VALIDATED COMPONENT SUMMARY

Name:	Apache mod_rewrite module
Version:	Versions 1.3.41; 2.0.63; 2.2.11
Validation Completed:	28th March 2009
Validation Facility:	Enex Testlab

INFORMATION MANAGEMENT COMPONENT VALIDATION

The National Archives is a government department and an executive agency under the Secretary of State for Justice, which has statutory and policy responsibility for Knowledge and Information Management (IM) for public sector information. It therefore sets standards and supports innovation on information management across the UK, in order to ensure the survival of records in whichever form they are created, be it paper or digital, and provides practical frameworks of best practice for use of public sector information.

In recognition that almost all the information created in government is now electronic, but that there is a risk that information risks becoming inaccessible as technologies and organisations change, the National Archives has been leading work on digital preservation as acknowledged in the Transformational Government Implementation Plan.

The National Archives has therefore generated a technical framework for Information Persistence for government departments and the public sector, to ensure the long term survivability of records from any systems, and guard against compromises of Integrity and Availability.

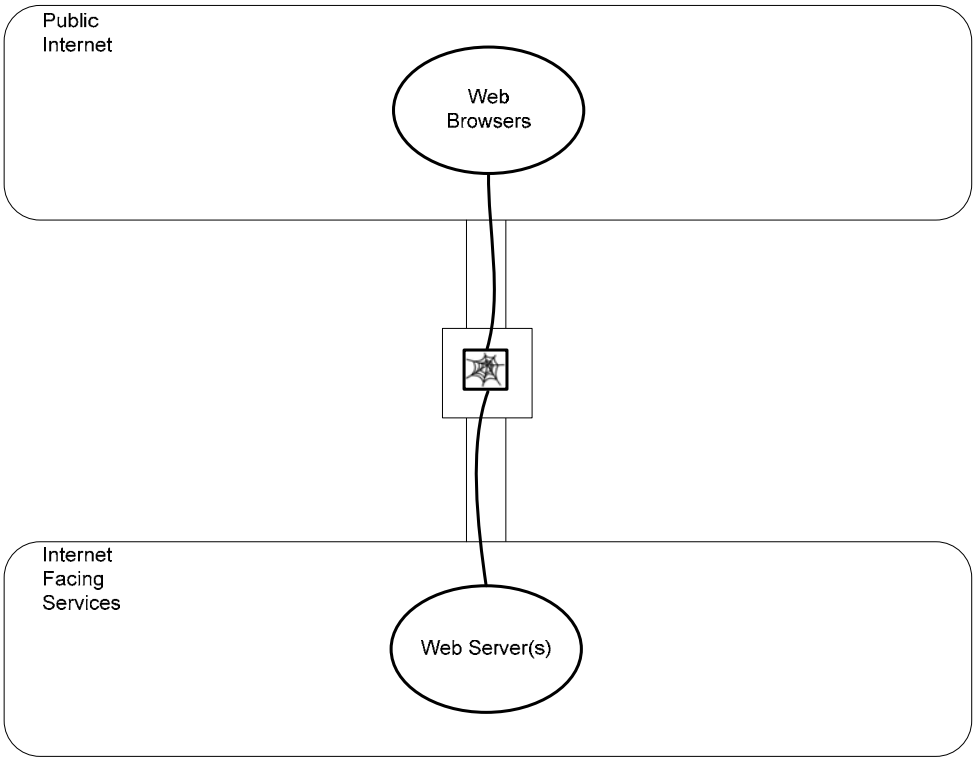
As part of this framework, a formalised system of validation of technical components has been established, to provide Stakeholders with confidence that such technologies have been independently reviewed for fitness for purpose.

COMPONENT OVERVIEW

Mod_Rewrite is a standard module packaged with the open source Apache web server available from Apache (http://www.apache.org). The module has been identified by the Stationery Office in response to a request from the National Archives to provide software that can help government departments manage URL persistence.

Mod_Rewrite is installed on Apache web server platforms to enable URL rewriting and redirection functionality to Apache. Apache server can be installed on both Microsoft and Linux server platforms to provide URL rewriting and redirection.

VALIDATION DEPLOYMENT SCENARIO



The component is expected to be deployed on web servers across central government departments. This may include servers owned and managed directly by the departments, servers managed by IT suppliers, or servers set up under arrangements such as co-location and virtual hosting.

There are expected to be one or more competent individuals in each implementing department (or their suppliers) assigned to manage the implementation of the product, and the initial and ongoing configuration of the implementation rules. Those personnel are not careless, willfully negligent, nor hostile.

The environment is expected to include a set of Pragmatic, Appropriate and Cost Effective (PACE) controls, in terms of a balanced set of Personnel, Physical, Procedural and Technical (P^3T) measures, to mitigate the Risks arising from the various Vectors (e.g. unauthorised access, physical damage, information release and malicious software) from various types of Adversity (e.g. directed Threats, such as Attacks, and collateral Hazards, such as extreme climatological events).

VALIDATION ENVIRONMENT

Although the Component will run on various platforms, the Claims made here relate only to the Apache versions listed above running on Windows Server 2003 (SR2 with SP2) and Red Hat Linux Enterprise version 5.

CONTROLS PROVIDED

The component provides support for the technical controls listed below, provided the deployment is commensurate with the assumptions, and that the overall organisational policies are supportive. Use of the product alone should not be taken to infer in any way compliance with the listed standard.

