National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

BEA WebLogic
Server V7.0 SP6
with BEA05-107.00 advisory patch

Report Number: CCEVS-VR-06-0006
Dated: 2006-01-27
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

1. Executive Summary

This document is intended to assist the end-user of this product with determining the suitability of the product in their environment. End-users should review both the Security Target (ST) which is where specific security claims are made, and this Validation Report (VR) which describes how those security claims were evaluated.

The evaluation of the BEA WebLogic application server software product was performed by CygnaCom Solutions, Inc. (an Entrust Company) in the United States and was completed on 27 January, 2006. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2, Evaluation Assurance Level 2 (EAL2) - augmented, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.2.

CygnaCom Solutions, Inc. is an approved NIAP Common Criteria Testing Laboratory (CCTL). The CCTL concluded that the Common Criteria assurance requirements for Evaluation Assurance Level 2 (EAL2) have been met and that the conclusions in its Evaluation Technical Report are consistent with the evidence produced.

This Validation Report is not an endorsement of BEA WebLogic V7.0 by any agency of the US Government and no warranty of the product is either expressed or implied.

1.1 BEA WebLogic Functionality

BEA WebLogic Server (WLS) is a J2EE application server that permits the integration of applications and databases. It supports tool sets that facilitate the separation of presentation, business logic and data.

WLS performs the following security functions, which are described in Section 3 of this report:

- Security Audit
- User Data Protection
- Identification & Authentication
- Security Management
- Protection of TSF Security Functions

1.2 Evaluation Details

Table 1-1 provides the required evaluation identification details.

Table 1-1. Evaluation Details

Item	Identification
Evaluation Scheme	US Common Criteria Evaluation and Validation Scheme (CCEVS)
Target of Evaluation	BEA WebLogic V7.0 SP6 with BEA05-107.00 advisory patch
EAL	EAL2 Augmented ALC_FLR.1
Protection Profile	None
Security Target	BEA WebLogic V7.0 SP6 with BEA05-107.00 advisory patch Security Target, Version 2-0-00, dated 29 November 2005
Developer	BEA Systems, Inc. 2315 North First Street San Jose, CA 95131
Evaluators	Herbert Markle CygnaCom Solutions, Inc. 7925 Jones Branch Drive, McLean, VA 22102-3321
Validator	Ralph Broom Mitretek Systems, Inc. 3150 Fairview Park Drive South Falls Church, VA 22042
Dates of Evaluation	29 September, 2003 to 27 January, 2006
Conformance Result	Part 2 extended, Part 3 conformant, and EAL2 augmented (ALC_FLR.1)
Common Criteria (CC) Version	CC, version 2.2, January 2004
Common Evaluation Methodology (CEM) Version	CEM version 2.2, January 2004
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation v1 Part 1 for BEA WebLogic Server v7.0 SP6 with BEA05-107.00 advisory patch, dated 2006-01-25. Evaluation Technical Report for a Target of Evaluation v1 Part 2 for BEA WebLogic Server v7.0 SP6 with BEA05-107.00 advisory patch, dated 2006-01-24.
Key words	Application Server BEA WebLogic J2EE

1.3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that **none** of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) identified below were applicable to this evaluation. The Validator reviewed the relevant international interpretations and determined that the Evaluation Team correctly performed this analysis. The following international interpretations were reviewed by the Validator: 86, 137, 146, 175, 180, 192, 220, 227, 228, 232, 243 and 254.

Interpretation 243 (“Must Test Setup And Cleanup Code Run Unprivileged?”) was relevant but did not apply, as no tests were run privileged with respect to the TOE Security Functions.

2. Identification of the TOE

2.1 Software

BEA WebLogic is a J2EE application server that runs on a Java Virtual Machine (JVM) that is installed on the host Operating System.

The TOE consists of the following components:

- The WebLogic Security Framework (WSF) – Manages the security "providers" that enforce specific security functions and is responsible for returning the access control decision
- The following security providers: Authentication, Identity Assertion, Credential Mapping, Authorization, Adjudication, Role Mapping, Auditing
- The Administration Server
- An embedded LDAP server

The following components are supplied with the TOE, but are not part of the TOE and were not evaluated:

- Servlet Containers
- EJB Containers
- Diagnostic Services
- Administration Client

The TOE consumer will need to provide the following:

- Appropriate hardware to run the operating system, including a system clock.
- A supported operating system to host the TOE. (e.g. MS Windows 2000)
- Sun Java 2 JVM 1.3.1 (installed as part of the Java 2 SDK 1.3.1)
- An appropriate network environment that is secured from threats via a firewall and WLS connection filters as described in the Administrative Guidance.
- Trained administrators; and
- Physical security of the TOE.

