When this document is printed, the document needs to be stamped top and bottom with the appropriate classification.

VL05 - Checklist Report

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:
Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Checklist: Apache Site 1.3.x

Vulnerability Key:	V0006247
STIG ID:	WA025
Release Number:	3
Status:	Active
Short Name:	WA025
Long Name:	Web content classification or sensitivity level has not been documented by proper authorities and appropriate labeling in not present.
IA Controls:	ECML-1 Marking and Labeling
Categories:	5.1 Device Labels for Classification 11.2 Dissemination
Effective Date:	29 Jun 2005

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: If the sensitivity level of the data on a web server is unknown a procedure must be in place to ascertain this sensitivity level. Once the sensitivity level is known it is the responsibility of the IAO or approving authority to document this level. This sensitivity level is defined as data that has or has not been reviewed and approved for release in accordance with DoD 5230.9. Provided the level of sensitivity is

known the web server can be defined as either a private or public web server and security controls can be applied accordingly. A DoD private web server as defined by the Department of Defense Instruction 8520.2 states: E2.1.12. DoD Private Web Server. For unclassified networks, a DoD private web server is any DoD-owned, operated, or controlled web server providing access to sensitive information that has not been reviewed and approved for release in accordance with DoD Directive 5230.9 (reference (q)) and DoD Instruction 5230.29 (reference (r)). For Secret Internet Protocol Router Network and other classified networks that are not accessible to the public, a DoD private web server is any server that provides access to information that requires need-to-know control or compartmentation. A DoD public web server is any DoD-owned, operated, or controlled web server providing access to information that has been reviewed and approved for release in accordance with DoD Directive 5230.9 (reference (q)) and DoD Instruction 5230.29 (reference (r)). The existence of unlabeled classified content is a de facto security incident. Thus a classified web server must contain correctly labeled material. These classified markings must be present on each page that contains classified content.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Information Assurance Officer
Web Administrator

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation
WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.5
WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.9

Checks: WA025 (Manual)

Interview the IAO or Web Master to determine whether documentation exists defining the sensitivity level of data published by the Web site. The reviewer should also randomly review a few pages from the web site, if is a classified web server, and evaluate if classification markings are utilized on the pages.

If the sensitivity level of the information for publication by the web server is not known and documented, this is a finding.

If the classified web site does not contain proper labeling of content, this is a finding.

Vulnerability Key: V0002239
STIG ID: WA030
Release Number: 8
Status: Active
Short Name: WA030
Long Name: Web content is not reviewed and approved by proper authorities prior to posting to a production web server.
IA Controls: DCPR-1 CM Process
Categories: 12.9 Documentation
Effective Date: 09 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑

Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: The organization or activity that sponsors the web site will have web content responsibility. These persons will ensure that all information is kept current and that information and scripting placed on the web server is reviewed and approved by a configuration management authority. The organization or activity that sponsors the web site will have web content responsibility. These persons will ensure that all information is kept current and that information and scripting placed on the web server is reviewed and approved by a configuration management authority and as needed by the Public Affairs Officer (PAO). Likewise, the reviewer should verify that local policies have been developed to ensure that all information has been reviewed and approved for posting by the originating organization according to the DoD Web Site Administration Policies & Procedures, 25 November 1998 (updated 11 January 2002) available at http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_correctio November 1998.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Information Assurance Officer
Designated Approving Authority
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.1

Checks: WA030 (Manual)

Reviewer should verify that local policies have been developed to ensure that all information has been reviewed and approved as needed by the Public Affairs Officer (PAO) for posting.

Proposed Questions:

How often does content change on the web site?
When content changes, how is the new content approved for publication?
Is the approval process documented in a local SOP?
Is the approval process documented in email?
Is the approval process documented in any manner?

Exceptions: Web applications where this Vulnerability is not applicable include computer or CD-ROM based training (CBT), document management applications, search and query applications or web sites designed for collaboration. Such applications will contain a rule-based structure for the posting and maintenance of content. In such cases, the rules by which such a site operates constitutes the review and approval process outlined in this requirement.

Vulnerability Key: V0013614
STIG ID: WA032
Release Number: 2
Status: Active
Short Name: WA032
Long Name: The Web Manager will ensure all interactive (CGI) programs used on the web server are documented, to include the language used and aim of the program, and that documentation is provided to the IAO.
IA Controls: ECSD-1 Software Development Change Controls
Categories: 12.9 Documentation
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable	Comments:

Not Reviewed	

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category III

Vulnerability Discussion: CGI is a standard for interfacing external applications with information servers, such as HTTP or web servers. The definition of CGI as web-based applications is not to be confused with the more specific .cgi file extension. CGI applications can be written in most programming language. Common applications involve acquiring data via a web page and the browser, executing the CGI application, and returning customized web content. There is a possibility of compromising security when using CGI. CGI programs that are carelessly written can grant the malicious user as much access to the server as a privileged account. Documenting these programs will allow the site to maintain an inventory of the interactive programs so that rogue programs are not installed and run from the web server.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.2

Checks: WA032 (Manual)

The Web Manager will ensure all CGI programs used on the web server are documented, to include the language used and aim of the program, and that documentation is provided to the IAO.

Proposed Questions:

Review the SOP that documents this process.
Ask to see an example of a documented program from the web server.

If the site cannot produce documentation that show they are maintaining documentation of interactive programs, this is a finding.

Vulnerability Key: V0002269

STIG ID: WA130

Release Number: 4

Status: Active

Short Name: WA130

Long Name: Scripts are not reviewed by a CCB or technical group and installation of scripts on the web server is not controlled.

IA Controls: ECSD-1 Software Development Change Controls
ECSD-2 Software Development Change Controls

Categories: 7.4 Testing
7.7 Code Validation
12.4 CM Process

Effective Date: 17 May 2001

Open	Comments:

☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category III

Vulnerability Discussion: Interactive scripts is a powerful means for enhancing web site functionality. Scripts are often executable at the operating system level and frequently exercise control over fundamental system resources (i.e start and stop programs, write data to the server, alter and delete data). A variety of scripting languages, middleware, is available for this purpose. Typically, this middleware involves the use of an interpreter. The opportunity for a malicious user to exploit poorly designed or untested web scripts is significant and has proven to be a leading cause of server compromises. This would apply to any operating system and any web server software in use. ASP, JSP, JAVA and PERL scripts are commonly found in these circumstances.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.1, Section 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WA130 (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine whether or not scripts are reviewed and evaluated for security issues prior to being installed on a production web server.

Another concern is that developers are allowed to directly install their own scripts onto the server. This should not be permitted. All interactive programs used on the web server should also be documented, to include the language used and aim of the program, and that documentation is provided to the IAO.

