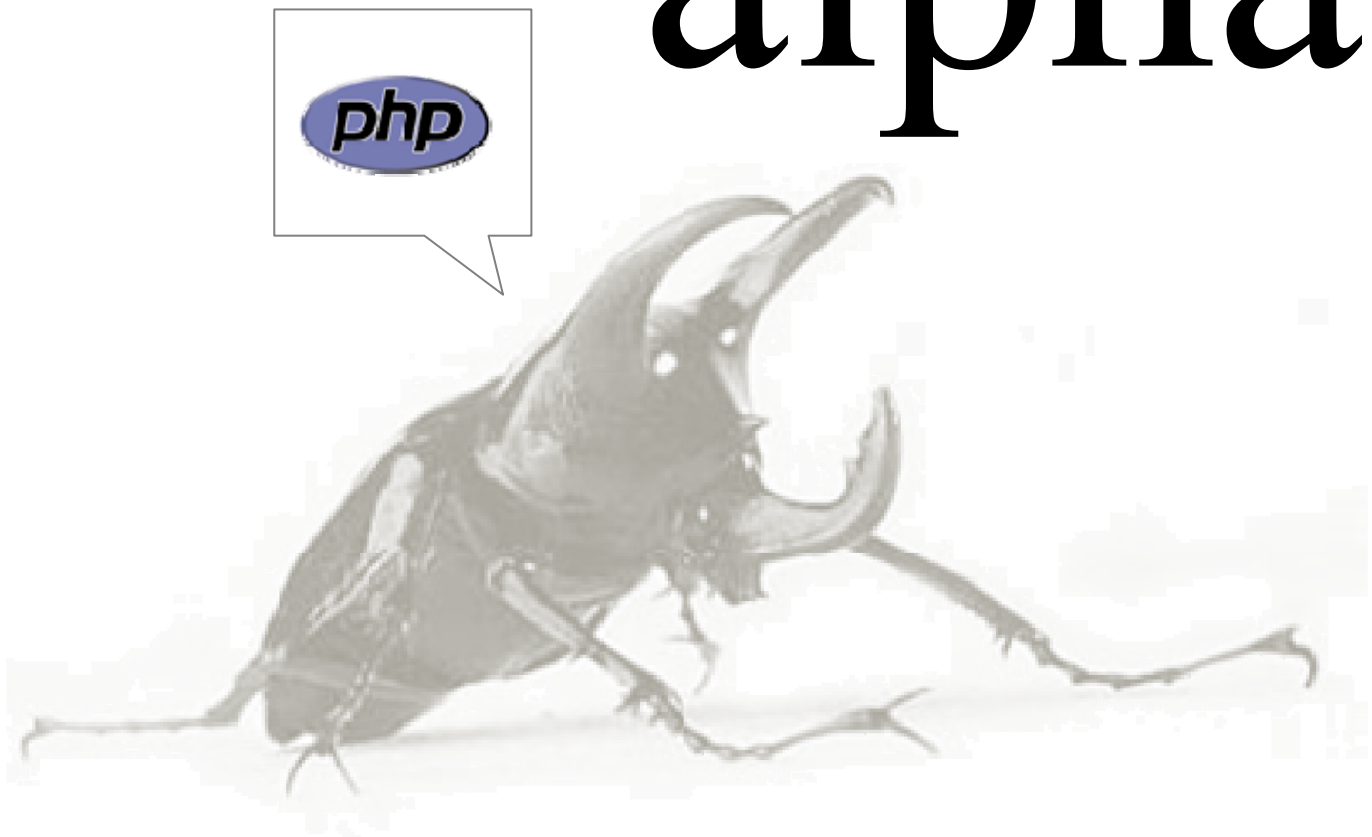
10/09

OWASP
The Open Web Application Security Project

Release Notes

OWASP ESAPI for PHP 1.0a

alpha



This page is intentionally blank

Foreword

This document summarizes the features of version 1.0a of the PHP language version of the OWASP Enterprise Security API (ESAPI). It outlines the features, platform information, and security control functionality. 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 Features

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 features in this release of ESAPI for PHP include:

- ESAPI locator and interface classes that are compliant with the ESAPI for Java version 1.4 design.
- ESAPI security control reference implementations for the following security controls:
    - AccessController
    - AccessReferenceMap
    - Authenticator
    - Encoder
    - EncryptedProperties
    - Encryptor
    - Executor
    - HTTPUtilities
    - IntrusionDetector
    - LogFactory
    - Randomizer
    - SecurityConfiguration
    - User
    - Validator
- Fixes for specific issues. For more information, see “Enhancements and Resolved Issues”.

2 Platform Information

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

Table 1: Platform Information

Manufacturer	Operating System	CPU Architecture	CPU Size	Compiler Version
Microsoft®	Windows XP Professional SP3	x86	32-bit	PHP 5.2
	<…to do…>	<…to do…>	<…to do…>	PHP 5.2
	<…to do…>	<…to do…>	<…to do…>	PHP 5.2
	<…to do…>	<…to do…>	<…to do…>	PHP 5.2
Sun	Solaris™ 10	SPARC v8+	32-bit	PHP 5.2
	<…to do…>	<…to do…>	<…to do…>	PHP 5.2
	<…to do…>	<…to do…>	<…to do…>	PHP 5.2
Red Hat®	Enterprise Linux AS 5.0	x86	32-bit	PHP 5.2
	<…to do…>	<…to do…>	<…to do…>	PHP 5.2
	<…to do…>	<…to do…>	<…to do…>	PHP 5.2

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

3 Interoperability

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

Table 2: Vendor Product Interoperability

Product	Version
apache-log4php	<…to do…track down version>
htmlpurifier	<…to do…track down version>
simpletest	<…to do…track down version>

4 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

ID	Description
<…to do…>	<…to do…>
<…to do…>	<…to do…>

5 Known Issues

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

Table 4: Known Issues

ID	Description
<…to do…>	<…to do…>
<…to do…>	<…to do…>

6 Documentation

The ESAPI for PHP documentation suite includes:

- This document, the *OWASP ESAPI for PHP Release Notes*, in Portable Document Format (PDF), with the latest information on ESAPI FOR PHP.
- This *OWASP ESAPI for PHP Installation Guide*, in Portable Document Format (PDF), with instructions on how to install and build ESAPI FOR PHP.
- <… to do… need interface docs…>
- <… to do… need programming manual…>

7 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.