2.2 Documentation

The following documents were used to validate the evaluation:

- Evaluation Technical Report for a Target of Evaluation v1 Part 1 for BEA WebLogic Server v7.0 SP6 with BEA05-107.00 advisory patch, dated 2006-01-25.
- Evaluation Technical Report for a Target of Evaluation v1 Part 2 for BEA WebLogic Server v7.0 SP6 with BEA05-107.00 advisory patch, dated 2006-01-24.

- Security Target v2-0-00 for BEA WebLogic Server v7.0 SP6 with BEA05-107.00 advisory patch, dated 2005-11-29.
- EAL2 ON-SITE TESTING Test Plan for BEA WebLogic Server v7.0 SP6 with BEA05-107.00 advisory patch, version 1.3.1 dated 2006-01-12.
- BEA WebLogic Server v7.0 SP6 with BEA05-107.0 advisory patch Common Criteria Configuration Management (ACM_CAP) version 1-0-03 dated 2005-11-29.
- BEA WebLogic Server v7.0 SP6 with BEA05-107.0 advisory patch Common Criteria Delivery Procedures (DEL) and Installation Overview (IGS) version 1-0-01 dated 2005-11-29.
- BEA WebLogic Server v7.0 SP6 with BEA05-107.0 advisory patch Common Criteria Administrator and User Guidance (AGD_ADM, AGD_USR) version 1-0-03, dated 2005-11-29.
- BEA WebLogic Server v7.0 SP6 with BEA05-107.0 advisory patch Common Criteria Flaw Remediation (ALC_FLR) version 1-0-01, dated 2005-11-29.
- BEA WebLogic Server v7.0 SP6 with BEA05-107.0 advisory patch Common Criteria Testing Documentation (ATE) version 1-0-01, dated 2005-11-29.
- BEA WebLogic Server v7.0 SP6 with BEA05-107.0 advisory patch Common Criteria Vulnerability Assessment (AVA) version 1-0-01, dated 2005-11-29.
- BEA WebLogic Server v7.0 SP6 with BEA05-107.0 advisory patch Common Criteria Functional Specification (FSP) version 1-0-03, dated 2005-11-29.
- BEA WebLogic Server v7.0 SP6 with BEA05-107.0 advisory patch Common Criteria High Level Design (HLD) version 1-0-02, dated 2005-11-29.
- BEA WebLogic Server v7.0 SP6 with BEA05-107.0 advisory patch Common Criteria Representation Correspondence (RCR) version 1-0-02, dated 2005-11-29.
- CygnaCom raw test results and logs, delivered as “from testing 2.88M.zip” on 2005-12-20.

3. Security Policy

BEA WebLogic V7.0 performs the following security functions:

- Security Audit
- User Data Protection
- Identification & Authentication
- Security Management
- Protection of TSF Security Functions

3.1 Security Audit

The TOE generates audit information for security-relevant events and enables authorized administrators to view the audit records.

The TOE generates audit records for the following events:

- Start-up of the audit functions
- Shutdown of the audit functions
- Simple authentication (username/password)
- Perimeter authentication (based on tokens)
- User account lockout for failed logons
- User account automatic lockout removal
- User account explicit lockout removal
- Access attempt
- Obtain Roles
- Role deployment
- Role undeployment
- Policy deployment
- Policy undeployment

Each audit record includes the date and time as obtained from the IT environment (OS), user identity (when applicable), type of event, and its outcome (success or failure). The audit records can be viewed by authorized administrators.

3.2 User Data Protection

WSF provides access control decisions to restrict access to protected entities through security providers that supply the following services:

- Authorization – Controls whether interactions between users and WLS entities are permitted.
- Role Mapping – Provides the Authorization provider with role information so that the Authorization Provider can determine if access is permitted.

- Adjudication – Resolves disagreements between multiple Authorization Providers.

Access control decisions are enforced by the containers that call the WebLogic Security Framework. The containers are supplied with the TOE but are not part of the TOE and were not evaluated.

3.3 Identification and Authentication

WLS identifies and authenticates application and administrative users. The TOE can be configured to permit anonymous application users, but not anonymous administrative users. The following Identification and Authentication services are supplied by security providers:

- Authentication – Users or system processes are verified. Users are authenticated via username and password.
- Identity Assertion – A special type of authentication using tokens, which validates and maps a CORBA Common Secure Interoperability (CSIv2) token to a username.

