Evaluated Configuration

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

January 2007

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

Evaluated Configuration for Oracle HTTP Server 10*g* Release 2 (10.1.2)

January 2007

Author: Julian Skinner.

Contributors: Peter Goatly and Ann Craig.

Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The information in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. Oracle Corporation does not warrant that this document is error free.

Contents

Contents

CHAPTER

1 Introduction

The Target of Evaluation (TOE) is Oracle HTTP Server 10*g* Release 2 (10.1.2).

Note that the full name of the release of the product being evaluated is Oracle HTTP Server for Oracle Application Server 10*g* Release 2 (10.1.2.0.2). This name is shortened to Oracle HTTP Server 10*g* Release 2 (10.1.2.0.2) in this document.

The TOE is hosted on two operating system platforms:

- Sun Solaris 8 2/02, and
- Sun Solaris 9 8/03.

This *Evaluated Configuration for Oracle HTTP Server 10g Release 2 (10.1.2)* document explains the manner in which the TOE must be configured along with the host operating system and network services so as to provide the security functionality and assurance as required under the Common Criteria for Information Technology Security Evaluation [CC].

The Evaluation Assurance Level for the TOE is EAL4 augmented with ALC_FLR.3. The Security Target used for the evaluation of the TOE is [ST].

1.1 Intended Audience

The intended audience for this document includes evaluators of the TOE, system integrators who will be integrating the TOE into systems, and accreditors of the systems into which the TOE has been integrated.

1.2 Organization

This document is composed of the following chapters:

Chapter 1 contains the introduction to the document;

Chapter 2 describes the physical environment of the TOE and the network services required to support the TOE;

Chapter 3 describes the host operating system, network services, and application configurations required to support the TOE;

Chapter 4 describes the configuration of the TOE;

Chapter 5 contains a step by step guide to the installation of the TOE in its evaluated configuration;

Annex A lists the software components installed as per section 5.2; and

Annex B lists the references that are used in this document.

Change bars indicate changes made since the previous issue of this document.

1.3 Format

Assertions about the configuration actions that are required to be performed are given identifiers to their left in bold Arial font, e.g. **[A-1]**. References to sections of documents listed in Annex B are in the format [*document, section*].

Mandatory evaluation configuration requirements use the words “must” and/or “shall” in each assertion.

Strongly recommended evaluation configuration requirements use the words “should” in each assertion.

CHAPTER

2

Physical Configuration

This chapter describes the physical and procedural requirements for maintaining the security of the TOE.

2.1 Physical Environmental Assumptions

[HS.A-1] The server machine hosting the TOE and its underlying operating system shall be located within controlled access facilities which will prevent unauthorized physical access by unprivileged users. Only authorized administrators of the systems hosting the TOE shall have physical access to those systems. Such administrators comprise Operating System Administrators, Web Server Administrators and Web Resource Administrators.

[HS.A-2] The processing resources of the network services required to support the TOE shall be located within controlled access facilities which will prevent unauthorized physical access.

[HS.A-3] The media on which authentication data for the underlying operating system data resides shall not be physically removable from the underlying operating system by unauthorized users.

[HS.A-4] The media on which the TOE audit data resides shall not be physically removable from the underlying operating system by unauthorized users.

[HS.A-5] Any on-line and/or off-line storage media on which security relevant data resides shall be located within controlled access facilities which will prevent unauthorized physical access.

2.2 Supporting Procedures

Procedures for the administration of the TOE security shall be established based on the contents of this document, the Security Target [ST], any site security policy that may be in force and [SRN-8] and [SRN-9]. Procedures for the TOE shall include the following:

- One or more competent individuals must be assigned to manage the TOE and the underlying system and the security of the information it contains who can be trusted not to abuse their privileges. Such individuals will each take one or more of the roles: Operating System Administrator, Web Server Administrator and Web Resource Administrator.
- Web server administrators shall distribute username and password pairs to users of the TOE in a secure manner and shall instruct these web users not to disclose their passwords to other individuals.
- Web server administrators should not keep records of cleartext passwords that have been generated and have been sent out to users of the TOE. Thus, if a user reports to an administrator that they have forgotten their password, a new password should be generated and sent to them.
- Web server administrators shall ensure that any password they supply to a user of the TOE is strong enough to satisfy the TOE's CC Strength of Function rating of SOF-*medium* (see Assertion **[HS.POST-7]** in section 4.2).

CHAPTER

3 Host Configuration

This chapter describes the configuration requirements for the systems which underly the TOE.

3.1 Sun Solaris Operating System

The TOE was evaluated and tested on two machines connected by a Local Area Network (LAN). One machine, acting as the server, was used to run the TOE software and the second machine, acting as the client, was used to run a web browser. The specification of these 2 machines can be found in [CRP234, Table III-2].

The TOE was evaluated and tested on both of Sun Solaris 8 and Sun Solaris 9 operating systems, which have both met Common Criteria security requirements for assurance level EAL4. Configuration requirements for these operating systems are provided in this section.

[HS.SS-1] If the operating system on which the TOE resides is Solaris 8 then it shall be installed and operated in a manner as described in [SRN-8]. If the operating system is Solaris 9 then it shall be installed and operated in a manner as described in [SRN-9].

[HS.SS-2] The UNIX filesystem (ufs) shall be used on all host machines supporting the TOE.

[HS.SS-3] The operating system administrator shall ensure that only administrative users are provided with operating system accounts for the system hosting the TOE and that such users are only given accounts and membership of groups as appropriate to their responsibilities. In particular, the *oracle* user account and the *oinstall* group should be available only to web server administrators.

3.1.1 Protection of Resources

[HS.PR-1] The operating system shall protect all of the installed TOE-related files and directories by means of its Discretionary Access Control mechanisms to ensure that they are accessible to authorized users only.

[HS.PR-2] To maintain the integrity of the audit timestamp, only operating system administrators shall have access to the operating system clock configuration. All other users shall have no access permissions for the operating system clock configuration.

3.1.2 Accounting and Auditing

[HS.AA-1] The operating system shall protect operating system audit trails or any other audit trails (e.g. audit log files) used by OHS against unauthorized modification and deletion by means of its Discretionary Access Control mechanisms.

[HS.AA-2] The directory containing the log files holding the TOE-generated audit data shall have permissions set for access only by web server administrators, and no access for all other users.
Note: such files are located by default in the *ServerRoot/logs* directory.

[HS.AA-3] The operating system administrator shall implement procedures that support the archiving of operating system audit trails and audit log files prior to audit trail or disk space exhaustion.

3.2 Network Services

[HS.NS-1] No network services other than HTTP are to be configured for the system hosting the TOE.

3.3 Applications

[HS.SA-1] No applications, other than standard web browsers, shall be permitted to run on any machines which access the network, unless they have been shown not to compromise the TOE’s security objectives stated in [ST].

CHAPTER

4 TOE Configuration

The TOE consists of software only. The TOE contains no hardware or firmware components and there are no hardware or firmware dependencies which affect the evaluation.

This chapter describes how the TOE must be configured in its evaluated configuration.

4.1 Pre-Installation Requirements

The actions **[HS.PRE-1]** to **[HS.PRE-3]** listed in this section are required before the installation of the TOE can be carried out as described in chapter 5.

[HS.PRE-1] In order for the Oracle HTTP Server 10g Release 2 (10.1.2) installation process to install successfully, the following lines must be present in the file `/etc/system` and a reboot must be performed:

```
set semsys:seminfo_semmni=100
set semsys:seminfo_semmns=256
set semsys:seminfo_semmsl=256
set shmsys:shminfo_shmmax=4294967295
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=100
set shmsys:shminfo_shmseg=10
```

[HS.PRE-2] An operating system group, which will be used by the Oracle software owner, must be created before installing OHS. Any legal name can be used for this group, but the convention is to use “`oinstall`”. The oinstall group can be created via the admintool GUI or via the `groupadd` command.

[HS.PRE-3] An operating system account that will be the Oracle software owner must be created before installing OHS. The conventional name used is “`oracle`” and this account will be used by the web server administrator for installing and configuring the TOE. When creating the account a primary group is required, which should be the oinstall group. The `oracle` account can be created via Solaris’s user account administration GUI or with the `useradd` command.

4.2 Post-Installation Requirements

Actions **[HS.POST-1]** to **[HS.POST-19]** listed in this section are required to be performed to increase the security of the evaluated configuration after OHS installation has been carried out as described in chapter 5. Throughout this section the term administrator refers to the web server administrator unless explicitly stated otherwise.

