

[REVS] Blindfolded SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0011.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 09/04/03

To: list@securiteam.com

Date: 4 Sep 2003 18:22:18 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Blindfolded SQL Injection

SUMMARY

The paper linked below explains several techniques improving the detection and exploitation of SQL injections with minimal knowledge of the target.

DETAILS

Until today, exploiting SQL Injection attacks depended on having the Web Server return detailed error messages or having any other source of information. As a result, many security administrators suppressed these error messages, assuming this would protect them from SQL Injection exploitation. This white paper shows, however, that suppressing the error messages does not provide real protection. The research done at WebCohort reveals a set of techniques that can be easily used by attackers in order to bypass this obstacle, making it clear those more substantial measures must be taken against SQL Injection attacks.

ADDITIONAL INFORMATION

The information has been provided by <mailto:research@webcohort.com> Ofer Maor & Amichai Shulman.

The original article can be found at:

Securiteam: [REVS] Blindfolded SQL Injection

<http://www.webcohort.com/Blindfolded_SQL_Injection.pdf>
http://www.webcohort.com/Blindfolded_SQL_Injection.pdf

=====

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
In order to subscribe to the mailing list, simply forward this email to: 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.