National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

IBM WebSphere Application Server

Report Number: CCEVS-VR-07-0013
Dated: March 16, 2007
Version: 1.8

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
Thompson, Dave

Validation Personnel:

Jean Hung
Jandria Alexander

Table of Contents

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 January 2007. 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 extended and Part 3 augmented, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 4, augmented with Basic Flaw Remediation (ALC_FLR.1) have been met.

The WebSphere Application Server 6.1.0.2 (hereafter referred to as the product) with specific patches as specified in Table 1 is a Java™ 2 Enterprise Edition (J2EE) 1.4 compliant run-time environment. The primary purpose of the product is to provide an environment for running and managing user-supplied enterprise applications. J2EE is a comprehensive set of specifications for designing, developing and deploying multi-tier, server-based applications.

The WebSphere Application Server TOE, which is software-only, enforces identification of request to protected resources, controls access to protected resources based upon security attributes, allows for the management of the security attributes associated with protected resources and users, and provides an invocation of SSL that requires a remote caller to invoke SSL using the configured algorithms so that the session is encrypted when the remote caller issues a request to the TOE over the remote interface of the IBM HTTP Server component. Note that the TOE does not perform the actual SSL encryption. The WebSphere Application Server TOE does not perform auditing or protection of the TSF, which includes domain separation and reference mediation. The product relies entirely on the environment to perform these functions.

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 4, 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	WebSphere Application Server V6.1.0.2 (32-bit) with interim fixes for APARs, PK29847, PK29933, PK30347, PK30831, PK31490, and PK33753. For the Solaris and HP platforms, APAR PK27217 is also required.
Security Target	WebSphere Application Server EAL4+ Security Target, V19, February 14, 2007
Evaluation Technical Report	Evaluation Technical Report for WebSphere Application Server; Part 1, Version 1.1, February 15, 2007.
Conformance Result	CC Part 2 extended, CC Part 3 conformant, EAL 4 augmented with ALC_FLR.1
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)	Jean Hung Jandria Alexander

3 Security Policy

The TOE identifies a client before performing any other TSF mediated action for the client. The TOE relies upon the IT environment to perform authentication using any one of the following methods: passwords-based, certificate-based, and LPTA token.

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:

- Protected methods of web server applications

- Protected methods of enterprise beans
- Configuration data and runtime state
- Naming directory
- Transactions and activities
- Protected resources of the built-in JMS Provider (the local bus, queue destination, temporary destination, topic space, topic space root and topics)
- Protected resources of the UDDI registry directory
- Methods and attributes in user MBeans

The TOE provides security management functions that provide a mechanism for dynamically configuring some security attributes used by TOE access control functions

The TOE provides an invocation of SSL function that requires a remote caller to invoke SSL using the configured algorithms so that the session is encrypted when the remote caller issues a request to the TOE over the remote interface of the IBM HTTP Server component. This function does not perform the actual SSL encryption, yet provides a mechanism for requiring requests from remote callers to be encrypted.

4 Assumptions

- It is assumed that the applications and operating system that the TOE interfaces, will not compromise the security of the TOE and where applicable, that they have been configured in accordance with manufacturer's installation guides and/or its evaluated configuration.
- It is assumed that the developers of all trusted user applications (user web server applications and user enterprise beans), resource adapters, and providers 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. Such items are to be 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.
- 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.
- It is assumed that the IT Environment supporting the TOE provides at least one of the supported authentication mechanisms identified within the evaluated configuration of the TOE.

5 Architectural Information

The following subsections describe the TOE components.

5.1 Product Application Server

The Product Application Server component is a set of containers, services, and resources that implement 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 Application 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 Application Server is started using the Java command provided by the Product Java 2 SDK. The Product Application Server is run in a single operating system process and JVM.

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

- User applications, and
- UDDI Registry Application.

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

Accepts local and remote requests: The Product Application 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 Application Server receives these requests directly. The requests over its remote interfaces come from clients. The Product Application Server receives these requests indirectly by means of the Product Java 2 SDK.

