OWASP

The Open Web Application Security Project

OWASP ESAPI for PHP 1.0a1
Release Notes

alpha

This page is intentionally blank

<div align="center">**OWASP ESAPI for PHP Release Notes**</div>

This document summarizes the features of version 1.0a1 of the PHP language version of the OWASP Enterprise Security API (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*. OWASP ESAPI Toolkits are designed to ensure that strong simple security controls are available to every developer in every environment.

<div align="center">**We'd Like to Hear from You**</div>

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

<div align="center">**Copyright and License**</div>

This page is intentionally blank

Table of Contents

This page is intentionally blank

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 core classes that are compliant with the ESAPI for Java version 1.4 design.

- ESAPI security control reference implementations for the following security controls:

    o Access Control

    o Input Validation

    o Output Escaping

    o Encryption

    o Random Numbers

    o Exception Handling

    o Logging

    o 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 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 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.

Table 2: Vendor Product Interoperability

Product	Version
apache-log4php	Pre-release version that includes fixes submitted by the ESAPI for PHP development team to the Apache log4php team. Note this version is included in the ESAPI for PHP distribution media.
htmlpurifier	4.0.0 Note this version is included

in the ESAPI for PHP distribution media.

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

FIRST RELEASE

Known Issues

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

Table 4: Known Issues

ID	Description
1234	Authentication not yet implemented.
1235	Identity not yet implemented.
1236	Intrusion detection not yet implemented.
1237	Access control partially-implemented.
1238	Input validation partially-implemented
1239	Output escaping partially-implemented
1240	Encryption partially- implemented
1241	Logging tests should check that records find their way into the log (Google Code Issue #4)
1242	BaseValidationRule is missing the sanitize function (Google Code Issue #8)

| 1243 | HTTPUtilities missing getParameter (Google Code Issue #15) |
| 1244 | Codec UTF-32 encoded strings not detected properly in codecs (Google Code Issue #26) |

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.

- The *OWASP ESAPI for PHP 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

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

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.