

# [UNIX] Database Password Disclosure and Cross-Site Scripting in Bugzilla

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00006.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 4 Feb 2007 16:59:54 +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>

-----

Database Password Disclosure and Cross-Site Scripting in Bugzilla

---

## SUMMARY

" <<http://www.bugzilla.org/>> Bugzilla is a Web-based general-purpose bugtracker tool originally developed and used by the Mozilla project." Multiple vulnerabilities have been discovered in Bugzilla, allowing remote attackers to disclosure database passwords and cause a cross site scripting vulnerability.

## DETAILS

Cross-Site Scripting:  
\* Bugzilla version 2.20.1 and above

Bugzilla does not properly escape some fields in generated Atom feeds, which leads to the potential for cross-site scripting in feed readers that support JavaScript and properly implement the Atom feed specification.

Reference:  
<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=367674](https://bugzilla.mozilla.org/show_bug.cgi?id=367674)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=367674](https://bugzilla.mozilla.org/show_bug.cgi?id=367674)

## [UNIX] Database Password Disclosure and Cross-Site Scripting in Bugzilla

Database password disclosure:

Vulnerable Versions: 2.23.3 only

Bugzilla development snapshot version 2.23.3 introduced the ability to run Bugzilla under mod\_perl on Apache. The mod\_perl initialization script included with Bugzilla defines a new <Directory> block in the Apache configuration for the directory containing Bugzilla. This block fails to include permission for .htaccess files to override file access permissions. The .htaccess file shipped with Bugzilla prohibits access by web browsers to read the localconfig file, which contains the username and password for connecting to the database server. If you are not running Bugzilla under mod\_perl, then this does not affect you.

Reference:

<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=367071](https://bugzilla.mozilla.org/show_bug.cgi?id=367071)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=367071](https://bugzilla.mozilla.org/show_bug.cgi?id=367071)

Fix:

The fixes for all of the security bugs mentioned in this advisory are included in the 2.20.4, 2.22.2, and 2.23.4 releases. Upgrading to these releases will protect installations from possible exploits of these issues.

Full release downloads, patches to upgrade Bugzilla from previous versions, and CVS upgrade instructions are available at:

<<http://www.bugzilla.org/download/>> <http://www.bugzilla.org/download/>

### ADDITIONAL INFORMATION

The original articles could be found at:

<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=367674](https://bugzilla.mozilla.org/show_bug.cgi?id=367674)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=367674](https://bugzilla.mozilla.org/show_bug.cgi?id=367674)  
<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=367071](https://bugzilla.mozilla.org/show_bug.cgi?id=367071)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=367071](https://bugzilla.mozilla.org/show_bug.cgi?id=367071)

=====

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

## [UNIX] Database Password Disclosure and Cross-Site Scripting in Bugzilla

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.