Proposed Questions:

Who approves the installation of scripts on the production web server?
What is the process for posting interactive programs to the web site?
Where is the list of documented interactive programs maintained?
Is the approval process documented in email? or in any manner?

If the scripts used on the web server are not filtered through a review process or CCB before posing and are not documented, this is a finding.

Exceptions: Web applications where this vulnerability is not applicable include computer or CD-ROM based training CBT), document management applications, search and query applications or web sites designed for collaboration. Such applications will contain a rule-based structure for the posting and maintenance of content.

Vulnerability Key: V0013615
STIG ID: WA150
Release Number: 1
Status: Active
Short Name: WA150
Long Name: Web applications or servers, which require restriction by user ID and password, do not require web users to have a user ID and password that provide access only to the web content.
IA Controls: IAIA-1 Individual Identification and Authentication
IAIA-2 Individual Identification and Authentication
Categories: 1.3 Identity Management
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)
Policy: All Policies
MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II
Vulnerability Discussion: Some web-based applications utilize the use of user IDs and passwords. In some cases these passwords are OS accounts and provide remote user access to other applications or databases. In this situation, the OS password policy applies. In other instances, the user ID and password scheme is determined by the application. In this case, the application's documentation should detail the policy to be followed to add users and select or change passwords. In cases where a Lightweight Directory Access Protocol (LDAP) server is used for authentication, the procedures for the web server suite should detail the web site's password policy. A process for changing the forgotten password should be followed. Password policies to include password strength will comply with the appropriate operating system STIG.
Documentable: No
Documentable Explanation:
Potential Impacts:
Responsibility:
References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.6
Checks: WA150 (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine if web applications or servers, which require restriction by user ID and password, require web users to have a user ID and password that provide access only to the web content. The intent is to ensure that web users do not have access beyond what is necessary to access the web site.

Proposed Questions:

Ask them to provide documentation to show how userids are assigned. This should detail how regular users and administrative users are assigned accounts.

If the site is using OS accounts for web access, ask how the accounts are segregated. Is this done with groups, permissions, etc.?

If the site cannot explain to your satisfaction that they have a process for ensuring web userids

are used to access only web content, then this is a finding.

Vulnerability Key: V0002240
STIG ID: WG110
Release Number: 5
Status: Active
Short Name: WG110
Long Name: The number of simultaneous requests is not limited for this web site.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 13.6 Denial of Service
Effective Date: 09 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: When the parameter for the number of simultaneous requests a web site is configured to service is set to unlimited, a denial of service attack attempted by an number of techniques is facilitated.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG110 - Apache (Manual)

Locate the httpd.conf file. This can be accomplished by a search/find on the local drives. Typically this is in: /usr/local/apache/conf/ or /etc/apache

If MaxKeepAliveRequests = 0, this is a finding.

If the parameter is not present, this is not a finding as the default value is 100.

Note: MaxKeepAliveRequests 0 is unlimited.

Vulnerability Key: V0006531
STIG ID: WG140
Release Number: 2

Status: Active
Short Name: WG140
Long Name: A private web server does not require subscriber certificates, issued from any DoD authorized Certificate Authority as an access control mechanism for web users.
IA Controls: IATS-1 Token and Certificate Standards
IATS-2 Token and Certificate Standards
Categories: 1.2 PKI
Effective Date: 29 Jun 2005

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)
Policy: All Policies
MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☐	☐	☐

Severity: Category II
Vulnerability Discussion: Restrictions based upon domain name, such as .gov or .mil are commonly used. In some cases, restriction down to the ip address of the host attempting to access the server is possible. Access can also require the client requesting a connection to a web server to possess a userid and password. However, per the DODI 8520.2 all private web servers are required to request a valid DOD PKI user certificate for authentication to access DOD private web sites. The use of non-standard port numbers is not an accepted solution to limiting access to a web server, as elementary port scanning tools will quickly reveal http and https services running on non-standard ports.
Documentable: No
Documentable Explanation:
Potential Impacts:
Responsibility: Web Administrator
References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.5
8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
Checks: WG140 - Apache (Manual)

Provided the SSL implementation module is mod_ssl or Apache-SSL, locate and open the httpd.conf file. Look for the directive "SSLVerifyClient require". The value "require" signifies that the client must present a valid certificate.

Note: this value may also be present in the access.conf file or in the ssl configuration file (ssl.conf or mod_ssl.conf or ssl-global.conf)

If the web site is not configured to require DoD client certificates or approved ECA certificates, this is a finding.

NOTE: The DODI 8520.2 requires this for both NIPRNet and SIPRNet, but at this point, this should only be marked as a finding for NIPRNet web sites.

Vulnerability Key: V0002245
STIG ID: WG170
Release Number: 5

Status: Active
Short Name: WG170
Long Name: Each readable web document directory does not contain either a default, home, index or equivalent file.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 2.2 Least Privilege
Effective Date: 10 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: The goal is to completely control the web users experience in navigating any portion of the web document root directories. Ensuring all web content directories have at least the equivalent of an index.html file is a significant factor to accomplish this end. Also, enumeration techniques, such as url parameter manipulation, rely upon being able to obtain information about the web server's directory structure by locating directories with default pages. This practice helps ensure that the anonymous web user will not obtain directory browsing information nor an error message that reveals the server type and version.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.4
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG170 - Apache (Manual)

From the httpd.conf locate the document root. Navigate to this directory. Ensure that in this directory there is an index.html or equivilent default page and perform the same check on any directories below the document root directory.

Windows Example:

DocumentRoot "d:/Apache Group/Apache/htdocs/test"

UNIX Example:

DocumentRoot /usr/local/share/apache/httpdocs/

If there is no index.html or equivilent default page in the document root directory, Apache will automatically produce a page entitled "Index of /" and display all the files in a directory browsing fashion. This can be avoided by ensuring that an index.html file is present in every directory. If there is no index.html in the document root directory or sub-directories, this is a finding.

Vulnerability Key: V0003333
STIG ID: WG205
Release Number: 5
Status: Active
Short Name: WG205
Long Name: The web document (home) directory is not in a separate partition from the web servers system files.
IA Controls: DCPA-1 Partitioning the Application
Categories: 2.2 Least Privilege
Effective Date: 05 Dec 2002

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: Web content is accessible to the anonymous web user. For such an account to have access to system files of any type is a major security risk that is entirely avoidable. To obtain such access is the goal of directory traversal and URL manipulation vulnerabilities. To facilitate such access by mis-configuring the web document (home) directory is a serious error. In addition, having the path on the same drive as the system folder compounds potential attacks such as drive space exhaustion.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References:

Checks: WG205 - Apache (Manual)

Locate the document root in the configuration file httpd.conf. Ensure that the location of the document root is not the root for the web server itself nor the operating system root directory.

Confirm that this is not the systems root partition nor the web root directory; if it is this is a finding.

