

[UNIX] PBLang Information Disclosure, Privileges Escalation and Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0063.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/15/05

To: list@securiteam.com

Date: 15 Mar 2005 15:50:41 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

PBLang Information Disclosure, Privileges Escalation and Cross Site Scripting

SUMMARY

" <<http://pblang.drmartinus.de/>> PBLang is a powerful flatfile Bulletin Board System. It combines many features of a professional board, but does not even require SQL support. It is completely based on text-file."

PBLang has been discovered to contain multiple vulnerabilities, these vulnerabilities allow a remote attacker to disclose sensitive information, to escalate his privileges and to cause cross side scripting.

DETAILS

Vulnerable Systems:

* PBLang version 4.65 and prior

Information Disclosure Vulnerability:

sendpm.php contains a flaw that allows a registered user to view other users' password hashes, as well as their PM's and other files in the forum (and outside of the forum directory too).

Securiteam: [UNIX] PBLang Information Disclosure, Privileges Escalation and Cross Site Scripting

Exploit:

By using the following URL:

[http://example.com/pblang/sendpm.php?to=\[username\]&subj=\[doesnt matter\]&num=1&orig=/home/public_html/pblang/db/members/\[username\]](http://example.com/pblang/sendpm.php?to=[username]&subj=[doesnt matter]&num=1&orig=/home/public_html/pblang/db/members/[username])

It will load [username]'s entire account information including the MD5'ed password hash and maybe hidden email information. It will be shown in web page's source code, not in the page itself, so right click and view page source. This method allows accessing any file in the system using web server's privileges, including /etc/passwd.

Privilege Escalation Vulnerability:

Flaws in delpm.php allow any registered user to delete anyone else's PM's as long as their logged in (doesn't need to be privileged). This could allow unprivileged users to harass other users.

Exploit:

The following URL can be used to test your system for the mentioned vulnerability:

[http://localhost/pblang/delpm.php?id=\[PMID\]&a=\[Target user name\]](http://localhost/pblang/delpm.php?id=[PMID]&a=[Target user name])

Cross Side Scripting:

The module pmpshow.php shows the PMs a user has received, however, the body of the received PM is not checked for any harmful characters like < > and ".

Exploit:

Type in the body of the PM your going to send a victim.
"<script language="javascript">alert("XSS");</script>"

An alert box saying "XSS" should pop up.

In addition, the modules pm.php and search.php are also vulnerable to cross side scripting.

ADDITIONAL INFORMATION

The information has been provided by <mailto:raven@tgs-security.com>
Raven.

=====

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.