OWASP
The Open Web Application Security Project

OWASP ESAPI for PHP Adapter 1.0a2

Installation Guide

alpha

This page is intentionally blank

OWASP ESAPI for PHP Adapter Installation Guide

This document provides instructions for installing version 1.0a2 of an OWASP Enterprise Security API (ESAPI) adapter that is compatible with the PHP language version of the ESAPI core module. ESAPI security control interfaces and reference implementations are collectively called the *ESAPI core module*. 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

About ESAPI for PHP Adapter

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.

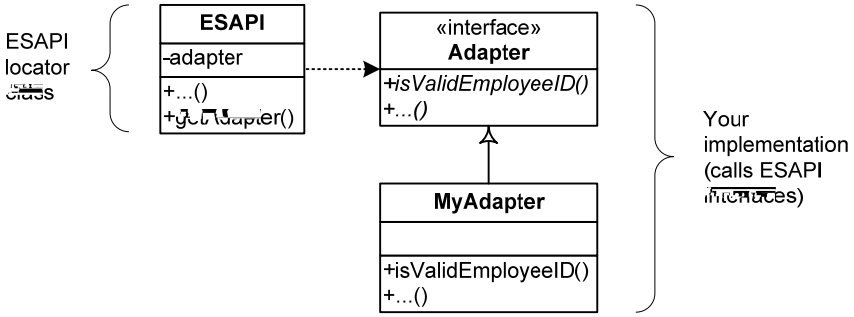


Figure: Extended Factory Pattern Adapter

The ESAPI for PHP distribution media contains the following:

- The PHP (`.php`) files comprising the ESAPI for PHP adapter example.
- Sample code.
- Product documentation consisting of:
  - This document, the *OWASP ESAPI for PHP Adapter Installation Guide*, in Portable Document Format (PDF), with instructions on how to install and build ESAPI for PHP Adapter.
  - The *OWASP ESAPI for PHP Adapter Release Notes*, in PDF, with the latest information on ESAPI for PHP Adapter.
  - The *OWASP ESAPI Design Patterns*, in PDF, which explores common ESAPI design patterns.

Prerequisites

Before you start the installation, ensure that:

- The system you are installing on has 1 MB of free disk space.
- You have read these installation instructions.
- You have installed ESAPI for PHP 1.0a1, and have set environment variables appropriately.

Installation

Distribution Directory Structure

The following describes the ESAPI for PHP distribution structure.

Directory	Content
`<root>/`	
`license.txt`	ESAPI license file
`readme.txt`	ESAPI readme file
`doc/`	ESAPI documentation
`sample/`	ESAPI sample source code
`src/`	ESAPI adapter source code

To install ESAPI for PHP Adapter:

1. Copy the `<root>/src/Adapter.php` file to the `<root>/src` directory on the target machine where the ESAPI for PHP core was installed.
2. Create a directory `<root>/src/adapters` on the target machine where the ESAPI for PHP core was installed.
3. Copy the `<root>/src/adapters/MyCompanyAdapter.php` file to the `<root>/src/adapters` directory on the target machine.
4. If you have not done so already as part of installing the ESAPI for PHP core, create a new project from source code using the ESAPI for PHP distribution.
5. Navigate to the `src` directory.
6. In `ESAPI.php`, add a private static member variable for the adapter to the ESAPI locator class and set its initial value to null:

```
private static $adapter = null;
```

7 In `ESAPI.php`, add a set of ESAPI security control get and set functions to the ESAPI locator class:

```
public static function getAdapter() {
       if ( is_null(self::$adapter) ) {
            require_once dirname(__FILE__).
                    '/adapters/MyCompanyAdapter.php';
            self::$adapter = new MyCompanyAdapter();
        }
        return self::$adapter;
    }

public static function setAdapter($adapter) {

        self::$adapter = $adapter;

    }
```

Build and Run the Samples

This release of ESAPI for PHP Adapter includes sample code to demonstrate its functionality.

To build the sample code:

1 Open the project created from ESAPI for PHP core and adapter source code.

2 Navigate to the location where you installed `ESAPI.xml`, the ESAPI configuration file, as part of installing the ESAPI for PHP core.

3 In `ESAPI.xml`, navigate to:

```
/esapi-properties/Validator/ValidationExpressions
```

4 In `ESAPI.xml`, duplicate `/regexp/SafeString`, and set the name of the `regexp` duplicate to "`EmployeeID`" and the value to "`[0-9][0-9][0-9][0-9][0-9][0-9]`".

5 Navigate to the `sample` directory.

6 In the SampleAdapter.php file, set the value of ESAPI configuration file to the correct path.

```
$ESAPI = new ESAPI(
       dirname(__FILE__)."/../ESAPI.xml");
```

7 Run the `SampleAdapter.php` file as a PHP script.

Uninstallation Instructions

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

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

This page is intentionally blank

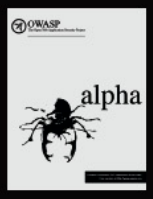
This page is intentionally blank

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.