OWASP Java Encoder Project

From OWASP

Main | Use the Java Encoder Project | Deploy the Java Encoder Project | Grave Accent Issue | Roadmap [edit]

The general API pattern is to utilize the Java Encoder Project in your user interface code and wrap all variables added dynamically to HTML with a proper encoding function. The encoding pattern is **"Encode.forContextName(untrustedData)"**, where "ContextName" is the name of the target context and "untrustedData" is untrusted output.

Basic HTML Context

```
<body><%= Encode.forHtml(UNTRUSTED) %></body>
```

HTML Content Context

```
<textarea name="text"><%= Encode.forHtmlContent(UNTRUSTED) %></textarea>
```

HTML Attribute context

```
<input type="text" name="address" value="<%= Encode.forHtmlAttribute(UNTRUSTED) %>" />
```

Generally **Encode.forHtml(UNTRUSTED)** is also safe but slightly less efficient for the above two contexts (for textarea content and input value text) since it encodes more characters than necessary but might be easier for developers to use.

CSS contexts

```
<div style="width:<= Encode.forCssString(UNTRUSTED) %>">
<div style="background:<= Encode.forCssUrl(UNTRUSTED) %>">
```

Javascript Block context

```
 <script type="text/javascript">
 var msg = "<%= Encode.forJavaScriptBlock(UNTRUSTED) %>";
 alert(msg);
 </script>
```

Javascript Variable context

```
<button
onclick="alert('<%= Encode.forJavaScriptAttribute(UNTRUSTED) %>');">
click me</button>
```

JavaScript Content Notes: **Encode.forJavaScript(UNTRUSTED)** is safe for the above two contexts, but encodes more characters and is less efficient.

Encode URL parameter values

```
<a href="/search?value=<%= Encode.forUriComponent(UNTRUSTED) %>&order=1#top">
```

Encode REST URL parameters

```
<a href="/page/<%= Encode.forUriComponent(UNTRUSTED) %>">
```

Handling an Full Untrusted URL

When handling a full url with the OWASP Java encoder, first verify the URL is a legal URL.

```
String url = validateURL(untrustedInput);
```

Then encode the URL as an HTML attribute when outputting to the page. Note the linkable text needs to be encoded in a different context.

```
<a href="<%= Encode.forHtmlAttribute(untrustedUrl) %>">
<%= Encode.forHtmlContent(untrustedLinkName) %>
</a>
```

To use in a JSP with EL

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
   "http://www.w3.org/TR/html4/loose.dtd">
<%@taglib prefix="e" uri="https://www.owasp.org/index.php/OWASP_Java_Encoder_Project" %>
<html>
   <head>
       <title><e:forHtml value="${param.title}" /></title>
   </head>
   <body>
       <h1>${e:forHtml(param.data)}</h1>
   </body>
</html>
```

Other contexts can be found in the org.owasp.Encode class methods, including CSS strings, CSS urls, XML contexts, URIs and URI components.

Retrieved from "https://www.owasp.org/index.php?title=OWASP_Java_Encoder_Project&oldid=203949"
Categories: OWASP Tool | OWASP Alpha Quality Tool | OWASP Project

- This page was last modified on 29 November 2015, at 12:51.
- This page has been accessed 96,434 times.
-