On installation OHS creates its main configuration file, `httpd.conf`. In that file is a directive, `ServerRoot`, that is configured to have the value:
`/home/oracle/STANDOHS/ohs`
Wherever `ServerRoot` is used below in this document, it will stand for
`/home/oracle/STANDOHS/ohs`

[HS.POST-1] The operating system administrator must add the following line to the `.profile` file of the `oracle` account:

```
LD_LIBARARY_PATH=ServerRoot/lib; export LD_LIBRARY_PATH
```

[HS.POST-2] The administrator must set file and directory operating system permissions to the most restrictive possible whilst still allowing operation.

The default directory in which OHS stores password and group files is
`ServerRoot/passwd`.
The permissions must be changed to 700.

The administrator shall ensure that only administrators have execute permission on the `htpasswd` file (located in `ServerRoot/bin`). The permissions must be changed to 700.

In the directory `ServerRoot/logs` no user except the `oracle` user should have access to the access log and error log files. Permissions on these files must be restricted to being read-only by setting them to 400.

[HS.POST-3] The administrator must perform the following edits to the file `httpd.conf`:

- Include the `mod_security` module:

  in the section Dynamic Shared Object (DSO) Support add the following:

  ```
  LoadModule security_module modules/mod_security.so
  ```

- Set default access for each directory containing web resources to the most restrictive possible (these restrictions can be overridden as required in specific directories).

  Search for the `<Directory />` directive and replace with:

  ```
  <Directory />
  
     Order Deny, Allow
  
     Deny from all
  
     Options none
  
     AllowOverride none
  
  </Directory>
  ```

- Ensure that web resources are only available for read access by disallowing all but the GET and HEAD HTTP request methods, as follows:

```
<Directory />
   <LimitExcept GET>
      Deny from all
   </LimitExcept>
</ Directory>
```

- Locate and change the setting of the `ServerTokens` and `ServerSignature` directives to provide the least amount of information:

```
ServerTokens None
ServerSignature Off
```

[HS.POST-4] The administrator must ensure that all directories in the Unix file system which contain web resources that are to be served by the TOE are referenced by a `<Directory>` section in the `httpd.conf` file. And that those `<Directory>` sections will contain directives such that anonymous web users can only access public material and that any material that is not deemed to be public will have the necessary access control directives applied e.g `<Require>`.

In addition, the administrator should ensure that each web resource administrator has write access to all directories in the Unix file system, which contain web resources to be served by the TOE that they have supplied.

[HS.POST-5] The following directives provided by `mod_security` should be added to the `httpd.conf` file to provide countermeasures against potential attacks against applications hosted by the web service:

```
SecFilterEngine On
SecFilterDefaultAction “deny,log,status:403”
SecFilterCheckURLEncoding On
SecFilterForceByteRange 1 255
```

Administrators wishing to protect against other types of attack on applications hosted by the web service can find examples of further uses of `mod_security`’s directives at `www.modsecurity.org/documentation/quick-examples.html`.

[HS.POST-6] The administrator shall ensure that password files are not accessible via the HTTP server. This can be achieved by storing the files in the `ServerRoot/passwd` directory.

[HS.POST-7] Using the `htpasswd` administration tool, the administrator shall create a unique username and password pair for each user of the TOE that is to be allocated a username. Such a password should be easy for the user to remember, but not easy for an attacker to guess. A good method of generating such passwords is to use one of the “pronounceable password” generators that can easily be found via the World Wide Web.

The password:

- shall be at least 6 characters in length,
- shall not contain the username or any obvious permutation of its characters,
- shall not contain the name of the user represented by the username (or any obvious permutation of the name’s characters), and

- shall be hashed for storage in the password file using the SHA-1 algorithm.

[HS.POST-8] The administrator shall ensure that if distributed configuration files are used, the files shall be named as `.htaccess` and permissions on these files are set to 600.

In addition, the administrator must not remove from the `httpd.conf` file the directive:

```
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
</Files>
```

which is present in the `httpd.conf` file once the TOE has been installed.

[HS.POST-9] When configuring web resources for authentication and authorization the administrator must ensure that the `Satisfy Any` directive is not used within any configuration files.

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

[HS.POST-11] [AHSD, 2.9] provides Security Tips for Apache installations that should be read by administrators as guidance for their installation of the evaluated configuration. For example, the installation process described in section 5.2 results in the establishment of a directory, `htdocs`, which is available to all users. The subdirectories of this directory should be established with permissions that are appropriate to the users which are authorized to access the material in these directories.

