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

January 2007

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

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

January 2007

Authors: Julian Skinner and Peter Goatly.

Contributors: Ann Craig.

Contents

CHAPTER

1 Introduction

This document is the security target for the Common Criteria evaluation of Oracle HTTP Server 10*g* Release 2 (10.1.2).

Identification and CC Conformance

Title: Security Target for Oracle HTTP Server 10*g* Release 2 (10.1.2)

Target of Evaluation (TOE): Oracle HTTP Server (OHS)

Release: 10*g* Release 2 (10.1.2.0.2)

Note that the full name of this release of the product 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 the documentation for this evaluation.

Operating System Platforms: Sun SPARC Solaris 8-2/02
for which [CRP182] is the Common Criteria certification report, and
Sun SPARC Solaris 9 8/03
for which [CR-383-4-26] is the Common Criteria certification report.

CC Conformance:

This Security Target conforms to [CC, Part 2] and [CC, Part 3]. All SFRs in the Security Target are derived from [CC], although some have been extended.

Assurance: EAL4 augmented with ALC_FLR.3[1].

Keywords: Oracle HTTP Server, OHS, security target, EAL4

Version of the Common Criteria [CC] used to produce this document: 2.3

1. ALC_FLR.3 provides assurance at the highest defined component level that there are flaw remediation procedures for the TOE by which discovered security flaws can be reported to, tracked and corrected by the developer, and by which corrective actions can be issued to TOE users in a timely fashion.

TOE Overview

Oracle HTTP Server (OHS) is the web server component of Oracle Application Server. OHS's primary function is to service requests from web users made through the HTTP protocol.

For this evaluation of OHS, the TOE is based on the Apache 2.0 HTTP Server. The TOE consists of the core part of OHS Server and the OHS modules that handle access control, authentication and audit logging, along with the `mod_security` module and `htpasswd`, which is the program for handling the files that hold web users' credentials.

The version of OHS being evaluated is the standalone deployment described in [OHSAG].

TOE Product Components

The Oracle product which constitutes the TOE is Oracle HTTP Server 10*g* Release 2 (10.1.2.0.2).

[ECD] defines how the TOE product must be installed in the evaluated configuration and defines the requirements for setting up the TOE environment.

Document Overview

Chapter 2 of this security target provides a high-level overview of the security features of Oracle HTTP Server. Chapter 3 identifies the assumptions, threats, and security policies of the TOE environment. Chapter 4 describes the security objectives for the TOE and for the environment needed to address the assumptions, threats, and security policies identified in Chapter 3. Chapter 5 identifies the Security Functional Requirements (SFRs), the Security Assurance Requirements (SARs) and the security requirements for the IT environment. Chapter 6 summarises each Security Function (SF) provided by Oracle HTTP Server to meet the security requirements. Chapter 7 covers the topic of protection profile conformance by the TOE and Chapter 8 provides the rationale for the security claims made within this security target.

Annex A contains a list of references, Annex B provides a glossary of the terms and Annex C summarises the relationship of this security target to the draft U.S. Government Protection Profile for Web Servers in Basic Robustness Environments [USWSPP].

Change bars indicate changes since the previous issue.

CHAPTER

2 TOE Description

This chapter describes the product features that provide security mechanisms and contribute to the security of a system using the TOE - Oracle HTTP Server (OHS). The security features of Oracle HTTP Server are explained primarily in [OHSAG, 8]. In general, these descriptions correspond to the specifications of IT security functions provided in Chapter 6 of this document.

The major elements of the OHS security architecture are described below, and the TOE is defined in terms of this architecture. The TOE's mechanisms for access control, identification and authentication, and accountability and auditing are summarised. Additional OHS security features that are not addressed by the security functional requirements of Chapter 5 are also briefly discussed.

OHS Architecture

The OHS architectural components are described in [OHSAG, 1].

HTTP

Hypertext Transfer Protocol (HTTP) is the underlying protocol used by the Web to format and transmit messages and to determine what actions web servers and browsers should take in response to various commands. HTTP is the protocol used between Oracle Application Server and clients.

HTTP messages consist of requests from the client to the server and responses from the server to the client. Each request message specifies the method to be applied to the web resource and the identifier of the resource.

HTTP/1.1 is defined in [RFC2616].

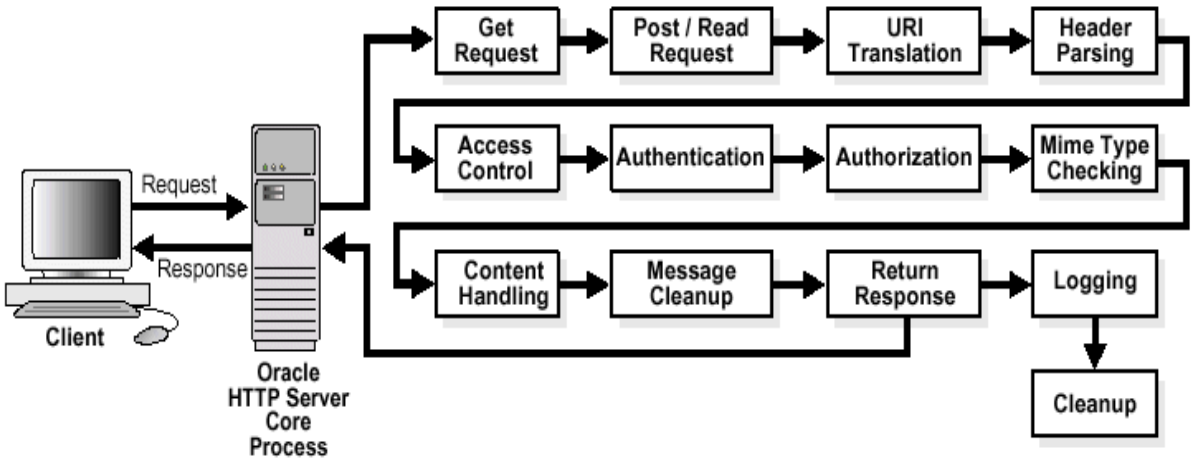
OHS Server

Oracle HTTP Server is the web server component of Oracle Application Server. For this evaluation of OHS, the TOE is based on the Apache 2.0 HTTP Server. Its primary function is to service requests from clients made through the HTTP protocol, although OHS can also be used as a proxy server, both forward and reverse. In addition, OHS allows programmers to develop their website(s) in a variety of programming languages.

OHS consists of the “OHS Core” that implements most of the basic functionality, OHS modules that implement the rest of this basic functionality and modules that provide functionality extensions. Many of the standard Apache modules are provided in OHS, which also includes several modules that are specific to Oracle Application Server components.

The OHS Server implements the steps for handling HTTP requests through its module or plug-in architecture. When requests from the client arrive at the HTTP Listener, they are processed in a sequence of steps determined by server defaults and configuration parameters. The figure below illustrates the steps for handling such requests. In the evaluated configuration for the TOE, the steps labelled "Authentication" and "Authorization" represent the processing of the `mod_auth` module.

Figure 1: Oracle HTTP Server Steps for Handling HTTP Requests



The OHS modules listed in [OHSAG, 7] that, in conjunction with the OHS Core, implement security functionality described in Chapter 6 of this document are:

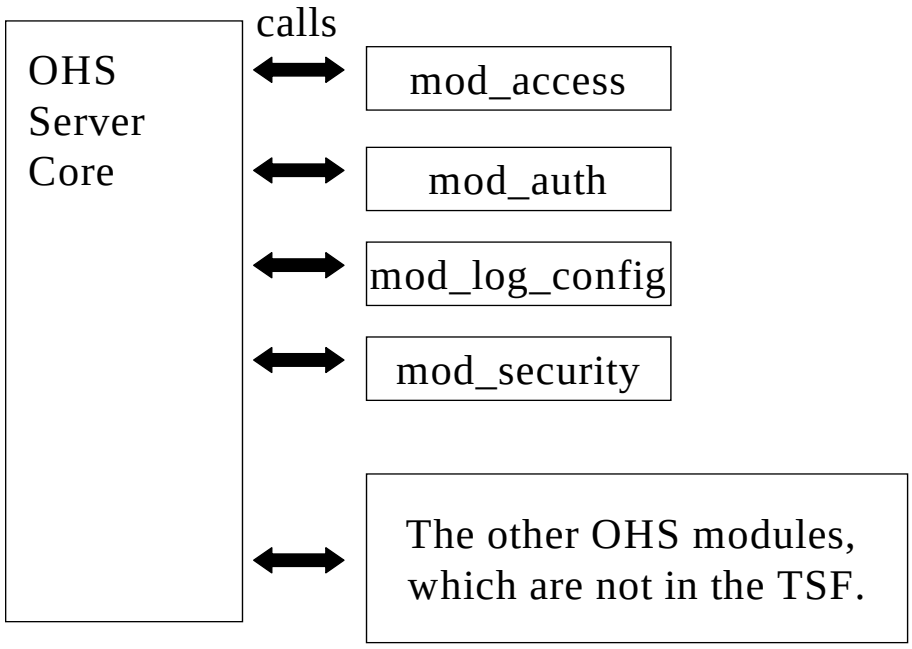
- `mod_access`
  which controls access to web resource based on characteristics of a request such as host name and IP address.
- `mod_auth`
  which implements basic authentication for web users via files-based user lists to control which users can access web resource.
- `mod_log_config`
  which provides configurable, customizable logging of server activities to achieve the TOE’s auditing requirements.

Details of these and the other modules included in OHS are given in [OHSAG, 7], which, where necessary, refers to [AHSD, 10] for further details.

One further module is included in the evaluated configuration for the TOE. This is `mod_security`, which is described in [MSUG]. This module is an open source intrusion detection and prevention engine for web applications. It operates embedded in the web server to shield applications from attacks. [ECD] describes how `mod_security` should be deployed in the evaluated configuration for the TOE.

The figure below illustrates the architecture of the OHS Server. There is a core part of the server that is responsible for receiving HTTP requests via its HTTP Listener and executing the required steps in servicing each request. A number of modules are provided for the core to call to implement the various phases of request handling. This diagram also shows that there is a limited number of modules that are in the TSF for this evaluation of OHS. The other OHS modules listed in [OHSAG, 7] are not involved in implementing the aspects of security that are defined in this document and in [ECD].

Figure 2: Oracle HTTP Server Architecture



httpd

`httpd` is the OHS Server program. It is designed to be run as a standalone daemon process. It creates a pool of child processes or threads to handle HTTP requests.

apachectl

`apachectl` is a front end to the OHS Server. Oracle Process Manager and Notification Server uses it to control the functioning of the `httpd` daemon. The command line interface into `apachectl` which OPMN uses is described in [AHSD, 8.4].

OPMN

In the evaluated configuration for the TOE, Oracle Process Manager and Notification Server (OPMN) is used by web server administrators to start, monitor and stop the OHS Server. The details of the interface to `opmnctl` are given in [OPMNSAG, 2:

opmnctl Detailed Command Description].

htpasswd

htpasswd 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. It is described in [AHSD, 8.10].

HTTP clients

HTTP clients send Hypertext Transfer Protocol requests to OHS's HTTP Listener, which is listening for HTTP messages at its port. Such clients are typically browsers such as Netscape and Internet Explorer operating on behalf of web users.

TOE Definition

The TOE for this evaluation of Oracle HTTP Server is defined to be the OHS Server core and the modules mod_access, mod_auth, mod_log_config and mod_security together with the htpasswd program. The version of OHS being evaluated is the standalone deployment described in [OHSAG], which is based on the source code of version 2.0.52 of the Apache HTTP Server.

The external interfaces into the TOE are:

- the HTTP message interface to the OHS Server via OHS's HTTP Listener; and
- the command line interface to htpasswd.

In the evaluated configuration, Oracle Process Manager and Notification Server (OPMN) is used to start, monitor and stop the OHS Server. opmnctl is the command-line interface through which OPMN is invoked in the TOE's evaluated configuration.

OPMN uses apachectl via its command line interface to control the functioning of the OHS Server.

Access Controls

All web resources hosted by the TOE can have access controls applied to them to restrict user access. Such controls are set through the use of directives in configuration files.

Host-based Access Control

To set host-based access controls, the deny, allow and order directives described in [AHSD, 6.2] are used. These directives can be applied to particular files, directories or URLs using the <File>, <Directory> or <Location> container directives. Examples of the usage of host-based access controls and the directives used can be found in [OHSAG, 8].

HTTP Method Limitations

OHS provides the Limit and LimitExcept directives described in [AHSD, 10.3] to restrict access to web resources based on the method specified in the HTTP request. The method(s) to be restricted are added to the Limit directive or, alternatively, those methods that are to be allowed should be added to the LimitExcept directive. These directives can be used in conjunction with the <File>, <Directory> or <Location> container directives. To ensure the security of the evaluated configuration, [ECD] requires web server administrators to use such directives in conjunction with the deny directive to disallow access by any method other than the GET or HEAD methods. This results in a read-only access control security policy for the TOE

in its evaluated configuration.

Initial Access Control Check

Early on in the request processing cycle, access control is applied based on the user's IP address, host name or other characteristics of the user's request (via the `Allow`, `Deny` and `Order` directives). In the evaluated configuration for the TOE the outcome of this stage in the cycle can be that access is refused or that access checking is passed to the next stage.

Anonymous Access

At this point in processing the request the user is granted access under an anonymous session with OHS if no `Require` directive applies to the web resource requested.

User Identification

In OHS a web user is required to be identified only if access is being requested to a web resource that has a `Require` directive applied to it. In such a case, the `AuthUserFile` and `AuthGroupFile` directives are used to identify the password file and group file to be used for the user identification and authentication processes when determining if the `Require` directive has been satisfied.

Usernames and passwords are stored together in password files by using the `htpasswd` program. Within each password file the username is unique, but a web user can have an entry in more than one password file. Each group file contains a group name followed by a list of the usernames that are members of that group (see [AHSD, 6.2] for a description). Within each group file, each group name must be unique, but a group with a particular name can have an entry in more than one group file.

Authentication

Authentication is the process by which the TOE validates the true identity of the web user making a connection. In OHS there are three different levels of user authentication:

- Anonymous;
- Password-based (Basic authentication); and
- SSL.

SSL based authentication involves the exchange of X.509 certificates. This method of authentication is outside the evaluated configuration of the TOE.

If the requested web resource has a `Require` directive applied to it, then the user must provide a username and password via the user's browser to gain access. The TOE checks the supplied password against the password for that web user stored in the relevant password file. If the passwords match, then authentication has been successful and access to the resource will be granted if the `Require` directive has been satisfied.

Note that when using Basic authentication the password is sent in cleartext over the network. To ensure that no security issues arise from this, [ECD] imposes appropriate constraints on the TOE's network environment. In particular [ECD] will require that no applications, other than those which communicate with the TOE by sending HTTP messages, shall be permitted to run on any client or server host machines which access the network, unless they have been shown not to compromise the TOE's security objectives as stated in [ST]. This restriction prevents the use of a 'password sniffer'.

Web Security Attributes

User Representation

The attributes of a web user that are relevant to the identification and authentication of users by the TOE are:

- username;
- password; and
- group membership.

The IP address and host name of the machine that originated the user's HTTP request are further attributes of the user that may be taken into account when the TOE is mediating access to the requested web resource.

Web Resource Security Attributes

In OHS, directives are included in configuration files to control access to web resource. [AHSD, 2.4] describes the main configuration file, `httpd.conf,` and the distributed configuration file, `.htaccess`.

The directives that are contained in the configuration files include `Directory`, which identifies a directory holding web resource that users can request access to, and `AuthName`, which defines the Realm name for the web resource held in the directory. The `AuthType` directive is always to be set to `Basic` in the evaluated configuration for the TOE. [AHSD, 6.2] describes these directives along with the `Require, AuthUserFile` and `AuthGroupFile` directives.

Auditing

Oracle HTTP Server ensures that relevant audit information about operations performed by web users can be recorded so that the consequences of these operations can later be linked to the user in question, and the user can be held accountable for his or her actions. OHS provides an error log and an access log for recording audit data.

Error Log

As described in [AHSD, 2.7], the server error log, whose name and location is set by the `ErrorLog` directive, is the place where OHS Server sends informational messages (such as OHS Server startup and shutdown messages), diagnostic information, and information on any errors that it encounters in processing requests. The `ErrorLog` directive can be used to specify that error log messages are to be output through a pipe to another process, rather than directly to a file.

Access Log

The server access log records information on all HTTP requests processed by the server (see [AHSD, 2.7]). The location and content of the access log are controlled by the `CustomLog` directive, which can be used to specify that access log messages are to be output directly to a named file or to another process through a pipe. The `LogFormat` directive can be used to simplify the selection of the contents of the logs.

Auditable Events

In the evaluated configuration OHS is configured to log errors and to log all attempts to access web resources.

Audit Records

The access log can be configured to include a variety of attributes in its log record, as

described in [AHSD, 2.7]. The default specified for the evaluated configuration is the Common Log Format (CLF). This includes the following information:

- host ID;
- user ID, if known;
- date/time;
- HTTP request line; and
- HTTP response status.

The format of the error log cannot be configured by the web server administrator. Each error log message includes at least the following information:

- date/time;
- the severity of the error; and
- the message, which indicates the type and outcome of the event.

Audit Analysis

OHS does not provide any tools for the analysis of the error log or access log files, although standard editors can be used to process and display their contents. However, the `ErrorLog` and `CustomLog` directives can be used to specify that log messages are to be output through a pipe to another process, rather than directly to a file. This capability enables a separate system for handling audit records to be implemented and used alongside OHS Server, where this system can incorporate:

- features for selectively storing in an audit trail the log messages piped to it;
- features for handling potential audit trail full conditions; and
- features for analysing and displaying the contents of the audit trail in a way that the web server administrator can customize.

Other Oracle HTTP Server Security Features

In addition to the security features described above, Oracle HTTP Server provides features which are related to security but do not directly address any of the functional requirements identified in this document. These features provide significant security capabilities to support robust and reliable web servers.

The features described below are **not** within the scope of this evaluation.

SSL

OHS can make sure that no data has been modified, deleted, replayed, or disclosed to unauthorized parties during transmission through the use of Secure Sockets Layer (SSL). The use of SSL by OHS for the secure transmission over the network of items such as user credentials for authentication will not be part of the configuration for this evaluation since it is assumed that the server and the clients used to access it are all within a secure network.

mod_oc4j

This OHS module is provided for the use of applications hosted by Oracle Application Server Containers for J2EE. It is not within the scope of this evaluation.

mod_ossl

This OHS module is a plug-in to Oracle HTTP Server that enables the server to use SSL. It is not within the scope of this evaluation.

mod_osso

This OHS module enables single sign-on for OHS users. It is not within the scope of this evaluation.

web applications

OHS can service HTTP requests which result in content being returned to the web user that has been generated dynamically by a web application. The OHS modules which support the use of such applications are within the evaluated configuration defined in [ECD], although the web applications themselves are outside the scope of this evaluation.

CHAPTER

3 Security Environment

This chapter identifies the IT assets protected by the TOE and the operational environment in which there are threats to these IT assets. It also covers the organisational security policies supported by the TOE and the assumptions for secure usage of the TOE.

IT Assets

The IT assets requiring protection consist of the web resources that can be served to web users as a result of HTTP requests received by the OHS Server. The data items used by the TOE in managing the security of the web resources are also to be protected.

The specific IT assets to be protected are:

- *Web resources* which are held in filestore so that the OHS Server can serve them to web users on receipt of suitable HTTP requests.
- *Configuration files* which are held in filestore to provide the directives governing access by web users to web resources.
- *Credential files* which are held in filestore to provide the web users' security attributes.
- *Web server audit data* generated by OHS Server during its operation.

The TOE provides protection for the web resources which it serves to web users, but the operating system underlying the TOE is also required to provide protection for configuration files, credential files and web server audit data.

[AHSD, 2.4] describes the main configuration file, `httpd.conf`, and the distributed configuration file, `.htaccess`. Password files and group files constitute the credential files. They are described in [AHSD, 8.10] and [AHSD, 6.2]. Audit data is put to the error log and the access log, which are described in [AHSD, 2.7].

Operational Environment

In the evaluated configuration defined in [ECD], the TOE executes on an operating system that provides identification and authentication of its users, discretionary access controls on filestore items, process isolation and audit functions. In addition, [ECD] requires the web server administrator to employ physical and procedural controls in a way that provides protection against attacks against the IT assets, the TOE, its underlying system and the network that it is connected to. The requirements for such controls are covered in the Assumptions section below.

Threats

The assumed threats to TOE security, along with the threat agents which might instigate these threats, are specified below. Each threat statement identifies a means by which the TOE and its underlying system might be compromised.

These threats will be countered by:

a) technical security measures provided by the TOE, in conjunction with

b) technical security measures provided by the underlying system, and

c) non-technical operational security measures (personnel, procedural and physical measures) in the environment.

Threat agents

The threat agents are:

- *Outsiders* who are persons that are not authorized users of the system underlying the TOE (operating system and/or network services and/or custom software);
- *Web Users* who are capable of sending HTTP requests to the TOE;
- *System Users* who are persons authorized to use the system underlying the TOE. System users may be:
  a) administrators, or
  b) web resource providers;
- *External Events* which are interruptions to operations arising from failures of hardware, power supplies, storage media, etc.

Threat agents can initiate the types of threats against the IT assets that are listed below.

Threats countered by the TOE

The threats in this section are countered by technical security measures provided by the TOE, supported by technical security measures provided by the underlying system and non-technical operational security measures in the environment.

T.DATA *Unauthorized Access via OHS Server.* A web user obtains unauthorized access to IT assets via an HTTP request sent to the OHS Server.

Note that this threat includes a web user accessing web resource for which they are not authorized by impersonating another web user.

T.ATTACK *Undetected Attack.* An undetected compromise of IT assets occurs as a result of an attacker attempting to perform actions, which the individual is not authorized to perform, via an HTTP

request sent to the OHS Server.

Note that this threat is included because, whatever countermeasures are provided to address the other threats, there is still a residual threat of a violation of the security policy occurring by attackers attempting to defeat these countermeasures (e.g. by attempting to crack a web user's password).

Threats countered only by the Operating Environment

TE.ACCESS *Unauthorized Access to IT Assets.* An outsider or system user obtains unauthorized access to IT assets other that via an HTTP request sent to the OHS Server.

Note that this threat includes a user accessing IT assets for which they are not authorized by impersonating another user who is authorized for such access.

TE.OPERATE *Insecure Operation.* Compromise of IT assets may occur because of improper configuration, administration, and/or operation of the composite system.

TE.CRASH *Abrupt Interruptions.* Abrupt interruptions to the operation of the TOE may cause security related data, such as audit data, to be lost or corrupted. Such interruptions may arise from human error or from failures of software, hardware, power supplies, or storage media.

Note that the security critical parts do not include the processing resources which are covered by A.PHYSICAL below.

Organisational Security Policies

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**.**

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

Assumptions

The TOE is dependent upon both technical IT and operational aspects of its environment.

TOE Assumptions

A.TOE.CONFIG It is assumed that the TOE is installed, configured, and managed in accordance with its evaluated configuration.

Note that, as stated in OE.INSTALL, [ECD] defines the evaluated configuration in detail. It states requirements for the installation and configuration of the underlying system, describes how to install the TOE from its issue media and specifies actions that must be taken by the administrator to ensure the security of the evaluated configuration. Examples of such actions are the setting of restrictive permissions on operating system files and the generation of strong passwords and their secure communication to users.

Underlying System Assumptions

A.PHYSICAL	The security-critical parts of the TOE and the underlying system (including processing resources and network services) are located within controlled access facilities which prevent unauthorized physical access.
A.SYS.CONFIG	The underlying system (operating system and/or secure network services) is installed, configured, and managed in accordance with its secure configuration documentation.
A.ACCESS	The underlying system is configured such that only the approved group of system users may obtain access to the system.
A.MANAGE	There will be one or more competent individuals 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.
A.PASSWORDS	Users and their passwords are entered and maintained in the appropriate password files by web server administrators. It is assumed that each web user's password is to be chosen to have sufficient strength and is to be securely communicated to the user by the administrator.
A.PR.ACCESS	Web resource providers are to be granted access by web server administrators only to the parts of the system underlying the TOE that are necessary in order that the providers can install and maintain their web resources.
A.PR.TRUST	Web resource providers will not intentionally attempt to violate the TOE security policy or any environmental security policies necessary for the correct operation of the TOE.
A.PR.CONTROL	Web server administrators will ensure that configuration files are set up to control access to web resources appropriately.
A.PEER	Any other IT components with which the TOE communicates are assumed to be under the same management control and operate under the same security policy.

CHAPTER

4 Security Objectives

This chapter describes the security objectives for the TOE and the IT and non-IT security objectives for the TOE's operational environment.

TOE Security Objectives

This section defines the IT security objectives that are to be satisfied by the TOE in combination with the IT security environment. These objectives relate to organisational security policies and threats against IT assets that are described in Chapter 3. Table 5 in chapter 8 correlates the TOE security objectives to each of the threats and security policies, showing that each threat is countered by at least one IT security objective, and that each security policy is satisfied by at least one IT security objective.

O.ACCESS The TOE must prevent the unauthorized access of IT assets via an HTTP request.

O.I&A The TOE must provide the means of identifying and authenticating a user of the TOE by methods that are appropriate for the web resource to which the user is requesting access.

O.AUDIT.GEN The TOE must provide the means of generating records of security relevant events in sufficient detail to help an administrator of the TOE to:

a) detect attempted security violations, or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise; *and*

b) hold individual web users accountable for any actions they perform that are relevant to the security of the TOE.

O.ADMIN The TOE, where necessary in conjunction with the underlying system, must provide functions to enable an au-

thorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized administrators can access such functionality.

Environmental Security Objectives

The following IT security objectives are to be satisfied by the environment in which the TOE is used.

OE.ADMIN The underlying system, in conjunction with the TOE, must provide functions to enable an authorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized administrators can access such functionality.

OE.I&A The underlying system must provide the ability to uniquely identify and authenticate administrators and web resource providers before they can access it.

OE.AUDIT.SYSTEM The underlying system must maintain a protected audit trail so that administrators can use it to detect and investigate security incidents.

OE.BANNER The underlying system must provide a banner that allows the display of restrictions of use, legal agreements and any other appropriate information to which users must consent before proceeding with their session.

OE.FILES The underlying system must provide access control mechanisms by which all of the TOE related files (including executables, run-time libraries, web resource files, configuration files, credential files and web server audit trail files) may be protected from unauthorized access.

OE.SEP The underlying operating system must provide the means to isolate the TOE Security Functions (TSF) and assure that the TSF components cannot be tampered with.

The following non-IT security objectives are to be satisfied by procedural and other measures taken within the TOE's environment.

OE.INSTALL Those responsible for the TOE must ensure that:

a) The TOE is delivered, installed, managed and operated in accordance with the operational documentation of the TOE, and in particular its evaluated configuration as defined in [ECD], and

b) The underlying system is installed and operated in accordance with its operational documentation. If the system components are certified under the Common Criteria, they should be installed and operated in accordance with the appropriate cer-

tification documentation.

Note that [ECD] defines the evaluated configuration of the TOE in detail. It states requirements for the installation and configuration of the underlying system, describes how to install the TOE from its issue media and specifies actions that must be taken by the administrator to ensure the security of the evaluated configuration. Such specified actions may emphasise items already documented in the TOE's administrator guidance documentation or may provide additional instructions to avoid potential security problems that relate to the evaluated configuration.

OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE that are critical to the security policy are protected from physical attack.

OE.AUDITLOG Administrators must ensure that audit facilities are used and managed effectively. These procedures shall apply to the TOE's audit trail and the audit trail for the underlying operating system. In particular:

a) Appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs before audit trail exhaustion to ensure sufficient free space;

b) Audit logs must be inspected on a regular basis and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future;

c) The system clocks must be protected from unauthorized modification (so that the integrity of audit timestamps is not compromised).

OE.RECOVERY Those responsible for the TOE must ensure that procedures are in place to ensure that, after system failure or other discontinuity, recovery without security compromise is obtained.

OE.TRUST.ADM Those responsible for the TOE must ensure that only administrators who are highly trusted have the operating system accounts, privileges and permissions which allow them to:

a) set or alter the configuration directives affecting audit record generation by the TOE;

b) set or alter the configuration of the audit trail maintenance system;

b) modify the contents of the audit trail;

c) create any web user account or modify any web user security attributes;

d) set or alter configuration directives that affect the ability of users to access web resources; or

e) set administrative permissions on files.

OE.TRUST.PROV Administrators must ensure that only web resource providers who are trusted not to intentionally violate the TOE security

policy have the operating system accounts, privileges and permissions which allow them to create, view, modify and delete web resource files that they are responsible for.

OE.AUTHDATA Those responsible for the TOE must ensure that the authentication data for each user account for the TOE and for each user account for the underlying system is held securely and not disclosed to persons not authorized to use that account. In particular:

a) The media on which the authentication data for the underlying operating system is stored shall not be physically removable from the underlying platform by unauthorized users;

b) Users shall not disclose their passwords to other individuals;

c) Usernames for the TOE and their passwords must be entered and maintained in the appropriate password files by web server administrators. As described in [ECD], each user's password is to be chosen to have sufficient strength and is to be securely communicated to the user by the administrator.

OE.MEDIA Those responsible for the TOE must ensure that the confidentiality, integrity and availability of IT assets held on storage media is adequately protected. In particular:

a) The on-line and off-line storage media on which web resources and security related data (such as operating system backups and audit trails) must not be physically removable from the underlying platform by unauthorized users;

b) The on-line and off-line storage media must be properly stored and maintained, and routinely checked to ensure the integrity and availability of the security-related data.

Table 6 in chapter 8 illustrates how each of the above objectives counters a threat, supports a policy, or maps to a secure usage assumption.

CHAPTER

5 IT Security Requirements

TOE Security Functional Requirements

Table 1 below lists the Security Functional Requirements (SFRs) for the TOE included in this Security Target. These TOE SFRs are listed in the order in which they are covered in this chapter and the table gives the section headings of the logical groupings of SFRs. This table identifies which Common Criteria operations (assignment (A), selection (S), refinement (R), and/or iteration (I)) have been applied to each requirement relative to Part 2 of [CC]. The text for such completed operations is highlighted with *ITALICISED CAPITAL LETTERS* within each requirement. SFRs that are extended relative to Part 2 of [CC] are indicated by adding the letter "T" after the component identifier.

The remainder of this section details the TOE SFRs for this Security Target. The functional requirements for the IT Environment to support the TOE SFRs are given in the section below entitled "Support for SFRs". Annex B provides definitions for various terms used in the functional requirements.

Table 1: List of TOE Security Functional Requirements

Element	Name	A	S	R	I
	SFRs under the heading "Web User SFP":				
FDP_ACC.1.1	Subset Access Control	X			
FDP_ACF.1.1	Security Attribute Based Access Control	X			
FDP_ACF.1.2	Security Attribute Based Access Control	X			
FDP_ACF.1.3	Security Attribute Based Access Control	X			
FDP_ACF.1.4	Security Attribute Based Access Control	X			
FMT_MSA.1.1	Management of Security Attributes	X	X		

Element	Name	A	S	R	I
FMT_MSA.3T.1	Management of Security Attributes	X	X	X	
FMT_MSA.3T.2	Management of Security Attributes	X		X	
	SFRs under the heading "Identification and Authentication":				
FIA_UID.1.1	Timing of Identification	X			
FIA_UID.1.2	Timing of Identification				
FIA_UAU.1.1	Timing of Authentication	X			
FIA_UAU.1.2	Timing of Authentication				
FIA_ATD.1.1	User Attribute Definition	X			
FIA_USB.1.1	User-subject Binding	X			
FIA_USB.1.2	User-subject Binding	X			
FIA_USB.1.3	User-subject Binding	X			
	SFRs under the heading "Security Management":				
FMT_REV.1T.1	Revocation	X	X	X	
FMT_REV.1T.2	Revocation	X			
FMT_SMF.1.1	Specification of Management Functions	X			
FMT_SMR.1.1	Security Roles	X			
FMT_SMR.1.2	Security Roles				
	SFRs under the heading "Security Audit":				
FAU_GEN.1.1	Audit Data Generation	X	X	X	
FAU_GEN.1.2	Audit Data Generation	X		X	
FAU_GEN.2.1	User Identity Association			X	

Web User SFP

The TOE SFRs in this section relate to the Web User Security Function Policy. This SFP controls access by web users to content via HTTP requests sent over the network to the TOE's web server.

FDP_ACC.1.1 The TSF shall enforce the *WEB USER SFP* on:

a) *SUBJECTS: PROCESSES ACTING ON BEHALF OF WEB USERS*;

b) *OBJECTS: CONTENT THAT CAN BE REQUESTED BY WEB USERS*; *AND*

c) *OPERATIONS: HTTP METHODS PROVIDING ACCESS TO CONTENT*.

Note that the HTTP methods are listed in [RFC2616, 9], but SFR FDP_ACF.1.2 requires that the TSF must deny the operation unless the HTTP method is GET or HEAD.

FDP_ACF.1.1 The TSF shall enforce the *WEB USER SFP* to objects based on the following:

a) *THE HOST NAME AND HOST ADDRESS OF THE COMPUTER ORIGINATING THE USER'S REQUEST TO ACCESS CONTENT, AND THE USER IDENTITY AND ACCESS CONTROL GROUP MEMBERSHIPS ASSOCIATED WITH THE USER; AND*

b) *THE REALM, CONTENT IDENTIFIER AND ACCESS CONTROL DIRECTIVES THAT APPLY TO THE CONTENT THE USER IS REQUESTING ACCESS TO.*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) *IF THE OPERATION IS NOT AN HTTP GET OR HEAD METHOD THEN THE OPERATION IS DENIED.*

b) *IF THERE ARE HOST-BASED ACCESS DIRECTIVES APPLYING TO THE CONTENT WHICH DENY THE REQUESTED ACCESS BY THE USER, THEN THE OPERATION IS DENIED.*

c) *IF THERE ARE USER-BASED ACCESS DIRECTIVES APPLYING TO THE CONTENT WHICH DENY THE REQUESTED ACCESS BY THE USER, THEN THE OPERATION IS DENIED.*

d) *OTHERWISE THE OPERATION IS ALLOWED.*

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *NONE*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *NONE*.

The FMT_MSA SFRs below cover the TSF's contribution to the management of the security attributes used to enforce the Web User SFP.

FMT_MSA.1.1 The TSF shall enforce the *WEB USER SFP* to restrict the ability to *QUERY, MODIFY, DELETE, CREATE* the security attributes *USER IDENTITY AND AUTHENTICATION DATA* to *WEB SERVER ADMINISTRATORS.*

Note that security requirement for the IT Environment FMT_MSA.1E.1 covers management of the security attributes used to enforce the Web User SFP that are not covered in FMT_MSA.1.1.

FMT_MSA.3T.1 The TSF shall enforce the *WEB USER SFP* to provide *NO* default values for the security attributes *USER IDENTITY AND AUTHENTICATION DATA* that are used to enforce the SFP.

FMT_MSA.3T.2 The TSF shall allow *NO USERS* to specify alternative initial values to override the default values *FOR THE SECURITY ATTRIBUTES USER IDENTITY AND AUTHENTICATION DATA* when an object or information is created.

Note that security requirement for the IT Environment FMT_MSA.3E covers static initialisation of the security attributes used to enforce the Web User SFP that are not covered in FMT_MSA.3T.

Identification and Authentication

The TOE SFRs under class FIA in this Security Target relate to the identification and authentication of web users when the Web User SFP has been invoked to control access by web users to content via HTTP requests. In addition, some FIA SFRs are used to cover the rules for the association of user security attributes with subjects acting on behalf of a user.

FIA_UID.1.1 The TSF shall allow *OPERATIONS ON CONTENT FOR WHICH THERE ARE NO USER-BASED ACCESS DIRECTIVES* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1.1 The TSF shall allow *OPERATIONS ON CONTENT FOR WHICH THERE ARE NO USER-BASED ACCESS DIRECTIVES* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) *HOST NAME OF THE COMPUTER ORIGINATING THE USER'S REQUEST TO ACCESS CONTENT (IF HOST NAME AVAILABILITY HAS BEEN CONFIGURED BY THE ADMINISTRATOR);*
b) *HOST ADDRESS OF THE COMPUTER ORIGINATING THE USER'S REQUEST TO ACCESS CONTENT;*
b) *USER IDENTITY;*
b) *GROUP MEMBERSHIPS;*
c) *USER AUTHENTICATION DATA.*

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user:

a) *THE HOST NAME OF THE COMPUTER ORIGINATING THE USER'S REQUEST TO ACCESS CONTENT (IF HOST NAME AVAILABILITY HAS BEEN CONFIGURED BY THE ADMINISTRATOR);*
b) *HOST ADDRESS OF THE COMPUTER ORIGINATING THE USER'S REQUEST TO ACCESS CONTENT;*
c) *USER IDENTITY;*
d) *GROUP MEMBERSHIPS;*
e) *USER AUTHENTICATION DATA.*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on behalf of users:

a) *AT THE START OF A SESSION WITH THE TSF, THE HOST NAME (IF AVAILABLE) AND HOST ADDRESS OF THE COMPUTER ORIGINATING THE USER'S REQUEST TO ACCESS CONTENT ARE ASSOCIATED WITH EACH SUBJECT ACTING ON BEHALF OF A USER;*
b) *IF THERE ARE USER-BASED ACCESS DIRECTIVES APPLYING TO THE CONTENT THAT THE USER IS REQUESTING TO ACCESS, THEN, PROVIDED THAT THE USER IS A VALID USER FOR THE CONTENT, THE USER*

IDENTITY WILL BE ASSOCIATED WITH EACH SUBJECT ACTING ON BEHALF OF THAT USER;

c) *IF RULE b) APPLIES, THEN THE AUTHENTICATION DATA AND ANY GROUP MEMBERSHIPS FOR THE USER WILL BE ACCESSIBLE TO EACH SUBJECT THAT IS RESPONSIBLE FOR CHECKING THE AUTHENTICATION AND AUTHORIZATION OF THE USER TO ACCESS THE CONTENT.*

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on behalf of users:

a) *ONCE THE VALUE OF A PARTICULAR SECURITY ATTRIBUTE HAS BEEN ASSOCIATED WITH A SUBJECT ACTING ON BEHALF OF A USER, THIS VALUE IS USED FOR THE SECURITY ATTRIBUTE FOR THE REMAINDER OF THE SESSION WITH THE TSF.*

Security Management

The TOE SFRs in this section relate to the general requirements for the TSF to manage the security attributes and security management roles that are under its control. The "Web User SFP" section above covers the specific requirements for the management of the security attributes used to enforce the Web User SFP.

FMT_REV.1T.1 The TSF shall restrict the ability to revoke security attributes *USER IDENTITY AND USER AUTHENTICATION DATA* associated with the *USERS* within the TSC to *WEB SERVER ADMINISTRATORS*.

Note that security requirement for the IT Environment FMT_REV.1E.1 covers revocation of the security attributes used to enforce the Web User SFP that are not covered in FMT_REV.1T.1.

FMT_REV.1T.2 The TSF shall enforce the rules:

a) *THE REVOCATION OF A USER'S USER IDENTITY AND USER AUTHENTICATION DATA BY THE TSF SHALL BE IN EFFECT WHEN THE USER NEXT REQUESTS TO ACCESS CONTENT.*

b) *THE REVOCATION OF A USER'S GROUP MEMBERSHIPS SHALL BE IN EFFECT WHEN THE USER NEXT ATTEMPTS TO ACCESS A CONTENT OBJECT;*

c) *THE REVOCATION OF A CONTENT OBJECT'S SECURITY ATTRIBUTES HELD IN A MAIN CONFIGURATION FILE SHALL BE IN EFFECT WHEN THE WEB SERVER IS NEXT STARTED UP.*

d) *THE REVOCATION OF A CONTENT OBJECT'S SECURITY ATTRIBUTES HELD IN A DISTRIBUTED CONFIGURATION FILE SHALL BE IN EFFECT WHEN A WEB USER NEXT ATTEMPTS TO ACCESS THE CONTENT OBJECT.*

Note that rules FMT_REV.1.2b)-d) relate to attributes whose revocation is covered by security requirement for the IT Environment FMT_REV.1E.1.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a) *MANAGING THE USER IDENTITY;*

b) *MANAGING USER AUTHENTICATION DATA.*

Note that security requirement for the IT Environment FMT_SMF.1E.1 covers management of the security attributes used to enforce the Web User SFP that are not covered in FMT_SMF.1.1.

FMT_SMR.1.1 The TSF shall maintain the roles:

a) *WEB USER*.

Note that security requirement for the IT Environment FMT_SMR.1E.1 covers the security management roles that are not covered in FMT_SMR.1.1.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Security Audit

The TOE SFRs under class FAU in this Security Target relate to the generation of audit data for security relevant TOE events.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions; and

b) *ALL AUDITABLE EVENTS LISTED IN TABLE 2 BELOW*.