3.4 Security Management

WLS supports four global roles: administrator, deployer, operator and monitor. These roles provide the capabilities needed to manage security functions. Anonymous users cannot be assigned a role, and thus cannot perform security management functions. WLS stores security provider data in an embedded LDAP database.

Credential Mapping allows WLS to log into remote (legacy) services on behalf of an authenticated subject. Administrators manage credential mapping through the TOE security management functions.

3.5 Protection of the TSF Security Functions

WLS encapsulates the applications it protects in containers subject to the TOE security framework. WLS itself is a collection of Java applications, each operating in its own domain to prevent interaction with each other or other untrusted entities. The majority of the services that protect the TSF come from the IT environment.

When invoked, the TOE ensures that its security policy enforcement functions are performed successfully.

4. Assumptions and Clarification of Scope

This section describes the security aspects of the environment in which the TOE is expected to operate.

4.1 Usage Assumptions

The assumptions listed below are not addressed by any IT requirements but instead rely on the procedural or administrative measures applied to the operating environment. Users must consider these assumptions and whether they are valid for the intended use of the product.

A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.NO_UNTRUSTED	There are no untrusted user accounts or software on the server platform
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment

4.2 Environmental Threats

The environmental threats listed below are addressed by either the TOE or the TOE IT environment (a combination of IT environmental requirements and the usage assumptions listed above).

T.BYPASS	An attacker may be able to bypass TOE protection mechanisms through WebLogic Server containers, the JVM, or Microsoft Windows 2000 Server operating system.
T.EXCESS_AUTHORITY	An administrative user may be granted more authority than they are trained to handle.
T.EAVESDROP	An attacker may be able to observe authentication data transmitted from a user to the TOE.
T.NO_TIME	Those responsible for the TOE may not be able to determine the sequence of security relevant events.
T.STORAGE	Audit data and other TSF data may be lost or modified.
T.TAMPER	An attacker may be able to tamper with TSF programs and data.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNACCOUNTABLE	Users of the TOE may not be held accountable for their actions.
T.UNAUTHORIZED_ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.
T.UNDETECTED_ACTIONS	The administrator may not have the ability to detect potential security violations, thus limiting the administrator’s ability to identify and take action against a possible security breach.

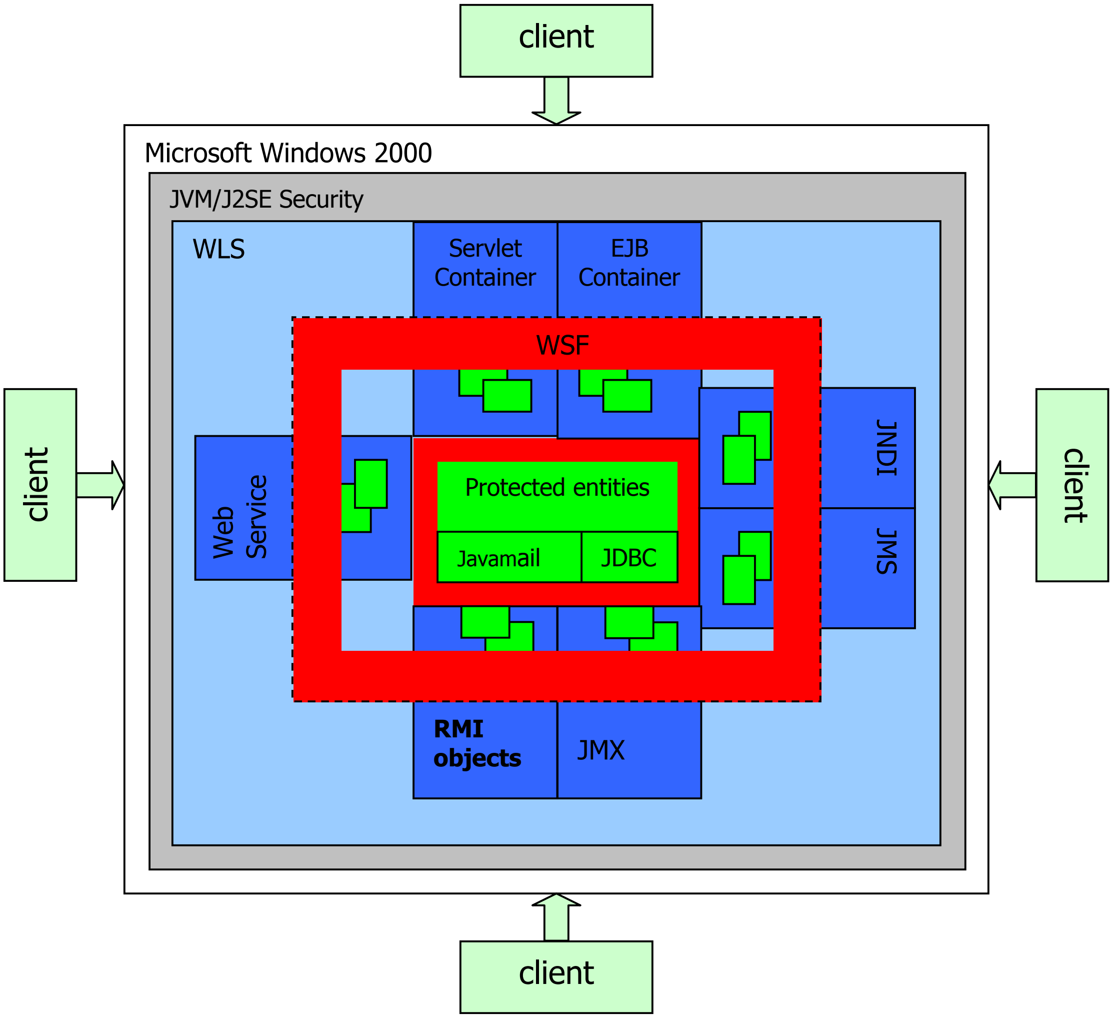
T.UNIDENTIFIED_USERS	An attacker may gain access to the TOE without being reliably identified allowing them to gain unauthorized access to data or TOE resources.

