ITA.4.1 Website Policy

Policy No: ITA.4.1
Policy Area e-Services
Policy Title Website Policy
Purpose To ensure government agencies have a trusted, reliable and secured web presence to the public (citizens, residents and commercial establishments).
Outcome Public can have easy and quick access to information and e-services that are accurate, updated and highly available. Proper security controls would also prevent malicious attacks and the distortion of government information. This would lead to higher public confidence and trust on the Oman Government.
Scope With the prevalence of the Internet, government agencies have to provide online access to information and e-services for the public. Whether outsourced or carry out internally, government agencies will have to ensure that quality and security measures and controls are consistently applied.
Policy Statements 1. ***Government agencies shall implement and maintain a website to provide government information and e-services that are highly available and accessible by the public including the disabled.*** 2. ***Government websites shall, minimally, be in Arabic and English.*** 3. ***Government websites and all official public digital correspondences shall be in the .gov.om domain names.*** 4. ***Government digital contents that are made public shall be hosted and stored in the Sultanate of Oman.***

Policy No: ITA.4.1
5. ***Government agencies shall implement quality controls to ensure that the content of information and e-services provided to the public are accurate and regularly updated.*** 6. ***Government agencies shall implement security measures to ensure availability and integrity of the information and e-services provided to the public.*** 7. ***Government agencies shall implement management controls to prevent the inappropriate disclosure of sensitive information.*** 8. ***Government agencies shall identify and manage the risks associated with the publishing of information and e-services so that the public will have confidence and trust in the government.*** 9. ***Government agencies that provide operationally critical information and e-services to the public shall have a business continuity plan in case of disasters.***
Exemptions (If any) Nil
Standards Compliance Requirements i. Government agencies shall have a formal and documented review and approval process for information and e-services provided to the public. ii. Government agencies shall have formal and documented quality and management control procedures. iii. Government websites shall be made available 98% throughout the year, i.e. the website can be down for a total of 8 days (or 192 hours) per calendar year. iv. The website shall comply with the following mandatory OeGAF Technical Reference Model (TRM) standards on service access: a. TA.SA.1.1 – use of HTTP b. TA.SA.1.2 – use of HTML

Policy No: ITA.4.1

c. TA.SA.1.4 – use of SMTP
d. TA.SA.1.5 – use of HTTPS for secured transactions

v. Government agencies shall carry out security assessment before the official launch of the government website and before major changes are applied; subsequently, the assessment should be carried out on annual basis.

vi. Government websites shall publish a disclaimer clause/section to prevent any possible legal and social non-compliance.

vii. Government websites shall publish a privacy policy to protect any information collected on the visitors of the website.

viii. Government websites shall publish information on how the agency can be contacted for more information, both by telephone and email.

ix. Government websites can link to other government websites and non-profit organisations. Links to private companies and individual's webpages are not encouraged.

x. Government websites will be subjected to verifications and assessments by ITA according to the above standards and others described below.

Others

Best Practices

- Implement a content management process that revolves around the life-cycle of information from developing, editing, reviewing, publishing, maintaining, updating and archiving. Typically, a content management system is also used to support this life-cycle of information management.

- Please refer to best practices described in OeGAF TRM Service Access Domain, in particular section '4.8 Best Practices' on high availability infrastructure, back up and the use of SAN.

Checklists

- **Ensure website hosting is secured according to ITA's** Guidelines on Securing Website

Policy No: ITA.4.1

- Carry out a risk assessment – technical, operations and management areas - before the launch of the website or before major website enhancements. Ensure that mitigation or remedial actions are available for high and medium risks. Please refer to ITA's Project Risk Assessment template.

References

ITA website (www.ita.gov.om) for more details on OeGAF, public website hosting & deployment checklist, and project risk assessment template.

عمان الرقمية
e.oman

هيئة تقنية المعلومات
سلطنة عمان
Information Technology Authority
Sultanate of Oman

Guidelines on Securing Website

Issue Date: 18/4/2012

VERSION: 2.0

Copyright Notice

This guideline on Securing Website serves as a quick companion to the ITA Website Policy. This document serves as a guide to government agencies that plan to deploy and maintain a government public web site.

This document has 2 parts. In Part 1, web applications (sites or portal) security checklist is developed to ensure government website is deployed and maintained efficiently and securely. In Part 2, a number of checklists are provided to ensure Securing government Public web server.

Part 1 – Web Application Security checklist

This checklist defines a set of requirements for verifying the effectiveness of security controls that protect Web applications (sites or portal). It focuses on the analysis of components that comprise the application layer of the Open Systems Interconnection Reference Model (OSI Model), rather than focusing on for example the underlying operating system or connected networks.

This checklist has to be filled by the relevant hosting personnel.

Completed	Action
Security Architecture	
Yes / No	All application components (either individual or groups of source files, libraries, and/or executables) that are present in the application are identified.
Yes / No	All components that are not part of the application but that the application relies on to operate are identified.
Yes / No	A high-level architecture for the application has been defined.
Yes / No	All application components are defined in terms of the business functions and/or security functions they provide.
Yes / No	All components that are not part of the application but that the application relies on to operate are defined in terms of the business functions and/or security functions they provide.
Authentication	
Yes / No	All authentication controls are enforced on the server side.
Yes / No	All authentication controls (including libraries that call external authentication services) have a centralized implementation.
Yes / No	All authentication controls fail securely.
Yes / No	The strength of any authentication credentials are sufficient to withstand attacks that are typical of the threats in the deployed environment.
Yes / No	All account management functions are at least as resistant to attack as the primary authentication mechanism.
Yes / No	If a maximum number of authentication attempts is exceeded, the account is locked for a period of time long enough to deter brute force attacks.
Yes / No	Re-authentication is required before any application-specific sensitive operations are permitted.
Yes / No	All authentication decisions are logged.
Yes / No	All authentication credentials for accessing services external to the application are encrypted and stored in a protected location (not in source code).
Yes / No	All code implementing or using authentication controls is not affected by any malicious code.

Session Management	
Yes / No	Sessions are invalidated when the user logs out.
Yes / No	Sessions timeout after a specified period of inactivity.
Yes / No	All pages that require authentication to access them have logout links.
Yes / No	Session id is never disclosed other than in cookie headers; particularly in URLs, error messages, or logs. This includes verifying that the application does not support URL rewriting of session cookies.
Yes / No	Session id is changed on login.
Yes / No	Session id is changed on re-authentication.
Yes / No	Session id is changed or cleared on logout.
Yes / No	Cookies which contain authenticated session tokens/ids have their domain and path set to an appropriately restrictive value for that site.
Yes / No	All code implementing or using session management controls is not affected by any malicious code.
Access Control	
Yes / No	Users can only access URLs for which they possess specific authorization.
Yes / No	Users can only access data files for which they possess specific authorization.
Yes / No	Direct object references are protected, such that only authorized objects are accessible to each user.
Yes / No	Directory browsing is disabled unless deliberately desired.
Yes / No	Users can only access services/ data for which they possess specific authorization.
Yes / No	The same access control rules implied by the presentation layer are enforced on the server side.
Yes / No	All user and data attributes and policy information used by access controls cannot be manipulated by end users.
Yes / No	All access controls are enforced on the server side.
Input Validation Requirements	
Yes / No	The runtime environment is not susceptible to buffer overflows, or that security controls prevent buffer overflows.
Yes / No	A positive validation pattern is defined and applied to all input.
Yes / No	All input validation failures result in input rejection or input sanitization.
Yes / No	A character set, such as UTF-8, is specified for all sources of input.
Yes / No	All input validation is performed on the server side.
Yes / No	A single input validation control is used by the application for each type of data that is accepted.
Yes / No	All input validation failures are logged.
Yes / No	All input validation controls are not affected by any malicious code.
Output Encoding/Escaping Requirements	
Yes / No	All untrusted data that are output to HTML (including HTML elements, HTML attributes, javascript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.

Yes / No	All output encoding/escaping controls are implemented on the server side.
Yes / No	Output encoding /escaping controls encode all characters not known to be safe for the intended interpreter.
Yes / No	All untrusted data that is output to SQL interpreters use parameterized interfaces, prepared statements, or are escaped properly.
Yes / No	All untrusted data that are output to XML use parameterized interfaces or are escaped properly.
Yes / No	All untrusted data that are included in operating system command parameters are escaped properly.
Yes / No	All untrusted data that are output to any interpreters not specifically listed above are escaped properly.
Yes / No	For each type of output encoding/escaping performed by the application, there is a single security control for that type of output for the intended destination.
Yes / No	All code implementing or using output validation controls is not affected by any malicious code.
Error Handling and Logging	
Yes / No	The application does not output error messages or stack traces containing sensitive data that could assist an attacker, including session id and personal information.
Yes / No	All server side errors are handled on the server.
Yes / No	All logging controls are implemented on the server.
Yes / No	Error handling logic in security controls denies access by default.
Yes / No	Security logging controls provide the ability to log both success and failure events that are identified as security-relevant.
Yes / No	All events that include untrusted data will not execute as code in the intended log viewing software.
Yes / No	Security logs are protected from unauthorized access and modification.
Yes / No	The application does not log application-specific sensitive data that could assist an attacker, including user's session ids and personal or sensitive information.
Yes / No	All code implementing or using error handling and logging controls is not affected by any malicious code.