Note that the selection operation for the FAU_GEN.1.1 element defined in Section 8.2 of [CC] Part 2 has effectively been completed with "for the *NOT SPECIFIED* level of audit"*. However, a refinement has been applied to omit these words for the sake of clarity*.

Table 2: Required Auditable Events

Component	Event	Additional Data
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP	None
FIA_UAU.1	All use of the authentication mechanism	None
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	None
FIA_USB.1	Success and failure of binding user security attributes to a subject (e.g. success and failure to create a subject)	None

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity *(IF APPLICABLE)*, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST *AND ANY OTHER AUDIT RELEVANT INFORMATION AS IDENTIFIED IN THE THIRD COLUMN OF TABLE 2 ABOVE*.

Note that the wording of FAU_GEN.1.2 includes the refinement "(if applicable)" for the sake of clarity, as per the wording for FAU_GEN.1.2 used in [USWSPP, 5.1.1], which was based on interpretation NIAP-0410.

FAU_GEN.2.1 *FOR AUDIT EVENTS RESULTING FROM ACTIONS OF IDENTIFIED USERS,* the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Note that the wording of FAU_GEN.2.1 includes the refinement "For audit events resulting from actions of identified users," for the sake of clarity, as per the wording for FAU_GEN.1.2 used in [USWSPP, 5.1.1], which was based on interpretation NIAP-0410.

TOE Security Assurance Requirements

The target assurance level is EAL4 as defined in Part 3 of the CC, augmented with ALC_FLR.3.

Security Requirements for the IT Environment

The TOE is a web server which is a software application built on top of an underlying IT platform. This IT platform, which consists of an operating system, network services and other supporting software (collectively referred to as the *system*) is required to provide controlled access services to ensure the secure operation of this application as follows:

- The operating system shall identify and authenticate users prior to providing access to the underlying system.
- The operating system shall provide the discretionary access control mechanisms required to support the TOE and the IT environment in ensuring files can only be accessed by authorized users.
- The operating system shall provide an auditing system to support the TOE and the IT environment by ensuring users can be held accountable for their access to IT assets other than via HTTP requests submitted to the OHS Server.
- The system shall provide backup, restore and other secure recovery mechanisms. Such mechanisms are to be capable of archiving and restoring the web server's audit trail.

Note that an operating system meeting the functional and assurance requirements defined in [CAPP], or equivalent, will meet the above requirements (although conformance to [CAPP] is not a mandatory requirement).

Support for SFRs

The specific functional requirements for the IT Environment which are needed to support the secure functioning of the TOE SFRs defined earlier in this chapter are listed in Table 3. The reasons for using these particular IT environment SFRs are covered in the last paragraph of Annex C. The IT environment SFRs in Table 3 are listed in the order in which they are covered in this chapter and the table gives the section headings of the logical groupings of SFRs. This table identifies which Common Criteria operations (assignment (A), selection (S), refinement (R), and/or iteration (I)) have been applied to the requirement relative to Part 2 of [CC]. The text for such completed operations is highlighted with *ITALICISED CAPITAL LETTERS* within each requirement.

All of the elements covered in this section have been refined relative to Part 2 of [CC]

so that the elements apply to the IT Environment rather than the TOE. Such elements have been distinguished from the SFRs that apply to the TOE by adding the letter “E” after the component identifier.

After Table 3, the remainder of this section gives the details of the SFRs for the IT Environment and indicates the purpose of these SFRs.

Table 3: List of Security Functional Requirements for the IT Environment

Element	Name	A	S	R	I
	SFRs under the heading “Content Provider SFP”:				
FDP_ACC.1E.1	Subset Access Control	X		X	
FDP_ACF.1E.1	Security Attribute Based Access Control	X		X	
FDP_ACF.1E.2	Security Attribute Based Access Control	X		X	
FDP_ACF.1E.3	Security Attribute Based Access Control	X		X	
FDP_ACF.1E.4	Security Attribute Based Access Control	X		X	
	SFRs under the heading “Web User SFP Support”:				
FMT_MSA.1E.1	Management of Security Attributes	X	X	X	
FMT_MSA.3E.1	Static Attribute Initialisation	X	X	X	
FMT_MSA.3E.2	Static Attribute Initialisation	X		X	
	SFRs under the heading “Security Management”:				
FMT_MOF.1E.1	Management of Security Functions Behaviour	X	X	X	
FMT_MTD.1E.1.1	Management of TSF Data	X	X	X	X
FMT_MTD.1E.1.2	Management of TSF Data	X	X	X	X
FMT_REV.1E.1.1	Revocation	X	X	X	X
FMT_REV.1E.1.2	Revocation	X	X	X	X
FMT_SMF.1E.1	Specification of Management Functions	X		X	
FMT_SMR.1E.1	Security Roles	X		X	
FMT_SMR.1E.2	Security Roles			X	
	SFRs under the heading “Security Audit”:				
FAU_SAR.1E.1	Audit Review	X		X	
FAU_SAR.1E.2	Audit Review			X	
FAU_SAR.2E.1	Restricted Audit Review			X	

Element	Name	A	S	R	I
FAU_SAR.3E.1	Selectable Audit Review	X	X	X	
FAU_SEL.1E.1	Selective Audit	X	X	X	
FAU_STG.1E.1	Protected Audit Trail Storage			X	
FAU_STG.1E.2	Protected Audit Trail Storage		X	X	
FAU_STG.3E.1	Action in Case of Possible Audit Data Loss	X		X	
FAU_STG.4E.1	Prevention of Audit Data Loss	X	X	X	
	SFRs under the heading "Protection of the TSF":				
FPT_SEP.1E.1	TSF Domain Separation			X	
FPT_SEP.1E.2	TSF Domain Separation			X	
FPT_STM.1E.1	Reliable Time Stamps			X	
	SFRs under the heading "Sessions with the IT Environment":				
FTA_SSL.1E.1	TSF-Initiated Session Locking	X		X	
FTA_SSL.1E.2	TSF-Initiated Session Locking	X		X	
FTA_SSL.2E.1	User-Initiated Locking			X	
FTA_SSL.2E.2	User-Initiated Locking	X		X	
FTA_SSL.3E.1	TSF-Initiated Termination	X		X	
FTA_TAB.1E.1	Default TOE Access Banners			X	

Content Provider SFP

The SFRs for the IT environment in this section cover the Content Provider Security Function Policy. This SFP controls access by content providers to content via software in the IT environment.

FDP_ACC.1E.1 The *IT ENVIRONMENT* shall enforce the *CONTENT PROVIDER SFP* on:

a) *SUBJECTS: PROCESSES ACTING ON BEHALF OF A CONTENT PROVIDER*;
b) *OBJECTS: CONTENT*; *AND*
c) *OPERATIONS: ALL IT ENVIRONMENT OPERATIONS PROVIDING ACCESS TO CONTENT*.

FDP_ACF.1E.1 The *IT ENVIRONMENT* shall enforce the *CONTENT PROVIDER SFP* to objects based on the following:

a) *THE OPERATING SYSTEM SECURITY ATTRIBUTES ASSOCIATED WITH THE CONTENT PROVIDER'S USERNAME; AND*
b) *THE OPERATING SYSTEM SECURITY ATTRIBUTES OF THE FILES CONSTITUTING THE CONTENT.*

FDP_ACF.1E.2 The *IT ENVIRONMENT* shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) *THE OPERATION IS ALLOWED IF AND ONLY IF THE RULES OF THE OPERATING SYSTEM'S DISCRETIONARY ACCESS CONTROL SFP ALLOW THE USER TO ACCESS THE FILES CONSTITUTING THE CONTENT USING THE REQUESTED FILE ACCESS METHOD.*

Note that the operating system permissions for the files constituting the content and the directories containing such files are to be set by the Web Server Administrator to allow access to them only by the appropriate content provider(s).

FDP_ACF.1E.3 The *IT ENVIRONMENT* shall explicitly authorize access of subjects to objects based on the following additional rules: *NONE.*

FDP_ACF.1E.4 The *IT ENVIRONMENT* shall explicitly deny access of subjects to objects based on the following additional rules: *NONE*.

Web User SFP Support

The FMT_MSA SFRs in this section cover the IT environment's contribution to the management of the security attributes used to enforce the Web User SFP.

FMT_MSA.1E.1 The *IT ENVIRONMENT* shall enforce the *WEB USER SFP* to restrict the ability to *MODIFY, DELETE, CREATE* the security attributes *GROUP MEMBERSHIPS, AND REALM, CONTENT IDENTIFIER AND ACCESS CONTROL DIRECTIVES FOR CONTENT OBJECTS* to *WEB SERVER ADMINISTRATORS.*

Note that FMT_MSA.1.1 and FMT_MSA.1E.1 together define the Web User SFP requirements for management of the security attributes used to enforce the SFP.

Note also that group memberships and access control directives are defined by the contents of associated operating system files. Changes to such files are under the control of the operating system's Discretionary Access Control SFP. The operating system permissions for the files are to be set to allow access to them only by the Web Server Administrator.

FMT_MSA.3E.1 The *IT ENVIRONMENT* shall enforce the *WEB USER SFP* to provide *NO* default values for security attributes *GROUP MEMBERSHIPS, REALM, CONTENT IDENTIFIER AND ACCESS CONTROL DIRECTIVES* that are used to enforce the SFP.

FMT_MSA.3E.2 The *IT ENVIRONMENT* shall allow *NO USERS* to specify alternative initial values to override the default values *FOR SECURITY ATTRIBUTES GROUP MEMBERSHIPS, REALM, CONTENT IDENTIFIER AND ACCESS CONTROL DIRECTIVES* when an object or information is created.

Note that FMT_MSA.3T.1, FMT_MSA.3T.2, FMT_MSA.3E.1 and FMT_MSA.3E.2 together define the Web User SFP requirements for static initialisation of the security attributes used to enforce the SFP.

Security Management

The SFRs for the IT environment in this section cover the management of the audit functions and the audit trail and the general management of the security attributes and security roles that are under the control of the IT environment.

FMT_MOF.1E.1 The *IT ENVIRONMENT* shall restrict the ability to *DISABLE, ENABLE AND MODIFY THE BEHAVIOUR OF* the *TOE AUDIT* functions to *THE WEB SERVER ADMINISTRATOR.*

Note that the behaviour of the TOE audit functions is defined by the relevant TOE configuration file(s). Changes to such files are under the control of the operating system's Discretionary Access Control SFP. The operating system permissions for the files are to be set to allow access to them only by the Web Server Administrator.

FMT_MTD.1E.1.1 The *IT ENVIRONMENT* shall restrict the ability to *QUERY, CLEAR* the *AUDIT TRAIL* to *WEB SERVER ADMINISTRATORS.*

Note that the audit trail is to be held in one or more files. Access to such files is under the control of the operating system's Discretionary Access Control SFP. The operating system permissions for the files are to be set to allow access to them only by the Web Server Administrator.

FMT_MTD.1E.1.2 The *IT ENVIRONMENT* shall restrict the ability to *QUERY, MODIFY* the *SET OF AUDITED EVENTS* to *WEB SERVER ADMINISTRATORS.*

Note that the set of audited events is to be defined in a relevant IT environment configuration file. Changes to such a file is under the control of the operating system's Discretionary Access Control SFP. The operating system permissions for the file are to be set to allow access to it only by the Web Server Administrator.

FMT_REV.1E.1.1 The *IT ENVIRONMENT* shall restrict the ability to revoke the security attribute *GROUP MEMBERSHIPS* associated with the *WEB USERS* within the TSC to *WEB SERVER ADMINISTRATORS*.

FMT_REV.1E.1.2 The *IT ENVIRONMENT* shall restrict the ability to revoke the security attributes *REALM, CONTENT IDENTIFIER AND ACCESS CONTROL DIRECTIVES* associated with the *CONTENT* within the TSC to *WEB SERVER ADMINISTRATORS*.

Note that FMT_REV.1T.1, FMT_REV.1E.1.1, FMT_REV.1E.1.2 and FMT_REV.1T.2 together define the Web User SFP requirements for the revocation of the security attributes used to enforce the SFP.

Note also that group memberships and access control directives are defined by the contents of associated operating system files. Changes to such files are under the control of the operating system's Discretionary Access Control SFP. The operating system permissions for the files are to be set to allow access to them only by the Web Server Administrator.

FMT_SMF.1E.1 The *IT ENVIRONMENT* shall be capable of performing the following security management functions:

a) *DISABLE, ENABLE AND MODIFY THE BEHAVIOUR OF THE TOE AUDIT FUNCTIONS;*

b) *MODIFY, DELETE, CREATE WEB USER GROUP MEMBERSHIPS AND REALM, CONTENT IDENTIFIER AND ACCESS CONTROL DIRECTIVES FOR CONTENT OBJECTS;*

c) *QUERY, CLEAR* the *AUDIT TRAIL;*

d) *QUERY, MODIFY* the *SET OF AUDITED EVENTS.*

Note that FMT_SMF.1.1 and FMT_SMF.1E.1 together define the requirements for the security management functions.

FMT_SMR.1.E.1 The *IT ENVIRONMENT* shall maintain the roles:

a) *WEB SERVER ADMINISTRATOR*;

b) *CONTENT PROVIDER*.

FMT_SMR.1E.2 The *IT ENVIRONMENT* shall be able to associate users with roles.

Note that FMT_SMR.1.1, FMT_SMR.1E.1, FMT_SMR.1.2 and FMT_SMR.1E.2 together define the requirements for the maintenance of security roles.

Security Audit

The TOE SFRs under class FAU in this Security Target relate only to the generation of audit data for security relevant TOE events. The SFRs for the IT environment in this section cover the capability to selectively record audit data, to review audit data, and to create and maintain an audit trail.

FAU_SAR.1E.1 The *IT ENVIRONMENT* shall provide *WEB SERVER ADMINISTRATORS* with the capability to read *ALL AUDIT INFORMATION* from the audit records.

FAU_SAR.1E.2 The *IT ENVIRONMENT* shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2E.1 The *IT ENVIRONMENT* shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3E.1 The *IT ENVIRONMENT* shall provide the ability to perform *SEARCHES* of audit data based on *THE VALUES OF AUDIT DATA ATTRIBUTES*.

FAU_SEL.1E.1 The *IT ENVIRONMENT* shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) *USER IDENTITY*;
b) *HOST IDENTITY*;
c) *EVENT TYPE*;
d) *SUCCESS OF EVENT*;
e) *FAILURE OF EVENT*.

FAU_STG.1E.1 The *IT ENVIRONMENT* shall protect the stored audit records from unauthorized deletion.

FAU_STG.1E.2 The *IT ENVIRONMENT* shall be able to *PREVENT* unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.3E.1 The *IT ENVIRONMENT* shall *IMMEDIATELY ALERT THE WEB SERVER ADMINISTRATOR BY DISPLAYING A MESSAGE AT THE LOCAL CONSOLE* if the audit trail exceeds *A PERCENTAGE OF STORAGE CAPACITY THAT IS SET BY THE WEB SERVER ADMINISTRATOR*.

FAU_STG.4E.1 The *IT ENVIRONMENT* shall *OVERWRITE THE OLDEST STORED AUDIT RECORDS* if the audit trail is full.

Note that the assignment operation for the FAU_STG.4.1 element defined in Section 8.6 of [CC] Part 2 has effectively been completed with "and NO OTHER ACTIONS". However, a refinement has been applied to omit these words for the sake of clarity.

Protection of the TSF

The SFRs for the IT environment under class FPT cover requirements for the protection of the TSF and the provision of reliable time stamps for use in audit records.

FPT_SEP.1E.1 The *IT ENVIRONMENT* shall maintain a security domain *FOR THE TSC* that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1E.2 The *IT ENVIRONMENT* shall enforce separation between the security domains of subjects in the TSC *AND THE SECURITY DOMAINS OF UNTRUSTED APPLICATIONS*.

FPT_STM.1E.1 The *IT ENVIRONMENT* shall be able to provide reliable time stamps for *USE BY THE TSF*.

Sessions with the IT Environment

The SFRs for the IT environment under class FTA cover requirements for controlling sessions with the IT environment.

FTA_SSL.1E.1 The *IT ENVIRONMENT* shall lock an interactive session after *A TIME PERIOD OF USER INACTIVITY SPECIFIED BY THE WEB SERVICE ADMINISTRATOR* by:

a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1E.2 The *IT ENVIRONMENT* shall require the following events to occur prior to unlocking the session: *REAUTHENTICATION BY THE USER ASSOCIATED WITH THE SESSION*.

FTA_SSL.2E.1 The *IT ENVIRONMENT* shall allow user-initiated locking of the user's own interactive session, by:

a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2E.2 The *IT ENVIRONMENT* shall require the following events to occur prior to unlocking the session: *REAUTHENTICATION BY THE USER ASSOCIATED WITH THE SESSION*.

Note that the local interactive sessions with the server machine covered by the above FTA_SSL.1E AND FTA_SSL.2E SFRs are for Web Server Administrators only. Content providers and Web Server Administrators connecting to the server machine for remote interactive sessions in the evaluated configuration are covered by SFR FTA_SSL.3E as follows:

FTA_SSL.3E.1 The *IT ENVIRONMENT* shall terminate a *REMOTE* interactive session after *A TIME PERIOD OF USER INACTIVITY SPECIFIED BY THE WEB SERVICE ADMINISTRATOR*.

FTA_TAB.1E.1 Before establishing a user session, the *IT ENVIRONMENT* shall display an advisory warning message regarding unauthorized use of the *SYSTEM*.

Minimum Strength of Function

The minimum strength of function for the TOE is *SOF-Medium*.

This Page Intentionally Blank

CHAPTER

6 TOE Summary Specification

TOE Security Functionality

This section contains a high-level specification of each Security Function (SF) of the TOE that contributes to satisfaction of the TOE Security Functional Requirements of chapter 5. The specifications cover three major areas: Web Security Attributes, Web Resource Access Control and Auditing.

Table 10 in chapter 8 shows that all the TOE SFRs are satisfied by at least one SF and that every SF is used to satisfy at least one TOE SFR (but note that SFRs FDP_ACF.1.3 and FDP_ACF.1.4 are not explicitly satisfied by any particular SF because these SFRs specify null functionality).

Web Resource Access Control

WAC.HOST If a web user requests access to a web resource that is associated with host-based access directives that deny access from the host name or IP address of the machine from which the web user is requesting access, then the request will be denied

WAC.GET If a web user requests access to web resources using any HTTP method other than 'GET' or 'HEAD', then the request will be denied.

Note that the HTTP methods are defined in [RFC2616, 9].

WAC.ASESS Provided that the request is not denied by WAC.HOST or WAC.GET, then if a web user requests access to a web resource for which there is no 'Require' directive then the web server will create an anonymous session for the web user to access that web resource.

Note that [ECD] instructs administrators not to use the 'Satisfy Any' directive. This ensures that any 'Require' directive must still be satisfied if access to a web resource is to be granted, even if access is allowed by a host-based directive.

WAC.USESS Provided that the request is not denied by WAC.HOST or WAC.GET, if a web user requests access to a web resource for which there is a 'Require' directive and Basic Authentication is specified, then if:

a) the web user provides a username for a user that satisfies the 'Require' directive; and

b) the web user provides a password which corresponds to the password stored for that user in the password file associated with the web resource;

then the web server will create a session for the web user to access that web resource.

Note that checking whether the user satisfies the 'Require' directive may involve accessing relevant group files to find out if the user is a member of any groups mentioned in the directive.

Web Security Attributes

WSA.PWDM Password files can be created and the usernames and passwords within them can be created, viewed, modified and deleted via the `htpasswd` facility, but only by Web Server Administrators. Users of the `htpasswd` facility must supply specific values when creating usernames and passwords because no default values are supplied.

Note that, in the evaluated configuration, Web Server Administrators will be required to create strong passwords and distribute them securely to web users, and appropriate operating system access permissions are to be set on password files so that only Web Server Administrators can access them.

WSA.PWD A password file can be associated with web resources.

Note that more than one password file can be in use by an instance of Oracle HTTP Server. Each such file would apply to different web resources. Within each password file each username is unique.

WSA.GROUP Group files contain a group name followed by a list of the usernames within that group. A group file can contain more than one named group. A group file can be associated with web resources.

Note that password files and group files are associated with web resources via the main configuration file (`httpd.conf`) and distributed configuration files (`.htaccess`), as described in [AHSD, 2.4].
In the evaluated configuration, only Web Server Administrators can maintain group files and the group names they contain. This is achieved by the Web Server Administrator setting appropriate operating system access permissions on these files.

WSA.ADDR When a web user requests to access a web resource, the web server can obtain the IP address and /or host name of the web user's machine from the HTTP request message.

Note that the format of an HTTP request is defined in [RFC2616, 5]. The availability of the host name will depend on whether the `HostnameLookup` directive has been used.

WSA.UEFF The security attributes for a web user requesting access to a web resource are the IP address and/or host name of the web user's machine and, where relevant, the username, the user's password and the groups that the user is a member of.
A web user security attribute will be effective in a user's session with the web server only if the user had that attribute at the start of the session.

Note that SFs WAC.ASESS and WAC.USESS describe the conditions under which the web server will start sessions for web resource access for which the user is anonymous or for which the user is identified.

WSA.REFF The security attributes of a web resource are the name of its realm, its file system identifier and a set of access directives. Such attributes are associated with the web resource via a configuration file.
A web resource's security attributes will be effective in a web user's session with the web server only if the configuration file held that attribute:

a) at the start of the web user's session, in the case of a distributed configuration file (`.htaccess`); or

b) when the web server was last started up, in the case of the main configuration file (`httpd.conf`).

Note that [OHSAG,8] describes how configuration files are used for Oracle HTTP Server.

Audit and Accountability

AUD.SUSD The web server can be configured to output an audit record when it is started up or shut down. This audit record includes the following information:

date and time of event; type of event; outcome of event.

Note that auditing begins when the web server is started up and ends when the web server is closed down. Web server startup and shutdown are audited in the error log for Oracle HTTP Server. The error log is configured as described in [AHSD, 2.7].

Note also that auditing to the error log can cause records to be written to a log file or to be passed to a program. The method by which this can be configured is described in [AHSD, 2.7: Piped Logs].

AUD.ACC The web server can be configured to output an audit record for every occurrence of a web user attempting to access a web resource. This audit record includes the following information:

IP address of the user; username (if it is known); date and time of event; HTTP request line; HTTP response code.

Note that attempts to access web resources are audited in the access log for Oracle HTTP Server, which is configured as described in [AHSD, 2.7]. If a web user requests access to a web resource for which there is a 'Require' directive, then the user will need to be identified and authenticated before the web server will start a session for the user to access the resource. Under such circumstances, the audit record will include the user's username and the HTTP response code (which is defined in [RFC2616, 6.1.1]) will indicate the outcome of the identification and authentication process.

Note also that auditing to the access log can cause records to be written to a log file or to be passed to a program. The method by which this can be configured is described in [AHSD, 2.7: Piped Logs].

Security Mechanisms and Techniques

A password is used for authentication of web users in the evaluated configuration (for which Basic Authentication is mandatory). The TOE encrypts passwords prior to storing them in the password file. The TOE password management functions (together called the PWD mechanism), when combined with the instructions to Web Server Administrators in [ECD] to choose strong passwords and to distribute them securely to web users, provide a Strength of Function level of *SOF-medium*.

Specific SFs supporting the claimed SOF are:

- WAC.USESS (SOF-Medium); *and*
- WAC.PWDM, which supports WAC.USESS by providing password management facilities.

Assurance Measures

The target assurance level is EAL4 augmented with ALC_FLR.3. The following table indicates the documentation that will be supplied to support each security assurance requirement for EAL4 and also the assurance requirement for ALC_FLR.3. No other specific assurance measures are claimed.

Table 4: TOE Assurance Measures

Component	Name	Documents
ACM_AUT.1	Partial CM Automation	Document(s) describing the TOE's configuration management will be provided.
ACM_CAP.4	Generation Support and Acceptance Procs	Document(s) describing the TOE's configuration management will be provided.
ACM_SCP.2	Problem Tracking CM Coverage	Document(s) describing the TOE's configuration management will be provided.
ADO_DEL.2	Detection of Modification	Document(s) describing the TOE's delivery procedures will be provided.
ADO_IGS.1	Installation, Generation, and Startup	Document(s) describing the TOE's installation and configuration will be provided.
ADV_FSP.2	Fully Defined External Interfaces	Document(s) covering the TOE's external interfaces will be provided.
ADV_HLD.2	Security Enforcing High-level Design	Document(s) describing the TOE's high level design will be provided.
ADV_IMP.1	Subset of the TSF Implementation	All of the TOE's source code will be provided.
ADV_LLD.1	Descriptive Low-level Design	Document(s) describing the TOE's low level design will be provided.

Table 4: TOE Assurance Measures

Component	Name	Documents
ADV_RCR.1	Informal Correspondence Demonstration	A demonstration of correspondence will be provided within the design documentation.
ADV_SPM.1	Informal TOE Security Policy Model	A document describing the TOE's Security Policy Model will be provided.
AGD_ADM.1	Administrator Guidance	Administrator guidance document(s) will be provided.
AGD_USR.1	User Guidance	User guidance document(s) will be provided.
ALC_DVS.1	Identification of Security Measures	Document(s) covering the security of the TOE's development environment will be provided.
ALC_LCD.1	Developer Defined Life Cycle Model	Document(s) covering the TOE's life cycle model will be provided.
ALC_TAT.1	Well Defined Development Tools	Document(s) covering the TOE's development tools will be provided.
ATE_COV.2	Analysis of Coverage	Document(s) describing the TOE's developer testing will be provided.
ATE_DPT.1	Testing - High-level Design	Document(s) describing the TOE's developer testing will be provided.
ATE_FUN.1	Functional Testing	Document(s) describing the TOE's developer testing will be provided.
AVA_MSU.2	Validation of Analysis	Document(s) providing guidance analysis for the TOE will be provided.
AVA_SOF.1	Strength of TOE Security Functions	Document(s) analysing the strength of the TOE security functions will be provided.
AVA_VLA.2	Independent Vulnerability Analysis	Document(s) providing vulnerability analysis for the TOE will be provided.
ALC_FLR.3	Systematic Flaw Remediation	Document(s) covering the flaw remediation procedures will be provided.

This Page Intentionally Blank

CHAPTER

7

Protection Profile Claims

PP Reference

This security target does not make any claims about Protection Profile conformance.

This Page Intentionally Blank

CHAPTER

8 Rationale

Security Objectives Rationale

This section demonstrates how the identified security objectives are suitable to counter the identified threats and meet the stated organisational security policies.

The threats for the TOE, the organisational security policies and the secure usage assumptions are stated in Chapter 3. The TOE security objectives and the environmental security objectives are stated in Chapter 4.

The table below covers those threats countered by the TOE and the security policies addressed by the TOE, showing that a threat is countered by at least one TOE security objective, and that each security policy is satisfied by at least one TOE security objective. This table does not cover threats and policies addressed purely by the environment. A *YES* in the table indicates that the identified TOE security objective is relevant to the identified threat or security policy.

