**安康市平利中学**

**攻防演习安全分析报告**

**2022年7月10日**

目录

[1 综述](#_Toc5952)

[2 渗透分析过程](#_Toc1611)

[2.1 渗透路径说明](#_Toc3700)

[2.2 渗透成果说明](#_Toc1676)

[2.2.1 成果1](#_Toc31545)

[2.2.2 成果2](#_Toc6726)

## 综述

经过演习指挥部授权，于2022年07月10日，对安康市平利中学进行了渗透评估，通过模拟真实网络攻击行为，评估系统是否存在可以被攻击者利用的漏洞以及由此因此引发的风险大小，为制定相应的安全措施与解决方案提供实际的依据。

渗透结果总结汇总如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **渗透系统对象** | **漏洞类型及** | **URL（可罗列）** | **数量** |
| 机房动力和环境监控系统 | 未授权访问后台 | [http://219.145.205.18:8022/main.asp](http://219.145.205.18:8022/main.asp" \t "_blank) | 1 |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |

## 渗透分析过程

### 渗透路径说明

互联网 机房动力和环境监控 系统（http://219.145.205.18:8022/main.asp，219.145.205.18）

### 渗透成果说明

#### 成果1

1. 成果目标基本情况

机房动力和环境监控系统

<http://219.145.205.18:8022/main.asp>

219.145.205.18

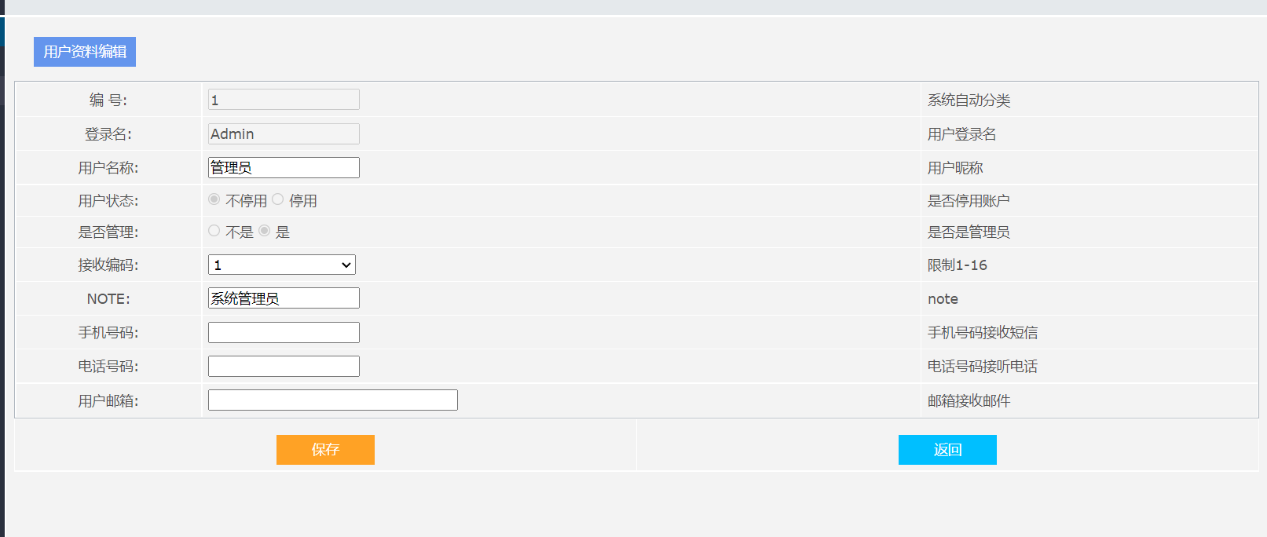
1. 成果说明
2. 漏洞情况及控制权限说明

主页存在未授权访问漏洞，禁用js可绕过重定向直接进入后台并获得管理员权限。并可控制iot设备。

1. 成果截图

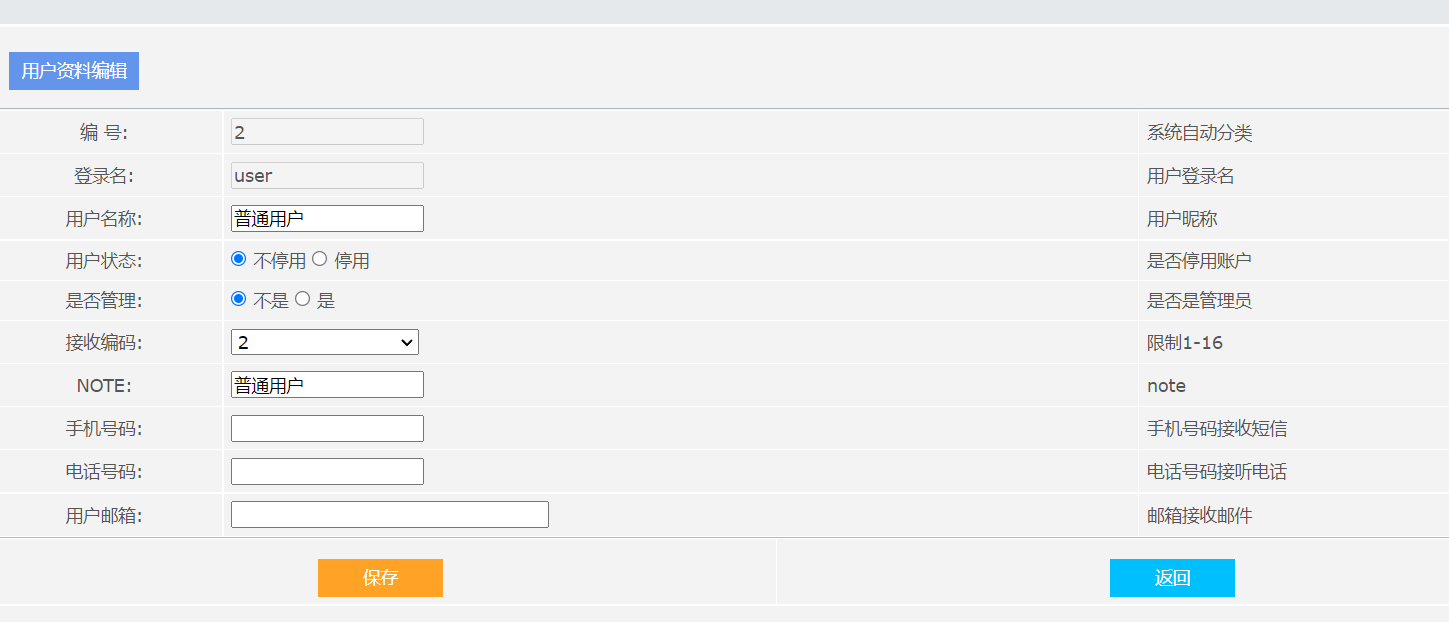


管理员权限2个





普通用户1个



配置文件泄露1份



Iot设备控制权限

