MOPS-2010-011: DeluxeBB newthread SQL Injection Vulnerability

May 6th, 2010

A SQL injection vulnerability was discovered in DeluxeBB that allows retrieving all the data from the database by adding new threads to the forum.

Affected versions

Affected is DeluxeBB <= 1.3

Credits

The vulnerability was discovered by Stefan Esser during the Month of PHP Security SQL Injecton Marathon.

About DeluxeBB

DeluxeBB is a powerful open source bulletin board, which helps you create your own web communities in less than 10 minutes.

The board is written completely in PHP and uses a MySQL database to store its content.
All pages are optimized for speed and security. We believe is not necessary to overload the software with features like many other forum providers, we always keep the speed, security and easy handling as our primary objectives.

Detailed information

This vulnerability was discovered during SQL Injection Marathon a PHP code auditing marathon performed by Stefan Esser. The basic idea of this initiative is to select random PHP applications and perform a short code audit on them. The maximum time spent on each application is 30 minutes and after the first found SQL injection usually the next application is audited.

During SQL Injection Marathon DeluxeBB was also audited and within 30 minutes it was possible to find a SQL injection vulnerability through the cookie. The offending code is located in the file newpost.php.

```
//inserting thread
$db->unbuffered_query("INSERT INTO ".$prefix."threads VALUES (NULL, '$info[fid]', '".$_COOK
$tid = $db->insert_id();
```

Here the cookie variable memberid is used directly in a SQL query which leads to SQL injection if magic_quotes_gpc is turned off. However in order to exploit this vulnerability the cookie variable membercookie has to be set to “guest” bescause otherwise the exploit won’t pass a previous check.

Proof of concept, exploit or instructions to reproduce

The following cookie data demonstrates how to trigger the vulnerability when adding a new thread to the forum. With this cookie in place the new thread will contain the admin username and password hash as subject. This data is enough to use the forum as admin afterwards.

```
membercookie=guest
memberid=xx',(select+concat(username,0x2e,pass)+from+deluxebb_users+limit+1),'none',0,0,0,0,0,'g
```

Notes

This vulnerability requires magic_quotes_gpc to be turned off, which is the recommended setting by the PHP developers.

This vulnerability was disclosed to the vendor at the same time as the general public.