Table P1.0 - Threat Matrix

Category	Name & Description
High Severity High Impact	• Unauthorized Access o In this category an individual gains logical or physical access without permission to a Government website, network, system, application, data, or other resource ▪ Examples: Known Vulnerability, Insufficient Authentication, Backdoor, Rootkit, Brute Force • Denial of Service (DoS) o An attack that *successfully* prevents or impairs the normal authorized functionality of government networks, systems or applications by exhausting resources. ▪ Examples: Abuse of Functionality, Improper website coding, High Traffic load, improper web traffic management, known DOS exploits, Bot-net Attack • Malicious Code o *Successful* installation of malicious software or other code-based malicious entity that infects an operating system or web application. ▪ Example: Trojan, Cross Site Request Forgery, Cross Site Scripting (XSS), Hidden Parameter Manipulation, Local File Inclusion (LFI),Malvertising, Malware, Misconfiguration, Sql Injection, Virus infection, Zombie infection,
Medium Severity Low Impact	• Scans/Probes/Attempted Access o This category includes any activity that seeks to access or identify a government computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. o Example: direct TCP/IP port scanning, OS fingerprinting,
Low Severity Low Impact	• Information Gathering o Indirect information gathering from 3rd party website (e.g. hexillion.net, whois websites) or through allow known services (https, http, Pop,SMTP) ▪ Example: banner identification, 3rd party information gathering via domain registrar web site, Social engineering

Part 2 - Securing Public Web server Checklist

Planning and Management of Web servers

Summary - The most critical aspect of deploying a secure Web server is careful planning prior to installation, configuration, and deployment. Careful planning will ensure that the Web server is as secure as possible and in compliance with all relevant organizational/government policies, process and procedures.

Many Web server security and performance problems can be traced to a lack of planning or management controls.

The importance of management controls cannot be overstated. In many organizations, the IT support structure is highly fragmented. This fragmentation leads to inconsistencies, and these inconsistencies can lead to security vulnerabilities and other issues.

The checklist below gives a list of factors that needs to be considered when planning and managing of Web Servers.

This checklist has to be filled by the relevant hosting personnel.

Completed	Action
Plan the Configuration and Deployment of the Web Server	
Yes / No	Identify functions of the Web server
Yes / No	Identify categories of information that will be stored, processed, and transmitted through the Web server
Yes / No	Identify security requirements of information.
Yes / No	Identify how information is published to the Web server
Yes / No	Identify the security requirements of other hosts involved (e.g., backend database or Web service)
Yes / No	Identify a dedicated host to run the Web server
Yes / No	Identify network services that will be provided or supported by the Web server
Yes / No	Identify the security requirements of any additional services provided or supported by the Web server
Yes / No	Identify how the Web server will be managed
Yes / No	Identify users and categories of users of the Web server and determine privilege for each category of user
Yes / No	Identify user authentication methods for the Web server and how authentication data will be protected
Yes / No	Identify how access to information resources will be enforced
Yes / No	Identify appropriate physical security mechanisms
Yes / No	Identify appropriate availability mechanisms
Choose Appropriate OS for Web Server	
Yes / No	Minimal exposure to vulnerabilities
Yes / No	Ability to restrict administrative or root level activities to authorized users only
Yes / No	Ability to control access to data on the server.

Yes / No	Ability to disable unnecessary network services (please provide few examples)that may be built into the OS or server software
Yes / No	Ability to control access to various forms of executable programs, such as CGI scripts and server plug-ins
Yes / No	Ability to log appropriate server activities to detect intrusions and attempted intrusions
Yes / No	Provision of a host-based firewall capability
Yes / No	Availability of experienced staff to install, configure, secure, and maintain OS
Choose Appropriate Platform for Web Server	
Yes / No	*Choose one:* General purpose OS Trusted OS Web server appliance Pre-hardened OS and Web server Virtualized platform

Securing the operating system for a Web server

Summary - Protecting a Web server from compromise involves hardening the underlying OS, the Web server application, and the network to prevent malicious entities from directly attacking the Web server. The first step in securing a Web server, hardening the underlying OS, is discussed at length in Part 2.

