Cross Site Scripting in Simple PHP Blog 0.8.1

Title: Cross Site Scripting in Simple PHP Blog 0.8.1
Release Date: 2013/03/01
Vulnerable Application: Simple PHP Blog 0.8.1
Type: Cross site scripting
Level: High (Low/High/Critical)
CVSS: 3.1 (Av:N/AC:L/Au:S/C:C/I:P/A:N)

Dognædis Ref.: DGS-SEC-14
CVE Ref.: CVE-2013-2285
Other Ref.:
Discover Credits: CodeV - Code Analyzer
Bulletin Author(s): LBragues - CodeV Team
Contact: irt@dognaedis.com

Overview:

Simplephpblog.com will give all users a venue to gather basic and complex information about the language, its uses, and recent updates or upgrades made. It will provide developers and people who are not very technical savvy assistance and support to better understand and use the language. The site is committed to provide a helping hand to everyone including tips and suggestions on choosing the web host for your website. It will provide data from the original PHP 5.0 to the PHP 5.4 that comes with all the bells and whistles there is in a modern web language. Articles and discussions on the PHP language, the PHP ecosystem and collaboration will be posted to give users the power to maximize its use when they do use it for their websites.

Scope:

File: <app_root>/scripts/sb_header.php
Vulnerable Argument(s): $cat
Code:

```
line 47: link rel="alternate" type="application/rss+xml" title="Get RSS 2.0 Feed" href="<?php print
BASEURL; ?>rss.php<?php echo $cat ?>" />
line 48: <link rel="alternate" type="application/rdf+xml" title="Get RDF 1.0 Feed" href="<?php print
BASEURL; ?>rdf.php<?php echo $cat ?>" />
line 49: <link rel="alternate" type="application/atom+xml" title="Get Atom 1.0 Feed" href="<?php print
BASEURL; ?>atom.php<?php echo $cat ?>" />
```

Proof(s) of Concept:

```
<app_root>/scripts/sb_header.php?category="/><script type="text/javascript">alert("XSS");</script><br>
```

Description:

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications that enables attackers to inject client-side script into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.

Impact:

Generally, by exploiting this kind of vulnerability, it might be possible to achieve possible attack vectors to various kinds of attacks such as:

- Session/Cookie theft
- Account Hijacking
- Identity theft
- Accessing confidential resources

- Accessing pay content
- Account Denial of service

Resolution:

Aiming a correct resolution of the identified vulnerability, the data obtained through the $_POST['rs'] input argument should be properly sanitized for HTML and following ECMAS usage.

Official Solution:

At the moment, there is no official solution for the reported vulnerabilities.

External References:

http://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)
http://en.wikipedia.org/wiki/Cross-site_scripting
http://en.wikipedia.org/wiki/Code_injection