IBMWe hereJ 源代码暴露漏洞-j2ee PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/289/2021_2022_IBMWe_here_c104_289947.htm raq id 1500 class Access Validation Error cve GENERIC-MAP-NOMATCH remote Yes local Yes published July 24, 2000 0updated July 24, 2000 vulnerable IBM Websphere Application Server 3.0.21 - Sun Solaris 8.0 - Microsoft Windows NT 4.0 - Linux kernel 2.3.x - IBM AIX 4.3 IBM Websphere Application Server 3.0 - Sun Solaris 8.0 - Novell Netware 5.0 - Microsoft Windows NT 4.0 - Linux kernel 2.3.x - IBM AIX 4.3 IBM Websphere Application Server 2.0 - Sun Solaris 8.0 - Novell Netware 5.0 - Microsoft Windows NT 4.0 - Linux kernel 2.3.x - IBM AIX 4.3 Certain versions of the IBM WebSphere application server ship with a vulnerability which allows malicious users to view the source of any document which resides in the web document root directory. This is possible via a flaw which allows a default servlet (different servlets are used to parse different types of content, JHTML, HTMl, JSP, etc.) This default servlet will display the document/page without parsing/compiling it hence allowing the code to be viewed by the end user. The Foundstone, Inc. advisory which covered this problem detailed the following method of verifying the vulnerability - full text of this advisory is available in the @#Credit@# section of this entry: "It is easy to verify this vulnerability for a given system. Prefixing the path to web pages with "/servlet/file/" in the URL causes the file to be displayed without being parsed or compiled. For example if the URL for a file "login.jsp" is: http://site.running.websphere/login.jsp then accessing http://site.running.websphere/servlet/file/login.jsp would cause the unparsed contents of the file to show up in the web browser."