[HS.POST-12] In the default `httpd.conf` file, auditing of user access is formatted (via the `LogFormat` and `CustomLog` directives) to include all of the items of information in the Common Log Format (CLF). This format is highly configurable, but the administrator must ensure that at least the items in the CLF are always included in the output.

[HS.POST-13] In the default `httpd.conf` file, error log records are output to a file located at ServerRoot/logs/error_log. This is achieved via the `ErrorLog` directive. The administrator must ensure that the `httpd.conf` file always contains an `ErrorLog` directive. This directive can be used to cause error log records to be output to a file or to be piped to a suitable audit trail management system.

[HS.POST-14] The administrator must ensure that the severity level of the Error Log is always set to `crit` or higher. This is achieved through usage of the `LogLevel` directive. The default level is `warn`.

[HS.POST-15] The administrator shall perform regular checks of the audit trail, looking for:

- evidence of attacks against the TOE's security policy.
- anonymous web users accessing web resources for which they are not intended to be authorized.
- evidence of any access to non-public information via web user accounts that are no longer intended to be used to access web resources.

[HS.POST-16] The administrator shall ensure that the TOE audit trail is kept to a reasonable size by archiving audit material when necessary and by purging the TOE audit trail (after first checking its contents as described in the assertion above).

The administrator should note that, if the TOE audit trail is not regularly purged, it can cause the disk space to fill up.

[HS.POST-17] The Security Audit section of [ST, 5] states that the Security Functional Requirements for audit in the TOE only cover the generation of audit data for security relevant TOE events. The Security Functional Requirements for the IT environment in this section of [ST] cover the capability to selectively record audit data, to review audit data, and to create and maintain an audit trail. The administrator must therefore ensure that the system in which the TOE is to be used has these capabilities.

[HS.POST-18] The TOE Definition section of [ST, 2] lists the OHS modules that are included in the TOE (in addition to OHS's core module). These are `mod_access`, `mod_auth`, `mod_log_config` and `mod_security`. The administrator shall not include in a configuration file any directives implemented by any of the other OHS modules if OHS is to remain in its evaluated configuration. For each directive, [AHSD, 12.3] indicates the page in [AHSD] that can be consulted to find which module implements it.

[HS.POST-19] The administrator shall remove all files from the directories `/fcgi-bin` and `/cgi-bin`. These directories are used to hold sample programs that must not be used in the evaluated configuration.

This Page Intentionally Blank

CHAPTER

5 Step by Step Guide

This chapter contains a step by step guide for web server administrators to install OHS in its evaluated configuration. It can be read in conjunction with [QUICK], which provides background information on the pre-installation requirements.

5.1 Operating System Installation / Configuration

Ensure that the intended physical environment is in accordance with the assumptions **[HS.A-1]** to **[HS.A-5]** listed in section 2.1 of this document.

Installation instructions for the two platforms, Sun Solaris 8 and Sun Solaris 9, are given separately below.

5.1.1 Installation of Sun Solaris 8

Install Sun Solaris 8 in accordance with chapter 3 and [SRN-8]. Also ensure the patches specified in [QUICK, 4.2: Patches Required for Solaris 8] are installed and are at a version number at least as high as is specified in that document.

5.1.2 Installation of Sun Solaris 9

Install Sun Solaris 9 in accordance with chapter 3 and [SRN-9]. Also ensure the patches specified in [QUICK, 4.2: Patches Required for Solaris 9] are installed and are at a version number at least as high as is specified in that document.

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

5.2.1 Step by Step Installation of Oracle HTTP Server 10*g* Release 2 (10.1.2)

This section outlines steps needed to set up OHS's evaluated configuration on Sun Solaris 8 and Sun Solaris 9. Those steps which are essential towards achieving OHS's Evaluated Configuration are highlighted in **bold**.

The information to be supplied by the web server administrator for each step is indicated on the Universal Installer screen. The items in quotes below are examples of what was supplied for a particular installation of OHS.

This section should be used in conjunction with the relevant installation manuals and assumes any prior installations of Oracle HTTP Server have been removed before the new installation starts.

