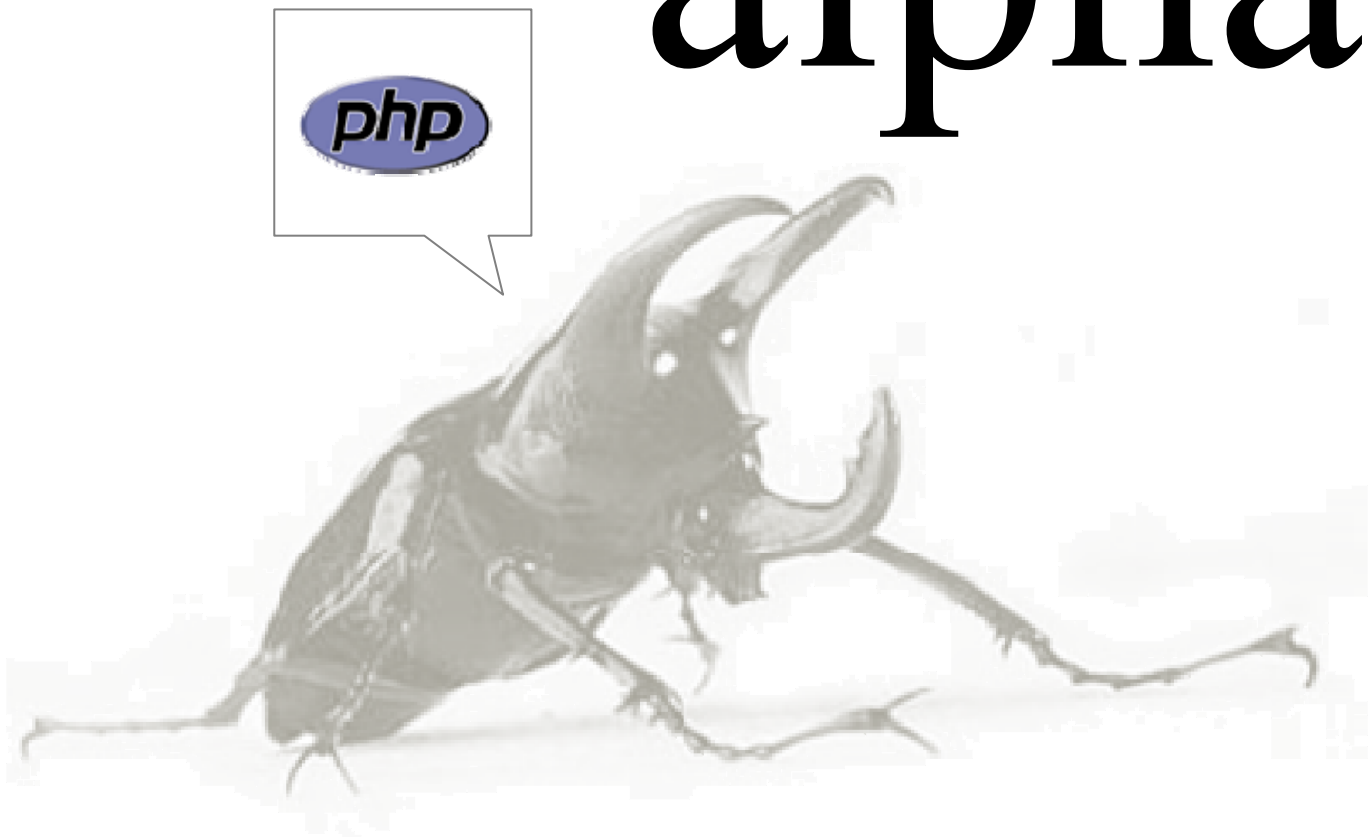
10/09

OWASP
The Open Web Application Security Project

Installation Guide

OWASP ESAPI for PHP 1.0a

alpha



This page is intentionally blank

Foreword

This document provides instructions for installing version 1.0a of the PHP language version of the OWASP Enterprise Security API (ESAPI). OWASP ESAPI toolkits help software developers guard against security-related design and implementation flaws. Just as web applications and web services can be Public Key Infrastructure (PKI) enabled (PK-enabled) to perform for example certificate-based authentication, applications and services can be OWASP ESAPI-enabled (ES-enabled) to enable applications and services to protect themselves from attackers.

We'd Like to Hear from You

Further development of ESAPI occurs through mailing list discussions and occasional workshops, and suggestions for improvement are welcome. Please address comments and questions concerning the API and this document to the ESAPI mail list, owasp-esapi@lists.owasp.org

Copyright and License

This page is intentionally blank

Table of Contents

This page is intentionally blank

1 About ESAPI for PHP

OWASP ESAPI toolkits help software developers guard against security-related design and implementation flaws. Just as web applications and web services can be Public Key Infrastructure (PKI) enabled (PK-enabled) to perform for example certificate-based authentication, applications and services can be OWASP ESAPI-enabled (ES-enabled) to enable applications and services to protect themselves from attackers.

