the SA password (note that we do have administrator access on the machine, but not on the database).

## DETAILS

The following is an explanation on how to get into a Sybase database on systems that we already have fully authorized Administrator access on them.

Like Microsoft's SQL server, Sybase permits three modes of authentication:

\* Standard security mode is where Sybase maintains its own user database -- with login names, passwords, and access rights -- and is probably the default. In this mode, the NT user accessing the server is never considered, so being an NT Administrator does not give you any special access.

\* Integrated security mode means that authenticated NT logons map to Sybase logons, so once you've passed the NT domain logon process, that

## Securiteam: [NT] Hacking Sybase/MS-SQL for the NT Administrator

credential gets you into the Sybase door as well. The mapping is not automatic: the DB administrator has to set up the NT -> Sybase user mappings explicitly and then grant rights to those mapped users. Its main benefit seems to be elimination of a separate database login step.

\* Mixed security is a hybrid of the previous two.

In "Integrated" security mode, there is further a method of translating otherwise unknown authentication attempts into a specific database user. Not all NT users necessarily map to a valid Sybase user, so the "DefaultLogon" is used to map unrecognized NT users into a single Sybase user. This could be used to provide a kind of generic "guest" access, and we believe that this is disabled by default.

We went into the registry under  
HKEY\_LOCAL\_MACHINE\SOFTWARE\SYBASE\Server\server\_name

Where "server\_name" is the name of the database server in question. A machine can run more than one database, and each is administered separately (they even have different NT services to manage).

If we set in the key the LoginMode to "1" and the DefaultLogin to "sa" and restart the associated NT service. We can run the Sybase SQL Central and connect while running as an otherwise unknown NT user, while we will be mapped to a "sa" account. This means that we are now an administrator of the database.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[steve@unixwiz.net](mailto:steve@unixwiz.net)> Stephen J. Friedl.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] Gaim Arbitrary Email Access"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)