

[REVS] SQL Injection Walkthrough

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0112.html>

From: support@securiteam.com

Date: 05/26/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 26 May 2002 20:52:16 +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.

SQL Injection Walkthrough

SUMMARY

The following article will try to help beginners with grasping the problems facing them while trying to utilize SQL Injection techniques, to successfully utilize them, and to protect themselves from such attacks.

DETAILS

1.0 Introduction

When a machine has only port 80 opened, your most trusted vulnerability scanner cannot return anything useful, and you know that the admin always patch his server, we have to turn to web hacking. SQL injection is one of type of web hacking that require nothing but port 80 and it might just work even if the admin is patch-happy. It attacks on the web application (like ASP, JSP, PHP, CGI, etc) itself rather than on the web server or services running in the OS.

This article does not introduce anything new, SQL injection has been widely written and used in the wild. We wrote the article because we would like to document some of our pen-test using SQL injection and hope that it may be of some use to others. You may find a trick or two but please check out the "9.0 Where can I get more info?" for people who truly deserve credit for developing many techniques in SQL injection.

1.1 What is SQL Injection?

It is a trick to inject SQL query/command as an input possibly via web pages. Many web pages take parameters from web user, and make SQL query to the database. Take for instance when a user login, web page that user name and password and make SQL query to the database to check if a user has valid name and password. With SQL Injection, it is possible for us to send crafted user name and/or password field that will change the SQL query and thus grant us something else.