

[<< Back to Dashboard](#)

Exploring the AntiSamy Plugin

Contents

- [Exploring the AntiSamy Plugin](#)
 - [Overview](#)
 - [Custom Policies](#)
 - [HtmlSanitizer](#)
 - [Returns](#)
 - [Arguments](#)
 - [Examples](#)
 - [Policies](#)

Overview

[OWASP AntiSamy](#) Project that provides [XSS](#) cleanup operations to ColdBox applications

Custom Policies

The AntiSamy plugin comes with several boilerplate policies that you can use, but we recommend creating your own policy to match your requirements. Once you do this, you can easily integrate it into the plugin in three steps:

1. Create a policy file based on the ones shipped and store it wherever you like in your application.
2. Create a custom setting in your application with the path to this custom file:

AntiSamy_Custom_Policy

```
// custom settings
settings = {
  AntiSamy_Custom_Policy = expandPath("#appMapping#/includes/MyAntiSamy.xml")
};
```

3. You can now call the AntiSamy's *HTMLSanitizer()* method with **custom** as the policy to use.

```
clean = getPlugin("AntiSamy").HTMLSanitizer(rc.text, "custom");
```

HtmlSanitizer

clean HTML from XSS scripts using the AntiSamy project. The available policies are *antisamy*, *ebay*, *myspace* or *slashdot*

Returns

- This function returns *Any*

Arguments

Key	Type	Required	Default	Description
HtmlData	string	Yes	---	The html text to sanitize
PolicyFile	string	No	<i>myspace</i>	Provide policy file to scan html. Available options are: antisamy , ebay , myspace , slashdot , custom
resultsObject	boolean	false	false	Return the cleaned HTML or the results object. By default it is the cleaned HTML

Examples

```
// Clean a single variable
rc.cleanData = getPlugin("AntiSamy").HtmlSanitizer(rc.comments);
rc.cleanData = getPlugin("AntiSamy").HtmlSanitizer(rc.comments,"ebay");

// Clean the entire request collection
for(key in rc){
  if( isSimpleValue(rc[key]) ){
    rc[key] = getPlugin("AntiSamy").HtmlSanitizer(rc[key]);
  }
}

clean = getPlugin("AntiSamy").HTMLSanitizer(rc.text,"custom");
```

Policies

The policies that we offer are all the [policies](#) offered by the OWASP Antisamy project:

- Ebay
- SlashDot
- AntiSamy
- MySpace
- Custom (Only if you declare the **AntiSamy_Custom_Policy** setting)