OWASP
The Open Web Application Security Project

# OWASP ESAPI for PHP Adapter 1.0a2

*Release Notes*

alpha

This page is intentionally blank

## OWASP ESAPI for PHP Adapter Release Notes

This document summarizes the features of version 1.0a2 of an OWASP Enterprise Security API (ESAPI) adapter that is compatible with the PHP language version of the ESAPI core module. It outlines the features, platform information, and security control functionality. ESAPI security control interfaces and reference implementations are collectively called the *ESAPI core module*. Encapsulating security control implementations are called *ESAPI adapters*. Encapsulating security control implementations are called *ESAPI adapters*. The OWASP ESAPI for PHP Adapter is an example of an encapsulating security control that implements an extended factory pattern.

## 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

# Features

The ESAPI for PHP Adapter example implements an extended factory pattern as depicted in the figure below that consists of a new ESAPI security control interface and corresponding implementation, which in turn calls ESAPI security control reference implementations and/or security control reference implementations that were replaced with your own implementations. The ESAPI locator class would be called in order to retrieve a singleton instance of your new security control, which in turn would call ESAPI security control reference implementations and/or security control reference implementations that were replaced with your own implementations.

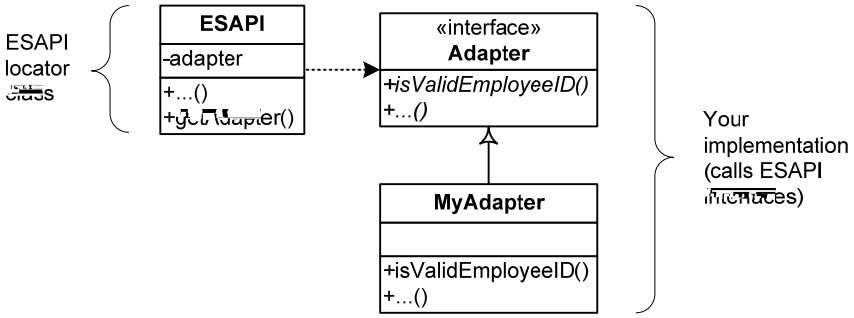



**Figure: Extended Factory Pattern Adapter**

The features in this release of ESAPI for PHP Adapter include:

- ESAPI adapter implements an example of an extended factory pattern as defined in *OWASP ESAPI Design Patterns*.
- ESAPI adapter reference implementation that calls the following security controls:
  - Input Validation
  - Security Configuration
- Fixes for specific issues. For more information, see "Enhancements and Resolved Issues".

# Platform Information

The following table lists the platforms and operating systems supported by ESAPI for PHP Adapter at the time of release, and details runtime environment information.

**Table 1: Platform Information**

| Manufacturer | Operating System | CPU Architecture | CPU Size | Interpreter Version |
|---|---|---|---|---|
| Microsoft® | Windows XP Professional SP3 | x86 | 32-bit | PHP 5.2.5 |
| | Windows Server 2003 | x86 | 32-bit | PHP 5.2.5 |
| | Windows Server 2008 | x86 | 32-bit | PHP 5.2.5 |
| | Windows Vista™ Enterprise | x86 | 32-bit | PHP 5.2.5 |
| | | | | PHP 5.2.5 |
| openSuSE | 10.3 | x86 | 32-bit | PHP 5.2.5 |
| | | | | PHP 5.2.5 |
| Sun | Solaris™ 10 | SPARC v8+ | 32-bit | PHP 5.2.5 |
| | | | | PHP 5.2.5 |
| Red Hat® | Enterprise Linux AS 5.0 | x86 | 32-bit | PHP 5.2.5 |



If you are interested in using ESAPI for PHP Adapter on a platform or operating system not listed above, email the ESAPI mail list, owasp-esapi@lists.owasp.org

## Interoperability

The following table lists the vendor products that have been tested and interoperate with ESAPI for PHP Adapter.

**Table 2: Vendor Product Interoperability**

| Product | Version |
|---|---|
| ESAPI for PHP core | 1.0a1 |

## Enhancements and Resolved Issues

The following table lists the enhancements and resolved issues in this release of ESAPI for PHP.

Table 3: Enhancements and Resolved Issues

FIRST RELEASE

| ID | Description |
|---|---|

## Known Issues

The following table lists the known issues in this release of ESAPI for PHP.

Table 4: Known Issues

NO KNOWN ISSUES

| ID | Description |
|---|---|

## Documentation

The ESAPI for PHP Adapter documentation suite includes:

- This document, the *OWASP ESAPI for PHP Adapter Release Notes*, in Portable Document Format (PDF), with the latest information on ESAPI for PHP Adapter.
- The *OWASP ESAPI for PHP Adapter Installation Guide*, in PDF, with instructions on how to install and build ESAPI for PHP.
- The *OWASP ESAPI Design Patterns*, in PDF, which explores common ESAPI design patterns.

# 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 ESAPI 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

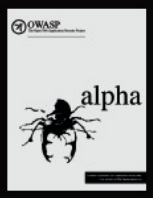
This page is intentionally blank

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

**ALPHA:** “Alpha Quality” book content is a working draft. Content is very rough and in development until the next level of publication.

**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 books title’s lifecycle, and is a final product.




**ALPHA**
PUBLISHED

**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 aatribute 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.