Step No.	Action	Result
1	Insert Oracle Application Server Companion CD 10*g* (10.1.2.0.2) CD-ROM 1. Follow the instructions given in [QUICK, 5] to start Oracle Universal Installer.	Oracle Universal Installer: Welcome window appears.
2	Click Next.	Specify Inventory Directory screen opens.
3	Ensure the Inventory path is suitable for the installation. example: “`export/home/oracle/oraInventory`” Click Ok.	This is the default path supplied on screen. Unix Group Name screen opens.
4	Enter Unix Group Name: example: “`oinstall`”	Execute orainstRoot.sh screen opens
5	Execute oraInstRoot.sh script as **root user** from the following directory: `export/home/oracle/oraInventory` The command to run theoraInstRoot.sh script is: **`sh oraInstRoot.sh`** Click Continue	This script is run only if this is the first installation on this computer. Specify File Locations screen opens.
6	Ensure the Oracle Home and full path are suitable for the installation. example: “`export/home/oracle/STANDOHS`” Click Continue.	This is the default option provided by the Universal Installer. Select a Product to Install screen opens
7	Select: **Oracle Web Server Services 10.1.2.0.2** Click Next	Select Installation Type screen opens

Step No.	Action	Result
8	Select: **Oracle HTTP Server with Apache 2.0** Click Next.	Specify Instance Name
9	Instance Name: ohs	Confirm Pre-Installation Requirements screen opens
10	Click Install	

5.2.2 Exclusions

Section A.1 lists the software components that are installed on the server by the Oracle Universal Installer during the installation of Oracle HTTP Server 10*g* Release 2 (10.1.2) as per section 5.2.1. Because this is an Oracle Application Server installation process, many of these components are not part of the TOE for this evaluation. Section A.2 lists the components that actually constitute the TOE. The other software components are not for use with the TOE in its evaluated configuration.

5.3 Client Installation

The TOE scope does not include any client software. During the evaluation of the TOE, client software and a web browser can be used outside of the TOE to send HTTP messages to the TOE in order to test its security features.

[HS.CA-1] Administrators shall ensure that no applications are installed that can be run on any client machines which access the network, unless they have been shown not to compromise the TOE's security objectives as stated in [ST].

This Page Intentionally Blank

ANNEX

A TOE Components

A.1 Server components

The following is a summary of all the components that are installed on the server by the Oracle Universal Installer during the installation of Oracle HTTP Server 10*g* Release 2 (10.1.2) as per section 5.2.1:

- Sun JDK extensions 10.1.2.0.0
- Sun JDK 1.4.2.0.6
- Java Runtime Environment 1.4.2.0.4
- Installer SDK Component 10.1.0.4.0
- Oracle One-Off Patch Installer 10.1.0.4.0
- Oracle Universal Installer 10.1.0.4.0
- Bali Share 1.1.18.0.0
- Oracle JFC Extended Windowing Toolkit 4.2.33.0.0
- Oracle HTTP Server 2 Welcome Pages 10.1.2.1.0
- Oracle Apache Modules 10.1.2.1.0
- Perl Interpreter 5.8.3.0.0
- Oracle Required Support Files 32 bit 10.1.0.1.0
- Oracle Required Support Files 32 bit Patch 10.1.0.4.2
- Oracle Extended Windowing Toolkit 3.4.38.0.0
- Documentation Required Support Files 10.1.0.3.0
- Oracle Ice Browser 5.2.3.6.0
- Oracle Help For Java 4.2.6.1.0
- Oracle Notification Service 10.1.2.1.0

- Oracle Process Management Notification 10.1.2.1.0
- HTTP Server Files 2.0.0.0.0
- Oracle Dynamic Monitoring Service 10.1.2.1.0
- Oracle 10g Real Application Clusters Common Files 10.1.0.2.0
- Oracle 10g Real Application Clusters Common Files Patch 10.1.0.4.2
- regexp 2.1.9.0.0
- Extended Windowing Toolkit 3.3.18.0.0 Beta
- Oracle Locale Builder 10.1.0.2.0
- Oracle Locale Builder Patch 10.1.0.4.2
- Enterprise Manager Minimal Integration 10.1.0.2.0 Beta
- Oracle Globalization Support 10.1.0.2.0
- Oracle Globalization Support Patch 10.1.0.4.2
- Oracle Net Required Support Files 10.1.0.2.0
- Oracle Net Required Support Files Patch 10.1.0.4.2
- Installation Common Files 10.1.0.2.0
- Installation Common Files Patch 10.1.0.4.2
- Oracle Display Fonts 10.1.2.0.0
- Oracle UIX 2.2.20.0.0
- Oracle Code Editor 1.2.1.0.0I
- SQL*Plus Required Support Files 10.1.0.2.0
- SQL*Plus Required Support Files Patch 10.1.0.4.2
- DBJAVA Required Support Files 10.1.0.2.0
- DBJAVA Required Support Files Patch 10.1.0.4.2
- XDK Required Support Files 10.1.0.2.0
- XDK Required Support Files Patch 10.1.0.4.2
- LDAP Required Support Files 10.1.0.2.0
- RDBMS Required Support Files 10.1.0.2.0
- RDBMS Required Support Files Patch 10.1.0.4.2
- Oracle Client Required Support Files 10.1.0.2.0
- Oracle Client Required Support Files Patch 10.1.0.4.2
- Agent Required Support Files 10.1.0.2.0
- Agent Required Support Files Patch 10.1.0.4.2
- SSL Required Support Files for InstantClient 10.1.0.2.0
- SSL Required Support Files for InstantClient Patch 10.1.0.4.2
- SSL Required Support Files 10.1.0.2.0

