

[TOOL] Automagic SQL Injector

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0064.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/21/05

To: list@securiteam.com

Date: 21 Nov 2005 16:01:36 +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>

Automagic SQL Injector

SUMMARY

DETAILS

The Automagic SQL Injector is part of the Sec-1 Exploit Arsenal provided as part of the Applied Hacking & Intrusion Prevention training courses.

In a nutshell it's an automated SQL injection tool designed to help save time on pen tests. It is only designed to work with vanilla Microsoft SQL injection holes where errors are returned.

The following features are currently supported:

- * Browse tables and dump table data to a CSV file (2 methods).
- * Upload files using debug script method.
- * Automagical UDP reverse shell
- * Interactive xp_cmdshell (simulated cmd.exe shell)

I plan to add other features such as a brute force account cracker and a module to search for other SQL servers using OPENROWSET().

For a demonstration please visit <http://scoobygang.org/magicsql/>

Securiteam: [TOOL] Automagic SQL Injector

Written for Active Perl (Windows), doesn't work too well on *nix.

Usage: perl C:\Automagic SQL injector\injector.pl <Options>

-h Target Host
-f Target File (e.g. /process_login.asp)
-t Type (POST|GET)
-q Is a leading single quote required (YES|NO)
-a Additional header such as a cookie. Enclose within ""
-d Database creation type (T|R). TEMP ## or regular table (Default is TEMP)

ADDITIONAL INFORMATION

To download the tool: <<http://scoobygang.org/automagic.zip>>

<http://scoobygang.org/automagic.zip>

The information has been provided by <<mailto:garyo@sec-1.com>> Gary O'leary-Steele.

=====

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.