

PHPProjekt multiple vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-04/0362.html>

From: Ulf Harnhammar (ulfh@update.uu.se)

Date: 04/25/02

Date: Thu, 25 Apr 2002 01:57:55 +0200 (CEST)

From: Ulf Harnhammar <ulfh@update.uu.se>

To: bugtraq@securityfocus.com

PHPProjekt multiple vulnerabilities

PROGRAM: PHPProjekt

VENDOR: Albrecht Guenther (ag@phprojekt.com) et al.

HOME PAGE: <http://www.phprojekt.com/>

VULNERABLE VERSIONS: all versions below 3.2

LOGIN REQUIRED: yes (some issues), no (some issues)

SEVERITY: high

DESCRIPTION:

"PHPProjekt is a groupware suite which supports communication and management of teams and companies via an Intranet and the Internet. It consists of multiple components, including a group calendar with resource booking, a time card system, project management, a request tracker, a mutual filesystem, a contact manager, a mail client, a forum, chat, notes, shared bookmarks, todo lists, a voting system, and reminders. Language files are available for over 20 languages, and an extensive help system is included."

(direct quote from the program's project page at Freshmeat)

PHPProjekt is written in PHP, and it is published under the terms of the GNU General Public License.

SECURITY HOLES:

I have found many security holes in this program. They can be divided into five categories:

- 1) Some of the scripts in the system require that the user is logged in, while others don't. The system differentiates between them by checking the current URL in the variable \$PHP_SELF to see if it contains strings like "sms" (the name of one of the scripts that don't require logging in contains that string). Unfortunately, \$PHP_SELF includes the PATH_INFO part of a request. This means that we can fool the system into thinking that we are accessing a script that doesn't need logging in, while in fact we are accessing a script that does. This is done by constructing a URL like

SecurityFocus Bugtraq: PHPProjekt multiple vulnerabilities

"http://www.somehost.com/phpprojekt/mail/mail_send.php/sms", where the PATH_INFO part is "/sms".

- 2) The upload functions in the system don't check if the variables related to an upload actually were set by uploading a file or if they are normal POST data. This can be used to make the system treat any file it can read, like "/etc/passwd", as the uploaded data.
- 3) Many SQL statements in the system include user data without enclosing it in apostrophes or quotes. This means that much more data than intended can be deleted or changed. If the system uses the parameter "id" in the string "UPDATE table SET name='Ulf' WHERE intTableID=\$id", giving "id" the value "intTableID" means that we will end up executing the statement "UPDATE table SET name='Ulf' WHERE intTableID=intTableID". This statement will change all names in the table to Ulf.
- 4) Some of the scripts that should require logging in never check if you are in fact logged in. This means that a person with insufficient privileges can view or edit data in the system, by posting the right data to those scripts.
- 5) Files are accessed without proper checking of their file names for slashes and dots. This means that we can read files outside of the PHPProjekt system by entering file names like "../../../../../etc/passwd".

COMMUNICATION WITH VENDOR:

The first security hole was reported to the vendor on the 15th of March, and the last one a couple of weeks later. Version 3.2, which is not vulnerable to any of these issues, was released on the 11th of April.

RECOMMENDATION:

I recommend that all administrators upgrade to version 3.2 immediately.

// Ulf Harnhammar
ulfh@update.uu.se

- **Previous message:** [Chris Green: "Re: Snort exploits"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)