The ESAPI for PHP distribution media contains the following:

- The PHP (`.php`) and XML(`.xml`) files comprising the ESAPI FOR PHP toolkit.
- Sample code.
- Product documentation consisting of:
    - This document, the *OWASP ESAPI for PHP Installation Guide*, in Portable Document Format (PDF), with instructions on how to install and build ESAPI FOR PHP.
    - <… to do… e.g. …This document, the *OWASP ESAPI for PHP Release Notes*, in Portable Document Format (PDF), with the latest information on ESAPI FOR PHP. >
    - <… to do… need interface docs…>
    - <… to do… need programming manual…>

This page is intentionally blank

2 Prerequisites

Before you start the installation, ensure that:

- The system you are installing on has 100 MB of free disk space.
- You have read these installation instructions.
- You have installed PHP 5.2 or above, and have set (for example) the Windows PATH environment variable appropriately.
- One or more of the following is installed:
    - Eclipse 3.5 or newer, with PDT 2.1 or newer
    - NetBeans 6.7 or newer

This page is intentionally blank

3 Installation

3.1 Distribution Directory Structure

The following describes the ESAPI for PHP distribution structure.

Directory	Content
`<root>/`	
`readme.txt`	
`PHP-ESAPI_1.0_install.pdf`	*OWASP ESAPI for PHP Installation Guide*
`PHP-ESAPI_1.0_ReleaseNotes.pdf`	*OWASP ESAPI for PHP Release Notes*
`doc/`	ESAPI interface documentation files
`lib/`	
`apache-log4php/`	
`htmlpurifier/`	
`simpletest/`	
`src/`	
`*.php`	ESAPI locator and interface classes
`codecs/`	
`errors/`	
`filters/`	
`reference/`	ESAPI sample reference implementation
`validation/`	
`sample/`	ESAPI sample source code

To install ESAPI for PHP:

1. Copy the ESAPI for PHP distribution directory structure into a suitable location on the target machine.
2. Copy the ESAPI for PHP configuration file (`ESAPI.xml`) from the `/test/testresources` directory to a suitable location outside of the document root on the target machine.

3.2 Build and Run the Samples

This release of ESAPI for PHP has samples to demonstrate the security controls of a sample ESAPI reference implementation.

- There is a main test script in the `AllTests.php` file in the `/test` directory.
- There is sample code in the form of ESAPI reference implementation tests in the `/test/reference` directory.
- There is a sample ESAPI for PHP configuration file and ESAPI reference implementation test data in the `/test/testresources` directory.

The simplest way to build and run the samples for ESAPI for PHP is to create an Integrated Development Environment (IDE) project from the source files.

To create a new Eclipse project from the source files:

1. Open the Eclipse IDE.
2. Create a new PHP project:
    a. From the File menu, select "New".
    b. From the New submenu, select "PHP Project".
    c. Specify a suitable project name in the "Project name" field.
    d. Select the "Create project from existing source" radio button, and specify the location on the target machine where ESAPI for PHP was copied.
3. Click on the "Finish" button.

To build the sample code and to run the samples using Eclipse:

1. Navigate to the `/test/AllTests.php` file using the Eclipse IDE "PHP Explore" tab.
2. Right-click on the `AllTests.php` file.
3. From the pop-up menu, select "Run As".
4. From the pop-up submenu, select "PHP Script".

The sample code output can then be examined from the Eclipse IDE "Browser Output" tab.

<…to do… add equivalent NetBeans instructions…>

4 Uninstallation Instructions

To uninstall ESAPI for PHP on all platforms, remove all files and directories created during the installation process.

This page is intentionally blank

5 Where to Go From Here

OWASP is the premier site for Web application security. The OWASP site hosts many projects, forums, blogs, presentations, tools, and papers. Additionally, OWASP hosts two major Web application security conferences per year, and has over 80 local chapters. The OWASP PHP project page can be found here http://www.owasp.org/index.php/ESAPI

The following OWASP projects are most likely to be useful to users/adopters of ESAPI:

- OWASP Application Security Verification Standard (ASVS) Project - http://www.owasp.org/index.php/ASVS
- OWASP Top Ten Project - http://www.owasp.org/index.php/Top_10
- OWASP Code Review Guide - http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
- OWASP Testing Guide - http://www.owasp.org/index.php/Testing_Guide
- OWASP Legal Project - http://www.owasp.org/index.php/Category:OWASP_Legal_Project

Similarly, the following Web sites are most likely to be useful to users/adopters of ESAPI:

- OWASP - http://www.owasp.org
- MITRE - Common Weakness Enumeration – Vulnerability Trends, http://cwe.mitre.org/documents/vuln-trends.html
- PCI Security Standards Council - publishers of the PCI standards, relevant to all organizations processing or holding credit card data, https://www.pcisecuritystandards.org
- PCI Data Security Standard (DSS) v1.1 - https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

This page is intentionally blank

This page is intentionally blank

THE ICONS BELOW REPRESENT WHAT OTHER VERSIONS ARE AVAILABLE IN PRINT FOR THIS BOOK TITLE.

ALPHA: "Alpha Quality" book content is a working draft. Content is very rough and in development until the next level of publishing.

BETA: "Beta Quality" book content is the next highest level. Content is still in development until the next publishing.

RELEASE: "Release Quality" book content is the highest level of quality in a book title's lifecycle, and is a final product.

ALPHA **BETA** **RELEASE**

YOU ARE FREE:

to Share – to copy, distribute and transmit the work

to Remix – to adapt the work

UNDER THE FOLLOWING CONDITIONS:

Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

OWASP
The Open Web Application Security Project

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.