Framework for Static Analysis of PHP Applications (Artifact)

David Hauzar and Jan Kofroň

Department of Distributed and Dependable Systems
Faculty of Mathematics and Physics
Charles University Prague, Czech Republic
{hauzar,kofron}@d3s.mff.cuni.cz

Abstract

This artifact is based on Weverca, a static analyzer framework for PHP applications. The aim of Weverca is to provide developers with a framework that would allow for an easy implementation of custom static analyses of PHP, while not coping with the dynamic language issues. The framework processes the input source code in two phases. In the first phase, the program-point graph is constructed, which has the dynamic constructs (eval, dynamic includes, type information) already resolved. The developer can then implement a custom static analysis in the second phase, exploiting the output of the first phase. The provided package is designed to support repeatability of the experiments of the companion paper: in particular to perform security (taint) analyses of two bundled applications. Instruction to compile and run the analyzer are also provided.

1998 ACM Subject Classification F.3.1 [Logics and Meanings of Programs] Specifying and Verifying and Reasoning about Programs

Keywords and phrases Static analysis, abstract interpretation, dynamic languages, PHP, security

Digital Object Identifier 10.4230/DARTS.1.1.11

Related Article David Hauzar and Jan Kofroň, "Framework for Static Analysis of PHP Applications", in Proceedings of the 29th European Conference on Object-Oriented Programming (ECOOP 2015), LIPIcs, Vol. 37, pp. 689–711, 2015.
http://dx.doi.org/10.4230/LIPIcs.ECOOP.2015.689

Related Conference 29th European Conference on Object-Oriented Programming (ECOOP 2015), July 5–10, 2015, Prague, Czech Republic

1 Scope

The artifact is designed to support repeatability of all the experiments of the companion paper, allowing users to test the Weverca analyzer on a variety of benchmarks. In particular, we bundle two PHP applications to test the functionality. They include myBloggie [2], a php mysql based weblog script, and NOCC [1], a webmail client providing webmail access to IMAP and POP3 accounts. We also bundle three simple scripts to test the application on a particular machine. The framework is also available under a web interface at http://perun.ms.mff.cuni.cz/weverca. The project web page with up-to-date information can be found at http://d3s.mff.cuni.cz/projects/formal_methods/weverca/. Note that the performance of the tool can be improved (in terms of running time and memory requirements and sometimes also a lower false-positive rate) comparing to the one reported in the paper.

Dagstuhl Artifacts Series, Vol. 1, Issue 1, Artifact No. 11, pp. 11:1–11:2
DAGSTUHL ARTIFACTS SERIES Dagstuhl Artifacts Series
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

2 Content

The artifact package includes:

- bin: folder containing the binaries. Both 32 and 64-bit binaries are available.
- php_sources: folder containing several PHP frameworks and applications to be analyzed by Weverca, especially the NOCC and MyBloggie PHP applications.
- src: folder containing the source of Weverca. It contains MS Visual Studio projects and a solution with setting
- index.html: Web page
- Example*.cmd/Mono_Example*.cmd: Scripts for running analysis of the examples contained in the php_sources folder for .NET/Mono.
- Example*.out: Outputs of the analyses, for reference.
- Test.cmd: The test script, whether the framework works on the machine.
- Test.out: The output of the test analysis.
- howto.pdf: Information for compiling and running the framework and description of the output of the framework.

3 Getting the artifact

The artifact endorsed by the Artifact Evaluation Committee is available free of charge on the Dagstuhl Research Online Publication Server (DROPS). The latest version of our code is available on the project webpage: http://d3s.mff.cuni.cz/projects/formal_methods/weverca/.

4 Tested platforms

The artifact is known to work on Windows 8.1 64-bit with .NET framework version 4.5+ and on Linux using mono 3. In the howto.pdf file accompanying the artifact, we provide instructions to build the framework under these systems. There is no particular reason why the system would not work on any newer versions of OSs and libraries.

5 License

GNU Lesser General Public License version 3 (http://www.gnu.org/licenses/).

6 MD5 sum of the artifact

e48e98ac2ee9796802637984c3ba932e

7 Size of the artifact

87 MB

Acknowledgments. The authors wish to thank the Weverca project team for their valuable contribution.

References

1 NOCC, http://nocc.sourceforge.net/

2 myBloggie, http://mybloggie.mywebland.com/