

[REVS] More Advanced SQL Injection Paper Released

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0081.html>

From: support@securiteam.com

Date: 06/19/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 19 Jun 2002 08:33:25 +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.

More Advanced SQL Injection Paper Released

SUMMARY

The linked paper will try to address the subject of SQL Injection in a Microsoft SQL Server/IIS/Active Server Pages environment, but most of the techniques discussed have equivalents in other database environments. It should be viewed as a "follow up", or perhaps an appendix, to the previous paper, "<http://www.securiteam.com/securityreviews/5UP010A6AA.html>> Advanced SQL Injection".

DETAILS

The paper covers in more detail some of the points described in its predecessor, providing examples to clarify areas where the previous paper was perhaps unclear. An effective method for privilege escalation is described that makes use of the OPENROWSET function to scan a network. A novel method for extracting information in the absence of 'helpful' error messages is described; the use of time delays as a transmission channel. Finally, a number of miscellaneous observations and useful hints are provided, collated from responses to the original paper, and various conversations around the subject of SQL injection in a SQL Server environment.

Securiteam: [REVS] More Advanced SQL Injection Paper Released

This paper assumes that the reader is familiar with the content of "Advanced SQL Injection".

ADDITIONAL INFORMATION

The full paper can be downloaded from:

<http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf>
http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf

The information has been provided by <<mailto:chris@ngssoftware.com>> Chris Anley.

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] WebBBS Remote Command Execution"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)