XOOPS MyTextSanitizer Filtering Bug Allows Remote Users to Conduct Cross−Site Scripting Attacks in many modules: News, newbb, private messages, signatures etc...

Source: http://www.derkeiler.com/Mailing−Lists/NT−Bugtraq/2003−04/0041.html

---

From: Doxical (*doxical_at_WANADOO.FR*)
Date: 04/26/03

```
Date:         Sat, 26 Apr 2003 18:13:38 +0200
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM
```

Date: 25/04/2003
Impact: Disclosure of authentication information, Execution of arbitrary code via network, Modification of user information, admin account hijacking.
Fix: yes

−−

Introduction

After the module glossary and gallery of xoops, we have found an another risk in MytextSanitizer who permit somme CSS injection in xoops versions 1.3.x to 2.x
Description of the MyTextSanitizer script :

This is just the function on xoops who filter spécial charactèrs or malicious scripts.

The vulnerability :

A remote user can bypass Sanitizer and conduct cross−site scripting attacks with a post in a topic in board (newbb) send malicious private message to admin, insert script in the news comment...

Example :

java script:alert%28document.cookie%29
with img tags

History:

−the team of xoops.org was prevented on 04/21/2003
−Patch are now available since 04/25/2003

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

Regards

www.blocus−zone.com

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
Have you discovered a security vulnerability related to Windows or a
commercial product which runs on Windows?

Need assistance crafting the format or translating your advisory to English?

Need to verify it, or having problems contacting the Vendor?

Contact mailto:Advisories@NTBugtraq.com

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo