KECS-CR-07-08

WEBS-RAY V2.0
Certification Report

Certification No. : KECS-NISS-0067-2007

May 2007

National Intelligence Service

IT Security Certification Center

This document is the certification report on WEBS-RAY V2.0 of Trinity Soft Co., Ltd.

Certification Committee

Ministry of Information and Communication: Cho, Gyu Jo
National Security Research Institute: Park, Jong Wook
Korea Institute of Science and Technology: Cha, Sung Deok
Chung-Ang University: Kwon, Young Bin
Korea University: Lee, Dong Hoon
Hannam University: Lee, Kang Soo
Hansei University: Kim, Seok Woo
Sungshin Women's University: Seo, Dong Soo

Certification Body

National Intelligence Service : IT Security Certification Center

Evaluation Body

Korea Information security Agency(KISA)

Table of Contents

1. Summary

This Report describes the certification result of Certification Body on the result of the EAL4 evaluation of WEBS-RAY V2.0 with regard to Information Security System Common Criteria (publicly announced on May 21, 2005, hereinafter referred to as "CC"). This Report describes the evaluation result and the adequacy and appropriateness of the evaluation result.

The evaluation on WEBS-RAY V2.0 was carried out by the Korea Information Security Agency and was completed on April 17, 2007. This report were written on the basis of the contents of the evaluation report submitted by the Korea Information Security Agency. The evaluation has been made that the product satisfies the CC V2.3 part 2 and EAL4 of the CC V2.3 part 3 assurance requirements, and is evaluated to be "appropriate" in accordance with the Clause 191 of the CC V2.3 part 1.

WEBS-RAY V2.0 is a software-based web application firewall product that provides interception function by detecting the attacks that can occur in the web by collecting White URL and key contents information in order to detect and intercept service attack on web-server, and was developed by the Trinity Soft Co., Ltd.

WEBS-RAY V2.0 is composed of Agent, which performs detection and interception function on the web attack, Master Server that manages the security policy and stores audit report, and Admin Console that supplies GUI to the administrator for security management including setting of security policy. TOE provides the following key security functions:

- Security management function allowed only for the authorized personnel
- Generation and protection of security audit data
- User data security function that detects and intercepts web attack and protects the web-contents in accordance with security policy
- Identification of external IT entity as well as identification and certification of authorized administrator
- System security function that inspects flawlessness of the TSF execution file and security policy, and verifies normal operation on TSF service DAEMON and communication channel on regular basis

The certification body has examined the evaluation activities and test

procedures of the evaluator, provided guidelines on technical issues and evaluation procedures, and reviewed the contents of each evaluation work package report and evaluation report. The certification body has confirmed that the evaluation results assure that TOE satisfies all security functions required and assurance requirements described in the Security Targets. Therefore, the certification body has certified that the observations and evaluation results of the evaluator are accurate and reasonable, and further that the evaluation result on the appropriateness is correct.

Scope of Certification Validity : The information contained in this certification report does not signify that WEBS-RAY V2.0 has been approved for application by the government organizations of the Republic of Korea or quality assurance on WEBS-RAY V2.0.

2. Identification Information

The following [Table 1] illustrates information for TOE identification.

[Table 1] TOE Identification

Evaluation Guidance	Korea IT Security Evaluation and Certification Guidance (May 21, 2005) Korea IT Security Evaluation and Certification Scheme (Jan. 1, 2007)
TOE	WEBS-RAY V2.0
Protection Profile	N/A
Security Target	WEBS-RAY V2.0 Security Target V2.1 (Feb. 8, 2007), Trinity Soft Co., Ltd.
ETR	WEBS-RAY V2.0 ETR, V1.1 (April 17, 2007)
Evaluation Results	Satisfies the CC V2.3 part 2 Satisfies the CC V2.3 part 3
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V2.3 (Aug. 2005)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V2.3 (Aug. 2005)
Sponsor	Trinity Soft Co., Ltd.
Developer	Trinity Soft Co., Ltd.
Evaluator	Evaluation Team II, IT Security Evaluation Division, KISA Jiho Bang, junghwan Park
Certification Body	National Intelligence Service

WEBS-RAY V2.0 is composed of software and the scope of target of evaluation refers only to the software that is installed in the operating system. Agent and Master Server is loaded and operated on the SUN Solaris 10 for x86 operating system, Agent loaded in module format on Apache 2.2 while Admin Console is installed and operated on Windows XP.