Vulnerability Key: V0002226
STIG ID: WG210
Release Number: 4
Status: Active
Short Name: WG210
Long Name: Web content directories anonymously shared via a network share.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.2 Least Privilege

Effective Date: 01 Dec 1999

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND Windows (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: Such sharing is a security risk when a web server is involved. Users accessing the share anonymously could experience privileged access to the content of such directories. Network sharable directories expose those directories and their contents to unnecessary access. Any unnecessary exposure increases the risk that someone could exploit that access and either compromises the web content or cause web server performance problems. NIST Guidelines for Securing Public Web Servers (par. 8.6 pg. 75, a principle reference for this document) states “Do not mount any file shares on the internal network from the Web server or vice versa”. The presence of shares is indicative of a remote management solution or a development server. Alternatives to shares are a secure ftp products or related remote admin tools.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References:

Checks: WG210 - Windows Apache (Manual)

The following directories must not be shared.

Drive Letter:\Apache Group\Apache\
Drive Letter:\Apache Group\Apache\htdocs

Note: these directories may vary from machine to machine. You can do a search of the server to find the httpd.conf file, which will contain the information you need.

The "DocumentRoot" directive will point to the document directory and the "ServerRoot" directive will identify the Apache server directory.

Using Explorer, locate the path identified above. Right click on the directory to be examined. Select Properties; Select the “Sharing” tab. If the "Share this folder" is selected, this is a finding.

NOTE: The presence of operating system shares on the web server is not an issue as long as the shares are not part of the web content directories. The use of shares to move content from one enviroment to another is permitted if the following conditions are met: they are approved by the IAM/IAO, the shares are restricted to only allow administrators write access, the use of the shares does not bypass the sites approval process for posting new content to the web server, and Developers are only permitted read access to these directories.

☐ Open ☐ Not a Finding ☐ Not Applicable	Comments:

☐ Not Reviewed	

Condition: Web Server AND UNIX (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: Such sharing is a security risk when a web server is involved. Users accessing the share anonymously could experience privileged access to the content of such directories. Network sharable directories expose those directories and their contents to unnecessary access. Any unnecessary exposure increases the risk that someone could exploit that access and either compromises the web content or cause web server performance problems. NIST Guidelines for Securing Public Web Servers (par. 8.6 pg. 75, a principle reference for this document) states “Do not mount any file shares on the internal network from the Web server or vice versa”. The presence of shares is indicative of a remote management solution or a development server. Alternatives to shares are a secure ftp products or related remote admin tools.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sections 3.7

Checks: WG210 - Unix Apache (Manual)

The entry for the ServerRoot and DocumentRoot directory can be found in the httpd.conf file.

The command /usr/bin/share or /usr/sbin/share will display all the file systems which are exported.

Look in the /etc/exports, /etc/mnttab or /etc/dfs/sharetab file. This file lists the file systems that the server exports. Look for the paths identified above. If these paths are present in either one of these files, this is a finding.

Vulnerability Key: V0002249
STIG ID: WG230
Release Number: 4
Status: Active
Short Name: WG230
Long Name: Web server administration is not performed over a secure path or at the console.
IA Controls: EBRU-1 Remote Access for User Functions
Categories: 8.1 Encrypted Data in Transit
Effective Date: 10 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND Windows (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category I

Vulnerability Discussion: Logging in to a web server via a telnet session or using http or ftp in order to perform updates and maintenance is a major risk. In all such cases, userids and passwords are passed in the plain text. Acquiring such account information over a network is routinely accomplished and made all the worse by the fact that the account information so obtained is for privileged users. A secure shell service or https needs to be installed and in use for these purposes. Another alternative is to administer the web server from the console, which implies physical access to the server.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.5
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks:

WG230 - Windows Apache (Manual)

Select START >> Programs and look for F-Secure or equivalent program. Some versions of Windows compatible SSH are F-Secure SSH Tunnel, SecureCRT, NT sshd, and Tera Term with TTSSH.

If all administration is done via the server console, this is not a finding.

For Example, remote desktop over an encrypted connection.

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND UNIX (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category I

Vulnerability Discussion: Logging in to a web server via a telnet session or using http or ftp in order to perform updates and maintenance is a major risk. In all such cases, userids and passwords are passed in the plain text. Acquiring such account information over a network is routinely accomplished and made all the worse by the fact that the account information so obtained is for privileged users. A secure shell service or https needs to be installed and in use for these purposes. Another alternative is to administer the web server from the console, which implies physical access to the server.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.5

Checks: WG230 - Unix Apache (Manual)

Verify that some variety of SSH is running on the web server platform.

Check for an ssh daemon, by querying the SA and Web Manager and use ps –ef | grep ssh

ssh or updates via the console only would satisfy this requirement.

If all administration is not done via the server console or ssh, this is a finding.

Vulnerability Key: V0013686
STIG ID: WG235
Release Number: 1
Status: Active
Short Name: WG235
Long Name: Remote authors or content providers are able to upload files to the DocumentRoot directory without the use of a secure encrypted logon and secure encrypted connection.
IA Controls: EBRU-1 Remote Access for User Functions
Categories: 8.1 Encrypted Data in Transit
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category I

Vulnerability Discussion: Logging in to a web server via a telnet session or using http or ftp in order to upload documents to the web site is a risk if proper encryption is not utilized to protect the data being transmitted. A secure shell service or https needs to be installed and in use for these purposes.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.6

Checks: WG235 (Manual)

Query the SA to determine if there is a process for the uploading of files to the web site. This process should include the requirement for the use of a secure encrypted logon and secure encrypted connection.

NOTE: See results from WG230 for data that will assist in the validation of this vulnerability.

If the remote users are uploading files without utilizing approved encryption methods , this is finding.

Vulnerability Key: V0002250
STIG ID: WG240
Release Number: 5
Status: Active
Short Name: WG240
Long Name: Logs of web server access and errors are not established and maintained.
IA Controls: ECAT-1 Audit Trail, Monitoring, Analysis and Reporting
ECAT-2 Audit Trail, Monitoring, Analysis and Reporting
Categories: 10.2 Content Configuration
Effective Date: 10 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: A major tool in exploring the web site use, attempted use, unusual conditions and problems are reported in the access and error logs. In the event of a security incident, these logs can provide the SA and Web Manager with valuable information. Without these log files, SAs and Web Managers are seriously hindered in their effort to respond appropriately to suspicious or criminal actions targeted at the web site. Message board and collaboration servers also need to log SMTP activity, JavaScript chat, uploads, errors, activity, and all HTTP requests.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.1 and Section 5.4
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG240 - Apache (Manual)

To verify that logging is being performed:

The httpd.conf file will contain information about the log files that are being used or will point to other conf files that are used to configure the auditing for the web server. Each server may be configured differently, so the following is one example of how a server may be configured.

