National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme
Validation Report

IBM WebSphere Application Server

Report Number: **CCEVS-VR-04-0082**
Dated: **December 2, 2004**
Version: **1.3**

National Institute of Standards and Technology
Information Technology laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

IBM Corporation
New Orchard Road
Armonk, NY 10504
USA

Evaluation Personnel:
SAIC Common Criteria Testing Laboratory, Columbia, Maryland
Reese, Cynthia
Diaz, Terrie
Pierre, Marie E.

Validation Personnel:
Santosh Chokhani, Orion Security Solutions

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Security Policy 3
4 Assumptions 3
4.1 Physical Security Assumptions 3
4.2 Personnel Security Assumptions 4
5 Architectural Information 4
5.1 Product Server 4
5.2 Product Wsadmin Tool 5
5.3 Product Client 5
6 Documentation 5
7 IT Product Testing 6
7.1 Developer Testing 6
7.2 Evaluation Team Independent Testing 6
8 Evaluated Configuration 7
9 Validator Comments 7
10 Security Target 7
11 List of Acronyms 8
12 Bibliography 9
13 Interpretations 10
13.1 International Interpretations 10
13.2 NIAP Interpretations 10
13.3 Interpretations Validation 10

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the IBM WebSphere Application Server. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the IBM WebSphere Application Server was performed by the SAIC Common Criteria Testing Laboratory in the United States and was completed during November 2004. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The St was written by IBM. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 conformant and Part 3 conformant, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 2, augmented with Basic Flaw Remediation (ALC_FLR.1) have been met.

The WebSphere Application Server product, the WebSphere Application Server 5.0.2.8 (hereafter referred to as *the product*) is a Java 2 Enterprise Edition (J2EE) 1.3 compliant run-time environment. The primary purpose of the product is to provide an environment for running and managing the components of user-supplied enterprise applications. The product TOE consists of a subset of the components provided with the product. This subset is comprised of those product components that are used to deploy and run user-supplied enterprise applications and to manage these applications by means of a scripting tool. Specifically, the product TOE consists of the following product components: Product Server, Product Client, and the Product Wsadmin Tool. In the evaluated configuration, all product TOE components must be installed on the same machine running a single operating system. Figure 1 below illustrates the TOE; components of the TOE are in the shaded boxes.

