Technical white paper

How to Use AntiSamy Feature in PPM Center

Table of contents

Introduction

This article intends to illustrate the AntiSamy feature in PPM Center. This feature gains wisdom from the OWASP AntiSamy project. Generally speaking, AntiSamy is an HTML, CSS, and JavaScript filter that sanitizes user input based on a policy file. For more information about OWASP AntiSamy project, see https://www.owasp.org/index.php/Category:OWASP_AntiSamy_Project.

For PPM, AntiSamy makes sure user's HTML, CSS and JavaScript input strictly follows rules defined by the policy file `antisamy-ppm.xml`. For example, if you enable the AntiSamy feature, you cannot open hyperlinks on request details page or project details page. This is because the hyperlink-kind input by default does not meet the rules defined by `antisamy-ppm.xml`. To make hyperlinks accessible in PPM, you can configure the policy file as you demand.

Enabling/Disabling the AntiSamy Feature

You can enable or disable the AntiSamy feature by setting the server configuration parameter `ENABLE_ANTISAMY` in the `server.conf` file.

If you set the parameter to `true`, your enable the AntiSamy feature. User's HTML, CSS, and JavaScript input will be monitored by the policy file `antisamy-ppm.xml`.

If you set the parameter to `false`, you disable the AntiSamy feature. User's HTML, CSS, and JavaScript input will not be monitored.

By default, the AntiSamy feature is enabled. And HP recommends that you keep the AntiSamy feature enabled.

Configuring AntiSamy Policy File

1. Open the policy file `antisamy-ppm.xml` located in the `<PPM_HOME>\conf` directory.
2. Configure the following sections of the policy file as you want.
   - **Directives**

     The following table shows the directives, their default values, and their impact on the AntiSamy filtering process.

Directive	Type	Default Value	Description
omitXmlDeclaration	boolean	true	When "useXHTML" is turned on, AntiSamy will automatically prepend the XML header. Enabling this feature will tell AntiSamy not to do that.
omitDoctypeDeclaration	boolean	true	When this feature is enabled, AntiSamy will automatically prepend the HTML doctype declaration.
maxInputSize	int	600000000	This directive specifies the maximum size (in bytes) of user input before it is validated.
useXHTML	boolean	true	When this feature is enabled, AntiSamy will output the sanitized data in XHTML format as opposed to just regular HTML.
formatOutput	boolean	true	When this feature is enabled, AntiSamy will automatically format the output according to some basic rules and indentation. Kind of like "pretty print."
embedStyleSheets	boolean	false	When the developer chooses to allow CSS, this directive will specify whether or not remote stylesheets found

			referenced in the user's input will be pulled down and embedded into the current user input.
connectionTimeout	int	5000	When "embedStyleSheets" is enabled, this timeout value (in milliseconds) will be used when fetching the offsite resource in question. This should be used to prevent validation threads from blocking when connecting to 3rd party systems that may purposefully act really slowly.
maxStyleSheetImports	int	3	This feature allows developers to specify how many remote stylesheets can be downloaded from any one input.

Note: The `antisamy-ppm.xml` file only deploys some of the directives provided by the OWASP AntiSamy project. You can include more directives when configuring the policy file. For more information about other directives, see *AntiSamy User Guide*.

- **Common Regular Expressions**

  You can declare regular expressions here that can be used in the rest of the policy file.

  Example:

  ```
  <regexp value="[a-zA-Z0-9\:\-_\.]+" name="htmlId"/>
  ```

  This regular expression is used to determine whether text in an `id` attribute is valid or not.

- **Common Attributes**

  You can declare attributes here that are common to many different tags.

  Example:

  ```
  <attribute name="id" description="The 'id' of any HTML attribute should
  not contain anything besides letters and numbers">
     <regexp-list>
  ```

```
      <regexp name="htmlId"/>
   </regexp-list>
</attribute>
```

This is where the `id` attribute is mapped to the `htmlId` regular expression.

- **Global Tag Attributes**

  You can declare attributes here that are global to all different tags.

  Example:

  ```
  <attribute name="id"/>
  ```

  The `id` attribute is global to all different tags.

- **Tags to Encode**

  You can declare tags that will not be removed, filtered, validated, or truncated, but encoded using HTML entities.

  Example:

  ```
  <tag>g</tag>
  ```

  The `g` tag does not actually do anything, but it is not malicious either, so you can encode it, rather than remove it.

- **Tag Rules**

  You can define parsing rules here that will be used for each tag individually. What happens to tags depends on what actions AntiSamy has decided to perform on it. PPM's AntiSamy policy file by default includes the following actions for tags.

  - **Remove**: When the tag rule action is set to "remove" for a given tag, the tag is deleted with all of its child text.

    Example:

    ```
    <tag name="script" action="remove"/>
    ```

  - **Validate**: When the tag rule action is set to "validate" for a given tag, PPM verifies if its attributes and children elements follow rules defined in the policy file.

    Example:

```
<tag name="a" action="validate">
  <attribute name="href">
    <regexp-list>
      <regexp name="ppm-report-token"/>
    </regexp-list>
  </attribute>
</tag>
```

- **Truncate**: When the tag rule action is set to "truncate" for a given tag, the element of the tag is kept, but all its attributes are removed.

  Example:

  ```
  <tag name="title" action="truncate"/>
  ```

  Note: Apart from the above tag rules, you can also use "default" and "filter" to build you own tag rules. For information about more tag rules, see *AntiSamy User Guide*.

- **CSS Rules**

  You can define parsing rules here that will be used for each CSS property individually. Only CSS defined in this section is allowed.

  Example:

  ```
  <property name="background-position" description="If a background image
  has been specified, this property specifies its initial position.">
     <literal-list>
        <literal value="top"/>
        <literal value="center"/>
        <literal value="bottom"/>
        <literal value="left"/>
        <literal value="center"/>
        <literal value="right"/>
        <literal value="inherit"/>
     </literal-list>
     <regexp-list>
        <regexp name="percentage"/>
        <regexp name="length"/>
     </regexp-list>
  </property>
  ```

  The CSS background position property is allowed only when it matches these rules. Its value must be a percentage, length, or one of the literal values such as "top" and "center".

3. Save the changes.

4. Restart PPM Server.

Usage Example

The `antisamy-ppm.xml` file by default has the following tag rule:

```
<tag name="a" action="validate">
  <attribute name="href">
    <regexp-list>
      <regexp name="ppm-report-token"/>
    </regexp-list>
  </attribute>
</tag>
```

This means if an end user inputs a hyperlink in a field, the hyperlink cannot be opened from the PPM pages, unless the hyperlink is in conformity with the regular expression "ppm-report-token", which is defined as follows in the policy file.

```
<regexp value="\[\w+\.\S+\]" name="ppm-report-token"/>
```

If you want to open hyperlinks from PPM pages, you should delete or edit the regulation expression in the above tag rule. For example, you can change the tag rule into the followings:

> **Caution:** The regular expression "ppm-report-token" mitigates most attack vectors such as XSS. If you delete this regular expression, some PPM pages will not be protected from XSS. HP highly recommends that you exercise caution when deleting or editing the regular expression.

```
<tag name="a" action="validate">
  <attribute name="href">
  </attribute>
</tag>
```

Or

```
<tag name="a" action="validate">
  <attribute name="href">
    <regexp-list>
      <regexp name="anything"/>
    </regexp-list>
  </attribute>
</tag>
```

where `<regexp value=".*" name="anything"/>`

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.