

[UNIX] E-Xoops Easy SQL Injection and Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0150.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/31/05

To: list@securiteam.com

Date: 31 Mar 2005 10:27:53 +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>

E-Xoops Easy SQL Injection and Cross Site Scripting

SUMMARY

" <www.exoops.info> XOOPS is an extensible, OO (Object Oriented), easy to use dynamic web content management system written in PHP. XOOPS is the ideal tool for developing small to large dynamic community websites, intra company portals, corporate portals, weblogs and much more."

SQL Injection and Cross Site Scripting vulnerabilities have been found in E-Xoops Easy Community Management System Forum System. These vulnerabilities can be exploited by potential attackers to compromise system's database integrity and/or execute malicious code in context of Internet browser of users visiting the site.

DETAILS

Vulnerable Systems:

* Community Management System Forum (E-XOOPS)

Cross Site Scripting:

Flaws in user input validation make [viewforum.php](#) vulnerable to Cross Site Scripting attacks:

Securiteam: [UNIX] E-Xoops Easy SQL Injection and Cross Site Scripting

Examples:

http://localhost/modules/newbb/viewforum.php?sortname=p.post_time&sortorder=ASC

[http://localhost/modules/newbb/index.php?viewcat=%22%3E%3Cscript%3Ealert\(document.cookie\)%3C/script%3E](http://localhost/modules/newbb/index.php?viewcat=%22%3E%3Cscript%3Ealert(document.cookie)%3C/script%3E&forum=25&refresh=Vai)

SQL Injection:

Lack of filtering of user provided input allows SQL Injection:

Examples:

http://localhost/modules/newbb/index.php?viewcat='SQL_INJECTION

<http://localhost/modules/sections/index.php?op=viewarticle>

<http://localhost/modules/sections/index.php?op=viewarticle&artid=9%2c+9%2c+9>

ADDITIONAL INFORMATION

The information has been provided by <mailto:dcrab@hackerscenter.com>

Dcrab.

The original article can be found at:

<<http://icis.digitalparadox.org/~dcrab>>

<http://icis.digitalparadox.org/~dcrab>

=====

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.