The reviewer may have to investigate the httpd.conf file to discover pointers to the locations of the other conf files. These can be identified in the httpd.conf file by the include statements.

Using the editior of your choice, search the httpd.conf file for the directive will point to the location of the apache error log. The following is the error log directive that you need to search for:

ErrorLog

Using the editior of your choice, search the httpd.conf file for the directive will point to the location of the apache access log. The following is the access log directive that you need to search for:

CustomLog

If these are not found in the httpd.conf file, search the httpd.conf file for include statements that point to the following files:

mod_log_config.conf
global.conf

The Include statements will point you to the directory that contains each of these files. (Both files may not be in the same directory)

Navigate to each directory and search the file to see if the CustomLog directive is included.

If specified, navigate to the directory location of both the error and access logs. Confirm the log files exist and have a current date indicating they are being written to.

If the web server does not have the error and access log directives configured and the log files don't exist, this is a finding.

Vulnerability Key: V0013688
STIG ID: WG242
Release Number: 2
Status: Active
Short Name: WG242
Long Name: Log file data does not include the required data elements.
IA Controls: ECAR-1 Audit Record Content
ECAR-2 Audit Record Content
ECAR-3 Audit Record Content
Categories: 10.2 Content Configuration
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)
Policy: All Policies
MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: A major tool in exploring the web site use, attempted use, unusual conditions and problems are reported in the access and error logs. In the event of a security incident, these logs can provide the SA and Web Manager with valuable information. Without these log files, SAs and Web Managers are seriously hindered in their effort to respond appropriately to suspicious or criminal actions targeted at the web site. In addition to having logging enable, it is also important to be capturing the correct information in the log files. Without the correct information, the support staff may not be able to respond properly to malicious activites or have the appropriate evidence to pursue follow on actions.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.1

Checks: WG242 - Apache (Manual)

To verify the log settings:

Default UNIX location: /usr/local/apache/logs/access_log

Default Windows location: :\Program Files\Apache Group\Apache\logs\access_log

If these directories do not exist, you can search the web server for the httpd.conf config file to determine the location of the logs.

Items to be logged are as shown in this sample line in the httpd.conf file:

LogFormat "%a %A %h %H %l %m %s %t %u %U \"%{Referer}i\" " combined

If the web server is not configured to capture the required audit events for all sites and virtual directories, this is a finding.

Following is the description of the various LogFormat options for your reference:

%a = Remote IP-address
%A = Local IP-address
%e = Ref: apache
%h = client IP address (Caveat: The IP address reported here is not necessarily the address of the machine at which the user is sitting. If a proxy server exists between the user and the server, this address will be the address of the proxy, rather than the originating machine.) Ref: apache
%H = The request protocol
%l = The RFC 1413 identity of the client determined by identd on the clients machine. This information is highly unreliable and should almost never be used except on tightly controlled internal networks. Apache httpd will not even attempt to determine this information unless IdentityCheck is set to "On". Ref: apache
%m = Request Method. Ref: apache
%s = Status. For requests that got internally redirected, this is the status of the *original* request --- %>s for the last.
%t = The time that the server finished processing the request. Ref: apache
%u = Remote user (from auth; this may be bogus if return status [%s] is 401) Ref: O'Reilly
%U = URL requested. Ref: apache

Vulnerability Key: V0002252
STIG ID: WG250
Release Number: 3
Status: Active
Short Name: WG250
Long Name: Users other than from the Auditors group have greater than read access to log files.
IA Controls: ECTP-1 Audit Trail Protection
Categories: 2.2 Least Privilege

Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND Windows (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: A major tool in exploring the web site use, attempted use, unusual conditions and problems are the access and error logs. In the event of a security incident, these logs can provide the SA and Web Manager with valuable information. To ensure the integrity of the log files and protect the SA and Web Manager from a conflict of interest related to the maintenance of these files, only the members of the Auditors group will be granted permissions to move, copy and delete these files in the course of their duties related to the archiving of these files.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.1

Checks:

WG250 - Windows Apache (Manual)

Determine permissions for log files:

Find the httpd.conf configuration file to determine the location of the log files. The location is indicated at the "ServerRoot" directive. The log directory is a sub-directory under the ServerRoot.

ex. :\Apache Group\Apache\logs

After locating the logs, use the Explorer to move to these files and examine their properties:

Properties >> Security >> Permissions. Permissions greater than Read, Execute should be noted for only the System and the Auditors Group.

If the SA, Web Manager or users other than the Auditors group have greater than read access to the log files, this is a finding.

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND UNIX (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑

Grid:				
	Sensitive	☑	☑	☑
	Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: A major tool in exploring the web site use, attempted use, unusual conditions and problems are the access and error logs. In the event of a security incident, these logs can provide the SA and Web Manager with valuable information. To ensure the integrity of the log files and protect the SA and Web Manager from a conflict of interest related to the maintenance of these files, only the members of the Auditors group will be granted permissions to move, copy and delete these files in the course of their duties related to the archiving of these files.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG250 - Unix Apache (Manual)

Look for the presence of log files at:

/usr/local/apache/logs/access_log

To ensure the correct location of the log files, examine the "ServerRoot" directive in the httpd.conf file and then navigate to that directory where you will find a subdirectory for the logs.

Determine permissions for log files, from the command line:

cd to the directory where the log files are located and enter the command:

ls –al *log

and note the owner and group permissions on these files.

File permissions should be set to:

root webadmin 750/640

Vulnerability Key: V0013689
STIG ID: WG255
Release Number: 2
Status: Active
Short Name: WG255
Long Name: Access to the web server log files is not restricted to Administrators, the user assigned to run the web server software, Web Manager, and Auditors.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.2 Least Privilege
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND UNIX (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: A major tool in exploring the web site use, attempted use, unusual conditions and problems are the access and error logs. In the event of a security incident, these logs can provide the SA and Web Manager with valuable information. Because of the information that is captured in the logs, it is critical that only authorized individuals have access to the logs.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.1

Checks: WG255 - Unix Apache (Manual)
Look for the presence of log files at:

/usr/local/apache/logs/access_log

To ensure the correct location of the log files, examine the "ServerRoot" directive in the htttpd.conf file and then navigate to that directory where you will find a subdirectory for the logs.

Determine permissions for log files, from the command line: cd to the directory where the log files are located and enter the command:

ls –al *log and note the owner and group permissions on these files. Only the Auditors, Web Managers, Administrators, and the account that runs the web server should have permissions to the files.

If any users other than those authorized have read access to the log files, this is a finding.

