Sense of Security	Authorisation: Jason Edelstein
	Release date: 28 February 2011

Sense of Security – Security Advisory – SOS-11-002

PHP Blog Insert Authentication Security Bypass

28 February 2011

PHP Blog Insert Authentication Bypass - Security Advisory - SOS-11-002

Release Date:	28-Feb-2011
Updated:	-
Vendor Notification Date:	14-Oct-2010
Product:	PHP Blog Insert
Platform:	Independent
Affected Versions:	All releases up to and including version 1.0.2
Severity Rating:	High
Impact:	Authentication security bypass
Attack Vector:	Remote without authentication
Solution Status:	No solution currently exists for this vulnerability
CVE Reference:	Not yet assigned

Details:

PHP Blog Insert is a simple blog engine designed to be inserted into an existing web site or application. It is written in PHP and uses a MySQL backend.

The application is vulnerable to an authentication bypass attack due to flawed and predictable access control and session management logic. The application assumes a user is authenticated as an administrator if a cookie is present within a web browser that is named the MD5 hash of the text string “admin”.

Successful exploitation of this vulnerability will result in an attacker gaining access to the administration functionality of the application without the use of valid credentials.

The software can be obtained from:

http://sourceforge.net/projects/php-blog-insert/

Proof of Concept:

Set a cookie within your browser for the appropriate path and domain of the vulnerable application with the name “21232f297a57a5a743894a0e4a801fc3” and any value. Navigate to a page that contains restricted administration functionality within the application such as add_entry.php or register.php.

Solution:

The vendor has not responded to our repeated email notifications and a private blog post on the author’s blog.

An updated release of PHP Blog Insert that corrects this vulnerability is not available.

Discovered by:

Sense of Security Labs.

About us:

We are the leading independent provider of IT security and risk management solutions in Australia, with expertise in assessment and assurance, as well as strategy and architecture, through to deployment and ongoing management.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

Telephone:	+61 (0)2 9290 4444
Fax:	+61 (0)2 9290 4455
Web:	http://www.senseofsecurity.com.au
E-mail:	info@senseofsecurity.com.au
Twitter:	@ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-11-002

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php