Processes requests for services: If the Product Application Server receives a request for a service, the Product Application 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 Application Server receives a request for a mapped method or HTML page in an user application or the UDDI Registry Application, the Product Application 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 application 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 Application Server.

5.4 Product HTTP Server and Product HTTP Server Plug-in

The Product HTTP Server and Product HTTP Server Plug-in are included in the TOE. Both reside in the same process, which is separate from the process in which the Product Application Server resides. The Product HTTP Server receives HTTP requests by remote HTTP Clients. The Product HTTP Server Plug-in forwards the requests to the Product Application Server.

6 Documentation

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

Configuration Item	Documentation Identification
Security Target	Security Target IBM EAL4 ST 19-BASE.doc V 19.0 dated 14 February 2007, WAS/EAL4/ST/19
Addendum	WAS6.1 EAL4 Addendum.doc Version 1.0 Dated 20 December 2006 WAS/EAL4/Addendum/01
Configuration Management	WAS EAL4 ACM v 30.doc Version 3.0 Dated 07 December 2006 WAS/EAL4/ACM/30 Attachments include: *CMVC95adminguide.pdf*, *CMVC95usersref.pdf, CMVC95whatis.pdf* *ITCS300v80.pdf* *ITCS104v3.0.pdf* *MrBuild_process.pdf* *MrBuild_Verify.pdf* *cdrom.cfg.pdf* *CDTracking.pdf* *access.lst.pdf* Configuration List WAS EAL4 Config List v30.doc V3.0 Dated 16 February 2007 WAS/EAL4/CL/30
Delivery and Operation	WAS EAL4 ADO v80.doc Version 8.0 Dated 21 December 2006 WAS/EAL4/ADO/80

Configuration Item	Documentation Identification
	Attachments include: ITCS104V3.0.pdf ITCS300V80.pdf Tequila3_02.pdf TQapplet7_00.pdf mD5ChecksumSample.pdf
LifeCycle Documents	WAS EAL4 ALCv50.doc Version 5.0 Dated 07 December 2006 WAS/EAL4/ALC/50 Attachments include: ITSC104v3.0.pdf ITCS300v8.0.pdf SWG-SP-0004-Rev4.pdf SWG-WI-0084-Rev4.pdf SWG-Process-0330-Rev8.pdf SWG-Process-0450-Rev3.pdf WAS EAL4 FLR 50.doc Version 5.0 Dated 07 December 2006 WAS/EAL4/FLR/50
Guidance	WAS EAL4 AGD 16.doc User Guidance V16 Dated 20 December 2006 WAS/EAL4/AGD/16
Design	Functional Specification: WAS EAL4 FS 10.doc Functional Specification V10.0 Dated 15 December 2006, WAS/EAL4/FS10 Security Policy Model: WAS EAL4 ADV_SPM v4.0.doc V 4.0 dated 18 August 2006, WAS/EAL4/ADV_SPM/40 RCR: WAS EAL4 RCR v50.doc V5.0 dated 16 November 2006 WAS/EAL4/RCR/50 High Level Design:

Configuration Item	Documentation Identification
	WAS EAL4 HLD 80.doc V 8.0 dated 15 December 2006 WAS/EAL4/HLD/80 WAS EAL4 TRM-HLD20.doc JetStream Component (TRM) HLD V2.0 dated 2 August 2006 Low Level Design: WAS EAL4 LLD NR 40.doc WAS/EAL4/LLD/40 dated 20 December 2006 WASEAL4LLD-zTransactions30.doc Dated 7 November 2005 WASEAL4LLD-AA-OverviewRelevantComponents1v40.doc updated 30 August 2006 WASEAL4LLD-AA-OverviewRelevantComponents2v30.ppt updated 30 August 2006 WASEAL4LLD-Adminv20.doc dated 17 August 2006 WASEAL4LLD-Authenticationv20.doc dated 12 July 2006 WASEAL4LLD-CSIv2-v20.doc dated 12 July 2006 WASEAL4LLD-EJBCollaboratorv40.doc Dated 01 August 2006 WASEAL4LLD-Messagingv40.doc dated 29 December 2006 WASEAL4LLD-Proxy10.doc dated 16 August 2006 WASEAL4LLD-RoleBasedAuthz-v30.doc dated 1 August 2006 WASEAL4LLD-SSLChannel30.doc dated 21 June 2006 WASEAL4LLD-TCPChannel30.doc dated 21 June 2006 WASEAL4LLD-Transaction20.doc dated 12 May 2006 WASEAL4LLD-UDDI20.doc dated 27 March 2006 WASEAL4LLD-WebCollaborator40.doc dated 15 June 2006

Configuration Item	Documentation Identification
	WASEAL4LLD-WebContainer20.doc dated 12 July 2006 WASEAL4LLD-WSAdmin20.doc dated 20 June 2006 WASEAL4LLD-zRuntime30.doc updated 16 August 2006 Reference Material: sib_output_javadoc-cc-o0629.39.zip javadocs – delivered 09 October 2006 rmm-JavaDoc.zip javadocs – delivered 09 October 2006 cc-javadoc.zip javadocs – CD delivered 10 October 2006 WAS EAL4 Jsclient_fap30.doc dated 30 August 2006
Test Documents	Functional Test: WAS EAL4 ATE 16.doc Functional Test / Test Coverage Analysis V16.0 Dated 1 February 2007 WAS EAL4 ATE 30 Messaging TestPlan.doc Messaging Security Test Plan V3.0 Dated 21 September 2006 WAS/EAL4/ATE/30/MSGTST WAS EAL4 ATE 30 MSGADMIN.doc Messaging Admin Scripting Test Plan V3.0 dated 17 August 2006 WAS/EAL4/ATE/30/MSGADM WAS EAL4 ATE 40 TATP.doc Transactions and Activities Test Plan V4.0 dated 7 September 2006 WAS/EAL4/ATE/40/TATP Test Logs: 15 December 2006 logs_cfg2_redhat(intel)_was-na-1.zip logs_cfg3_redhat(intel)_was-na-1.zip logs_cfg3_redhat(intel)_was-na-2.zip logs_cfg2_redhat(z)_was-na-1.zip logs_cfg3_redhat(z)_was-na-1.zip logs_cfg3_redhat(z)_was-na-2.zip logs_cfg2_suse(z)_was-na-1.zip

Configuration Item	Documentation Identification
	logs_cfg3_suse(z)_was-na-1.zip logs_cfg3_suse(z)_was-na-2.zip logs_cfg2_redhat(ppc)_was-na-1.zip logs_cfg3_redhat(ppc)_was-na-1.zip logs_cfg3_redhat(ppc)_was-na-2.zip logs_cfg2_SunOS_ccsun27_was-na-1.zip logs_cfg3_SunOS_was-na-1.zip logs_cfg3_SunOS_was-na-2.zip logs_cfg2_suse(ppc)_was-na-1.zip logs_cfg3_suse(ppc)_was-na-1.zip logs_cfg3_suse(ppc)_was-na-2.zip logs_cfg2_AIX_was-na-1.zip logs_cfg3_AIX_was-na-1.zip logs_cfg3_AIX_was-na-2.zip logs_cfg2_Win2003_was-na-1.zip logs_cfg3_Win2003_was-na-1.zip logs_cfg3_Win2003_was-na-2.zip logs_cfg2_HP-UX_was-na-1.zip logs_cfg3_HP-UX_was-na-1.zip logs_cfg3_HP-UX_was-na-2.zip zos_final_logs.zip
Vulnerability Documents	WASv6 EAL4 VLAv60.doc Vulnerability Analysis V6.0 Dated 12 December 2006 WAS/EAL4/VLA/v60 WAS MSU Analysis40.doc Misuse Analysis V4.0 Dated 1 November 2006 WAS/EAL4/AVA_MSU/40
Source Code	WASEAL4Source_C_1003.zip Delivered 03 October 2006 WASEAL4Source_1002.zip Delivered 02 October 2006 SelectedSourceDescription3.doc Delivered 02 October 2006

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. The evaluation team determined that both the test configuration of the vendor testing and of the team testing efforts substantiated the evaluated configuration as specified in the Security Target and in the installation and configuration guidance. Additional information regarding the test configuration and the evaluation team testing activity is included in the Final Evaluation Report.

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 the TSFI. The testing covered all the security functional requirements in the ST including: invocation of SSL, Identification, Access Control, and Security Management which are all the security functions for the TOE. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

The developer testing approach is automated primarily using the (Software Testing Automation Framework (STAF) test tool. The automation framework takes care of test setup, execution and cleanup for all provided tests.

The evaluators ensured that the developer test configuration tested the evaluated version of the TOE as specified in Table 1 of this document. The evaluators reviewed the developer actual test results and ensured that the developer ran their test successfully on all platforms identified in the Security Target as identified below:

- AIX® 5.3 (64-bit);
- HP-UX 11i v2 (64-bit PA-RISC);
- Linux® Redhat 4 on PPC (64-bit) / Intel™ / z/OS®
- Linux SuSE Enterprise Edition 9 (SLES 9) on PPC (64-bit) / z/OS;
- Sun Solaris 10 (64-bit);
- Microsoft® Windows® 2003;

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 TSFI and security functions as described in the functional specification. The evaluation team executed all of the developer's test suite successfully. The evaluation team devised and conducted an independent set of team tests and penetration tests that addressed each of the security functions claimed in the Security Target. The tests devised by the evaluation team were devised to enhance the developer test suite and based on the developer's vulnerability analysis, the evaluation team's design and test analysis, and other general knowledge about the product and product type.

During team testing, the evaluation team installed and configured the TOE according to the evaluated guidance documentation on Microsoft Windows 2003 (one of several operating systems upon which the TOE can be installed). This is acceptable given that the operating system is not within the scope of the TOE and the evidence substantiates the claim that the security behavior of the TOE is the same regardless of its supporting operating system. The evaluation team then ran all of the developer tests, the independent team tests and the penetration tests.

The evaluation team provided rationale in the Final Evaluation Technical Report (ETR) to justify that the team testing effort provided sufficient coverage of the security functions and platforms.

The test configuration used during team testing is the same as that used to support the developer testing (as described above).

8 Evaluated Configuration

The following table lists the product components and indicates whether each component is included in or excluded from the TOE. Both the “required” and the “optional” components are part of the TOE.

Product Component	WebSphere Application Server
Product Application Server	Required
Product Client	Required
Product Tools and applications	Required – only the product wsadmin tool
Product HTTP Server	Optional
Product HTTP Server Plug-Ins	Optional – only the plug-ins for the Product HTTP Server
Product Java 2 SDK	Not in TOE

The evaluated configuration does not impose any restrictions upon hardware other than the hardware must support the operating system.

9 Validator Comments

The users should be aware that the TOE only identifies users, but does no authentication. The TOE depends on the Environment (i.e., underlying operating system for this feature).

For token based authentication, and for transport security, the TOE relies on the Environment to generate the keys, protect the keys, to perform the basic cryptographic functions, and to carry out applicable cryptographic protocols. Thus, any of these security critical functions have not been evaluated as a part of this evaluation.

10 Security Target

See Table 1.

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, Version 2.2 Revision 256, January 2004.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.2 Revision 256, January 2004.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, Version 2.2 Revision 256, January 2004.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 2.2 Revision 256, January 2004.

[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, Version 2.2, January 2004.

[7] Final Evaluation Technical Report for IBM WebSphere Application Server EAL4+ Part 2, Version 1.1, February 15, 2007.

[8] WebSphere Application Server EAL4 Security Target, Version 19. February 14, 2007.

[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 EAL4 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 no 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.