

# Online BookMarks Multiple SQL Injection/XSS Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-12/msg00053.html>

---

- *From:* [security@xxxxxxxxxxx](mailto:security@xxxxxxxxxxx)
  - *Date:* 3 Dec 2006 14:33:33 -0000
- 

3/12/06

Vigilon Advisory <http://www.vigilon.com/vg-onlinebookmarks-3-12-2006.txt>

---

-----  
Application: OnLine Bookmarks  
Web Site: <http://www.frech.ch/online-bookmarks/>  
Versions: 0.6.12  
Platform: linux, windows, freebsd, sun  
Bug: Cross Site Scripting and SQL injection.  
Fix Available: No  
Severity: High  
-----

- 1) Introduction
- 2) Bug
- 3) The Code
- 4) Fix
- 5) About Vigilon

=====  
1) Introduction  
=====

online-bookmarks is a Bookmark management system to store your Bookmarks, Favorites and Links right in the WWW where they actually belong. It is meant for people who work often with different computers and browsers.

=====  
2) Bug  
=====

1. SQL Injection
2. Multiple Cross site Scripting

=====  
3) Proof of concept.

=====  
login with username '  
login with password '

=====  
4) Fix  
=====

The author notified about the security issues two months ago.  
some of the problems were fixed at version 0.6.12 however  
sql injection and some cross site cripting are still exists.  
no patched version been released.

=====  
5) About Vigilon  
=====

Vigilon Inc. is a security software company that helps organizations,  
and the security providers that serve them,  
reduce business risk while lowering operational security costs.  
using the Continual Vigilance platform.

=====  
6) Disclaimer  
=====

The information within this paper may change without notice. Use of this  
information constitutes acceptance for use in an AS IS condition. There are  
NO warranties with regard to this information. In no event shall the author  
be liable for any damages whatsoever arising out of or in connection with  
the use or spread of this information. Any use of this information is at the  
user's own risk.

=====  
7) FeedBack  
=====

Please send suggestions, updates, and comments to:

Security@xxxxxxxxxx  
<http://www.vigilon.com>