

[REVS] SQL Injection Attacks by Example

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0105.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/25/05

To: list@securiteam.com

Date: 25 Jan 2005 19:00:10 +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>

SQL Injection Attacks by Example

SUMMARY

SQL Injection is caused by unverified/unsanitized user input, and its main idea is to convince the application to run SQL code that it was not intended to run.

If the application is creating SQL strings naively, i.e. on the fly, and then running them, it's straightforward to create some real surprises. There have been other papers on SQL injection, including some that are much more detailed, but this one shows the rationale of discovery as much as the process of exploitation.

DETAILS

Introduction:

A customer asked that Steve Friedl check out his intranet site, which was used by the company's employees and customers. This was part of a larger security review, and though Steve Friedl had not actually used SQL injection to penetrate a network before, Steve Friedl was pretty familiar with the general concepts. Steve Friedl was completely successful in this engagement, and wanted to recount the steps taken as an illustration.

ADDITIONAL INFORMATION

Securiteam: [REVS] SQL Injection Attacks by Example

The information has been provided by <mailto:steve@unixwiz.net> Steve Friedl.

The original article can be found at:

<<http://www.unixwiz.net/techtips/sql-injection.html>>

<http://www.unixwiz.net/techtips/sql-injection.html>

=====

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.