5. Evaluated Configuration

The evaluated configuration platform consists of a single Microsoft Windows 2000 Server SP4 running Sun Java 2 JVM 1.3.1. WLS was installed and configured according to supplied administrator guidance. An external workstation was used to conduct testing and evaluation.

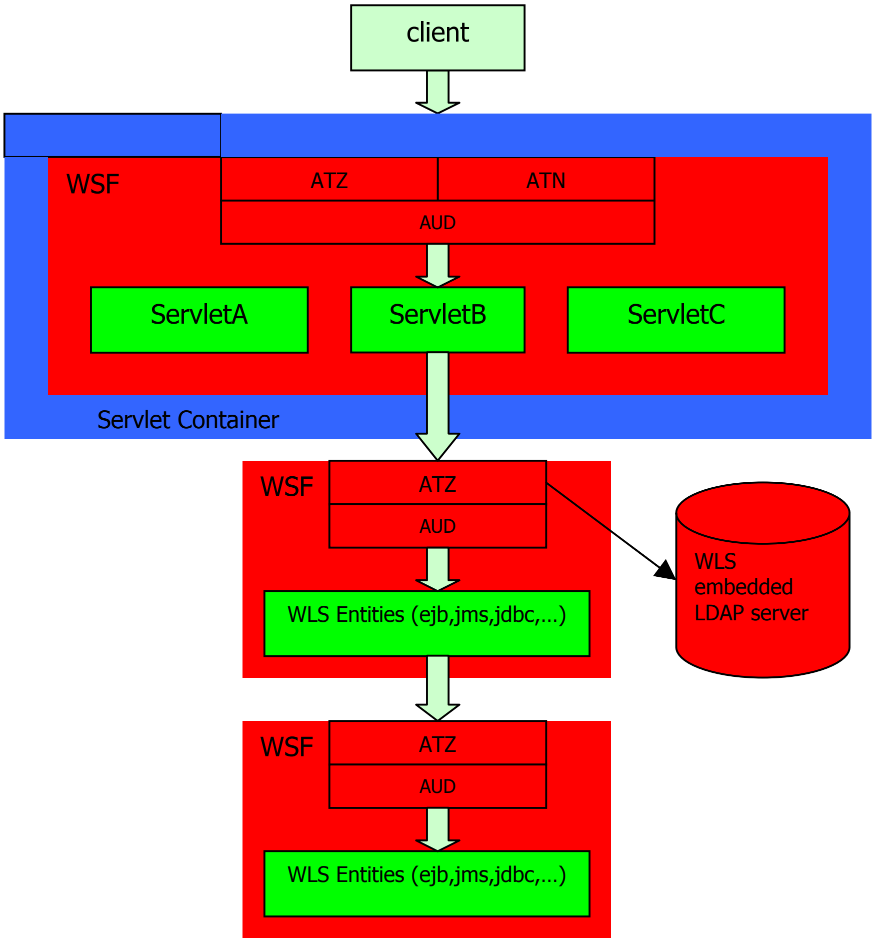
5.1 Architectural Information

The diagram below depicts the access control mechanism (the WSF) in red and the entities it protects in green.



