

[REVS] Advanced SQL Injection in Oracle Databases

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0022.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/06/05

To: list@securiteam.com

Date: 6 Feb 2005 18:35:50 +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>

Advanced SQL Injection in Oracle Databases

SUMMARY

The linked presentation shows, with many examples, how the SQL Injection vulnerabilities in applications that use Oracle databases can be exploited and how to prevent this. The topics also include buffer overflow attacks and examples using some of the recently discovered vulnerabilities in Oracle software.

DETAILS

Topics (37 slides):

- * Introduction
- * SQL Injection attacks
 - o How to exploit
 - o Exploit examples
 - o SQL Injection in functions defined with AUTHID CURRENT_USER
 - o How to get around the need for CREATE PROCEDURE privilege –

Example

- o How to protect
- * Buffer overflow attacks
 - o How to exploit

Securiteam: [REVS] Advanced SQL Injection in Oracle Databases

- o Exploit examples
- o Detecting an attack
- * Remote attacks using SQL Injection in a web application
 - o Exploit examples
 - o Web application worms
 - o How to protect
- * Summary
- * Conclusions

ADDITIONAL INFORMATION

The information has been provided by <mailto:secemf@yahoo.com.ar> Esteban Martinez Fayo.

The original article can be found at:

<http://security-papers.globint.com.ar/oracle_security/sql_injection_in_oracle.php>
http://security-papers.globint.com.ar/oracle_security/sql_injection_in_oracle.php

=====

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.