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND Windows (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: A major tool in exploring the web site use, attempted use, unusual conditions and problems are the access and error logs. In the event of a security incident, these logs can provide the SA and Web Manager with valuable information. Because of the information that is captured in the logs, it is critical that only authorized individuals have access to the logs.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.1

Checks:

WG255 - Windows Apache (Manual)
Determine permissions for log files

Find the httpd.conf configuration file to determine the location of the log files. The location is indicated at the "ServerRoot" directive. The log directory is a sub-directory under the ServerRoot.

ex. :\Apache Group\Apache\logs

After locating the logs, use the Explorer to move to these files and examine their properties:

Properties >> Security >> Permissions.

Administrators: Read
Auditors: Full Control
Web Managers: Read
WebServer Account: Read/Write/Execute

If anyone other than the Auditors, Administrators, Web Managers, or the account that runs the web server has access to the log files, this is a finding.

Vulnerability Key: V0002254
STIG ID: WG260
Release Number: 4
Status: Active
Short Name: WG260
Long Name: Web sites still under development exist on a production server.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 11.2 Dissemination
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category III

Vulnerability Discussion: In the case of a production web server, areas for content development and testing will not exist, as this type of content is only permissible on a development web site. The process of developing on a functional production web site entails a degree of trial and error and repeated testing. This process is often accomplished in an environment where debugging, sequencing and formatting of content are the

main goals. The opportunity for a malicious user to obtain files that reveal business logic and login schemes is high in this situation. The existence of such immature content on a web server represents a significant security risk that is totally avoidable.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.8
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks:

WG260 (Manual)

The reviewer should query the IAO, SA and Web Manager to find out if development web sites are being housed on production web servers.

Definition: A production web server is any web server connected to a production network, regardless of its role.

Proposed Questions:

Do you have development sites on your production web server?
What is your process to get development web sites / content posted to the production server?
Do you use under construction notices on production web pages?

You can also do a manual check or navigation of the web site via a browser could be used to confirm the information provided from interviewing the web staff. Graphics or text which proclaim Under Construction or Under Development are frequently used to mark folders or directories in that status.

If under construction or development web content is discovered on the production web server, this is a finding.

Vulnerability Key: V0006373
STIG ID: WG265
Release Number: 7
Status: Active
Short Name: WG265
Long Name: The approved DoD banner page is not in place on the web server.
IA Controls: ECWM-1 Warning Message
Categories: 11.6 Warning Banners
Effective Date: 29 Jun 2005

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑

Public	☐	☐	☐

Severity: Category III

Vulnerability Discussion: A consent banner will be in place to make prospective entrants aware that the web site they are about to enter is a DoD web site and their activity is subject to monitoring. The May 9, 2008 Policy on Use of Department of Defense (DoD) Information SystemsStandard Consent Banner and User Agreement, establishes interim policy on the use of DoD information systems. It requires the use of a standard Notice and Consent Banner and standard text to be included in user agreements. The requirement for the banner is for web sites with security and access controls. These are restricted and not publicly accessible. If the web site does not require authentication / authorization for use, then the banner does not need to be present.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG265 (Manual)

The reviewer should query the IAO, SA and Web Manager on this point.

A manual check of the document root directory for a banner page file (such as banner.html) or navigation to the web site via a browser can be used to confirm the information provided from interviewing the web staff.

The following banner page must be in place:

“You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.”

Option 2: If your system cannot meet the character limits to store this amount of text in the banner, the following is another option for the warning banner:

"I've read & consent to terms in IS user agreem't."

NOTE: This has to be displayed only once when the individual enters the site and not for each page.

If the access controlled web site does not display this banner page before entry, this is a finding.

NOTE: If the web site does not require authentication / authorization for use, then the banner

does not need to be present.

Vulnerability Key: V0002258
STIG ID: WG290
Release Number: 4
Status: Active
Short Name: WG290
Long Name: The web client account access to the content and scripts directories is not limited to read and execute.
IA Controls: ECLP-1 Least Privilege
Categories: 2.2 Least Privilege
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND Windows (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category I

Vulnerability Discussion: Excessive permissions for the anonymous web user account are one of the most common faults contributing to the compromise of a web server. If this user is able to upload and execute files on the web server, the organization or owner of the server will no longer have control of the asset.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sectoin 3.10
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG290 - Windows Apache (Manual)

Locate the document root directory in httpd.conf. Also locate any and all active content that might not be located in the document root.

From the Services option in Administrative tools, you can view the properties of the Apache web server service to determine the account that is being used to run the web server.

If the Microsoft ‘everyone’ account has access to these directories, this is a finding.

If the web client account access to the content and scripts directories is not limited to read and execute, this is a finding.

☐ Open ☐ Not a Finding	Comments:

☐ Not Applicable ☐ Not Reviewed	

Condition: Web Server AND UNIX (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category I

Vulnerability Discussion: Excessive permissions for the anonymous web user account are one of the most common faults contributing to the compromise of a web server. If this user is able to upload and execute files on the web server, the organization or owner of the server will no longer have control of the asset.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.10
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG290 - Unix Apache (Manual)

In default installs, the user nobody will be the web client account. However, the SA or Web Manager may have created an account such as webusr to more explicitly deal with this issue.

There are two checks required.

Locate the document root (provided in the httpd.conf file) and any and all content that might not be located in the doc root.

Permissions for this user should be world permissions and on these files must be 400 and directories 500 or more restrictive.

You can use the ls -l command to view the permission on these directories and files.

If the files do not meet the requried permissions of no more than read and execute, this is a finding.

If used, locate all the cgi scripts directories (provided in the httpd.conf file as 'ScriptAlias') and any and all cgi scripts that might not be located in the cgi-bin.

Permissions for this user should be world permissions and on these files must be 500 and directories 500 or more restrictive.

You can use the ls -l command to view the permission on these directories and files.

If the files do not meet the requried permissions of no more than read and execute, this is a finding.

Vulnerability Key: V0002260
STIG ID: WG310
Release Number: 4
Status: Active

Short Name: WG310
Long Name: A Private web server responds to requests from public search engines.
IA Controls: ECLP-1 Least Privilege
Categories: 2.2 Least Privilege
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☐	☐	☐

Severity: Category II

Vulnerability Discussion: Search engines are constantly at work on the Internet. Search engines are augmented by agents, often referred to as spiders or bots, that endeavor to capture and catalog web site content. In turn, these search engines make the content they obtain and catalog available to any public web user. Such information in the public domain defeats the purpose of a Limited or Certificate-based web server, provides information to those not authorized access to the web site, and could provide clues of the sites architecture to malicious parties.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.4
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG310 - Apache (Manual)

Query the SA to determine what type of restriction from public search engines is in place.

In the document root directory check for a file named robots.txt which contains at least the following content:

User-agent: *
Disallow: /

Note: The robots.txt file must be placed in the document root directory. Additional restrictions can be stated in the robots.txt file. The above example will disallow access to all directories in the document root directory.