The Checklist below gives a list of factors that need to be considered, when securing the operation system for a Web Server.

Completed	Action
Patch and Upgrade OS	
Yes/No	Create, document, and implement a patching process
Yes/No	Keep the test servers disconnected from networks or on an isolated testing network that severely restricts communications until all patches have been installed and tested and approve for production environment deployment
Yes/No	Identify and install all necessary patches and upgrades to the OS
Yes/No	Identify and install all necessary patches and upgrades to applications and services included with the OS
Yes/No	Identify and mitigate any unpatched vulnerabilities
Remove or Disable Unnecessary Services and Applications	
Yes/No	Disable or remove unnecessary services and applications
Configure OS User Authentication	
Yes/No	Remove or disable unneeded default accounts and groups
Yes/No	Disable non-interactive accounts
Yes/No	Create the user groups for the particular computer
Yes/No	Create the user accounts for the particular computer
Yes/No	Check the organization's password policy and set account passwords appropriately (e.g., length, complexity)

Yes/No	Prevent password guessing (e.g., increase the period between attempts, deny login after a defined number of failed attempts)
Yes/No	Install and configure other security mechanisms to strengthen authentication
Configure Resource Controls Appropriately	
Yes/No	Deny read access to unnecessary files and directories
Yes/No	Deny write access to unnecessary files and directories
Yes/No	Limit the execution privilege of system tools to system administrators
Install and Configure Additional Security Controls	
Yes/No	Select, install, and configure additional software to provide needed controls not included in the OS, such as antivirus software, antispyware software, rootkit detectors, host-based intrusion detection and prevention software, host-based firewalls, and patch management software
Test the Security of the OS	
Yes/No	Identify a separate identical system
Yes/No	Test OS after initial install to determine vulnerabilities
Yes/No	Test OS periodically (e.g., quarterly) to determine new vulnerabilities

Securely installing and configuring a Web server

Summary - Once the OS has been installed and secured, installing the chosen Web server software can begin. Before starting this process, read the Web server manufacturer's documentation carefully and understand the various options available during the installation process. Also, be sure to visit the manufacturer's Web site or a vulnerability database Web site, such as the National Vulnerability Database (NVD, CVE), SecurityFocus.com, Oman National CERT Advisory Database to determine whether there are known vulnerabilities and related patches available that should be installed or configured as part of the setup process. Only after these preliminary steps are accomplished should the installation be started. Note that this discusses only generic installation and configuration procedures; specific directions for particular Web servers are available from Web server manufacturers and from security checklist repositories.

A partially configured and/or patched server should not be exposed to external networks (e.g., the Internet) or external users. In addition, internal network access should be as limited as possible until all software is installed, patched, and configured securely. Insecure Web servers can be compromised in a matter of minutes after being placed on the Internet. While it is ideal to fully harden the platform before placing it on the network, it is not always feasible. For example, some application development tool combinations cannot be installed, configured, and tested on top of a pre-hardened OS and Web server configuration. In such situations, stepwise or incremental hardening is a viable option to consider, with full validation of complete hardening occurring at production deployment.

The Checklist below gives a list of factors that need to be considered, when securely installing and configuring a Web Server.

Completed	Actions
	Securely Install the Web Server
Yes/No	Install the Web server software on a dedicated host or a dedicated virtualized guest OS