- SSL Required Support Files Patch 10.1.0.4.2
- Parser Generator Required Support Files 10.1.0.2.0
- Parser Generator Required Support Files Patch 10.1.0.4.2
- Precompiler Required Support Files 10.1.0.2.0
- Precompiler Required Support Files Patch 10.1.0.4.2
- PL/SQL Required Support Files 10.1.0.2.0
- PL/SQL Required Support Files Patch 10.1.0.4.2
- Platform Required Support Files 10.1.0.2.0
- Platform Required Support Files Patch 10.1.0.4.2
- Oracle Core Required Support Files 10.1.0.2.0
- Oracle Core Required Support Files Patch 10.1.0.4.2
- Required Support Files 10.1.0.2.0
- Enterprise Manager plugin Common Files 10.1.0.2.0 Beta
- Enterprise Manager plugin Common Files 10.1.0.4.2
- Assistant Common Files 10.1.0.2.0
- Assistant Common Files Patch 10.1.0.4.2
- Oracle Wallet Manager 10.1.0.2.0
- Oracle Wallet Manager 10.1.0.4.2
- Secure Socket Layer 10.1.0.2.0
- Secure Socket Layer Patch 10.1.0.4.2
- XML Parser for C 10.1.0.2.0
- XML Parser for C Patch 10.1.0.4.2
- Oracle HTTP Server 10.1.2.1.0
- Apache Standalone 10.1.2.1.0
- Web Server Services 10.1.2.0.2

A.2 Evaluated Configuration Boundaries

The evaluated configuration of the TOE shall comprise exactly the following software components:

- Oracle HTTP Server 10.1.2.1.0
- Oracle Process Management Notification 10.1.2.1.0

A.3 Client components

There are no client components in the TOE.

The following is a list of all the components that were installed on the two client machines during the installation of client software for use in testing the TOE in its evaluated configuration.

- Netscape 7.2 (on one machine), and
- Internet Explorer 6 (on the other machine).

ANNEX

B References

[AHSD] *Apache HTTP Server Documentation Version 2.0,*
Apache Software Foundation,
available on the World Wide Web at
www.mirrorservice.org/sites/ftp.apache.org/httpd/docs/httpd-docs-2.0.54.en.pdf.

[CC] *Common Criteria for Information Technology Security Evaluation,*
Version 2.3, August 2005.

[CRP234] *Common Criteria Certification Report No. CRP234*
Oracle HTTP Server 10g Release 2 (10.1.2)
UK IT Evaluation and Certification Scheme, January 2007.

[MSUG] *mod_security Reference Manual v1.8.5,*
26 October 2004,
available on the World Wide Web at
http://web.archive.org/web/20041029030014/www.modsecurity.org/documentation/modsecurity-manual.pdf

[OHSAG] *Oracle HTTP Server Administering a Standalone Deployment Based on Apache 2.0 10g Release 2 (10.1.2),*
Oracle Corporation.

[QUICK] *Oracle Application Server10g: Quick Installation Guide 10g Release 2 (10.1.2) for Solaris Operating System (SPARC),*
Oracle Corporation.

[SRN-8] *Solaris 8 2/02 Security Release Notes, Common Criteria Certification*, Version 0.3, May 21 2003, Sun Microsystems.

[SRN-9] *Solaris 9 8/03 Security Release Notes, Common Criteria Certification*, Version 0.2a, January 11, 2005, Sun Microsystems.

[ST] *Security Target for Oracle HTTP Server 10g Release 2 (10.1.2),* Oracle Corporation**.**