The location of the document root can be found in the httpd.conf config file, at the DocumentRoot directive.

If no means of restriction is in place (e.g. userid and password, domain or IP restriction, user PKI certificate) or a robots.txt file is not in use, this is finding.

NOTES: It is recommended to do both. Also, this applies to both SIPRNet and NIPRNet web servers.

Vulnerability Key: V0002262
STIG ID: WG340
Release Number: 5
Status: Active
Short Name: WG340
Long Name: A Private web server is not using TLS.
IA Controls: ECCT-1 Encryption for Confidentiality (Data in Transit)
ECCT-2 Encryption for Confidentiality (Data in Transit)
Categories: 1.2 PKI
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☐	☐	☐

Severity: Category II

Vulnerability Discussion: SSL/TLS encryption is a required security setting for a private web server. This check precludes the possibility that a valid certificate has been obtained, but SSL/TLS has not been activated or is not being used. Transactions encrypted with trusted certificates are necessary when the information being transferred is not intended to be accessed by all parties on the network. To the extent that this standard applies, this check is valid for the SIPRNet also.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.13
8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling

Checks: WG340 - Apache (Manual)

Provided Apache-SSL or mod_ssl are being used. Find and open the httpd.conf file in a text editor or use command line tools to open the file.

NOTE1: These directives are in the context of the “server config” or “virtual host” they may be found in the httpd.conf file, or a virtual host config file. This may also include a config file that has bee “Included” via the httpd.conf or other config file.

Look for the existence of the SSLProtocol directive. This directive can be used to control the SSL protocol flavors mod_ssl should use when establishing its server environment. Clients then can only connect with one of the provided protocols.

SSLProtocol TLSv1 – is the required setting for this check. If SSLProtocol is not set to TLSv1 this would be a finding.

Also, look for the existence of the SSLEngine directive. This directive toggles the usage of the SSL/TLS Protocol Engine. This is usually used inside a <VirtualHost> section to enable SSL/TLS for a particular virtual host. By default the SSL/TLS Protocol Engine is disabled for both the main

server and all configured virtual hosts.

“SSLEngine on” - is the required setting for this check. If it is not set to on or does not exist, this would be a finding.

Both the SSLEngine and SSLProtocol directives must be set correctly or this is a finding.

NOTE2: In some cases the web servers are configured in an environment to support load balancing. This configuration most likly utilizes a content switch to contol traffic to the various web servers. In this situration, the SSL certificated for the web sites may be installed on the content switch vs, the individual web sites. This solution is acceptable as long as the web servers are isolated from the general population LAN. We don't want users to have the ability to bypass the content switch to access the web sites.

Vulnerability Key: V0013694
STIG ID: WG342
Release Number: 2
Status: Active
Short Name: WG342
Long Name: Public web servers that use SSL do not use the correct version to provide encrypted sessions.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 1.2 PKI
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)
Policy: All Policies
MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☐	☐	☐
Sensitive	☐	☐	☐
Public	☑	☑	☑

Severity: Category II
Vulnerability Discussion: SSL/TLS encryption is a required security setting for a private web server. This check precludes the possibility that a valid certificate has been obtained, but SSL/TLS has not been activated or is not being used. Transactions encrypted with trusted certificates are necessary when the information being transferred is not intended to be accessed by all parties on the network. To the extent that this standard applies, this check is valid for the SIPRNet also.
Documentable: No
Documentable Explanation:
Potential Impacts:
Responsibility: System Administrator
Web Administrator
References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.13
Checks: WG342 - Apache (Manual)

Provided Apache-SSL or mod_ssl are being used. Find and open the httpd.conf file in a text editor or use command line tools to open the file.

NOTE1: These directives are in the context of the “server config” or “virtual host” they may be found in the httpd.conf file, or a virtual host config file. This may also include a config file that has bee “Included” via the httpd.conf or other config file.

Look for the existence of the SSLProtocol directive. This directive can be used to control the SSL protocol flavors mod_ssl should use when establishing its server environment. Clients then can only connect with one of the provided protocols.

SSLProtocol TLSv1 – is the required setting for this check. If SSLProtocol is not set to TLSv1 this would be a finding.

Also, look for the existence of the SSLEngine directive. This directive toggles the usage of the SSL/TLS Protocol Engine. This is usually used inside a <VirtualHost> section to enable SSL/TLS for a particular virtual host. By default the SSL/TLS Protocol Engine is disabled for both the main server and all configured virtual hosts.

“SSLEngine on” - is the required setting for this check. If it is not set to on or does not exist, this would be a finding.

Both the SSLEngine and SSLProtocol directives must be set correctly or this is a finding.

NOTE2: In some cases the web servers are configured in an environment to support load balancing. This configuration most likly utilizes a content switch to contol traffic to the various web servers. In this situration, the SSL certificated for the web sites may be installed on the content switch vs, the individual web sites. This solution is acceptable as long as the web servers are isolated from the general population LAN. We don't want users to have the ability to bypass the content switch to access the web sites.

If the web site's server certificate is not utilizing TLS, this is a finding.

Vulnerability Key: V0002263
STIG ID: WG350
Release Number: 3
Status: Active
Short Name: WG350
Long Name: A private web server that executes a web application does not have a DoD Certificate.
IA Controls: IATS-1 Token and Certificate Standards
IATS-2 Token and Certificate Standards
Categories: 1.2 PKI
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☐	☐	☐

Severity: Category II

Vulnerability Discussion: This check verifies that DoD is the sites CA. The certificate is actually a DoD issued server certificate used by the organization being reviewed. This is used to verify the authenticity of the web site to the user. If the certificate is not for the server (Certificate belongs to), if the certificate is not issued by DoD (Certificate was issued by), or if the current date is not included in the valid date (Certificate is valid from), then there is no assurance that the use of the Certificate is valid. The entire purpose of using a certificate is therefore compromised.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.12
8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling

Checks:

WG350 (Manual)

Open browser window and browse to the appropriate site. Before entry to the site you should be presented with the servers DOD PKI credentials. Review these credentials for authenticity.

Find an entry which cites:

Issuer:
CN = DOD CLASS 3 CA-3
OU = PKI
OU = DoD
O = U.S. Government
C = US

NOTE: The "InstallRoot3.0_SAG" document, which is included on the SRR CD, has a complete list of DoD certificates.

If the server is running as a public web server this finding should be Not Applicable.

NOTE: In some cases the web servers are configured in an environment to support load balancing. This configuration most likly utilizes a content switch to contol traffic to the various web servers. In this situration, the SSL certificated for the web sites may be installed on the content switch vs, the individual web sites. This solution is acceptable as long as the web servers are isolated from the general population LAN. We don't want users to have the ability to bypass the content switch to access the web sites.