Yes/No	Apply any patches or upgrades to correct for known vulnerabilities
Yes/No	Create a dedicated physical disk or logical partition (separate from OS and Web server application) for Web content
Yes/No	Remove or disable all services installed by the Web server application but not required (e.g., gopher, FTP, remote administration)
Yes/No	Remove or disable all unneeded default login accounts created by the Web server installation
Yes/No	Remove all manufacturer documentation from server
Yes/No	Remove any example or test files from server, including scripts and executable code
Yes/No	Apply appropriate security template or hardening script to the server
Yes/No	Reconfigure HTTP service banner (and others as required) NOT to report Web server and OS type and version
	Configure OS and Web Server Access Controls
Yes/No	Configure the Web server process to run as a user with a strictly limited set of privileges
Yes/No	Configure the Web server so that Web content files can be read but not written by service processes
Yes/No	Configure the Web server so that service processes cannot write to the directories where public Web content is stored
Yes/No	Configure the Web server so that only processes authorized for Web server administration can write Web content files
Yes/No	Configure the host OS so that the Web server can write log files but not read them
Yes/No	Configure the host OS so that temporary files created by the Web server application are restricted to a specified and appropriately protected subdirectory
Yes/No	Configure the host OS so that access to any temporary files created by the Web server application is limited to the service processes that created the files
Yes/No	Install Web content on a different hard drive or logical partition than the OS and Web server application
Yes/No	If uploads are allowed to the Web server, configure it so that a limit is placed on the amount of hard drive space that is dedicated for this purpose; uploads should be placed on a separate partition
Yes/No	Ensure that log files are stored in a location that is sized appropriately; log files should be placed on a separate partition
Yes/No	Configure the maximum number of Web server processes and/or network connections that the Web server should allow
Yes/No	Ensure that any virtualized guest OSs follow this checklist
Yes/No	Ensure users and administrators are able to change passwords
Yes/No	Disable users after a specified period of inactivity
Yes/No	Ensure each user and administrator has a unique ID
	Configure a Secure Web Content Directory
Yes/No	Dedicate a single hard drive or logical partition for Web content and establish related subdirectories exclusively for Web server content files, including graphics but excluding scripts and other programs

Yes/No	Define a single directory exclusively for all external scripts or programs executed as part of Web server content (e.g., CGI, ASP)
Yes/No	Disable the execution of scripts that are not exclusively under the control of administrative accounts. This action is accomplished by creating and controlling access to a separate directory intended to contain authorized scripts
Yes/No	Disable the use of hard or symbolic links (e.g., shortcuts for Windows)
Yes/No	Define a complete Web content access matrix. Identify which folders and files within the Web server document should be restricted and which should be accessible (and by whom)
Yes/No	Check the organization's password policy and set account passwords appropriately (e.g., length, complexity)
Yes/No	Use the robots.txt file, if appropriate
Yes/No	Configure anti-spambot protection, if appropriate (e.g., CAPTCHAs, nofollow, or keyword filtering)

Securing Web Content

Summary - The two main components of Web security are the security of the underlying server application and OS, and the security of the actual content. Of these, the security of the content is often overlooked. Maintaining effective content security itself has two components. The more obvious is not placing any proprietary, classified, or other sensitive information on a publicly accessible Web server, unless other steps have been taken to protect the information via user authentication and encryption (see Part 2 - Section 7). The less obvious component of content security is avoiding compromises caused by the way particular types of content are processed on a server. As organizations have gotten better at protecting and hardening their network perimeters, OSs, and Web servers, attackers have increasingly turned to exploiting vulnerabilities in Web applications and the way information is processed on Web servers. These application layer attacks exploit the interactive elements of Web sites.

The Checklist below gives a list of factors that need to be considered, when securing Web Content.

Completed	Actions
Ensure that none of the following types of information are available on or through a public Web server	
Yes/No	Classified records
Yes/No	Internal personnel rules and procedures
Yes/No	Sensitive or proprietary information
Yes/No	Personal information about an organization's personnel
Yes/No	Telephone numbers, e-mail addresses, or general listings of staff unless necessary to fulfill organizational requirements
Yes/No	Schedules of organizational principals or their exact location (whether on or off the premises)

Yes/No	Information on the composition, preparation, or optimal use of hazardous materials or toxins
Yes/No	Sensitive information relating to internal security
Yes/No	Investigative records
Yes/No	Financial records (beyond those already publicly available)
Yes/No	Medical records
Yes/No	Organization's physical and information security procedures
Yes/No	Information about organization's network and information system infrastructure
Yes/No	Information that specifies or implies physical security vulnerabilities
Yes/No	Plans, maps, diagrams, aerial photographs, and architectural plans of organizational building, properties, or installations
Yes/No	Copyrighted material without the written permission of the owner
Yes/No	Privacy or security policies that indicate the types of security measures in place to the degree that they may be useful to an attacker
	Establish an organizational-wide documented formal policy and process for approving public Web content that—
Yes/No	Identifies information that should be published on the Web
Yes/No	Identifies target audience
Yes/No	Identifies possible negative ramifications of publishing the information
Yes/No	Identifies who should be responsible for creating, publishing, and maintaining this particular information
Yes/No	Provides guidelines on styles and formats appropriate for Web publishing
Yes/No	Provides for appropriate review of the information for sensitivity and distribution/release controls (including the sensitivity of the information in aggregate)
Yes/No	Determines the appropriate access and security controls
Yes/No	Provides guidance on the information contained within the source code of the Web content
	Maintain Web user privacy
Yes/No	Maintain a published privacy policy
Yes/No	Prohibit the collection of personally identifying data without the explicit permission of the user and collect only the data that is absolutely needed
Yes/No	Prohibit the use of "persistent" cookies
Yes/No	Use the session cookie only if it is clearly identified in published privacy policy
	Mitigate indirect attacks on content
Yes/No	Ensure users of the site are aware of the dangers of phishing and pharming attacks and how to avoid them
Yes/No	Validate official communication by personalizing emails and providing unique identifying (but not confidential) information only the organization and user should know
Yes/No	Use digital signatures on e-mail if appropriate

Yes/No	Perform content validation within the Web application to prevent more sophisticated phishing attacks (e.g., cross-site scripting based attacks)
Yes/No	Personalize Web content to aid in users' identifying fraudulent Web sites
Yes/No	Use token-based or mutual authentication if applicable
Yes/No	Suggest the use of Web browsers or browser toolbars with phishing/ pharming protection
Yes/No	Use current versions of DNS software with the latest security patches
Yes/No	Install server-side DNS protection mechanisms
Yes/No	Monitor organizational domains and similar domains
Yes/No	Simplify the structure of organization domain names
Yes/No	Use secure connections for logins
Yes/No	If necessary, engage a vendor to provide stronger anti-phishing/ anti-pharming measures
	Client-side active content security considerations
Yes/No	Weigh the risks and benefits of client-side active content
Yes/No	Take no actions without the express permission of user
Yes/No	When possible, only use widely-adopted active content such as JavaScript, PDF, and Flash
Yes/No	When possible, provide alternatives (e.g., HTML provided along with PDF)
	Maintain server-side active content security
Yes/No	Only simple, easy-to-understand code should be used
Yes/No	Limited or no reading or writing to the file system should be permitted
Yes/No	Limited or no interaction with other programs (e.g., sendmail) should be permitted
Yes/No	There should be no requirement to run with suid privileges on Unix or Linux
Yes/No	Explicit path names should be used (i.e., does not rely on path variable)
Yes/No	No directories have both write and execute permissions
Yes/No	All executable files are placed in a dedicated folders
Yes/No	SSIs are disabled or the execute function is disabled
Yes/No	All user input is validated
Yes/No	Web content generation code should be scanned or audited
Yes/No	Dynamically created pages do not create dangerous metacharacters
Yes/No	Character set encoding should be explicitly set in each page
Yes/No	User data should be scanned to ensure it contains only expected input, (e.g., a-z, A-Z, 0-9); care should be taken with special characters or HTML tags
Yes/No	Cookies should be examined for any special characters
Yes/No	Encryption mechanism is used to encrypt passwords entered through scripts forms
Yes/No	For Web applications that are restricted by username and password, none of the Web pages in the application should be accessible without executing the appropriate login process

Yes/No	All sample scripts are removed
Yes/No	No third-party scripts or executable code are used without verifying the source code

Using Authentication and Encryption Technologies

Summary – Ministry and government Web servers often support a range of technologies for identifying and authenticating users with differing privileges for accessing information. Some of these technologies are based on cryptographic functions that can provide an encrypted channel between a Web browser client and a Web server that supports encryption.

Without user authentication, organizations will not be able to restrict access to specific information to authorized users. All information that resides on a public Web server will then be accessible by anyone with access to the server. In addition, without some process to authenticate the server, users will not be able to determine if the server is the "authentic" Web server or a counterfeit version operated by a malicious entity.

Encryption can be used to protect information traversing the connection between a Web browser client and a public Web server. Without encryption, anyone with access to the network traffic can determine, and possibly alter, the content of sensitive information, even if the user accessing the information has been authenticated carefully. This may violate the confidentiality and integrity of critical information.

The Checklist below gives a list of factors that need to be considered, when using Authentication and Encryption Technologies.