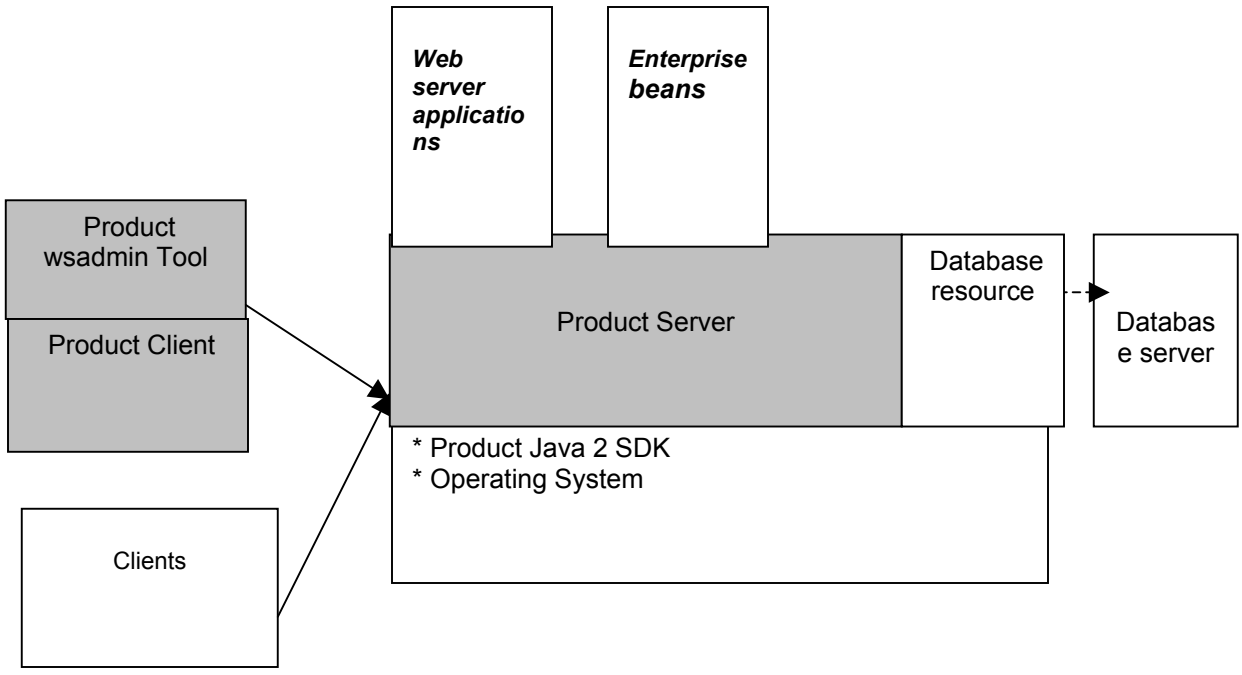

Figure 1: TOE Overview

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 2, augmented with Basic Flaw Remediation (ALC_FLR.1) evaluation. Therefore the validation team concludes that the SAIC CCTL findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	IBM WebSphere Application Server v5.0.2.8
Security Target	*WebSphere Application Server EAL2 Security Target, V2.9,* 1 December 2004
Evaluation Technical Report	*Evaluation Technical Report for IBM WebSphere Application Server*; Version 1.2, 30 November, 2004.
Conformance Result	CC Part 2 conformant, CC Part 3 conformant, EAL 2 augmented with ALC_FLR.1

Item	Identifier
Sponsor	IBM Corporation New Orchard Road Armonk, NY 10504
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, Maryland 21046
CCEVS Validator(s)	Santosh Chokhani Orion Security Solutions 1489 Chain Bridge Road, Suite 300 Mclean, Virginia 22101

3 Security Policy

The TOE identifies a client before performing any other TSF mediated action for the client. The client passes its user ID and password to the TOE. The TOE issues a request to the operating system to validate the user ID and password. If the TOE receives a response that the user ID and password are valid, the TOE issues a request to the operating system for the groups to which the client is a member. If the client does not supply a user ID and password or if the operating system determines that the user ID and password are not valid, the TOE does not process the request.

The TOE permits a client to access a protected resource only if a user or group ID of the user is mapped to a role that has permission to access the resource. The resources protected by the TOE are:

- Methods in enterprise beans
- Methods and HTML pages in web server applications
- Administration Service
- Naming Service

4 Assumptions

4.1 Physical Security Assumptions

- It is assumed that the applications and operating system that the TOE interfaces, will not compromise the security of the TOE.
- It is assumed that the operating system and the TOE will be configured in accordance with the manufacturer's installation guides and/or its evaluated configuration.
- It is assumed that the developers of all local applications (web server applications and enterprise beans) will comply with all the guidelines and restrictions specified in the User Guidance document.

- It is assumed that all software and hardware, including network and peripheral devices, have been approved for the transmittal of protected data.
- It is assumed that all software and hardware, including network and peripheral devices are physically protected against threats to the confidentiality and integrity of the data.
- It is assumed that all hardware used in the operating environment is physically secured.

4.2 Personnel Security Assumptions

- It is assumed that there are one or more competent individuals that are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, willfully negligent or hostile.

5 Architectural Information

The product TOE consists of the following components which are included in the product:

- The Product Server
- Product Wsadmin Tool
- Product Client

The remaining product components are excluded from the TOE during installation and configuration because they do not implement the primary purpose of the product and are not required to facilitate the product management functions. In the evaluated configuration, all product TOE components must be installed and run on the machine running a single operating system.

5.1 Product Server

The Product Server component is a set of containers, services, and resources that provide an environment for running enterprise applications and their components and for programmatically managing enterprise applications and their components.

The Product Server is included in the TOE because it implements the primary purpose of the product, which is to provide an environment for running enterprise applications and their components and for programmatically managing enterprise applications and their components.

The Product Server performs the following functions:

- Starts up
- Loads local components
- Accepts local and remote requests
- Processes requests for services
- Processes requests for mapped methods and HTML pages

Starts up: The Product Server is started using the Java command provided by the Product Java 2 SDK. The Product Server is run in a single operating system process and JVM.

Loads local components: The Product Server starts the following components:

- Web server applications, and
- Enterprise beans.

These components are run in the same operating system process and JVM that the Product Server is using. Therefore, these components are called "local components."

Accepts local and remote requests: The Product Server accepts requests over its local and remote interfaces. The requests over its local interfaces come from the local components (web server applications and enterprise beans). The Product Server receives these requests directly. The requests over its remote interfaces come from clients. The Product Server receives these requests indirectly by means of the Product Java 2 SDK.

Processes requests for services: If the Product Server receives a request for a service, the Product Server processes any required security and, if security is successful, processes the requested service.

Processes requests for mapped methods and HTML pages: If the Product Server receives a request for a mapped method or HTML page in a local component (web server application or enterprise bean), the Product Server processes any required security and then, if security processing is successful, invokes the mapped method or HTML page.

5.2 Product Wsadmin Tool

The Product Wsadmin Tool is a tool that provides a scripting interface for managing enterprise applications and their components.

The Product Wsadmin Tool is included in the TOE because it provides a scripting tool that facilitates the management of enterprise applications.