All interactions with and between protected entities are mediated by the WebLogic Security Framework (WSF).

In the next diagram, the red WSF components are further broken down into Authorization (ATZ), Authentication (ATN) and Auditing (AUD) functions and the embedded LDAP server is illustrated. The Administration Console is not depicted, but is also protected by the WSF.



The TOE contains the following interfaces and security functions:

- WSF Interfaces:
  - Authorization Manager
  - Role Manager
  - Principle Authenticator
  - Credential Manager
  - Auditing Interfaces
- WLS Security Functions:
  - Security Audit
  - User Data Protection – Authorization (Access Control)
  - Identification and Authorization
  - Security Management
  - Protection of the TOE Security Functions

Security Providers are modules that integrate into the WLS Security Framework to provide security services to applications. Providers included in the TOE are:

- Authentication
- Identity Assertion
- Credential Mapping
- Authorization
- Adjudication
- Role Mapping
- Auditing

Dark blue represents the containers for entities that may be accessed by client. The containers enforce the access control decisions made by the WSF. While the interfaces between the WSF and containers were tested, the containers themselves are outside the TOE and were not evaluated.

6. Evaluation and Validation Process and Conclusions

This section describes the evaluation process used by the team and the activities the Validator performed to gain confidence in the evaluation team's analysis.

The evaluation team conducted a review of the WebLogic Server product based on functional requirements as specified in the Security Target and assurance requirements as required for EAL2.

The EAL2 assurance requirements include the following:

Table 6-1. EAL2 Components

EAL2 Component	EAL2 Component Title
ASE	Evaluation of Security Target
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

The EAL2 evaluation was augmented with ALC_FLR.1, Life Cycle Flaw Remediation.

In addition, two explicit Security Functional Requirements were added:

- Security attribute-based access control decision (FDP_ACF_EXP.1)
- Non-bypassability of the WSF TOE Security Policy (FPT_RVM_EXP.1)

6.1 Evaluation of the Security Target (ASE)

The evaluation team applied each EAL2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies. The team also confirmed that the ST contains a statement of security requirements claimed to be met by the BEA WebLogic product that are consistent with the Common Criteria, and product security function descriptions that support those requirements.

The Validator reviewed the Evaluation team's work units and compared them with the Security Target to determine that the work units were performed correctly.

6.2 Evaluation of the Configuration Management Capabilities (ACM)

Configuration Management (CM) systems are put in place to provide a method of tracking changes to the portions of the TOE that they control. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; that the configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. **The consumer must request the evaluated version of the product.**

The evaluation team analyzed the CM process and determined that TOE components and documentation have unique references and that a system is in place to track release configurations of the TOE and changes to its components.

The Validator reviewed the Evaluations team's work units and evidence to determine that the work units were performed correctly.

6.3 Evaluation of Delivery and Operations Documents (ADO)

The evaluation team analyzed the documentation of the procedures used to ensure that the TOE is delivered, installed, generated and started in the same way that the developer intended it to be and that it was delivered without modification. **The consumer must obtain the appropriate evaluation configuration documentation from BEA Systems.**

The Validator reviewed the Evaluations team's work units, evidence and TOE documentation to determine that the work units were performed correctly.

6.4 Evaluation of the Development (ADV)

The evaluation team inspected the design documentation to determine that the TOE Security Functions (TSF) could be understood, were consistent and that they supported the claims in the ST. The design documentation consists of a functional specification describing the TOE in terms of internal subsystems and a high-level design which describes how those subsystems work together.

The Validator reviewed the Evaluations team's work units, the TOE functional specification and user and administrator guidance to determine that the work units were performed correctly.

6.5 Evaluation of the Guidance Documents (AGD)

The evaluation team analyzed the documentation that describes how to operate the TOE in a secure manner and compared it with the actual operation of the TOE. The product includes both an administrator Graphical User Interface (GUI) and a command-line interface; only the administrator GUI is part of the TOE and was evaluated.

The Validator reviewed the Evaluations team's work units, test results and user and administrator guidance to determine that the work units were performed correctly.