Control Title	Control Details	Standards Cross Reference
Inventory of Assets	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.	ISO/IEC 27001 A7.1.1
Information back-up	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	ISO/IEC 27001 A.10.5.1
Information Exchange	System shall only release information (eye readable or non eye readable) to authorised person(s)	ISO/IEC 27001 A.10.8
Protection of organizational records	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	ISO/IEC 27001 A.15.1.3

VALIDATED CLAIMS

The following specific functionality has been successfully tested in the environment and usage scenario as described above:

Ref	Claims Statements
AMW 01	The module uses htaccess files in which URL rewriting and redirection rules can be programmed by users.
AMW 02	The module can be programmed to rewrite or redirect one or more individual URLs, and/or all URLs matching one or more specified patterns, using the PCRE syntax. Different rewrite/redirection behaviours can be specified for each URL or group of URLs affected. Redirection rules can both include and exclude URLs from rewriting or redirection.
AMW 03	Redirection configuration htaccess files cannot be modified or adversely affected through use of malicious URL injection methods.
AMW 04	When using "RewriteRule" entries to specify URL patterns for redirection, the module functions with URL and query string lengths within the limits supported by the server software.
AMW 05	On multi-site Apache installations, the component can be installed either for all sites collectively, or for one or more sites individually.
AMW 06	The module makes no modification to the content of the page, only to the URL
AMW 07	Rewrite activity can be logged to files on a directory specified by the user if

	desired. This does not affect the main Apache logging.
AMW 08	The module has support for Unicode, URL characters, and UK and foreign language content in use on central government websites, based on redirection rules written in the English language.
AMW 09	Installation of the module introduces no known malicious software into the system
AMW 10	The module makes no alteration to the original case of the URL unless specifically programmed to do so in the htaccess files.
AMW 11	The module communicates directly only with the web server(s) on which it is installed and attempts no direct communication with external systems.

PUBLICLY KNOWN VULNERABILITIES

The following publicly listed vulnerabilities from the Common Vulnerabilities and Exposures (CVE) database and/or the (US) National Vulnerability Database (NVD) were found to apply to this Component at the time of testing. Treatment is available for all to mitigate their effects.

ID	Summary	Treatment
CVE-2007-0450	Directory traversal vulnerability	If using *Tomcat*, ensure Version 5.x is greater than 5.5.52 and Version 6.x is greater than 6.0.10
CVE-2006-3747	Off-by-one error in the ldap scheme handling in the Rewrite module (mod_rewrite)	Ensure *Apache httpd* is at least v2.2.3 for *2.2.x* fork, v2.0.59 for *2.0.x* fork and 1.3.37 for *1.3.x* fork
CVE-2003-0542	Multiple stack-based buffer overflows in (1) mod_alias and (2) mod_rewrite for Apache	Ensure *Apache httpd* is at least v2.0.48 for *2.0.x* fork and 1.3.29 for *1.3.x* fork
CVE-2001-1072	Apache with mod_rewrite enabled on most UNIX systems allows remote attackers to bypass RewriteRules	Ensure *RewriteRule* directives are written correctly so that the rules will capture more than one slash
CVE-2000-1206	Vulnerability in Apache allows remote attackers to retrieve arbitrary files.	Ensure *Apache httpd* is at least 1.3.11 for *1.3.x* fork
CVE-2000-0913	mod_rewrite in Apache allows remote attackers to read arbitrary files	Ensure *Apache httpd* is at least 1.3.12 for *1.3.x* fork

OPERATIONAL AND RISK MANAGEMENT CONSIDERATIONS

Although the component will run on various other platforms, the Claims validated here relate only to the versions specified.

In deploying and operating the Component, it is assumed that Information Assurance (IA) risk assessment to either system and/or the data it is envisaged to handle attracts no higher baseline requirement than that derived from the UK National Annual Threat Assessment (ATA) and the UK National Strategic Risk Assessment (NSRA) / National Risk Planning Assumptions (NRPA).

It is furthermore assumed that the risk management measures already put in place for corporate infrastructure(s) on which the Component is deployed have mitigated any increased differential risk factors to a level commensurate with the application of baseline measures.

When installing the Component on Red Hat Enterprise Linux 5.3 from the specified source code packages, the user must specifically enable mod_rewrite during the source code compilation process, and check that the correct installation of mod_rewrite has occurred thereafter.

COMPONENT STATEMENT OF APPLICABILITY

The Component described in this document has been independently assessed by the listed Validation Facility, which is a Test Laboratory approved by the UK Accreditation Scheme (UKAS) under ISO/IEC 17025:2005 "*General requirements for the competence of testing and calibration laboratories*".

This Claims made for the Component, and the Testing, have been subjected to scrutiny by a Technical Authority within the National Archives, in their capacity as the government department having statutory and policy responsibility for Knowledge and Information Management (IM) of public sector information.

It has been concluded that, when installed, configured and operated correctly, as described in associated documentation and herein, this Component is suitable for performing the Claimed functionality in support of public sector IM activities, subject to the operational and risk management considerations noted herein.

The information has been provided in good faith, and **is based on the component version and usage scenario(s) as detailed in this document**. This information is not therefore designed for any particular implementation, and we therefore cannot guarantee accuracy or relevance for any specific purpose. The Validation Testing is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in any Product or IA Service, or the IS environment supporting such a Product or Service.

We do not accept responsibility for any information omitted, or errors in this information. We do not have any responsibility for the accuracy, availability, completeness or usefulness of any of the information provided.

No other terms, conditions, representations or warranties will apply.

References we make to any specific product, process or service by trade name, trademark manufacturer, or otherwise, or linking to other websites or material are not endorsements or recommendations.

The views and opinions of the National Archives shall not be used for advertising or product endorsement purposes. This information is for official purposes, and the contents may not be used for commercial purposes.

Approved By

Name:	Ian Bryant	Signature:	*Ian Bryant*
Role:	IMCV Technical Authority	Date:	27th April 2009