System requirements of the WEBS-RAY V2.0 are illustrated in the [Table 2] below.

[Table 2] WEBS-RAY V2.0 Specification

Item		Minimum Specification
Agent	CPU	Intel Pentium IV 1GHz

	Memory	512MB
	Interface	10/100/1000 Ethernet Card 1개
	HDD	9GB
	Operating environment	SUN Solaris 10 for x86 Apache 2.2
Master Server	CPU	Intel Pentium IV 1GHz
	Memory	512MB
	Interface	10/100/1000 Ethernet Card 1개
	HDD	18GB
	Operating environment	SUN Solaris 10 for x86 MySQL 4.1
Admin Console	CPU	Intel Pentium III 600MHz
	Memory	256MB
	Interface	10/100/1000 Ethernet Card 1개
	HDD	40GB
	O/S	Windows XP

3. Security Policy

TOE is operated in compliance with the following security policies:

Security audit :

Security related events must be recorded and maintained in order to track the responsibilities on activities related to security, and the recorded data must be reviewed.

Secure administration :

The authorized administrator must manage TOE with secure method.

4. Assumptions and Scope

4.1 Assumptions

TOE evaluated shall be installed and operated in compliance with the following presumptions:

A. Physical security :

TOE is located in secured environment, physically, that can only be accessed by authorized personnel.

A. Security maintenance :

In the event of changes in the security environment due to change in network composition, host composition, web-server and web application, the changed environment and security policy must be reflected on the TOE operation policy immediately in order to maintain security at level equivalent to the previous environment.

A. Reliable administrator :

The authorized administrator of TOE is void of ill intentions, has been trained appropriately on the TOE administrations functions, and executes responsibilities accurately in accordance with the administrative guidelines.

A. Fortification of operating system :

Vulnerability within the operating system shall be removed in advance by completely eliminating services (service port) or means within the operating system that are not necessary by the TOE in order to assure reliability and security on the operating system.

A. Fortification of Web-server :

Vulnerability shall be eliminated in advance by removing unnecessary programs existing in the web-server and patching with the latest version by TOE in order to assure reliability and security on web-server.

A. Secured external server :

Reliability and security on the server is assured by receiving the latest time from the NTP server in order to maintain reliable time of TOE.

A. Secured SSL :

SSL to be used between TOEs shall be operated securely and the confidentiality of data conveyed between the TOEs assured.

A. Secured DB :

Securely store the audit data generated at the TOE in order to assure the security of DB used in search and arrangement of audit data.

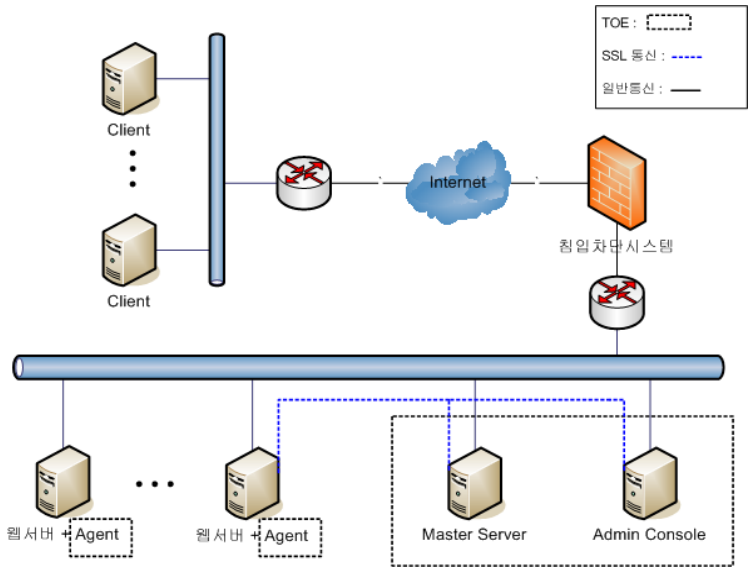
4.2 Scope to counter a Threat

Although TOE provides means of coping with the security threats at a level appropriate for the IT environment that TOE requires, TOE does not provide means of coping with direct physical attack that makes it operate abnormally. However, TOE provides means of coping with the logical attack that are generated by source of threat with low level of specialized knowledge, resources and motivation within the network connected to TOE.