The Product Wsadmin Tool is a Java client application and must reside on the same operating system as the Product Client and is run in the same operating system process and JVM as the Product Client. In the evaluated configuration the product Wsadmin tool and the product client must run on the same machine and under the same operating system as the product server.

An administrator can use this tool to execute administrative scripting commands. The Product Wsadmin Tool processes these commands by calling the AdminClient API of the Product client.

5.3 Product Client

The Product Client component is a set of application programming interfaces (APIs) that provide an environment for running clients to enterprise applications.

The Product Client is included in the TOE because it is required by the Wsadmin Tool.

In the evaluated configuration, the administrator starts the Product Client using the Wsadmin command file. The Wsadmin command file causes the Java 2 SDK to start the Product Client and then causes the Product Client to start the Product Wsadmin Tool. Both the Product Client and the Product Wsadmin Tool run in a single process and use a single JVM. After the Product Client starts, it accepts AdminClient API requests from the Product Wsadmin Tool and processes these requests by calling a remote interface to the Administration Service of the Product Server.

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

Design documentation

WebSphere Application Server EAL2 Functional Specification, V3.0, 18 October, 2004
WebSphere Application Server EAL2 High Level Design, V3.0, 18 October 2004
WebSphere Application Server EAL2 Representation Correspondence, V2.0, 10 September 2004

Guidance documentation (Installation, Start-up, Administration and User Guide)

WebSphere Application Server EAL2 AGD Guidance, V2.1, 4 November 2004

Configuration Management

WebSphere Application Server v 5.0.2.8 EAL2 Configuration Management, Issue 1.1, 14 September 2004

WebSphere Application Server v 5.0.2.8 EAL2 Configuration List, Issue 3.6, 1 December 2004

Delivery and Operation documentation

WebSphere Application Server EAL2 Delivery Document, V1.4, 29 Oct 2004

Flaw Remediation

Server EAL2 extended with ALC_FLR.1 Flaw Remediation, Issue 1.2, 19 October 2004

Test documentation

Websphere Application Server EAL2 Security Target Functional Tests (ATE_FUN) and Test Coverage Analysis (ATE_COV), V2.1, 19 November 2004

Vulnerability Assessment documentation

Vulnerability Analysis for WebSphere Application Server 5.0.2.8, V 3.0, 17 November 2004

Security Target

WebSphere Application Server EAL2 Security Target, V2.9, 1 December 2004

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all TOE Security Functions: Identification, Access Control, and Security Management which is all the security functions for the TOE. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests and penetration tests. Although the evaluation team performed a sample of the developer's test suite, the selected tests were representative of the TOE Security Functions.

8 Evaluated Configuration

The evaluated configuration consisted of the components identified in the table below.

Table 2 - Hardware and Software Components

Component	Description
WebSphere Application Server components	The TOE
Java 2 SDK	Processes Java commands
AIX 5.2; HP-UX 11i; Linux SuSE Linux Enterprise Edition (SLES) 8; Linux Red Hat 2.1; Sun Solaris 8; or Microsoft Windows 2003	Operating System to provide Identification and Authentication and other IT functions

9 Validator Comments

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

10 Security Target

WebSphere Application Server EAL2 Security Target, V2.9, 1 December 2004

11 List of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTML	Hyper Text Markup Language
ID	Identifier
IBM	International Business Machines
J2EE	Java 2 Enterprise Edition
JVM	Java Virtual Machine
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
SAIC	Science Applications International Corporation
SDK	Software Development Kit
ST	Security Target
TOE	Target Of Evaluation
TSF	**TOE** Security Function
VR	Validation Report

.

12 Bibliography

The validation team used the following documents to prepare the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Final Evaluation Technical Report for IBM WAS Part 2, Version 1.2, November 30 2004.

[8] WebSphere Application Server EAL2 Security Target, Version 2.9. December 1, 2004.

[9] Common Criteria Evaluation and Validation Scheme for IT Security, *Guidance to Validators of IT Security Evaluations*. Scheme Publication # 3, Version 1.0, January 2002.

13 Interpretations

13.1 International Interpretations

The evaluation team performed an analysis of the international interpretations and applied those that were applicable and had impact to the TOE evaluation as the CEM work units were applied.

The following international interpretations were applied to the IBM WebSphere Application Server EAL2 Security Target:

- 058 – Confusion over Refinement
- 064 – Apparent Higher Standard for Explicitly Stated Requirements
- 065 – No Component to Call Out Security Function Management
- 103 – Association of Access Control Attributes with Subjects and Objects

13.2 NIAP Interpretations

The Evaluation Team determined that the following NIAP interpretations were applicable to this evaluation:

13.3 Interpretations Validation

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.