### 资产: https://10.122.72.180:9000

|  |  |
| --- | --- |
| 漏洞名称 | 不安全的crossdomain.xml文件【原理扫描】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | - |
| 端口(服务)： | - |
| 风险描述： | 浏览器安全模型通常会阻止一个域中的Web内容访问另一域中的数据。这通常被称为“相同来源政策”。 URL策略文件授予跨域读取数据的权限。它们允许默认情况下不允许的操作。默认情况下，URL策略文件位于目标服务器的根目录中，名称为crossdomain.xml（例如，位于www.example.com/crossdomain.xml）。
当在crossdomain.xml文件中指定了域时，站点将声明它愿意允许该域中任何服务器的操作员获取策略文件所在的服务器上的任何文档。部署在该网站上的crossdomain.xml文件将服务器打开到所有域（支持使用单个星号“ \*”作为纯通配符），如下所示：
<cross-domain-policy>
<allow-access-from domain="\*" />
</cross-domain-policy>
此做法适用于公共服务器，但不应用于位于防火墙后面的站点，因为它可能允许访问保护区。它不适用于要求以密码或cookie形式进行身份验证的站点。在使用跨域策略文件时，使用基于cookie进行身份验证的通用做法来访问私有或用户特定数据的站点应格外小心。 |
| 风险影响： | 使用不安全的跨域策略文件可能会使您的站点遭受各种攻击。 |
| 解决方案： | 仔细评估将允许哪些站点进行跨域调用。 考虑网络拓扑以及将受跨域策略的配置或实施影响的任何身份验证机制。 |
| 参考资料： | http://www.adobe.com/devnet/flashplayer/articles/cross\_domain\_policy.html
http://blogs.adobe.com/stateofsecurity/2007/07/crossdomain\_policy\_files\_1.html |
| 协议类型： | - |
| 风险举证： | https://10.122.72.180:9000 |
| 请求： | GET /crossdomain.xml HTTP/1.1Host: 10.122.72.180:9000User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00770 |

### 资产: http://10.122.72.180:8080/jointframe/login

|  |  |
| --- | --- |
| 漏洞名称 | OPTIONS方法启用【原理扫描】 |
| 风险等级： | 低 |
| 高可利用： | 否 |
| CVE编号： | - |
| 端口(服务)： | - |
| 风险描述： | 此Web服务器上启用了HTTP OPTIONS方法。 OPTIONS方法提供了Web服务器支持的方法列表，它表示对有关由Request-URI标识的请求/响应链上可用的通信选项的信息的请求。 |
| 风险影响： | OPTIONS方法可能会公开敏感信息，这些信息可能有助于恶意用户准备更高级的攻击。 |
| 解决方案： | 建议在Web服务器上禁用OPTIONS方法。 |
| 参考资料： | https://www.owasp.org/index.php/Testing\_for\_HTTP\_Methods\_and\_XST\_(OWASP-CM-008) |
| 协议类型： | - |
| 风险举证： | http://10.122.72.180:8080/jointframe/login |
| 请求： | OPTIONS /jointframe/login HTTP/1.1Host: 10.122.72.180:8080User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-aliveContent-Length: 0 |
| 漏洞ID： | SF-2022-00754 |