

master patches-hotfixes / com.dotcms.security.matrixparams /



swicken-dotcms dotCMS/core#23002 - Changed null return to a strin... on Sep 15 History

..

build/libs	2 months ago
gradle/wrapper	6 months ago
src/main/java/com/dotcms/security/matrixparams	2 months ago
.gitignore	6 months ago
README.md	4 months ago
build.gradle	6 months ago
gradlew	6 months ago
gradlew.bat	6 months ago

☰ README.md

MatrixParameter Security Interceptor

This plugin adds a web interceptor that prevents dotCMS from accepting "matrix" parameters in uris. A matrix parameter is a non-standard parameter list that is started with a semi-colon. Java app servers like tomcat and old school j2ee applications used to use matrix parameters to encode the JSESSIONID on the end of a url, e.g. urls like:

```
https://oldapplication.com/index.jsp;JSESSIONID=AAABBB4532154
```

The issue is that by allowing matrix parameters allows for security filters based on URIs to be bypassed, in this example the dotCMS XSS prevention filter.

In an abundance of caution, this Interceptor also disallows other non-standard URI characters that are commonly used in attacks. Below is a list of characters that are explicitly disallowed.

```
";",
"..",
"//",
"/./",
"\\",
"?",
"%3B", // encoded semi-colon
"%2E", // encoded period '.'
"%2F", // encoded forward slash '/'
"%5C", // encoded back slash '\'
"%3F", // encoded questionmark
"%3D", // encoded equals
"%00", // encoded null
"\0", // null
"\r", // carriage return
"\n", // line feed
"\f" // form feed
```

With this interceptor installed, if any of the above characters are found in the request URI, dotCMS will return a 404 response.


How to install this plugin

The jar files can be downloaded directly and added to your dotCMS instance. You can find the binary [here](https://github.com/dotCMS/patches-hotfixes/blob/master/com.dotcms.security.matrixparams/build/libs/). This version works on dotCMS versions 5.1.6 and greater.

<https://github.com/dotCMS/patches-hotfixes/blob/master/com.dotcms.security.matrixparams/build/libs/>

The sha256 values for the hotfix file is:

File	sha256
com.dotcms.security.matrixparams-0.1.jar	bd29545bd40ab7ee9efaaa30c3f4ba96bfdd7d05ae



How to build the plugin

To build the OSGI jars run `./gradlew clean jar`

This will build a jar in the `build/libs` directory.

- **To install this plugin:** Upload the bundle jars files using the dotCMS UI (*CMS Admin->Dynamic Plugins->Upload Plugin*).
- **To uninstall this plugin:**

Undeploy the bundle jars using the dotCMS UI (*CMS Admin->Dynamic Plugins->Undeploy*).