Vulnerability Key: V0002227
STIG ID: WG360
Release Number: 5
Status: Active
Short Name: WG360
Long Name: Symbolic links are used in the web document (content) directory tree.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 01 Dec 1999

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition:

Web Server AND UNIX (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category III

Vulnerability Discussion: A symbolic link allows a file or directory to be referenced using a symbolic name raising a potential hazard if symbolic linkage is made to a sensitive area. When web scripts are executed and symbolic links are allowed, the web user could be allowed to access locations on the web server that are outside the scope of the web document root or home directory.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.14
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks:

WG360 - Unix Apache (Manual)

For Unix Systems Only

Locate the directories containing the web content, i.e. /usr/local/apache/htdocs.

Use ls –al

An entry such as the following would indicate the presence and use of symbolic links:

lr-xr—r-- 4000 wwwusr wwwgrp 2345 Apr 15 data -> /usr/local/apache/htdocs

Such a result found in a web document directory is a finding. Additional Apache configuration check in the httpd.conf file:

```
<Directory /[website root dir]>
   Options FollowSymLinks
   AllowOverride None
</Directory>
```

The above configuration is incorrect and is a finding. The correct configuration is:

```
<Directory /[website root dir]>
   Options SymLinksIfOwnerMatch
   AllowOverride None
</Directory>
```

Finally, the target file or directory must be owned by the same owner as the link, which should be the non-privileged account with access to the web content.

Vulnerability Key: V0002228
STIG ID: WG400
Release Number: 3
Status: Active
Short Name: WG400
Long Name: All interactive programs are not placed in a designated directory with appropriate permissions.
IA Controls: DCPA-1 Partitioning the Application

Categories: 2.2 Least Privilege
12.4 CM Process

Effective Date: 01 Dec 1999

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND UNIX (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: CGI scripts represents one of the most common and exploitable means of compromising a web server. By definition, CGI are executable by the operating system of the host server. All CGI program files need to segregated into their own directory to simplify the protection of these files. Having them in their own directory all to control permissions at the directory level vs. file by file. ASP, JSP, JAVA and PERL scripts are commonly found in these circumstances. Limiting CGI or equivalent scripts to special directories gives the Web Manager or SA control over what goes into those directories. Allowing users to execute CGI scripts in any directory should only be considered if you trust users not to write scripts which will deliberately or accidentally expose the server to an attack. These files, if left in directories from which the anonymous web user could read the source code, would make it easier for someone to understand and attack the web server.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sectoin 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG400 - Unix Apache (Manual)

To preclude access to the servers root directory, ensure the following directive is in the httpd.conf file. This entry will also stop users from setting up .htaccess files which can override security features configured in httpd.conf.

```
<DIRECTORY /[website root dir]>
  AllowOverride None
</DIRECTORY>
```

If the AllowOverride None is not set, this is a finding.

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND Windows (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: CGI scripts represents one of the most common and exploitable means of compromising a web server. By definition, CGI are executable by the operating system of the host server. While access control is provided via the web service, the execution of CGI programs is not otherwise limited unless the SA or Web Manager take specific measures. CGI programs can access and alter data files, launch other programs and use the network. CGI programs can be written in any available programming language. C, PERL, PHP, Javascript, VBScript and shell (sh, ksh, bash) are popular choices. Apache: suexec must be enabled to ensure that scripts run in the proper context.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG400 - Windows Apache (Manual)

To preclude access to the servers root directory, ensure the following directive is in the httpd.conf file. This entry will also stop users from setting up .htaccess files which can override security features configured in httpd.conf.

```
<DIRECTORY /[website root dir]>
  AllowOverride None
</DIRECTORY>
```

If the AllowOverride None is not set, this is a finding.

Vulnerability Key: V0002229
STIG ID: WG410
Release Number: 4
Status: Active
Short Name: WG410
Long Name: Interactive scripts do not have proper access controls.
IA Controls: ECLP-1 Least Privilege
Categories: 2.2 Least Privilege
Effective Date: 01 Dec 1999

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: CGI scripts represents one of the most common and exploitable means of compromising a web server. By definition, CGI are executable by the operating system of the host server. While access control is provided via the web service, the execution of CGI programs is not otherwise limited unless the SA or Web Manager take specific measures. CGI programs can access and alter data files, launch other programs and use the network. CGI programs can be written in any available programming language. C, PERL, PHP, Javascript, VBScript and shell (sh, ksh, bash) are popular choices. CGI is a standard for interfacing external applications with information servers, such as HTTP or web servers. The definition of CGI as web-based applications is not to be confused with the more specific .cgi file extension. ASP, JSP, JAVA and PERL scripts are commonly found in these circumstances.

Documentable: No

Documentable Explanation:

Potential Impacts: With Windows and IIS using .asp or .jsp files, the comparable directory is the Scripts directory. Security is enhanced with virtual directories because it adds another level of abstraction to the site, altering the way in which Internet users access the information. Read, Write, Directory Browsing, Scripts only, and Scripts and executables are IIS permissions, which can be applied to a virtual directory and all of the files and folders contained within it; Scripts permissions for the web client accounts should be the setting. Read permission allows a client to download files stored in a virtual directory or subdirectory. Only directories that contain information to be published or downloaded should have Read permission set. To prevent clients from downloading executable files or scripts that always contain sensitive information and application logic, these files will be located in separate directories without Write permission. Instead, these virtual directories should have Script only permission so web clients can run them. Only the Scripts setting should be used. Additional configuration checks for IIS using .asp files are noted below and covered as noted by this check. IIS: IUSR_machinename NTFS account permissions – Read and Execute Locate all but the default.asp or equivalent file in a separate directory (ies) IIS: Internet Services Manager Settings on Home Directory tab, Execute Permissions: Script

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sectio 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks:

WG410 - Apache (Manual)

Query the SA to determine if and CGI (includes all languages) are used as part of the web site.

If interactive scripts are being used, check the permissions of these files to ensure they meet the following permissions:

Unix:

interactive script files root WebAdmin 551

Windows:

interactive script files

Administrators	Full Contol
WebManagers	Modify
System	Full Control
Webserver Account	Read/Execute

If the interactive scripts do not meet the above permissions or are less restrictive, this is a finding.

Vulnerability Key: V0002270
STIG ID: WG430
Release Number: 3
Status: Active
Short Name: WG430
Long Name: Anonymous FTP users can access interactive scripts.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.2 Least Privilege
Effective Date: 25 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND Windows (Target: Apache Site 1.3.x)
Policy: All Policies
MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II
Vulnerability Discussion: The directory containing the CGI scripts, or equivalent scripting files such as PERL or asp file, must not be accessible to anonymous users via FTP. This applies to all directories that contain scripts that can dynamically produce web pages in an interactive manner; that is based upon user provided input. Such scripts contain information that could be used to compromise a web service, access system resources or deface a web site.
Documentable: No
Documentable Explanation:
Potential Impacts:
Responsibility: System Administrator
Web Administrator
References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)
Checks: WG430 - Windows (Manual)
Locate the directory containing the CGI, PERL, ASP, JS or JSP scripts.