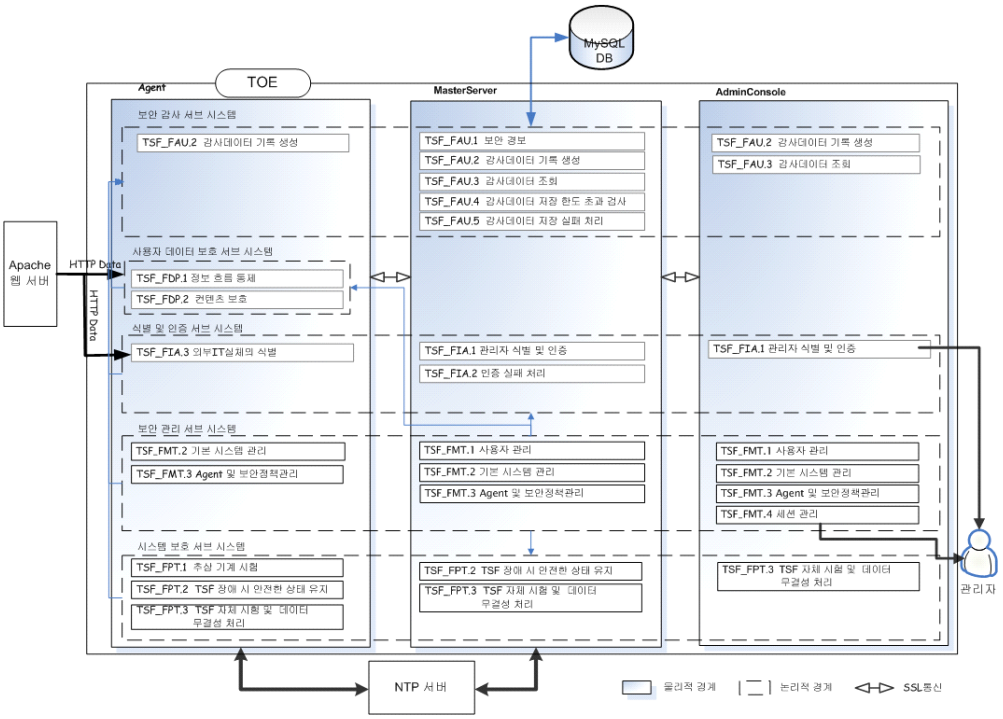
All Security Targets and polices are described in order to provide means of countermeasure against identified security threats.

5. TOE Information

TOE is installed and operated within internal network or DMZ, which is protected by network security product such as invasion interception system. The operating environment is illustrated in the [Figure 1] with fundamental structure illustrated in the [Figure 2] below.



[Figure 1] TOE Operating Environment



[Figure 2] Basic Structure of TOE

TOE is composed of the following 5 sub-systems.

- **Security Audit Subsystem(SA)**

Audit record data can be verified for each log, contents alteration log, work log and notice message even in the event of invasion by transmitting the audit data generated by each subsystem (User data Protection subsystem, Identification and Authentication subsystem, Security Management subsystem, System Protection subsystem) to Master Server and by storing in the MySQL DB. Furthermore, in the event of exceeding the limit set as the base value by examining the storage and saturation limit of audit record data stored in MySQL DB, the disc of the audit record storage shall be recognized as being exhausted and stop all TSF service with the exception of access and back-up of authorized administrator, in order to prevent storage of any more audit record information.

- **User Data Protection Subsystem(UP)**

Invasion and traffic analysis process on HTTP(S) request that accesses the web application and HTTP(S) response transmitted to the user domain is being carried out, as well as prevents detoured access and rejection of service for such. In the event of occurrence of abnormal attack, corresponding attacks are detected and intercepted with audit record generated on such abnormal access. Key contents files are registered as target of monitoring and hash value stored for the registered files in order to examine presence of changes in accordance with period of examination for flawlessness and to generate audit record in the vent of changes.

- **Identification and Authentication Subsystem(IA)**

It performs identification and certification functions for the administrator who manages TOE, and identification of external IT entity (client). It provides identification and certification function for administrator through log-in page provided in the Admin Console, and reflects number of failure to access the administrator and monitor account, and details of certification setting on termination of account with the exception of the super-administrator account. In the event of failure to log-in, it conveys the details of such failure to the security Management subsystem (SM).

- **Security Management Subsystem(SM)**

It provides GUI that can generate, change and delete TSF data including policies on control of information flow and alteration of contents. Furthermore, it performs examination of flawlessness of execution code of TSF of TOE and information of properties of various security policies, setting of policies, status inquiry and changes on TSF and TSF data.

- **System Protection Subsystem(SP)**

Regularly (30 seconds) verifies TSF service DAEMON disability and

communications disability at the time of operation and during regular operation in order to maintain normal operation as well as secured status of Agent, Master Server and Admin Console. In the event of occurrence of DAEMON disability, enable maintenance of secured status by re-operating the corresponding service DAEMON by monitoring process. In the event of occurrence of problems in the control channel by verifying the status of the control channel on regular basis, it is assessed as problem in the communication status, and transmits the stored audit record to Master Server once the communication is resumed after having stored the audit record until the communication is resumed. In addition, it performs flawlessness examination on execution code of TSF, security policy file, system operation file and security policy table file at the time of start-up and at every designated period (base value of 5 minutes). In the event of occurrence of error on flawlessness, security alarm contents are conveyed to the authorized personnel in accordance with the prescribed countermeasure activity information, and the administrator shall execute verification on the flawlessness error through viewing of the outcome.

6. Guidance

Manual provided by TOE is as follows:

- WEBS-RAY V2.0 Administrator Guidance V2.0, Dec. 12, 2007

7. TOE Test

7.1 Developer's Test

- Test Method

The developer has derived at the test items with consideration for the security functions of the product. Each test item is described in the test manual. Each test item described in the test manual includes the following detailed items:

- Test No./testing entity: Person identifying the test item and developer who participated in the test
- Test goal: Describes the test goal including security function and security module being subjected to test
- Test environment: Detailed test environment for execution of test
- Detailed test procedure: Detailed procedures for testing the security functions
- Anticipated result: Outcome of test anticipated to be obtained upon execution of test procedures
- Actual result: Outcome of test obtained upon actual execution of test procedures
- Comparison of anticipated and actual results: Outcome of comparison of anticipated and actual results

The evaluator has evaluated the validity of test including the test environment, test procedures, analysis of scope of test and detailed design test of the test manual. The evaluator has verified that the test and test results of the developer were appropriate for the evaluation environment.

- Test Configuration

Test environment described in the test manual includes detailed environment such as composition, TOE, server to which TOE is installed or system subjected to security control. Furthermore, it describes detailed test environment such as necessary test tools for testing of each test item.

- Test Scope Analysis/Low-Level Design Test

Detailed evaluation results are described in the ATE_COV and ATE_DPT evaluation results.

- Test Result

Test manual describes anticipated and actual results of each test item. Actual result can be verified not only through the video clips of the actual product but also audit record.

7.2 Evaluator's Test

The evaluator installed TOE by using the evaluation environment and tools that are same as those of developer's test, and tested entire test items provided by the developer. The evaluator has verified that the actual results coincide with anticipated result in all test items.

Furthermore, the evaluator has confirmed that the actual results coincided with the anticipated result by devising and testing separate evaluator's test items on the basis of the developer's test.

The evaluator has verified that, as the result of execution of vulnerability test, no vulnerability can be abused under the evaluation environment.

The test results of the evaluator have assured that TOE operates normally as described in the design document.

8. Evaluation Configuration

The evaluator has composed test environment, which is coherent with the environment composition specified in the [ST], for the test.

- Computer: 5 units (3 units of computer for installation of TOE, 2 units of computer for attacker and for monitoring)
  - CPU : More than 1.5Ghz
  - RAM : More than 512MByte
  - H.D.D. : More than 40MB

The following software was used in composing the evaluation environment:

- SUN Solaris 10 for x86
- Windows XP
- MySQL 4.1
- Apache 2.2.4

All security functions that TOE provides are included in the scope of evaluation, and evaluation environment was composed in accordance with each detailed security properties of each security function and environment setting method.

9. Evaluation Result

Common Criteria for Information Technology Security Evaluation V2.3 and Common Methodology for Information Technology Security Evaluation V2.3 have been applied to evaluation. Evaluation concluded that TOE satisfies the EAL4 Evaluation Assurance Level requirements of the Part 2 and 3 of Common Criteria for Information Security System. Details of evaluation results are described in the evaluation report.

- ST evaluation (ASE)

The evaluator made its evaluation by applying the working unit of ASE Common Evaluation Methodology.