Completed	Actions
Configure Web Authentication and Encryption Technologies	
Yes/No	For Web resources that require minimal protection and for which there is a small, clearly defined audience, configure address-based authentication
Yes/No	For Web resources that require additional protection but for which there is a small, clearly defined audience, configure address-based authentication as a second line of defense
Yes/No	For Web resources that require minimal protection but for which there is no clearly defined audience, configure basic or digest authentication (better)
Yes/No	For Web resources that require protection from malicious bots, configure basic or digest authentication (better) or implement mitigation techniques discussed in Section 5.2.4
Yes/No	For organizations required to comply with FIPS 140-2, ensure the SSL/TLS implementation is FIPS-validated
Yes/No	For Web resources that require maximum protection, configure SSL/TLS
Configure SSL/TLS	
Yes/No	Ensure the SSL/TLS implementation is fully patched
Yes/No	Use a third-party issued certificate for server authentication (unless all systems using the server are organization-managed, in which case a self-signed certificate could potentially be used instead)

Yes/No	For configurations that require a medium level of client authentication, configure server to require username and password via SSL/TLS
Yes/No	For configurations that require a high level of client authentication, configure server to require client certificates via SSL/TLS
Yes/No	Ensure weak cipher suites are disabled (see Table 7.1 for the recommended usage of Federal cipher suites)
Yes/No	Configure file integrity checker to monitor Web server certificate
Yes/No	If only SSL/TLS is to be used in the Web server, ensure access via any TCP port other than 443 is disabled
Yes/No	If most traffic to the Web server will be via encrypted SSL/TLS, ensure that appropriate logging and detection mechanisms are employed in the Web server (because network monitoring is ineffective against encrypted SSL/TLS sessions)
Protect Against Brute Force Attacks	
Yes/No	Use strong authentication if possible
Yes/No	Use a delay after failed login attempts
Yes/No	Lock out an account after a set number of failed login attempts
Yes/No	Enforce a password policy
Yes/No	Blacklist IP addresses or domains known to attempt brute force attacks
Yes/No	Use log monitoring software to detect brute force attacks

Implementing a Secure Network Infrastructure

Summary– The network infrastructure that supports the Web server plays a critical role in the security of the Web server. In most configurations, the network infrastructure is the first line of defense between the Internet and a government Web server. Network design alone, however, cannot protect a Web server. The frequency, sophistication, and variety of attacks perpetrated today lend support to the idea that Web security must be implemented through layered and diverse protection mechanisms (defense-in-depth). This section discusses those network components that can support and protect Web servers to further enhance their overall security. Although security issues are paramount, network infrastructure considerations are influenced by many factors other than security, including cost, performance, and reliability.

The checklist below gives a list of factors to be considered when using implementing a Secure Network Infrastructure.

Completed	Actions
Identify Network Location	
Yes/No	Web server is located in a DMZ, or Web server hosting is outsourced
Assess Firewall Configuration	

Yes/No	Web server is protected by a firewall; if it faces a higher threat or is more vulnerable, it is protected by an application layer firewall
Yes/No	Firewall controls all traffic between the Internet and the Web server
Yes/No	Firewall blocks all inbound traffic to the Web server except TCP ports 80 (HTTP) and/or 443 (HTTPS), if required
Yes/No	Firewall blocks (in conjunction with the IDS) IP addresses or subnets that the IDPS reports are attacking the organizational network
Yes/No	Firewall notifies the network or Web server administrator of suspicious activity through an appropriate means
Yes/No	Firewall provides content filtering (application layer firewall)
Yes/No	Firewall is configured to protect against DoS attacks
Yes/No	Firewall detects malformed or known attack URL requests
Yes/No	Firewall logs critical events
Yes/No	Firewall and firewall OS are patched to latest or most secure level
Evaluate Intrusion Detection and Prevention Systems	
Yes/No	Host-based IDPS is used for Web servers that operate primarily using SSL/TLS
Yes/No	IDPS is configured to monitor network traffic to and from the Web server after firewall
Yes/No	IDPS is configured to monitor changes to critical files on Web server (host-based IDPS or file integrity checker)
Yes/No	IDPS blocks (in conjunction with the firewall) IP addresses or subnets that are attacking the organizational network
Yes/No	IDPS notifies the IDPS administrators or Web server administrator of attacks through appropriate means
Yes/No	IDPS is configured to maximize detection with an acceptable level of false positives
Yes/No	IDPS is configured to log events
Yes/No	IDPS is updated with new attack signatures frequently (e.g., on a daily basis)
Yes/No	Host-based IDPS is configured to monitor the system resources available in the Web server host
Assess Network Switches	
Yes/No	Switches are used to protect against network eavesdropping
Yes/No	Switches are configured in high-security mode to defeat ARP spoofing and ARP poisoning attacks
Yes/No	Switches are configured to send all traffic on network segment to network-based IDPS
Evaluate Load Balancers	
Yes/No	Load balancers are used to increase Web server availability
Yes/No	Load balancers are augmented by Web caches if applicable

Evaluate Reverse Proxies	
Yes/No	Reverse proxies are used as a security gateway to increase Web server availability
Yes/No	Reverse proxies are augmented with encryption acceleration, user authentication, and content filtering capabilities, if applicable

Administering the Web Server

Summary - After initially deploying a Web server, administrators need to maintain its security continuously. This section provides general recommendations for securely administering Web servers.