Table 5: Correlation of Threats and Policies to TOE Security Objectives

Threat/ Policy	O.I&A	O.ACCESS	O.AUDIT. GEN	O.ADMIN
T.DATA	YES	YES		YES
T.ATTACK	YES		YES	
P.ACCOUNT	YES		YES	

The following table illustrates how each of the environmental security objectives counters a threat, supports a policy or maps to a secure usage assumption.

Table 6: Mapping of Environmental Security Objectives to Threats, Policy, and Secure Usage Assumptions

Environmental Objective	Counters Threat	Supports Policy	Maps to Secure Usage Assumptions
OE.INSTALL	TE.OPERATE		A.TOE.CONFIG, A.SYS.CONFIG, A.MANAGE, A.ACCESS, A.PEER
OE.PHYSICAL			A.PEER, A.PHYSICAL
OE.AUDITLOG	T.ATTACK		A.MANAGE
OE.RECOVERY	TE.CRASH		A.MANAGE
OE.TRUST.ADM	TE.ACCESS		A.MANAGE, A.ACCESS
OE.TRUST.PROV	TE.ACCESS		A.ACCESS, A.PROVIDER
OE.AUTHDATA	T.DATA		A.MANAGE, A.ACCESS
OE.MEDIA	TE.CRASH		A.MANAGE
OE.ADMIN	T.DATA, T.ATTACK, TE.ACCESS		A.MANAGE, A.ACCESS
OE.I&A	TE.ACCESS		
OE.AUDIT.SYSTEM	T.ATTACK	P.ACCOUNT	
OE.BANNER		P.BANNER	
OE.FILES	T.DATA, T.ATTACK, TE.ACCESS		A.MANAGE
OE.SEP	T.DATA, T.ATTACK	P.ACCOUNT	A.MANAGE

T.DATA Rationale

T.DATA (*Unauthorized Access via OHS Server)* is directly countered by O.ACCESS, which ensures access to IT assets via HTTP requests is controlled. O.I&A gives support by providing the means of identifying the web user attempting to access an IT asset so that access controls can be based on the user's identity. O.ADMIN and OE.ADMIN provide support by controlling access to configuration and credential files by TOE management functions that might otherwise enable circumvention of access controls. OE.FILES prevents unauthorized users gaining direct access to configuration and credential files to enable the circumvention of access controls on HTTP requests. OE.AUTHDATA ensures that authentication data is held securely to stop it being used by unauthorised users to authenticate to the TOE. OE.SEP prevents TSF components being tampered with and ensures the isolation of web user sessions that could otherwise result in unauthorized access to IT assets.

T.ATTACK Rationale

T.ATTACK (*Undetected Attack)* is countered directly by O.AUDIT.GEN and OE.AUDIT.SYSTEM which ensure the TOE has the means of recording security relevant events which could be indicative of an attack aimed at defeating the TOE security features. O.I&A provides support by allowing audit records to include

data identifying the user in a way which is appropriate to the web resource being accessed. OE.ADMIN provides support by controlling access to audit directives in configuration files, which only administrators must be allowed to view and modify. OE.FILES provides support by preventing users gaining direct access to audit trail files to modify or remove evidence of an attack. OE.AUDITLOG ensures audit data is correctly managed by the administrator so that it can be used to detect attacks. OE.SEP prevents TSF components being tampered with and ensures the isolation of web user sessions that could otherwise result in attacks on TOE security features being undetected.

P.ACCOUNT Rationale

P.ACCOUNT is satisfied by by O.AUDIT.GEN and OE.AUDIT.SYSTEM which ensures the TOE has the means of recording and accessing audit records that identify web users performing security-relevant actions. O.I&A provides support by allowing audit records to include data identifying the user in a way which is appropriate to the web resource being accessed. OE.SEP prevents TSF components being tampered with and ensures the isolation of web user sessions that could otherwise result in users' security-relevant actions not being recorded.

P.BANNER Rationale

P.BANNER is satisfied by OE.BANNER, which ensures that the underlying system provides an appropriate banner feature. This is essential in many environments, for example in UK Ministry of Defence systems and systems operated by US Federal Government departments.

TE.ACCESS Rationale

TE.ACCESS (*Unauthorized Access to IT Assets)* is directly countered by OE.FILES, which prevents unauthorized users gaining direct access to web resource files, configuration files, credential files and audit trail files. OE.I&A gives support by providing the means of identifying the system user attempting to access an IT asset so that file access controls can be based on the user's identity. OE.ADMIN provides support by controlling access to IT assets by TOE management functions that might otherwise enable circumvention of access controls. OE.TRUST.ADM and OE.TRUST.PROV ensure that file permissions and Access Control Lists on IT asset files are set appropriately to prevent system users gaining unauthorized access.

TE.OPERATE Rationale

TE.OPERATE (*Insecure Operation)* is countered directly by OE.INSTALL, which ensures that the TOE and its underlying platform are correctly installed, managed and operated.

TE.CRASH Rationale

TE.CRASH (*Abrupt Interruptions)* is countered by OE.MEDIA and OE.RECOVERY. These ensure that suitable recovery mechanisms are in place to recover from a crash and that the media used during the crash recovery is able to maintain the confidentiality, integrity and availability of the TOE.

Assumptions Rationale

This section demonstrates how the non-IT security objectives map to the TOE secure usage assumptions.

A.TOE.CONFIG is directly provided by OE.INSTALL part a) because [ECD] defines the evaluated configuration of the TOE.

A.SYS.CONFIG is directly provided by OE.INSTALL part b).

A.PHYSICAL is directly provided by OE.PHYSICAL.

A.ACCESS is provided by OE.INSTALL, OE.TRUST.ADM, OE.TRUST.PROV,

OE.AUTHDATA, and OE.ADMIN.

A.MANAGE is provided by OE.TRUST.ADM, supported by OE.INSTALL, OE.AUDITLOG, OE.AUTHDATA, OE.MEDIA, OE.ADMIN, OE.FILES, OE.RECOVERY and OE.SEP.

A.PROVIDER is provided by OE.TRUST.PROV.

A.PEER is provided by OE.PHYSICAL and OE.INSTALL. Since connected systems will require a physical connection to the TOE to be established they fall into the scope of OE.PHYSICAL.

Security Requirements Rationale

Suitability of TOE Security Requirements

The table below correlates the IT security objectives to the SFRs which satisfy them (as indicated by a *YES*), showing that each IT security objective is satisfied by at least one SFR, and that each SFR satisfies at least one IT security objective.

Table 7: Correlation of TOE Security Objectives to Security Functional Requirements

Requirement	O.I&A	O.ACCESS	O.AUDIT.GEN	O.ADMIN
FDP_ACC.1		YES		
FDP_ACF.1		YES		
FMT_MSA.1	YES	YES		YES
FMT_MSA.3T	YES	YES		YES
FIA_UID.1	YES	YES		
FIA_UAU.1	YES			
FIA_ATD.1	YES	YES	YES	
FIA_USB.1		YES		
FMT_REV.1T	YES	YES		YES
FMT_SMF.1	YES	YES		YES
FMT_SMR.1		YES		YES
FAU_GEN.1			YES	
FAU_GEN.2			YES	

O.I&A Suitability

O.I&A is directly provided by FIA_UID.1 and FIA_UAU.1, which provide the means of identifying and authenticating users of the TOE. FIA_ATD.1 provides a set of user attributes for each user while FMT_MSA.1, FMT_MSA.3T, FMT_REV.1T and FMT_SMF.1 specify the TOE's controls over the management of these attributes.

O.ACCESS Suitability

O.ACCESS is directly provided by FDP_ACC.1 which defines the access control policy and FDP_ACF.1 which specifies the access control rules. FMT_REV.1T enforces revocation of security attributes. FIA_ATD.1, FMT_SMR.1 and FIA_USB.1 ensure the TOE maintains the relevant security attributes and role of a web user and that such attributes are associated with subjects created to act on his or her behalf. FIA_UID.1 ensures users are identified prior to any TSF-mediated access actions on content for which there is a user-based access directive. FMT_MSA.1, FMT_MSA.3T and FMT_SMF.1 provide support for the management of security attributes to control access to directory objects.

O.AUDIT.GEN Suitability

O.AUDIT.GEN is directly provided by FAU_GEN.1 which generates audit records for all security relevant events. FAU_GEN.2 supports the enforcement of individual accountability by ensuring the web user responsible for each event can be identified appropriately. FIA_ATD.1 provides for the maintenance of user security attributes whose values can be included in audit records.

O.ADMIN Suitability

O.ADMIN is directly provided by FMT_MSA.1, FMT_MSA.3T, FMT_REV.1T, FMT_SMF.1 and FMT_SMR.1 which specify the TOE's controls over the management of security attributes.

The rationale above demonstrates the suitability of the TOE security requirements.

Suitability of Security Requirements for the IT Environment

The Security Requirements for the IT Environment section of Chapter 5 defines a set of SFRs for the IT environment to support the TOE SFRs. In addition, it provides general requirements for the IT environment to ensure the secure operation of the TOE that are described informally in order not to unduly limit the environments that can satisfy them. These general requirements are together sufficient to meet the following objectives for the IT environment defined in Chapter 4: OE.ADMIN, OE.I&A, OE.AUDIT.SYSTEM, OE.FILES and OE.SEP.

The table below shows how the SFRs for the IT environment are mapped to the security objectives for the IT environment (*YES* indicates where there is a mapping).

Table 8: Mapping of Security Objectives for the IT Environment to SFRs

Requirement	OE. ADMIN	OE.I&A	O.AUDIT. SYSTEM	OE.FILES	OE.SEP	OE. BANNER
FDP_ACC.1E				YES		
FDP_ACF.1E				YES		
FMT_MSA.1E	YES			YES		
FMT_MSA.3E	YES			YES		
FMT_MOF.1E			YES			
FMT_MTD.1E	YES		YES			

Table 8: Mapping of Security Objectives for the IT Environment to SFRs

Requirement	OE. ADMIN	OE.I&A	O.AUDIT. SYSTEM	OE.FILES	OE.SEP	OE. BANNER
FMT_REV.1E	YES			YES		
FMT_SMF.1E	YES		YES	YES		
FMT_SMR.1E	YES					
FAU_SAR.1E			YES			
FAU_SAR.2E			YES			
FAU_SAR.3E			YES			
FAU_SEL.1E			YES			
FAU_STG.1E			YES			
FAU_STG.3E			YES			
FAU_STG.4E			YES			
FPT_SEP.1E					YES	
FPT_STM.1E			YES			
FTA_SSL.1E		YES				
FTA_SSL.2E		YES				
FTA_SSL.3E		YES				
FTA_TAB.1E						YES

The rationale for these mappings is as follows:

- FMT_MSA.1E, FMT_MSA.3E, FMT_MTD.1E, FMT_REV.1E, FMT_SMF.1E and FMT_SMR.1E, which specify the IT environment's controls over the management of the TOE, its security functions and its security attributes, map to OE.ADMIN.
- FTA_SSL.1E, FTA_SSL.2E and FTA_SSL.3E control the operating system session locking features that inhibit the possibility of users taking over sessions, which have been left by administrators and web resource providers, to gain access to IT assets on the web server machine for which they are not authorized. These SFRs map to OE.I&A.
- FMT_MOF.1E, FMT_MTD.1E and FMT_SMF.1E, which relate to management by the IT environment of the audit functions and the audit trail, and FAU_SAR.1E, FAU_SAR.2E, FAU_SAR.3E, FAU_SEL.1E, FAU_STG.1E , FAU_STG.3E and FAU_STG.4E, which provide audit record management functionality, are mapped to OE.AUDIT.SYSTEM. Also mapped to OE.AUDIT.SYSTEM is FPT_STM.1E, which covers the provision by the IT environment of reliable time stamps for inclusion in audit records.
- FDP_ACC.1E, which defines the file access control policy for web resource providers, and FDP_ACF.1E, which specifies the web content file access con-

trol rules, and FMT_MSA.1E, FMT_MSA.3E, FMT_REV.1E, and FMT_SMF.1E, which cover the IT environment's contribution to the management of web users' credential files, all map to OE.FILES.

- FPT_SEP.1E, which covers requirements for the IT environment to provide separation features to protect the TOE, is mapped to OE.SEP.
- OE.BANNER is directly provided by FTA_TAB.1E, which covers requirements for the IT environment to provide a feature by which advisory warning messages can be displayed before a user starts a session with the operating system underlying the TOE.

Dependency Analysis

The table below demonstrates that all dependencies of functional components are satisfied. This analysis covers all TOE SFRs and SFRs for the IT environment.