Using a right click on the web content directory and related scripts directory. Using the Properties Tab, examine the access rights for the scripts, cgi-bin, cgi-shl, scripts or equivalent directory. Anonymous ftp users must not have access to these directories.

If the CGI directory can be accessed by any group that does not require access; this is a finding.

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND UNIX (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: The directory containing the CGI scripts, or equivalent scripting files such as PERL or asp file, must not be accessible to anonymous users via FTP. This applies to all directories that contain scripts that can dynamically produce web pages in an interactive manner; that is based upon user provided input. Such scripts contain information that could be used to compromise a web service, access system resources or deface a web site.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sectoin 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG430 - Unix (Manual)

Locate the directory containing the CGI, PERL, ASP or JSP scripts.

Using ls –al, examine the file permissions on the CGI scripts directory.

If the directory can be accessed by any group that does not require access (i.e. FTP users), this is a finding.

Vulnerability Key: V0002272
STIG ID: WG460
Release Number: 3
Status: Active
Short Name: WG460
Long Name: PERL is being used without the taint option.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 7.2 Writing Secure Code
Effective Date: 25 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND Windows (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑

Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: PERL (Practical Extraction and Report Language) is an interpreted language optimized for scanning arbitrary text files, extracting information from those text files, and printing reports based on that information. The language is often used in shell scripting and is intended to be practical, easy to use and efficient means of generating interactive web pages for the user. Unfortunately many widely available freeware PERL programs (scripts) are extremely insecure. This is most readily accomplished by a malicious user substituting input to a PERL script during a POST or GET operation. Consequently, the founders of PERL have developed a mechanism named taint that protects the system from malicious input sent from outside the program. When the data is tainted, it cannot be used in programs or functions such as eval(), system(), exec(), pipes, or popen(). The script will exit with a warning message. It is vital that if PERL is being used, the following line appear in the first line of PERL scripts: #!/usr/local/bin/perl –T

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sectoin 4.5

Checks: WG460 - Windows (Manual)

It is vital that if PERL is being used the following line appear in the first line of PERL scripts:

#!/usr/local/bin/perl –T

The reviewer will normally use Notepad to view the content of a PERL script. Normally the form method that calls the script will contain the –T switch.

CGI Scripts running on non-UNIX Servers typically do not recognize the magical #!/usr/local/bin/perl first line of the script. Instead, the web server knows what language to execute the server with because of an operating system or web server configuration variable.

For example, for IIS on Windows, you should change the association of Perl scripts to run with "taint mode on". A more reasonable way to get around the problem is by creating a second extension under Windows such as tcgi or tgi and associate it with taint mode Perl. Then, rename the scripts with the new extension to activate taint mode on them.

If the server is using PERL and scripts do not include a call to the taint option, this is a finding.

NOTE: This applies to PERL scripts that are used as part of the web server and not all PERL scripts that are on the system.

NOTE: If the mod_perl module is installed, and the directive “PerlTaintCheck on” in the httpd.conf is used this satisfies the requirement.

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND UNIX (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: PERL (Practical Extraction and Report Language) is an interpreted language optimized for scanning arbitrary text files, extracting information from those text files, and printing reports based on that information. The language is often used in shell scripting and is intended to be practical, easy to use and efficient means of generating interactive web pages for the user. Unfortunately many widely available freeware PERL programs (scripts) are extremely insecure. This is most readily accomplished by a malicious user substituting input to a PERL script during a POST or GET operation. Consequently, the founders of PERL have developed a mechanism named taint that protects the system from malicious input sent from outside the program. When the data is tainted, it cannot be used in programs or functions such as eval(), system(), exec(), pipes, or popen(). The script will exit with a warning message. It is vital that if PERL is being used, the following line appear in the first line of PERL scripts: #!/usr/local/bin/perl –T

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.5

Checks: WG460 - Unix (Manual)

It is vital that if PERL is being used the following line appear in the first line of PERL scripts:

#!/usr/local/bin/perl -T

1) grep perl httpd.conf |grep -v '#'

You should also check /apache/sysconfig.d/loadmodule.conf for perl

NOTE: The name of the loadmodule.conf may vary by installation

If Apache doesn't have the mod_perl module loaded then it doesn't use perl and this is Not Applicable and the check can stop here.

2) grep -i 'PerlTaintCheck' httpd.conf

If 'PerlTaintCheck on'is set, this is not a finding and the check can stop here.

NOTE: If the PerlTaintCheck is a part of an Included config file, this meets the requirement.

3) Check each individual perl script

From the ServerRoot directory: find . -name '*.pl'
From the DocumentRoot directory: find . -name '*.pl'

Examine the beginning of every perl script for -T option. If the -T option is not specified in any perl script, this is a finding.

NOTE: This applies to PERL scripts that are used as part of the web server and not all PERL scripts that are on the system.

NOTE: If the mod_perl module is installed, and the directive "PerlTaintCheck on" in the httpd.conf is used this satisfies the requirement.

Vulnerability Key: V0002265
STIG ID: WG490
Release Number: 6
Status: Active
Short Name: WG490
Long Name: Java software installed on the web server is not limited to class files and the JAVA virtual machine.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 7.7 Code Validation

Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Apache Site (Target: Apache Site 1.3.x)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category III

Vulnerability Discussion: From source code in a .java or .jpp file, the Java compiler produces a binary file with an extension of .class. The .java or .jpp file would therefore reveal sensitive information regarding an applications logic and permissions to resources on the server. By contrast the .class file, because it is intended to be machine independent, is referred to a bytecode. Bytecodes are run by the Java Virtual Machine, JVM, or Java Runtime Environment, JRE, via a browser configured to permit Java code.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Secton 4.7

Checks: WG490 (Manual)

Search the web content directory and scripts directory for Java code other than .class, . jre and .jvm. Executables such as java.exe, jre.exe, and jrew.exe are permitted; but .java and .jpp files are not allowed on a production web server.

The reviewer should check for .java files in the web content directory

Unix:

Search the web content directory and scripts directory for Java code file other than .class.

Use: find / -name *.java or find / -name *.jpp

Windows:

Search the web content directory and scripts directory for Java code file other than .class.

Use: Start [Right Click] >> Search *.java with “look in local hard drives”; find *.jpp with “look in local hard drives”

If Java code with a .java or .jpp extensions are found in the web content or scripts directories, this is a finding.

Vulnerability Count - 29