### 资产: https://219.233.250.34:4343/amOnline/zdjk-company-base/login

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | web.xml 配置文件备份泄露漏洞【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： | 在此目录中找到一个备份/临时配置文件。 已经确认此文件包含Web应用程序部署描述符（通常存储在文件/WEB-INF/web.xml中）。几种流行的文本编辑器（例如Vim和Emacs）会自动为您编辑的文件创建备份副本，并为其命名，例如“wp-config.php~”或“ web.xml~”。 如果在编辑过程中文本编辑器崩溃或SSH连接断开，则可能无法正确清除临时备份文件。 另外，有时开发人员会创建此类文件来备份其工作，或者由管理员在备份Web服务器时创建备份。 | |
| 风险影响： | 配置文件将泄露敏感信息，这些信息将帮助恶意用户进行更高级的攻击。 | |
| 解决方案： | 从Web服务器上删除此文件。 作为附加步骤，建议在组织内实施安全策略，以禁止在可从Web访问的目录中创建临时/备份文件。 | |
| 参考资料： | http://www.owasp.org/index.php/Testing\_for\_Old \_Backup\_and\_Unreferenced\_Files\_(OWASP-CM-006) | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/login | |
| 请求： | GET /amOnline/zdjk-company-base/WEB-INF/web.xml HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 |
| 漏洞ID： | SF-0000-0603 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | IBM WebSphere application 源代码泄露【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： | WebSphere Application Server可以允许远程攻击者绕过安全性限制。 基于Web的应用程序（包括在WebSphere Application Server上运行的Web服务应用程序）可以泄露war文件中包含的应用程序特定文件，包括web-inf和meta-inf目录下的文件。 攻击者可能利用此漏洞在war文件中包含的服务器上查看或执行文件。 禁用管理安全性后，此漏洞也会影响WebSphere管理控制台。 受影响的用户： IBM WebSphere Application Server v5.1、6.0、6.1和7.0用户。 | |
| 风险影响： | 攻击者可打开指定的应用程序的文件，一遍查看内容或执行。 | |
| 解决方案： | 升级到最新版本的WebSphere或应用PK81387安全修复程序。https://www.ibm.com/support/pages/pk81387-7001-possible-application-source-file-exposure | |
| 参考资料： | https://www.ibm.com/support/pages/pk81387-7001-possible-application-source-file-exposure http://www-01.ibm.com/support/docview.wss?uid=swg24022456 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/login | |
| 请求： | GET /amOnline/zdjk-company-base/%2e/WEB-INF/web.xml HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 |
| 漏洞ID： | SF-0000-0606 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | web.xml 配置文件泄露【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： | WEB-INF/web.xml部署描述符文件描述了如何在Servlet容器（例如Tomcat）中部署Web应用程序。 通常，此文件不应能被访问。 但是，Sangfor通过使用各种编码和目录遍历变体能够读取此文件的内容。 | |
| 风险影响： | 配置文件将泄露敏感信息，这些信息将帮助恶意用户进行更高级的攻击。 | |
| 解决方案： | 限制访问 web.xml文件。 | |
| 参考资料： | https://www.likecs.com/show-206306.html https://blog.csdn.net/u011393648/article/details/115331103 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/login | |
| 请求： | GET /amOnline/zdjk-company-base/./WEB-INF/web.xml HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 |
| 漏洞ID： | SF-0000-0604 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/theme/ | |
| 请求： | GET /amOnline/zdjk-company-base/theme/ HTTP/1.1 |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/img/ | |
| 请求： | GET /amOnline/zdjk-company-base/img/ HTTP/1.1 |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/js/ | |
| 请求： | GET /amOnline/zdjk-company-base/js/ HTTP/1.1 |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/login | |
| 请求： | GET /amOnline/zdjk-company-base/login HTTP/1.1 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36 Accept-Encoding : gzip, deflate Accept : \*/\* Connection : keep-alive |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/cdn/ | |
| 请求： | GET /amOnline/zdjk-company-base/cdn/ HTTP/1.1 |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/fonts/ | |
| 请求： | GET /amOnline/zdjk-company-base/fonts/ HTTP/1.1 |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/ | |
| 请求： | GET /amOnline/zdjk-company-base/ HTTP/1.1 Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9 Upgrade-Insecure-Requests : 1 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36 |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/theme/lightTheme/theme/ | |
| 请求： | GET /amOnline/zdjk-company-base/theme/lightTheme/theme/ HTTP/1.1 |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/theme/lightTheme/theme/fonts/ | |
| 请求： | GET /amOnline/zdjk-company-base/theme/lightTheme/theme/fonts/ HTTP/1.1 |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/cdn/notice/ | |
| 请求： | GET /amOnline/zdjk-company-base/cdn/notice/ HTTP/1.1 |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/css/ | |
| 请求： | GET /amOnline/zdjk-company-base/css/ HTTP/1.1 |
| 漏洞ID： | SF-0000-0368 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 内网IP地址泄露【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： | 一个或多个IP地址被泄露，可能是内网IP地址泄露，IP地址可能用于后续的攻击中。 | |
| 风险影响： | 攻击者可以获取敏感IP地址，并将这些信息利用到后续的攻击中。 | |
| 解决方案： | 修改源代码，避免返回敏感信息。 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://219.233.250.34:4343/amOnline/zdjk-company-base/theme/lightTheme/ | |
| 请求： | GET /amOnline/zdjk-company-base/theme/lightTheme/ HTTP/1.1 |
| 漏洞ID： | SF-0000-0368 | |