|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 网站配置文件泄露 | 国发4.2系统  http://183.136.177.105:880/jointframe/login | 中 | http://183.136.177.105:880/jointframe/web/WEB-INF/web.xml | 1 | WEB漏洞 |
| 内部IP路径信息泄露 | 低 | http://183.136.177.105:880/jointframe/static/js/app.dbc6c573.js | 1 | WEB漏洞 |
| 开启了OPTIONS方法 | 低 | http://183.136.177.105:880/jointframe/login | 1 | WEB漏洞 |
| 点击劫持漏洞 | 低 | http://183.136.177.105:880/jointframe/login | 1 | WEB漏洞 |

### **国发4.2系统-网站配置文件泄露**

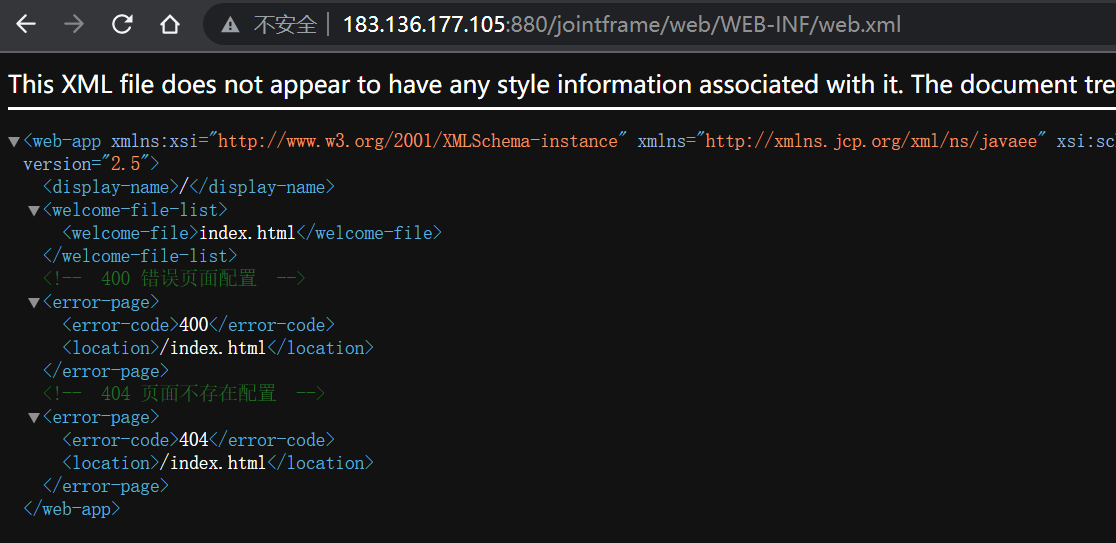
* 漏洞描述：

网站Web服务配置文件可被任意用户访问，可能导致网站应用部署等敏感信息的泄露，为后续攻击提供帮助。

* 漏洞地址：

http://183.136.177.105:880/jointframe/web/WEB-INF/web.xml

* 验证：



* 整改建议：

删除网站配置文件及目录，或禁止访问这些文件。

### 国发4.2系统内部IP路径信息泄露

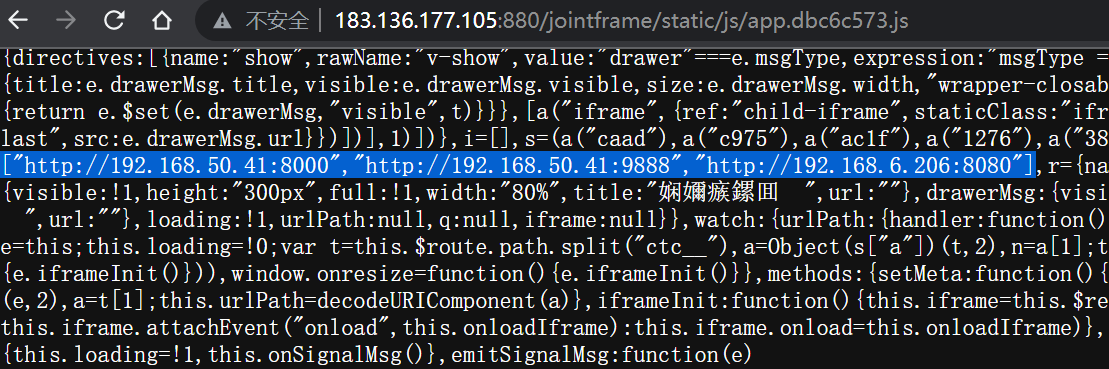
* 漏洞描述：

在页面中或者返回的响应包中泄露了敏感信息，敏感信息包括存在目标主机的内部路径及IP地址。通过这些信息，给攻击者渗透提供了可利用途径。

* 漏洞地址：

http://183.136.177.105:880/jointframe/static/js/app.dbc6c573.js

* 验证：



* 整改建议：

1、不影响业务或功能的情况下删除或禁止访问泄露敏感信息页面。

2、在服务器端对相关敏感信息进行模糊化处理。

### 国发4.2系统开启了OPTIONS方法

* 漏洞描述：

攻击者可利用OPTIONS方法获取服务器的信息，将会造成服务器信息暴露，如中间件版本、支持的HTTP方法等。通过OPTIONS方法发现服务器还开启了PUT、DELETE、PATCH危险方法。攻击者可以通过这些危险方法对目标展开进一步攻击。

* 漏洞地址：

http://183.136.177.105:880/jointframe/login

* 验证：



* 整改建议：

建议修改配置，禁用OPTINOS方法及其他危险方法。

### 国发4.2系统-点击劫持漏洞

* 漏洞描述：

攻击者在网页上插入一个不可见的iframe，使用者在不知情的情况下点击iframe页面的一些功能性按钮上，从而可能导致个人信息泄漏，甚至自动下载木马。

* 漏洞地址：

http://183.136.177.105:880/jointframe/login

* 验证：



* 整改建议：

设置X-Frame-Options响应头。

它有三个可选的值：DENY、SAMEORIGIN、ALLOW-FROM origin。当值为DENY时，浏览器会拒绝当前页面加载任何frame页面；若值为SAMEORIGIN，则frame页面的地址只能为同源域名下的页面；若值为ALLOW-FROM，则可以定义允许frame加载的页面地址。