Table 9: Functional Component Dependency Analysis

Component Reference	Component	Dependencies	Dependency Reference
1	**FDP_ACC.1**	FDP_ACF.1	2
2	**FDP_ACF.1**	FDP_ACC.1 FMT_MSA.3T	1 4
3	**FMT_MSA.1**	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	1 11 10
4	**FMT_MSA.3T**	FMT_MSA.1 FMT_SMR.1	3 11 See Note 1 below
5	**FIA_UID.1**	-	-
6	**FIA_UAU.1**	FIA_UID.1	5
7	**FIA_ATD.1**	-	-
8	**FIA_USB.1**	FIA_ATD.1	7
9	**FMT_REV.1T**	FMT_SMR.1	11 See Note 1 below
10	**FMT_SMF.1**	-	-
11	**FMT_SMR.1**	FIA_UID.1	5
12	**FAU_GEN.1**	FPT_STM.1E	31 See Note 2 below
13	**FAU_GEN.2**	FAU_GEN.1 FIA_UID.1	12 5

Table 9: Functional Component Dependency Analysis

Component Reference	Component	Dependencies	Dependency Reference
14	**FDP_ACC.1E**	FDP_ACF.1E	15 See Note 3 below
15	**FDP_ACF.1E**	FDP_ACC.1E FMT_MSA.3E	14 17
16	**FMT_MSA.1E**	FDP_ACC.1E FMT_SMR.1E FMT_SMF.1E	14 22 21
17	**FMT_MSA.3E**	FMT_MSA.1E FMT_SMR.1E	16 22
18	**FMT_MOF.1E**	FMT_SMR.1E FMT_SMF.1E	22 21
19	**FMT_MTD.1E**	FMT_SMR.1E FMT_SMF.1E	22 21
20	**FMT_REV.1E**	FMT_SMR.1E	22
21	**FMT_SMF.1E**	-	-
22	**FMT_SMR.1E**	(FIA_UID.1)	See Note 4 below
23	**FAU_SAR.1E**	FAU_GEN.1	12 See Note 5 below
24	**FAU_SAR.2E**	FAU_SAR.1E	23
25	**FAU_SAR.3E**	FAU_SAR.1E	23
26	**FAU_SEL.1E**	FAU_GEN.1 FMT_MTD.1E	12 19
27	**FAU_STG.1E**	FAU_GEN.1	12
28	**FAU_STG.3E**	FAU_STG.1E	27
29	**FAU_STG.4E**	FAU_STG.1E	27
30	**FPT_SEP.1E**	-	-
31	**FPT_STM.1E**	-	-
32	**FTA_SSL.1E**	(FIA_UAU.1)	See Note 4 below
33	**FTA_SSL.2E**	(FIA_UAU.1)	See Note 4 below

Table 9: Functional Component Dependency Analysis

Component Reference	Component	Dependencies	Dependency Reference
34	**FTA_SSL.3E**	-	-
35	**FTA_TAB.1E**	-	-

Note 1: The nature of the extensions to SFRs FMT_MSA.3 and FMT_REV.1 does not impact on the dependencies as defined for the CC Part 2 components from which they are derived. The extensions relate to the fact that the TSF only provides the ability to manage some of the security attributes used to enforce the Web User SFP. The security requirements for the TOE FMT_MSA.1, FMT_MSA.3T, FMT_REV.1T, FMT_SMF.1 and FMT_SMR.1 cover the TSF's contribution to the management of the security attributes that are used to enforce the Web User SFP. The security requirements for the IT environment FMT_MSA.1E, FMT_MSA.3E, FMT_MOF.1E, FMT_MTD.1E, FMT_REV.1E, FMT_SMF.1E and FMT_SMR.1E cover the IT environment's contribution to the management of the rest of the security attributes that are used to enforce the Web User SFP.

Note 2: The security requirement for the IT environment FPT_STM.1E.1 satisfies the dependency of the SFR FAU_GEN.1.2 for the provision of reliable time-stamps.

Note 3: The security requirements for the IT environment FDP_ACC.1E and FDP_ACF.1E are included to cover the Content Provider Security Function Policy, which is not provided in the TSF.

Note 4: These dependencies on FIA_UID.1 and FIA_UAU.1 relate to the Identification and Authentication feature of the operating system rather than of the TOE. The requirements for this feature are covered via general requirements for the IT environment to ensure the secure operation of the TOE, which are described informally in the Security Requirements for the IT Environment section of Chapter 5.

Note 5: The security requirements for the IT environment FAU_SAR.1E, FAU_SAR.2E, FAU_SAR.3E, FAU_SEL.1E, FAU_STG.1E, FAU_STG.3E and FAU_STG.4E are included because the TSF only provides the capability to generate audit data. It does not provide the capability to selectively record audit data, to review audit data, or to create and maintain an audit trail.

Dependency analysis of the security assurance requirements

EAL4 is a self-contained assurance package and ALC_FLR.3 has no dependencies on any other component.

Demonstration of Mutual Support

The dependency analysis provided in the table above demonstrates mutual support between functional components, showing that all dependencies required by Part 2 of the CC are satisfied.

The following supportive dependencies exist for the TOE and the IT environment to prevent bypassing of and tampering with the TOE SFRs:

FIA_UID.1 and FIA_UAU.1 together with FIA_ATD.1 and FMT_MSA.1 provide support to all TOE SFRs which rely on the identification of individual web users,

namely: FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_SMR.1, FAU_GEN.1, FAU_GEN.2 and FMT_SMF.1.

FMT_MSA.1 and FMT_MSA.1E provide support to FDP_ACC.1, FDP_ACF.1 and FMT_SMF.1 by controlling the modification of security attributes.

FMT_MSA.3T and FMT_MSA.3E provide support to FDP_ACC.1 and FDP_ACF.1 by ensuring security attributes are explicitly set by administrators and not by default when newly created.

FMT_REV.1 and FMT_REV.1E provide support to FDP_ACC.1 and FDP_ACF.1 by enforcing revocation of security attributes.

FAU_STG.1E, FAU_STG.3E and FAU_STG.4E support FAU_GEN.1 by managing the storage of audit records in the audit trail, and dealing with the audit trail full condition.

FMT_MTD.1E supports FAU_STG.1E, FAU_STG.3E, FAU_STG.4E and FMT_SMF.1E by protecting the integrity of the audit trail.

FAU_SEL.1E supports FAU_STG.1E by providing the means of limiting the events to be audited, thereby ensuring that the administrator can avoid the available space for the audit trail being exhausted except under exceptional circumstances.

FPT_SEP.1E supports FDP_ACC.1 and FDP_ACF.1 by providing separate domains for subject sessions to prevent web users from gaining unauthorized access to other users' data.

FDP_ACC.1E and FDP_ACF.1E support FMT_MTD.1E, FAU_STG.1E and FMT_SMF.1E by preventing unauthorized modifications to the audit trail files. They also support FMT_MSA.1 and FMT_MSA.1E by preventing unauthorized modifications of files containing security attributes.

Strength of Function Validity

The PWD mechanism is the only TOE mechanism that is probabilistic or permutational, and has a strength of SOF-*medium*, which is an appropriate claim for environments that demand EAL4 assurance. A strength of function of SOF-*medium* is intended to provide enough protection against straight forward or intentional attack from threat agents having a moderate attack potential.

Assurance Requirements Appropriate

The target assurance level is EAL4, augmented with ALC_FLR.3. EAL4 is appropriate because the TOE is designed for use within environments where asset owners require up to EAL4 assurance to reduce the risk to those assets to an acceptable level.

ALC_FLR.3 has been included in addition to EAL4 to cause the evaluation of the TOE's flaw remediation procedures which OHS users need to be in place following the release of the TOE. These procedures are required to offer continuing assurance to users that OHS provides secure storage of and access to the data which is crucial to their enterprise's success.

To meet this requirement, the flaw remediation procedures must offer:

- the ability for TOE users to report potential security flaws to Oracle,
- the resolution and correction of any flaws with assurance that the corrections introduce no new security flaws, and
- the timely distribution of corrective actions to users.

ALC_FLR.3 is the ALC_FLR component which is at an appropriate level of rigour to cover these requirements.

TOE Summary Specification Rationale

This section demonstrates that the TOE Security Functions and Assurance Measures are suitable to meet the TOE security requirements.

TOE Security Functions Satisfy Requirements

The table on the next page demonstrates that for each TOE SFR the TOE security functions are suitable to meet the SFR, and the combination of TOE security functions work together so as to satisfy the SFR:

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FDP_ACC.1.1	WAC.HOST WAC.GET WAC.ASESS WAC.USESS	WAC.HOST, WAC.GET, WAC.ASESS and WAC.USESS cover the rules controlling access by a web user to web resource via the web server in response to a method contained in an HTTP request.
FDP_ACF.1.1	WSA.GROUP WSA.ADDR WSA.REFF WAC.HOST WAC.ASESS WAC.USESS	WAC.HOST covers the rule by which access can be denied to the web user on the basis of the host name or IP address of the machine from which the user is requesting access. WAC.ASESS covers the rule by which the user can be granted anonymous access. WAC.USESS covers the rule by which access is permitted if a check on the username and/or group membership(s) for the user is successful. All three of these SFs involve checking the access control directives that apply to the web resource being requested by the user. The file system path name for the web resource and its associated realm are used when looking for the directives that are relevant to the user's request to access the web resource. The applicability of these web resource security attributes to a web user's session are covered in WSA.REFF. WSA.ADDR states that the host name and IP address of the machine from which the user is requesting access can be obtained from the HTTP request. WSA.GROUP states that a group file can be associated with a web resource. This association is used when checking for a user's group membership.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FDP_ACF.1.2	WSA.ADDR WSA.UEFF WSA.REFF WAC.HOST WAC.GET WAC.ASESS WAC.USESS	WAC.GET covers the rule by which access can be denied to the web user if the HTTP method is not GET or HEAD. WAC.HOST covers the rule by which access can be denied to the web user on the basis of the host name or IP address of the machine from which the user is requesting access. WSA.ADDR states how the host name and host address of the computer originating the user's HTTP request are obtained from the HTTP request. If there is a 'Require' directive applying to the web resource, WAC.USESS covers the rule by which access is allowed only if a check on the username and/or group membership(s) shows that the 'Require' directive has been satisfied. WAC.HOST and WAC.USESS involve checking the access control directives that apply to the web resource being requested by the user and may also involve checking the user's security attributes. The applicability of the web resource security attributes and the web user's security attributes to the user's session are covered in WSA.REFF and WSA.UEFF. WAC.ASESS covers the rule by which the user is granted anonymous access if access is not denied via WAC.GET or WAC.HOST and no 'Require' directive applies to the web resource.
FDP_ACF.1.3	N/A	This SFR does not mandate any functionality. It is included for compliance with the CC.
FDP_ACF.1.4	N/A	This SFR does not mandate any functionality. It is included for compliance with the CC.
FMT_MSA.1.1	WSA.PWDM	WSA.PWDM covers creation and access to password files only by administrators.
FMT_MSA.3 T.1	WSA.PWDM	WSA.PWDM states that no default values are provided on creation of usernames and passwords in password files by administrators.
FMT_MSA.3 T.2	WSA.PWDM	WSA.PWDM states that no default values are provided on creation of usernames and passwords in password files by administrators, hence there are no default values to be overridden.
FIA_UID.1.1	WAC.ASESS	WAC.ASESS states that if a web user requests access to a web resource that does not have a 'Require' directive applied to it, then the web server creates an anonymous session for the user to access the web resource.
FIA_UID.1.2	WAC.USESS	WAC.USESS states that if a web user requests access to a web resource that has a 'Require' directive applied to it, then the web server creates a session for the user only after the user has supplied a username that satisfies the 'Require' directive.
FIA_UAU.1.1	WAC.ASESS	WAC.ASESS states that if a web user requests access to a web resource that does not have a 'Require' directive applied to it, then the web server creates an anonymous session for the user to access the web resource.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FIA_UAU.1.2	WAC.USESS WSA.PWD	WAC.USESS states that if a web user requests access to a web resource that has a 'Require' directive applied to it, then the web server creates a session for the user only after the user has supplied a password that corresponds to the password stored for that user in the relevant password file. WSA.PWD states that a web resource can be associated with a password file.
FIA_ATD.1.1	WSA.UEFF	WSA.UEFF lists the user security attributes that can be associated with a user's session with the web server. These correspond to the security attributes listed in the SFR.
FIA_USB.1.1	WSA.PWD WSA.GROUP WSA.ADDR WSA.UEFF	WSA.UEFF lists the user security attributes that can be associated with a user's session with the web server. WSA.ADDR states how the host name and host address of the computer originating the user's HTTP request are obtained for a session. WSA.PWD states that a password file (which holds the username and password) can be associated with a web resource that a user requests to access. WSA.GROUP states that a group file,which lists the names of users that are members of the group, can be associated with a web resource that a user requests to access.
FIA_USB.1.2	WSA.PWD WSA.GROUP WSA.ADDR WSA.REFF WAC.USESS	WSA.ADDR states how the host name and host address of the computer originating the user's HTTP request are obtained from the HTTP request. WSA.PWD states that a password file (which holds the username and password) can be associated with a web resource that a user requests to access. WSA.GROUP states that a group file,which lists the names of users that are members of the group, can be associated with a web resource that a user requests to access. WSA.REFF covers how access directives become effective for a user's session with the web server. WAC.USESS states that, if the web resource requested by the user has a 'Require' directive associated with it, then a sesion is only created for the user if the user provides a username that satisfies the 'Require' directive (which will involve checking if the user is a member of any groups mentioned in the 'Require' directive) and the user provides a password that matches the password stored for the user in the password file associated with the web resource.
FIA_USB.1.3	WSA.UEFF	WSA.UEFF lists the user security attributes that can be associated with a user's session with the web server and states that a web user security attribute will be effective in a user's session with the web server only if the user had that attribute at the start of the session.
FMT_REV.1 T.1	WSA.PWDM	WSA.PWDM states that only administrators can access password files. Hence only they can delete usernames and passwords in order to revoke them.
FMT_REV.1 T.2	WSA.UEFF WSA.REFF	WSA.UEFF and WSA.REFF state the conditions under which the user and web resource security attributes are effective for a user's session and hence when a change to revoke such attributes becomes effective.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FMT_SMF.1.1	WSA.PWDM	WSA.PWDM states that the web user identity and authentication data is managed through the use of the `htpasswd` utility.
FMT_SMR.1.1	WSA.UEFF WAC.ASESS WAC.USESS	The TOE's maintenance of the "web user" role is implicit in SFs WSA.UEFF, WAC.ASESS and WAC.USESS. WAC.ASESS and WAC.USESS cover the circumstances under which the TOE will create a session for a web user. WSA.UEFF defines the web user's security attributes that are applicable for the session.
FMT_SMR.1.2	WSA.ADDR	Users who can send HTTP requests to the web server to attempt to start a session to access a web resource are associated with the web user role. WSA.ADDR states how the host name and host address of the computer originating the user's HTTP request are associated with every such HTTP request.
FAU_GEN.1.1	AUD.SUSD AUD.ACC	AUD.SUSD covers auditing of the start-up and shut-down of the web server, which is when web server auditing is started up and shut down. AUD.ACC covers auditing of access to web resources.
FAU_GEN.1.2	AUD.SUSD AUD.ACC WAC.USESS WSA.UEFF	AUD.SUSD and AUD.ACC describe the information held in the audit records generated. WAC.USESS describes the conditions under which the user is identified for the user's session with the web server to access the web resource requested. WSA.UEFF lists the user security attributes that can be associated with a user's session with the web server, and hence can be included in the audit record.
FAU_GEN.2.1	AUD.ACC WAC.USESS WSA.UEFF	AUD.ACC describes the information held in the audit records to identify the user. WSA.UEFF lists the user security attributes that can be associated with a user's session with the web server, and hence can be included in the audit record. WAC.USESS describes the conditions under which the user is identified for the user's session with the web server to access the web resource requested. The IP address of the machine from which the web user is requesting access, which is one of the user's security attributes, is always included in audit records.