Introduction of the Security Target is perfect with coherence with other parts of the Security Target and accurately identifies the Security Target. TOE explanation enables one to understand the goal and functionality of the TOE, is logical and perfect with internal coherence, as well as being described with coherence with other parts of Security Target.

Security environment provides the clearly defined and consistent security issues induced from the TOE and TOE security environment by defining it into presumptions, threats and security policies of the organization, and is described completed and coherently. Security targets satisfy the identified threats, accomplish identified security policy of the organization, and satisfied the described presumptions.

IT security requirements are completely and coherently described, and provide foundation appropriate for development of TOE for accomplishment of security targets. TOE summary specifications accurately and coherently defines the security functions and assurance criteria, and satisfy the TOE security requirement described. Security Target accurately realizes the protection profile accommodated.

Therefore, Security Target is complete, coherent, technically appropriate, and is valid for usage as resultantly corresponding basic material of TOE evaluation.

- Configuration Management evaluation (ACM)

The evaluator made its evaluation by applying working unit of ACM Common Evaluation Methodology. It has been confirmed thatthe developer performs its control by suing automation tool for corrections on expression of realization from the configuration management documents. From the configuration management documents, it was confirmed that the developer clearly and definitively identifies configuration items related to TOE and TOE, ability to changes such items are

appropriately controlled. From the configuration management documents, it was verified that the developer executed configuration management on expression of minimum realization of TOE, evaluation evidences required in the assurance component of ST, and security defects.

Therefore, configuration management documents enable the consumer to identify evaluated TOE, assure unique identification of configuration items, and assure that the procedures used to control and track the TOE changes by the developer are appropriate.

- Delivery and Operation evaluation (ADO)

The evaluator made evaluation by applying the working unit of ADO Common Evaluation Methodology. Distributed documents, in the event of distributing the TOE to user, describe all procedures for maintenance of the security of TOE, and detection of changes and replacement of TOE. Procedures and phases for secured installation and start-up of generation of TOE are documented. As the result, it has been verified that environment for TOE is safely composed.

Therefore, distribution and operational documents are appropriate for assuring installation, generation and start-up of TOE in the manner same as that intended by the developer and distribution without changes in TOE.

- Development evaluation (ADV)

The evaluator made evaluation by applying the working unit of ADV Common Evaluation Methodology. Functional specification appropriately describes the TOE security functions, and explains that TOE security functions are sufficient to satisfy the security function requirements for Security Target. Furthermore, it appropriately describes the external interface of TOE. Security policy model is clear and definitive with coherence in describing the rules and properties of the security policy, and describes to enable coping with the security functions described in the functional specifications.

The fundamental design describes the TSF as sub-system, which is a key composition element, appropriately describes the interface of the sub-system and accurately realizes functional specification. Detailed design describes the internal actions of the TOE security functions as mutual relationship as well as dependency relationship between modules. Detailed design is sufficient to satisfy the security function requirement of Security Target, and is accurately and effectively elaborates the basic design.

Expression of realization is sufficient to satisfy the security function requirement of Security Target, and accurately realizes the detailed design. Accordance of

expression illustrates that the developer has accurately and perfectly realized the requirements of the Security Target as functional specification, basic design, detailed design and expression of realization.

Therefore, documents that accord the functional specification, which explains the external interface of TOE, basic design that explains the TOE structure as internal sub-system, detailed design that explains the TOE structure as internal module, expression of realization, which is source code level explanation, and expressions that copes with each other in order to assure coherence of such means of expression of TOE in the development are appropriate for understanding of the methods provide TOE security functions.

- Guidance evaluation (AGD)

The evaluator made evaluation by applying the working unit of AGD Common Evaluation Methodology. Administrator Manual describes the methods of accessing the security administrations interface by the administrator, explanations and precautions on each menu provided in the security administrations interface with examples. It has been confirmed that the details described in the administrator manual are executed accurately.

- Life Cycle Support evaluation (ALC)

The evaluator made evaluation by applying the working unit of ALC Common Evaluation Methodology. It was confirmed that the security control of the developer on development environment was appropriate for TOE design necessary for secured operation of TOE and in provision of confidentiality and flawlessness of realization of TOE. It was also confirmed that the developer is using documented TOE life cycle model. It was confirmed that the developer has used well-defined development tool that can generate results that are coherent and predictable.

Therefore, life cycle support appropriately describes the procedures used by the developer during development, maintenance and repair of TOE including security procedures and tools used in all processes of TOE development.

- Tests evaluation (ATE)

The evaluator made evaluation by applying the working unit of ATE Common Evaluation Methodology. The test manual describes the test goal, test procedures and outcome for each phase as well as illustrates examples of outcome on the security functions specified in the security target. It was confirmed that the details of test described in the test manual are accurate by repeatedly performing the test procedures including function test and module test for each phase of development provided. It was further confirmed that the operation of security function that was

realized during the development process coincides, and the accuracy of the developer's test confirmed through independent execution of the evaluator's test.

- Vulnerability Assessment evaluation (AVA)

The evaluator made evaluation by applying the working unit of AVA Common Evaluation Methodology. It was confirmed that the manual is not misunderstood, is not irrational and is not contracted in misuse analysis. It was also confirmed that secured procedures have been taken on all operation modes, and that unsecured status can be prevented and detected if the manual is used. Declaration of Strength of Function was made on all probabilities and permutation mechanism of Security Target, and it was confirmed that the analysis on Strength of Function declaration of the developer was accurate.

Analysis of vulnerability appropriately describes clearly known vulnerabilities of TOE and its countermeasures through realization of functions or clear indication of operating environment in the guidelines or manual. The evaluator has confirmed the accuracy of vulnerability analysis by performing independent vulnerability analysis. In the vulnerability analysis, it was confirmed that TOE does not have vulnerability of possibility of abuse by attacker with low level of attack within intended environment.

Therefore, it was confirmed that, on the basis of the vulnerability analysis of the developer and evaluator as well as penetration test of the evaluator, there is no defectiveness or weakness that can be abused within intended environment in TOE.

10. Recommendations

- This product is a web application firewall product that can detect and intercept attacks using HTTP/HTTPS protocol, and may be fragile towards attacks using protocols other than HTTP/HTTPS. Therefore, network security products such as invasion interception system, invasion prevention system and invasion detection system must be installed and operated in front of network inorder to elevate the security effect of this TOE.

- This product has WhiteURL collection/management function that collects/manages web documents that are normally operated and services in web server. Web documents that are collected/managed in WhiteURL can be accessed externally. Therefore, in the event of collection and management of key directory and documents in WhiteURL, precautions must be taken in the event of selection of target of management by WhiteURL since it can be exposed to ill-intended attacker. That is, at the time of installation and operation of this TOE, selection on the target of WhiteURL must be preceded.

- Trinity Soft Co., Ltd., in the event of occurrence of new web-related vulnerability, provides up-dating rule for this TOE in order to renew the web attack rule. As such, the administrator shall maintain the latest web attack detection rule by verifying up-dates through the web-site of Trinity Soft Co., Ltd. on regular basis.

- Although this product provides administrator notification function in the event of reaching the critical value due to exhaustion of storage space for audit record, the administrator ought to continuously monitor the usage of the storage space and secure storage space for audit report without fully relying on the notification function.

11. Acronyms and Glossary

Abbreviations & terms below were used in the report.

(1) Abbreviation

CC Common Criteria
EAL Evaluation Assurance Level
SOF Strength of Function
ST Security Target
TOE Target of Evaluation

(2) Terms

TOE
An IT product or system and its associated guidance documentation that is the subject of an evaluation

Audit Record
The audit data to store the event records which are related to the security of TOE

User
Any entity (human user or external IT entity) outside the TOE that interacts with the TOE

Authorised user
A user who may, in accordance with the TSP, perform an operation

External IT entity
Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE

WhiteURL
Registration of page that is normally operated and serviced on web-server is referred to as White URL collection, and the collected files are referred to as White URL

Web Application Firewall
Information security product that audits the HTTP/HTTPS packet and controls the flow in order to detect and intercept attacks using the vulnerabilities of web-server or web application

12. Reference

Certification body has used the following documents to produce the certification report :

[1] Common Criteria for Information Technology Security Evaluation (May 21, 2005)
[2] Common Methodology for Information Technology Security Evaluation V2.3
[3] Korea IT Security Evaluation and Certification Guidance (May 21, 2005)
[4] Korea IT Security Evaluation and Certification Scheme (Jan. 1, 2007)
[5] WEBS-RAY V2.0 Security Target V2.1 (Feb. 8, 2007)
[6] WEBS-RAY V2.0 ETR V1.1 (April 17, 2007)