CVE-2016-9681

Report for the Andmeturve (2017) course

Author: Anton Tšugunov

Supervisor: Meelis Roos

Tartu 2017
Introduction

Serendipity is a PHP-powered weblog engine which gives its users an easy way to maintain their blogs. Not only is it designed for casual bloggers but also offers a framework with the possibility of professional applications.

Vulnerability description

The Serendipity engine before version 2.0.5 has multiple cross-site scripting vulnerabilities that make it possible for remote authenticated users to insert their own HTML code or web scripts into trusted web sites by sending a simple POST request. It is even possible to rewrite the existing content of the pages using the web scripts.

This is possible because the categories or directory names created by the customized POST request are put on the website pages without any limitation, meaning that if a category name is a script, then it will be put on the page as a working script. The same goes for the directory name.

Impact

The web scripts inserted into websites can access cookies, sessions tokens and other private information/data used by the browser with the attacked site.

Rewriting the existing HTML code can enable the attacker to replace links on the site to links that go to malware or virus containing websites, phishing sites or use the whole page for phishing. For example: creating a fake login form and steal passwords. The victim will have no way of knowing whether the login form is real or not without purposely looking at the source code.

Solution

The solution is very simple: new category and directory names should be validated for safety and all the special characters should be escaped. The same thing was done to fix the issue:
The previously saved and then printed

\$serendipity['POST']['name']

was replace by

\$new_dir

which is on it’s own created by the following code:

\$new_dir = serendipity_uploadSecure(\$serendipity['POST']['parent'] . '/' . serendipity_makeFilename(\$serendipity['POST']['name']),
\$new_dir = str_replace(array('...', '/'), array('', '/' ), \$new_dir);

Function

serendipity_makeFilename()

validates the posted directory name.

As for category name, the previously printed

\$cat.category_name

was replaced with

\$cat.category_name|escape.

Serendipity is using a template engine called Smarty.
The “escape” token is used in the Smarty template engine to escape all the HTML, JS or other types of special characters recognized by browsers:

Is this enough to remove the vulnerability?

Any pieces of code inserted into HTML require special characters to even separate themselves from the rest of the page source.

The executed solution has removed the possibility of inserting the special characters into page code by exploiting the display of the category/directory names.

The vulnerability has been removed.

Sources used:

3. https://github.com/s9y/Serendipity/commit/e2a665e13b7de82a71c9bbb77575d15131b72be
4. https://github.com/s9y/Serendipity/blob/e2a665e13b7de82a71c9bbb77575d15131b72be/include/admin/images.inc.php