6.6 Evaluation of the Test Documentation and Testing Activity (ATE)

The evaluation team examined the developer tests to ensure that those tests would confirm that the TOE behaves as specified in the design documentation and in accordance with the TSF requirements as specified in the ST. In addition, the evaluation team independently performed the entire suite of developer tests and compared them to the developer test results.

The Validator reviewed the Evaluations team's work units, test results and developer test results to determine that the work units were performed correctly.

6.7 Vulnerability Assessment Activity (AVA)

The evaluation team examined the TOE for flaws or weaknesses in its intended environment and conducted its own penetration testing. The team reviewed the developer's claims for the strength of specific security functions, performed searches for obvious vulnerabilities and conducted a sample penetration test. The sample penetration test included an external network scan of the TOE server, attempts to use common default username/password combinations, tests of an unprivileged user on the server attempting to access application data and configuration files, overflow tests on the login interface, examination of registry entries for plaintext passwords, etc.

The Validator reviewed the Evaluations team's work units, test results and penetration test to determine that the work units were performed correctly.

6.8 Life Cycle Assessment Activity (ALC)

The evaluation team examined the developer processes and procedures for flaw remediation. This is to determine whether the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users.

The Validator reviewed the Evaluations team’s work units and evidence to determine that the work units were performed correctly.

6.9 Summary of the Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s performance of the entire vendor test suite also demonstrates the veracity of the claims in the ST.

7. IT Product Testing

Because of the availability of an automated test suite, independent testing covered all of the developer tests.

Testing was conducted from 14 November 2005 to 18 November 2005 at the BEA Systems facility in Burlington, MA. The testing was conducted by Herb Markle, representing the CCTL CygnaCom. Functional and vulnerability testing was conducted, including a full execution of the developer test suite. Because the developer test suite was automated, the evaluator altered several tests to create failures. This demonstrated the correctness of the test scripts and reporting mechanisms.

Testing focused on the interfaces and security functions detailed in Section 5.

The test configuration was as described in Section 5. Evaluated Configuration, with the Sun Java 2 JVM 1.3.1 running on Microsoft Windows 2000 SP4. The approach used was functional test-case design. This exercises valid system functions to determine that they perform as expected when presented with various options, users or configurations.

8. Validator Comments/Recommendations

This is a software-only TOE. The Validator determined that the evaluation and all of its activities were performed in accordance with the CC, the CEM and CCEVS practices.

- TOE testing was performed through automated scripts that were spot-checked for proper results. The automated test scripts tested all claimed TOE security functions.
- Password strength settings can be set lower than the CEM permits. Specific requirements and documentation were added to inform TOE users about how to set password strength.
- Administrator guidance was added to caution administrators to ensure they were not observed or had keystrokes recorded when generating new administrator passwords via the command line.
- The Quality Assurance (QA) system was enhanced with a specific regimen to verify CC requirements.

- The interface between the WSF and containers was tested, but the container enforcement mechanism is outside the TOE and was not tested.

The Validator agrees that the CCTL presented appropriate rationales to support the Results of Evaluation presented in Section 4 of the ETR, volume 1, and the Conclusions presented in Section 5 of the ETR, volume 2.

The Validator therefore concludes that the evaluation and the Pass results for the TOE identified below is complete and correct:

BEA WebLogic Server V7.0 SP6 with BEA05-107.00 advisory patch

9. Security Target

The Security Target (ST) reference for this product is "Security Target v2-0-00 for BEA WebLogic Server v7.0 SP6 with BEA05-107.00 advisory patch" dated 2005-11-29. The ST describes what the TOE does, defines the functional claims that the developer is making for the TOE and which standards / specifications the TOE is claimed to conform with.

The conformance claims for this product are:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, January 2004, CCIMB-2004-01-002.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, January 2004, CCIMB-2004-01-002, at Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.1 (Flaw Remediation).

10. List of Acronyms

Acronym	Definition
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
EAL2	Evaluation Assurance Level 2
ETR	Evaluation Technical Report
GUI	Graphical User Interface
NIAP	National Information Assurance Partnership
SSL	Secure Sockets Layer
TOE	Target of Evaluation
TSF	TOE Security Functions

11. Bibliography

In addition to the documents specified in section 2.2 Documentation, the following documents were used in compiling this Validation Report:

- Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004:
  - Part 1: Introduction and General Model

  - Part 2: Security Functional Requirements
  - Part 2: Annexes
  - Part 3: Security Assurance Requirements
- Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004: