122-B

COMMON CRITERIA CERTIFICATION REPORT No. CRP234

Oracle HTTP Server 10*g*
Release 2 (10.1.2)

Running on Sun Solaris 8 2/02 and Solaris 9 8/03

Issue 1.0

January 2007

UK Certification Body
CESG, Hubble Road
Cheltenham, GL51 0EX
United Kingdom

**ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	**Oracle Corporation**
Product and Version	**Oracle HTTP Server 10*g* Release 2 (10.1.2)**
Description	Oracle HTTP Server (OHS) is the web server component of Oracle Application Server. The primary function of OHS is to serve requests from web users made through the HTTP protocol.
CC Part 2	**Extended**
CC Part 3	**Conformant**
EAL	**EAL4** augmented with ALC_FLR.3
CLEF	**LogicaCMG UK Limited**
Date authorised	January 2007

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 ([a] - [c]). The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [d], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [i], the Common Evaluation Methodology (CEM) [j], and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no exploitable vulnerabilities have been found. It is not an endorsement of the product.

Trademarks:

All product or company names are used for identification purposes only and may be trademarks of their respective owners.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Oracle HTTP Server 10*g* Release 2 (10.1.2) to the Sponsor, Oracle Corporation, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [d], which specifies the functional, environmental and assurance requirements.

Evaluated Product

3. The version of the product evaluated was:

Oracle HTTP Server 10*g* Release 2 (10.1.2).

Note that the full name of this version of the product is **Oracle HTTP Server for Oracle Application Server 10*g* Release 2 (10.1.2.0.2)**. This is shortened to **Oracle HTTP Server 10*g* Release 2 (10.1.2)**, or simply **OHS**, in this report.

4. The Developer was Oracle Corporation.

5. OHS is a web server that has been built on the Apache Web Server infrastructure (Apache 2.0 HTTP Server). Its primary function is to service requests from clients made through the HTTP protocol. It is the web server component of Oracle Application Server.

TOE Scope

6. The scope of the TOE comprises the following modules and software components:

a) Oracle HTTP Server 10*g* Release 2 (10.1.2):

   i) mod_access;

   ii) mod_auth;

   iii) mod_log_config;

   iv) mod_security.

b) OHS tools, specifically the following command-line tools, which provide essential features by which OHS can be maintained and administered securely:

   i) htpasswd – an executable program which creates and updates the flat files used to store usernames and their associated passwords for basic authentication of web users;

   ii) Oracle Process Management Notification 10.1.2.1.0.

7. The scope of the evaluation applies to the TOE:

   a) when running on the Sun Solaris Version 8 2/02 operating system (identified in this report as 'Solaris8'), which has previously been certified to EAL4 [k];

   b) when running on the Sun Solaris Version 9 8/03 operating system (identified in this report as 'Solaris9'), which has previously been certified to EAL4 [l].

8. The Evaluated Configuration Document [m] defines how the TOE must be installed in its evaluated configuration and defines the requirements for setting up the TOE. Attention is drawn to those configuration instructions, particularly:

   a) [HS.POST-2] which sets the permissions to the 'ServerRoot/passwd' (default directory in which OHS stores password and group files) to the most restrictive possible while still allowing operation;

   b) [HS.POST-3] which sets the default access for each directory containing a web resource to the most restrictive possible;

   c) [HS.POST-10] which requires Administrators to ensure that the realm names, as used in AuthName directives, are unique across all configuration files (httpd.conf and .htaccess) used by OHS;

   d) [HS.CA-1] which seeks to prevent unauthorized, potentially malicious applications running on client or server host machines with access to the network.

9. The section 'Other Oracle HTTP Server Security Features' in Chapter 2 of the Security Target [d] lists the features of OHS that lie outside the boundary of the TOE for this evaluation. These are:

- Secure Sockets Layer (SSL);
- mod_oc4j;
- mod_ossl;
- mod_osso;
- web applications.

10. An overview of the product and its security architecture can be found in Chapter IV 'Product Security Architecture'.

Protection Profile Conformance

11. The Security Target [d] makes no claim for conformance to any Protection Profile. However, it is based as closely as possible on the draft US Government Protection Profile for Web Servers in Basic Robustness Environments [e]. Its relationship to that draft Protection Profile is summarised in Annex C of the Security Target.

Security Claims

12. The Security Target [d] fully specifies the TOE's security objectives, the threats which these objectives counter and the Security Functional Requirements (SFRs) and security functions to elaborate the objectives.

13. All of the SFRs are taken from CC Part 2 [h], apart from the following two SFRs which are extended relative to CC Part 2:

a) FMT_MSA.3 is an extended component, derived from FMT_MSA.3 and comprising the following two elements:

   i) FMT_MSA.3T.1;

   ii) FMT_MSA.3T.2.

b) FMT_REV.1 is an extended component, derived from FMT_REV.1 and comprising the following two elements:

   i) FMT_REV.1T.1;

   ii) FMT_REV.1T.2.

In both cases, the intent is that the TOE, in combination with its IT environment, collectively meets the requirements of FMT_MSA.3 and FMT_REV.1 for the static initialisation and revocation of security attributes used to enforce the Web User Security Function Policy.

14. The Security Target [d] groups the specification of the security functions as follows:

- Web Resource Access Control;
- Web Security Attributes;
- Audit and Accountability.

Security Policy

15. The TOE security policies are detailed in the Security Target [d]:

a) Chapter 5 explicitly identifies the *Web User Security Function Policy*, with which the TOE must comply, in the following SFRs of the TOE:

   - (user data protection): FDP_ACC.1 and FDP_ACF.1.

b) Chapter 5 implicitly identifies the *Content Provider Policy*, with which the IT Environment must comply, in the following SFRs for the IT environment.

   - (user data protection): FDP_ACC.1E and FDP_ACF.1E.

16. The Security Target [d] identifies the following Organisational Security Policy (OSP), with which the TOE must comply:

a) *P.BANNER:* The system underlying the TOE will display restrictions of use, legal agreements or any other appropriate information to which users consent by accessing the system.

b) *P.ACCOUNT:* Web users will be held accountable for their actions within the TOE.

Strength of Function Claims

17. The Security Target [d] claims that the minimum Strength of Function (SOF) for the TOE is SOF-Medium.

18. That claim applies only to the user password mechanism. User authentication is required to ensure that a user has the required permissions to access an OHS web resource.

19. The Security Target [d] identifies that the following security functions support the claimed SOF:

a) WAC.USESS (SOF-Medium); and

b) WAC.PWDM, which supports WAC.USESS by providing password management facilities.

Evaluation Conduct

20. The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication (UKSP) 01 and 02 [a - c]. The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

21. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [d], which prospective consumers are advised to read. To ensure the Security Target gave an appropriate baseline for CC evaluation, it was first itself evaluated. The TOE was then evaluated against the baseline.

22. The evaluation was performed in accordance with the following requirements:

- the EAL4 requirements specified in CC Part 3 [i];
- the Common Evaluation Methodology (CEM) [j];
- the appropriate interpretations.

23. The Certification Body monitored the evaluation which was carried out by the LogicaCMG Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [d]. The results of this work, completed in December 2006, were reported in ETR1 [r], ETR2 [s] and ETR3 [t].

Conclusions and Recommendations

24. The conclusions of the Certification Body are summarized in the Certification Statement on page ii.

25. **Prospective consumers of Oracle HTTP Server 10*g* Release 2 (10.1.2) should understand the specific scope of the certification by reading this report in conjunction with the Security Target [d]**. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

26. **This Certification Report is only valid for the evaluated TOE**. This is specified in Chapter III 'Evaluated Configuration'.

27. **The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration**. Chapter II 'Product Security Guidance' below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

28. **Certification is not a guarantee of freedom from security vulnerabilities**; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether these patches have further assurance. The installation of patches for security vulnerabilities, whether or not they have further assurance, should improve the security of the product.

II. PRODUCT SECURITY GUIDANCE

Introduction

29. The evaluation addresses the requirements specified in the Security Target [d]. The results of this work were reported in the ETRs ([r], [s] and [t]).

30. The following sections note considerations that are of particular relevance to purchasers of the product.

Delivery

31. When a consumer orders the TOE from the Vendor, Oracle provides the consumer with an order number and an invoice detailing the items ordered. The order is shipped via a trusted carrier to the consumer, who is informed separately of the carrier identity and the shipment details (e.g. waybill number). Packages are marked with the name and address of the sender (i.e. Oracle), name and address of the addressee (i.e. the consumer) and the Oracle logo.

32. The consumer receives the order as a package labelled as Oracle Application Server 10*g* Release 2 (10.1.2.0.2) Media Pack v2, Build Date 26/01/2006. The CD pack has part number B26306-01 v2. Within the CD pack there is Oracle Application Server Companion CD 10*g* (10.1.2.0.2) for Solaris Operating System (SPARC), part number B24477-01.

33. The consumer should check that the order number of the delivery is the same as the order number on the invoice, and that the part numbers of all items supplied are the same as those indicated on the invoice.

34. The above measures are intended to ensure that a third party could not masquerade as the Vendor and supply potentially malicious software. Nevertheless, the consumer must rely on Oracle's manufacturing procedures and the trust placed in the carrier, to counter the threat of interference to the order along the delivery path. The Evaluators confirmed that Oracle would use a high security courier, or other measures, if required by the consumer.

35. On receiving the TOE, the consumer should check that it is the evaluated version and should check that the security of the TOE has not been compromised during delivery.

36. Oracle also makes components of the TOE available for download from Oracle's website http://edelivery.oracle.com , via the instructions given on that site. This allows the integrity of each item downloaded to be verified via the digest value that is supplied for it. Download of components of the TOE was outside the scope of the evaluation. **The Certification Body recommends that, where the threat of spoofing of the Oracle website is considered relevant to the TOE's operational environment, then consumers should obtain delivery of the TOE via physical media only (e.g. CD-ROMs for software, printed books for documentation).**

Installation and Guidance Documentation

37. The only users of the TOE in its evaluated configuration are users and administrators. Administrators install the TOE, then set up and maintain web resources so that the Oracle HTTP Server is able to receive and respond to HTTP messages from users outside the scope of the TOE. Only administrators require direct interaction with the TOE.

38. Guidance to administrators regarding security of the TOE is provided in the Evaluated Configuration Document [m], which also indicates how the TOE's environment can be secured. The procedures in that document that are relevant to non-administrative users are generally limited to common-sense measures.

39. The Evaluated Configuration Document [m] refers to other supporting documentation ([n], [o] and [p]) as appropriate.

40. The Evaluated Configuration Document [m] is released by Oracle to consumers on request. It is anticipated that Oracle may also make it available for download from one of its websites (e.g. via http://www.oracle.com/technology/deploy/security).

Flaw Remediation

41. Oracle's flaw remediation information for consumers is available from two websites:

a) Oracle's 'MetaLink' website (http://metalink.oracle.com), which enables consumers with an Oracle support contract to:

   i) email details of flaws to Oracle, and receive technical support, by submitting a Technical Assistance Request;

   ii) receive email alerts from Oracle regarding flaws, fixes and workarounds;

   iii) read alerts and news posted on the MetaLink website by Oracle regarding flaws, fixes and workarounds;

   iv) download patches from Oracle via the MetaLink website.

b) Oracle's public website (http://www.oracle.com), which enables other consumers and the public to:

   i) email details of security flaws to Oracle, at secalert_us@oracle.com;

   ii) read alerts and news posted on the public website by Oracle regarding flaws, fixes and workarounds.

42. Oracle currently issues patches via the Internet only (at http://metalink.oracle.com), where they are available only to consumers with an Oracle support contract as noted above. **Consumers can guard against spoofing by phoning Oracle support and asking them to check their patch download audit log; an entry in the log would confirm that Oracle initiated the download.**

III. EVALUATED CONFIGURATION

TOE Identification

43. The TOE is uniquely identified as:

Oracle HTTP Server 10*g* Release 2 (10.1.2).

Note that the full name of this version of the product is **Oracle HTTP Server for Oracle Application Server 10*g* Release 2 (10.1.2.0.2).** This is shortened to **Oracle HTTP Server 10*g* Release 2 (10.1.2)**, or simply **OHS**, in this report.

TOE Documentation

44. The relevant guidance documents, as evaluated for the TOE or referenced from the evaluated documents, were:

- OHS Security Target [d];
- OHS Evaluated Configuration Document [m];
- Oracle Application Server Quick Installation & Upgrade Guide for Solaris [n];
- OHS Standalone Administrator's Guide Based on Apache 2.0 [o];
- OPMN Server Administrator's Guide [p].

TOE Configuration

45. The TOE should be installed, configured and maintained in accordance with the Evaluated Configuration Document [m].

46. Annex A.2 of the Evaluated Configuration Document [m] specifies exactly the software components that compromise the evaluated configuration of the TOE.

Environmental Requirements

47. The security of the TOE depends not only on secure administration of the TOE, but also on secure administration of the host operating system server and other services utilised under the OHS specification.

Test Configuration

48. The environmental configuration used by the Developer to test the TOE is summarised in the table below:

Machine	Sun Ultra 60, used as the server and the client
Processor	295 MHz CPU
Memory	1 GB RAM
Operating System	Solaris 8 2/02
Drives	2x 20GB hard drives, 3.5" floppy drive, CD drive
Network Connection	10/100 BaseT network connection on the motherboard

Table III-1: Environment Configuration (Developer's Tests)

49. The environmental configuration used by the Evaluators to test the TOE is summarised in the table below:

Machine	Sun Ultra 60, used as the server
Processor	450 MHz CPU
Memory	1 GB RAM
Operating System	Solaris 8 2/02
Drives	40 GB hard drive, 3.5" floppy drive, CD drive
Network Connection	10/100 BaseT network connection on the motherboard
Machine	Sun Ultra 60, used as the server
Processor	450 MHz CPU
Memory	1 GB RAM
Operating System	Solaris 9 8/03
Drives	40 GB hard drive, 3.5" floppy drive, CD drive
Network Connection	10/100 BaseT network connection on the motherboard
Machine	Compaq Armada M700, used as the client
Processor	845 MHz CPU
Memory	256 MB RAM
Operating System	Windows XP with Internet Explorer v5
Drives	20 GB hard drive, 3.5" floppy drive, CD drive
Network Connection	10/100 BaseT network connection on the motherboard

Table III-2: Environment Configuration (Evaluators' Tests)

50. Further details of the Developer's testing and the Evaluators' testing are given in Chapter V 'Product Testing'.

IV. PRODUCT SECURITY ARCHITECTURE

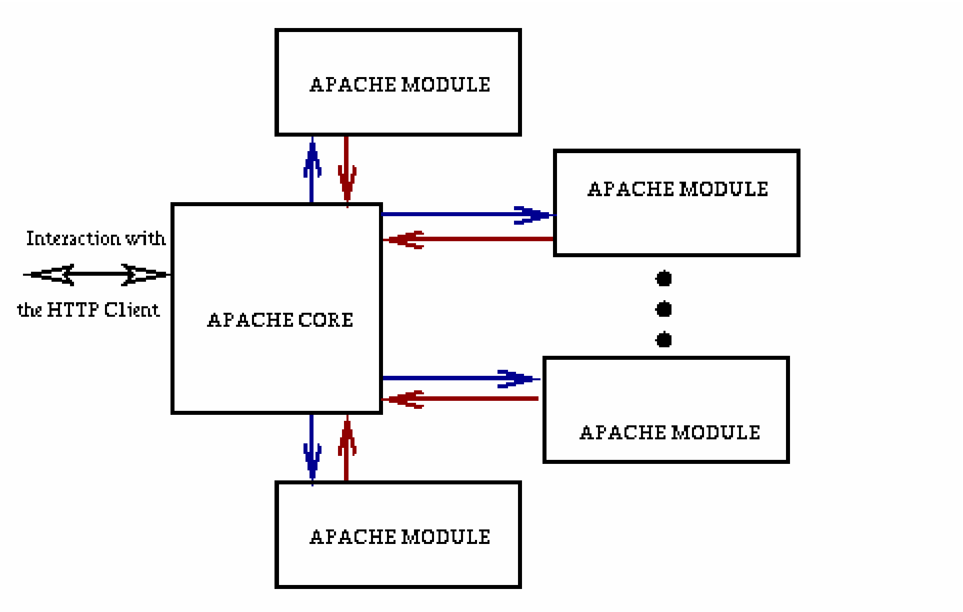
51. This Chapter gives an overview of the main product architectural features. Other details of the scope of evaluation are given in Chapter III ‘Evaluated Configuration’.

Product Description and Architecture

52. OHS is a web server that has been built on the Apache Web Server infrastructure (for this evaluation it is based on the Apache 2.0 HTTP Server). Its primary function is to service requests from clients made through the HTTP protocol. It is the web server component of Oracle Application Server.

53. OHS consists of an HTTP Listener to receive client requests and a set of modules that implement and provide extensions to the basic functionality of OHS. Many of the standard Apache modules are provided in OHS, which also includes several modules that are specific to Oracle Application Server components.

54. The figure below illustrates the high level conceptual architecture of the Apache HTTP Server, which is also the architecture for the OHS Server. There is a core part of the server that is responsible for defining and following the steps in servicing a request and a number of modules are provided to implement the different phases of request handling.



Design Subsystems

55. The design subsystems of the TOE are:

a) OHS Server. This is based on the Apache 2.0 HTTP Server, for this evaluation. Its primary function is to service requests from clients made through the HTTP protocol.

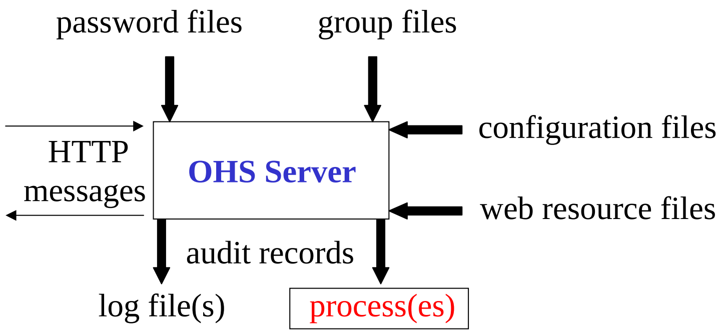
b) Oracle Process Manager and Notification Server (OPMN): This is used by web server administrators to start, monitor and stop the OHS Server.

c) Run-Time Tool (apachectl): This is a front end to the OHS Server. It is used by the OPMN Server to control the functioning of the httpd daemon.

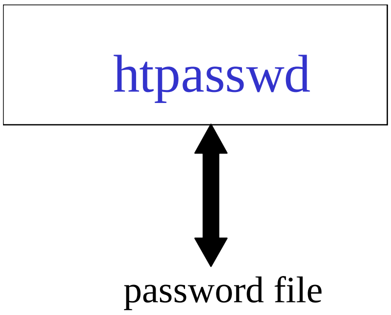
d) Essential Administration Tools (htpasswd): This is the executable program which creates and updates the flat files used to store usernames and their associated passwords for basic authentication of web users.

Hardware and Firmware Dependencies

56. The figure below illustrates input/output for the OHS Server, for which network and disk access is achieved via the operating system.



57. The figure below illustrates input/output for the htpasswd program, which is the part of the TOE that performs security attribute management. Disk access is achieved via the operating system.



Product Interfaces

58. The external interfaces into the TOE are:

    a) the HTTP message interface to the OHS Server via the OHS HTTP Listener;

    b) the command line interface to htpasswd.

V. PRODUCT TESTING

Developer's Testing

59. The Developer installed and tested the TOE on the platform stated in Table III-1.

60. The Developer tested the security mechanisms, the security functions, the subsystems and the external interfaces of the TOE, using automated tests.

61. The Developer provided the evaluators with a Multi-platform Rationale [q]. The rationale argued that the results obtained for the Solaris 8 2/02 platform were equally valid for the Solaris 9 8/03 platform, given that the TOE was unchanged, the OS interfaces it relies upon are unchanged, and both platforms are certified. The rationale closely follows the approach described in [f].

Evaluators' Testing

62. The Evaluators installed and tested the TOE on the platforms stated in Table III-2.

63. Evaluator testing was carried out using a web browser.

64. The Evaluators assessed the Developer's testing approach, coverage, depth and results. This included the following:

a) the Evaluators checked that the Developer's testing approach covered the TOE's security mechanisms, security functions, subsystems and external interfaces;

b) the Evaluators witnessed all of the Developer's tests;

c) the Evaluators performed independently-devised functional tests to cover the security functions.

65. The Evaluators' findings confirmed that:

a) the Developer's testing approach, depth, coverage and results were all adequate;

b) the Developer's tests covered the TOE's security mechanisms, security functions, subsystems and external interfaces;

c) (for the Developer's tests witnessed by the Evaluators): the actual test results were consistent with the expected test results and any deviations were satisfactorily accounted for;

d) (for the Evaluators' independently-devised functional tests): the actual test results were consistent with the expected test results;

e) (for the developer's Multi-platform Rationale [q]): no difference in the TOE behaviour was observed when the tests were run on either platform (Solaris 8 2/02 and Solaris 9 8/03).

66. The Evaluators' then performed penetration testing of the TOE. Those tests searched for potential vulnerabilities in the features of the TOE.

67. From checking various sources on the Internet, the Evaluators found no publicly known exploitable vulnerabilities regarding the TOE's environment that could be used to compromise the TOE.

68. The Evaluators found that all relevant, publicly known vulnerabilities had been resolved in the TOE and/or its guidance documentation (e.g. in the Evaluated Configuration Document [m]), such that those vulnerabilities were not exploitable for the TOE.

69. The results of the Evaluators' penetration testing confirmed that all identified potential vulnerabilities in the TOE have been addressed, i.e. the TOE in its intended environment has no exploitable vulnerabilities.

Vulnerability Analysis

70. The Evaluators searched for vulnerabilities regarding the TOE. They also searched for vulnerabilities regarding the TOE's environment that could be used to compromise the TOE.

71. The Evaluators' vulnerability analysis was based on public domain sources, Oracle's Vulnerability Analysis document submitted to the evaluators, and on the visibility of the TOE given by the evaluation process.

Platform Issues

72. The TOE was evaluated on the Solaris 8 2/02 and Solaris 9 8/03 operating system platforms and hardware platforms specified in Table III-2.

73. The certified configuration is for OHS Server running on those platforms only, i.e. it excludes all other platforms.

VI. REFERENCES

[a] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[b] CLEF Requirements - Startup and Operation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[c] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

[d] Security Target for Oracle HTTP Server 10*g* Release 2 (10.1.2),
Oracle Corporation,
Issue 0.5, January 2007.

[e] US Government Protection Profile for Web Servers in Basic Robustness Environments,
Version 0.61, December 17, 2004,
available on the World Wide Web at
http://niap.nist.gov/pp/draft_pps/pp_draft_websrv_br_v0.61.pdf

[f] UK CC Interpretation 012: Multi-Platform TOEs,
UK IT Security Evaluation and Certification Scheme,
29 October 2004.

[g] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Interpretations Management Board,
CCIMB-2005-08-001, Version 2.3, August 2005.

[h] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2005-08-002, Version 2.3, August 2005.

[i] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2005-08-003, Version 2.3, August 2005.

[j] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
CEM-2005-08-004, Version 2.3, August 2005.

[k] Common Criteria Certification Report No. P182:
Sun Solaris Version 8 2/02,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, April 2003.

[l] Common Criteria Certification Report no. 383-4-26-CR:
Sun Solaris Version 9 8/03,
Canadian Common Criteria Evaluation and Certification Scheme,
Issue 1.0, 27 January 2005.

[m] Evaluated Configuration for Oracle HTTP Server 10*g* Release 2 (10.1.2),
Oracle Corporation,
Issue 0.9, January 2007.

[n] Oracle Application Server Quick Installation and Upgrade Guide,
10*g* Release 2 (10.1.2) for Solaris Operating System (SPARC),
Oracle Corporation,
Part No. B14089-01, December 2004.

[o] Oracle HTTP Server Administering a Standalone Deployment Based
on Apache 2.0, 10*g* Release 2 (10.1.2),
Oracle Corporation,
Part No. B14009-02, July 2005.

[p] Oracle Process Manager and Notification Server Administrator's Guide,
10*g* Release 2 (10.1.2),
Oracle Corporation,
Part No. B13996-01, December 2004.

[q] Multi-platform Rationale for Oracle HTTP Server 10*g* Release 2 (10.1.2),
Oracle Corporation,
Issue 0.2, September 2006.

[r] Task LFL/T231 Evaluation Technical Report 1,
LogicaCMG CLEF,
310.EC202082:30.1.2, Issue 1.0, 12 July 2006.

[s] Task LFL/T231 Evaluation Technical Report 2,
LogicaCMG CLEF,
310.EC202082:30.2.3, Issue 1.0, 18 October 2006.

[t] Task LFL/T231 Evaluation Technical Report 3,
LogicaCMG CLEF,
310.EC202082:30.3.2, Issue 1.0, 30 November 2006.

VII. ABBREVIATIONS

CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTTP	Hypertext Transfer Protocol
OHS	Oracle HTTP Server
OPMN	Oracle Process Manager and Notification Server
OSP	Organisational Security Policy
SFR	Security Functional Requirement
SOF	Strength of Function
TOE	Target of Evaluation
UKSP	United Kingdom Scheme Publication