The table below shows that all the SFRs are satisfied by at least one SF and that every SF is used to satisfy at least one SFR (but note that SFRs FDP_ACF.1.3 and FDP_ACF.1.4 are not explicitly satisfied by any particular SF because these SFRs specify null functionality).

Table 11: Mapping of SFs to SFRs

	FDP					FIA								FMT								FAU		
	ACC.1.1	ACF.1.1	ACF.1.2	ACF.1.3	ACF.1.4	UID.1.1	UID.1.2	UAU.1.1	UAU.1.2	ATD.1.1	USB.1.1	USB.1.2	USB.1.3	MSA.1.1	MSA.3T.1	MSA.3T.2	REV.IT.1	REV.IT.2	SME.1.1	SMR.1.1	SMR.1.2	GEN.1.1	GEN.1.2	GEN.2.1
WSA.PWDM														Y	Y	Y	Y		Y					
WSA.PWD									Y		Y	Y												
WSA.GROUP		Y									Y	Y												
WSA.ADDR		Y	Y								Y	Y									Y			
WSA.UEFF			Y							Y	Y		Y					Y		Y			Y	Y
WSA.REFF		Y	Y									Y						Y						
WAC.HOST	Y	Y	Y																					
WAC.GET	Y		Y																					
WAC.ASESS	Y	Y	Y			Y		Y												Y				
WAC.USESS	Y	Y	Y				Y		Y			Y								Y			Y	Y
AUD.SUSD																						Y	Y	
AUD.ACC																						Y	Y	Y

Assurance Measures Rationale

Table 3 in chapter 6 shows that, for each Security Assurance Requirement, there is an appropriate assurance measure.

PP Claims Rationale

This security target makes no claims about Protection Profile conformance.

This Page Intentionally Blank

ANNEX

A 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.

[CAPP] *Controlled Access Protection Profile,*
Version 1.d, NSA, October 1999.

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

[CR-383-4-26] *Certification Report, EAL4+ Evaluation of Sun Microsystems Inc. Solaris 9 Release 8/03,*
Version 1.0, Evaluation Number 383-4-26-CR,
Government of Canada Communications Security Establishment, 27th January 2005.

[CRP182] *Common Criteria Certification Report No. P182 Sun Solaris Version 8 2/02,*
Issue 1.0, UK IT Evaluation and Certification Scheme, April 2003.

[ECD] *Evaluated Configuration for Oracle HTTP Server10g Release 2 (10.1.2),*
Oracle Corporation, to be developed.

[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 (10.1.2),*
Oracle Corporation.

[OPMNSAG] *Oracle Process Manager and Notification Server Administrator's Guide 10g (10.1.2),* Oracle Corporation.

[RFC2616] *Hypertext Transfer Protocol -- HTTP/1.1,*
Request For Comments (RFC) 2616 of the Internet Engineering Task Force,
June 1999,
available on the World Wide Web at http://www.ietf.org/rfc.htm

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

ANNEX

B Glossary

Acronyms

CGI	Common Gateway Interface
DSO	Dynamic Shared Object
HTTP	Hypertext Transfer Protocol
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target Of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

URL	Uniform Resource Locator
URI	Uniform Resource Identifier

Terms

If a term described below has [CC] written after it, then this term is defined in the IT security evaluation scheme. All other terms relate to Oracle HTTP Server (OHS). [OHSAG, Glossary], [AHSD, 12.1] and [RFC2616] cover the full set of terms for OHS, together with Apache and the HTTP protocol. The terms used in this document are described below.

Access Control

A method of limiting access to data. When a web user sends an HTTP request to Oracle HTTP Server, OHS limits access to the requested web resource object based on directives held in one or more configuration files and based on the user's security attributes.

Apache

A public domain HTTP server derived from the HTTP server developed by the National Center for Supercomputing Applications. For this evaluation of OHS, the TOE is based on the Apache 2.0 HTTP Server.

Audit Log

The audit log is made up of records output by the HTTP server, where each record holds the audit data for one event.

Authentication

The process of verifying the identity of a user, device, or other entity in a host system, often as a prerequisite to granting access to resources in a system.

Common Gateway Interface (CGI)

A standard definition for an interface between a web server and an external program that allows the program to service HTTP requests.

Configuration File

A text file containing directives that control the configuration of OHS. The main configuration file is called `httpd.conf`. The file `.htaccess` is placed inside the web tree and applies configuration directives to the directory where it is placed and all subdirectories.

Connection

A transport layer virtual circuit established between two programs for the purpose of communication.

Content Handler

An internal OHS representation of the action to be performed when a file is requested. Generally, files have implicit handlers, based on the file type. Normally, all files are simply served by the server, but certain file types are "handled" separately. For example, the `cgi-script` handler designates files to be processed as CGIs.

crypt

The irreversible cryptographic hash function `crypt` generates a message digest from given data. OHS's `.htpasswd` program can perform `crypt` on passwords before storing them in password files.

Directive

A configuration command that controls one or more aspects of OHS's behaviour. Directives are placed in configuration files.

Dynamic Shared Object (DSO)	An OHS module compiled separately from the OHS Server program binary that can be loaded on demand.
Entity	The information transferred as the payload of an HTTP request or response. An entity consists of metainformation in the form of entity-header fields and content in the form of an entity-body.
Filter	A process applied to data that is sent or received by the server. Input filters process data sent by the client to the server, while output filters process documents on the server before they are sent to the client.
Gateway	A server which acts as an intermediary for some other server. Unlike a proxy, a gateway receives requests as if it were the origin server for the requested resource. The requesting client may not be aware that it is communicating with a gateway.
Hook Function	A function that OHS calls at a defined stage (or "hook") during the processing of an HTTP request. An OHS module can register one or more of its functions to be called via such hooks.
HTTP Client	A program that establishes connections for the purpose of sending HTTP requests to an HTTP Server.
Hypertext Transfer Protocol (HTTP)	Hypertext Transfer Protocol (HTTP) is the underlying format used by the web to format and transmit messages and to determine what actions web servers and browsers should take in response to HTTP commands. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred. HTTP is the protocol used between Oracle Application Server and clients.
MD5	MD5 is an irreversible cryptographic hash function that generates a 128-bit message digest from given data. OHS's `.htpasswd` program can perform a variant of MD5 on passwords before storing them in password files.
Method	An HTTP method is an action to be performed on a resource, specified on the request line of the HTTP message by the client.
MIME-type	A way to describe the kind of document being transmitted by the HTTP server. Its name comes from the fact that its format is borrowed from the Multipurpose Internet Mail Extensions. It consists of a major type and a minor type, separated by a slash, for example `text/html` and `image/gif`. A typical place where MIME-types are to be found is in the Content-Type header field of HTTP messages that contain an entity-body.
Mutex	Mutual exclusion or mutex is a mechanism by which multiple program threads can take turns accessing the same resource (e.g. a file), to avoid the threads interfering with each other's use of that resource.
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations. Objects are visible through the TSFI and are composed of one or more TOE resources encapsulated with security attributes. [CC]
OHS Module	Whereas a module is a part of a program that can be compiled independently to form

	object code, an OHS module is a particular kind of module that declares and handles one or more directives. OHS modules that are compiled into the OHS `httpd` binary are called static modules, while modules that are stored separately and can be optionally loaded at run-time are called dynamic modules.
Origin Server	The server on which a given resource resides or is to be created.
Password File	A file used by OHS's `htpasswd` program for storing a username and password for one or more web users.
Platform	Software and hardware underlying the TOE.
Proxy	An intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients.
Request	An HTTP request message from a client to a server includes, within the first line of that message, the method to be applied to the resource, the identifier of the resource, and the protocol version in use.
Realm	A name associated with a file-system directory and its sub-directories via an OHS `Directory` directive and an `AuthName` directive.
Resource	A network data object or service that can be identified by a URI.
Response	After receiving and interpreting an HTTP request message, a server responds with an HTTP response message.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE. [CC]
Security Attribute	Information associated with subjects, users, and/or objects which is used for the enforcement of the TSP. [CC]
Security Domain	The set of objects that a subject has the ability to access.
Security Function (SF)	A part or parts of the TOE which have to be relied upon for enforcing a closely related subset of the rules from the TSP. [CC]
Security Function Policy (SFP)	The security policy enforced by a SF. [CC]
Security Functional Requirement (SFR)	A security functional requirement defined in a protection profile or security target. [CC]
Server	A program that accepts connections in order to service requests by sending back responses. Any given program may be capable of being both a client and a server. The use of these terms refers only to the role being performed by the program for a particular connection, rather than to the program's capabilities in general.
SHA-1	SHA-1 is an irreversible cryptographic hash function that generates a 160-bit message digest from given data. OHS's `htpasswd` program can perform SHA-1 on passwords before storing them in password files. Administrators are required to specify

	that SHA-1 is to be used by `htpasswd` when storing passwords in the evaluated configuration.
SOF-medium	A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential. [CC]
Strength of Function (SOF)	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms. [CC]
Subject	An entity within the TSC that causes operations to be performed. [CC]
System	A specific IT installation, with a particular purpose and operational environment [CC]
Target Of Evaluation (TOE)	The product or system being evaluated. [CC]
TOE Resource	Anything usable or consumable in the TOE. [CC]
TOE Scope of Control (TSC)	The set of interactions which can occur with or within a TOE and are subject to the rules of the TSP. [CC]
TOE Security Functions (TSF)	A set consisting of all the software of the TOE that must be relied on for the correct enforcement of the TSP. [CC]
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE. [CC]
TSF Interface (TSFI)	A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF. [CC]
Uniform Resource Locator (URL)	A Uniform Resource Identifier that identifies a resource via a representation of its primary access mechanism (e.g. its network location). URLs are usually made up of a scheme, like http or https, a hostname, and a path, for example: `http://httpd.apache.org/docs-2.1/glossary.html`.
Uniform Resource Identifier (URI)	A compact string of characters for identifying an abstract or physical resource. It is formally defined by RFC 2396.
User	Any entity (human or machine) outside the TOE that interacts with the TOE. [CC]
User Agent	The client which initiates an HTTP request. This is typically a browser.

This Page Intentionally Blank

ANNEX

C Relationship to WSPP

Use of USWSPP

This Security Target makes no claim for conformance to any Protection Profile. However, it is based as closely as possible on the draft U.S. Government Protection Profile for Web Servers in Basic Robustness Environments [USWSPP]. The relationship of the OHS Security Target to [USWSPP] is summarised in this annex.

For this evaluation of OHS, an assessment has been made of the likely content of [USWSPP] when it has been certified, and this has been used as a guide when choosing items to include in the OHS ST.

Threats

[USWSPP, 3.1] covers the threats to be countered by the TOE and its environment. The Security Target for OHS excludes the threats in [USWSPP, 3.1] related to reading TCP/IP messages off the network using a network traffic analyser. This is because, having read [USWSPP, 7.4.4], which describes cases typifying a Basic Robustness environment, the authors believe that there is no need to counter such threats in such an environment. In addition, [ECD] will have the effect of disallowing the installation of a network traffic analyser in the evaluated configuration for OHS, because such a device would only be installed in order to compromise the TOE's security policy. This would contravene the instructions given in [ECD], which require that no applications, other than those which communicate with the TOE by sending HTTP messages, shall be permitted to run on any client or server host machines which access the network, unless they have been shown not to compromise the TOE's security objectives as stated in [ST].

Organisational Security Policies

Since this document includes no threats to do with reading TCP/IP messages off the network using a network traffic analyser, the organisational security policies in [USWSPP, 3.2] that relate to cryptography are not included in this ST.

Security Objectives

Since this document includes no threats to do with reading TCP/IP messages off the network using a network traffic analyser and the OSPs do not involve cryptography, the security objectives in [USWSPP, 4] that relate to cryptography are not included in

this ST.

IT Security Requirements

Since this document includes no OSPs that involve cryptography, the IT security requirements in [USWSPP, 5] that relate to cryptography are not included in this ST. In addition, the split of Security Functional Requirements between the TOE and the environment in the OHS ST is different from that chosen for [USWSPP, 5] to match the actual security functionality that is present in OHS.

Chapter 5 of this document has SFRs for the Web User SFP, which is a policy for controlling web users' access to web resource. These SFRs disallow all HTTP methods other than GET and HEAD, although they have the same effect as the SFRs in [USWSPP, 5] for a Web User SFP that disallows all HTTP methods other than GET. This is because OHS effectively treats the HEAD method as a GET method which returns no body.

Chapter 5 of this document has SFRs for the IT environment equivalent to the SFRs in [USWSPP, 5.2] that cover:

- a Content Provider Security Function Policy;
- security management functions for audit, group files and configuration files;
- various audit record selection features;
- audit trail handling and analysis; and
- requirements on the operating system such as for the protection of the TSF and for session timeouts and banners.