Vital activities include handling and analyzing log files, performing regular Web server backups, recovering from Web server compromises, testing Web server security regularly, monitor the web server perimeter security and performing remote administration securely.

The checklist below gives a list of factors to be considered when administering a Public Web Server.

Nowadays, websites are also delivered over multiple channels like Mobiles and Kiosk. It will be good if we can cover some points related to those channels as well. We can refer to Service Access Domain in OeGAF TRM.

This should be included in an appropriate web content management process as already mentioned in comments above. Refer to #Point No. 9 above.

Completed	Actions
Perform Logging	
Yes / No	Use the combined log format for storing the Transfer Log or manually configure the information described by the combined log format to be the standard format for the Transfer Log
Yes / No	Enable the Referrer Log or Agent Log if the combined log format is unavailable
Yes / No	Establish different log file names for different virtual Web sites that may be implemented as part of a single physical Web server
Yes / No	Use the remote user identity as specified in RFC 1413
Yes / No	Store logs on a separate (syslog) host
Yes / No	Ensure there is sufficient capacity for the logs
Yes / No	Archive logs according to organizational requirements
Yes / No	Review logs daily
Yes / No	Review logs weekly (for more long-term trends)
Yes / No	Use automated log file analysis tool(s)
Perform Web Server Backups	
Yes / No	Create a Web server backup policy

Yes / No	Back up Web server differentially or incrementally on a daily to weekly basis
Yes / No	Back up Web server fully on a weekly to monthly basis
Yes / No	Periodically archive backups
Yes / No	Maintain an authoritative copy of Web site(s)
Yes / No	Installation of Oman National CERT Content integrity Agent
Yes / No	Inform Oman Nationa CERT of the urliand requests for it to be monitored
Recover From A Compromise	
Yes / No	Report the incident to the organization's computer incident response capability
Yes / No	Isolate the compromised system(s) or take other steps to contain the attack so additional information can be collected
Yes / No	Investigate similar hosts to determine if the attacker has also compromised other systems
Yes / No	Consult, as appropriate, with management, legal counsel, and Public Prosecutor officials expeditiously
Yes / No	Analyze the intrusion
Yes / No	Restore the system
Yes / No	Test system to ensure security
Yes / No	Reconnect system to network
Yes / No	Monitor system and network for signs that the attacker is attempting to access the system or network again
Yes / No	Document lessons learned
Security Tests	
Test via Oman National CERT	
Yes / No	Contact Oman National CERT and request for Security Assessment
Yes / No	Mitigate Security Assessment findings by Oman National CERT
In-House Security Test	
Yes / No	Periodically conduct vulnerability scans on Web server, dynamically generated content, and supporting network
Yes / No	Update vulnerability scanner prior to testing
Yes / No	Correct any deficiencies identified by the vulnerability scanner
Yes / No	Conduct penetration testing on the Web server and the supporting network infrastructure
Yes / No	Correct deficiencies identified by penetration testing
Conduct Remote Administration and Content Updates	
Yes / No	Use a strong authentication mechanism (e.g., public/private key pair, two-factor authentication)

Yes / No	Restrict hosts that can be used to remotely administer or update content on the Web server by IP address and to the internal network
Yes / No	Use secure protocols (e.g., SSH, HTTPS)
Yes / No	Enforce the concept of least privilege on remote administration and content
Yes / No	updating (e.g., attempt to minimize the access rights for the remote administration/update accounts)
Yes / No	Change any default accounts or passwords from the remote administration utility or application
Yes / No	Do not allow remote administration from the Internet unless mechanisms such as VPNs are used
Yes / No	Do not mount any file shares on the internal network from the Web server or vice versa
OCERT Intrusion Detection and Monitoring Service	
Yes / No	Contact Oman National CERT and request for Intrusion Detection and Monitoring Service
Yes / No	Fulfill and make provision for the requirement of the requested service
Yes / No	Confirm date of commission of service

End of Document